

security

manager

Τιμή: 5€

Το AI αλλάζει την Ασφάλεια

- “Διαχείριση Ποιότητας”... μια Σταθερά!
- Θερμική απεικόνιση ανίχνευσης θερμοκρασίας
- Μετάβαση σε Δικτυακές Πλατφόρμες
- Η εξέλιξη των συστημάτων συναγερμού ...προς το εξυπνότερο!



Η εξέλιξη της Europol στη Διεθνή Αστυνομική Συνεργασία



Η Ασφάλεια στην Περιφερειακή Ανάπτυξη



ΕΠΑΓΓΕΛΜΑΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ



- Πιστοποιημένοι πίνακες συναγερμού κατά GRADE 2
- Ενσωματωμένος ασύρματος δέκτης και ποικιλία ασύρματων αισθητήρων GRADE 2
- Ενσωματωμένο GPRS (SIA-IP) με 2 κάρτες SIM
- ΔΩΡΕΑΝ υπηρεσία Cloud (PERFECTA CONTROL) για Smartphone
- Δυνατότητα οικιακού αυτοματισμού
- Ακουστική επαλήθευση συναγερμού με ακρόαση χώρου
- Ποιοτική κατασκευή με 5 χρόνια εγγύηση
- Εύκολος προγραμματισμός από PC (PERFECTA SOFT) ή πληκτρολόγιο





ΑΣΥΡΜΑΤΟΣ ΣΥΝΑΓΕΡΜΟΣ ΤΗΣ ΣΕΙΡΑΣ AX

Η ΣΥΝΟΛΙΚΗ ΛΥΣΗ ΣΥΝΑΓΕΡΜΟΥ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΝΙΑΙΑ ΠΛΑΤΦΟΡΜΑ

Το AXHub είναι η τελευταία καινοτομία στα συστήματα συναγερμού. Συνδέει περιφερειακά ασφαλείας όπως ανιχνευτές κίνησης και αισθητήρες μετατόπισης, παράλληλα με συσκευές ασφαλείας όπως αισθητήρες καπνού και αερίου για την ασφαλή φύλαξη των ανθρώπων. Εύκολο στην εγκατάσταση και χρήση μέσω της εφαρμογής έξυπνων συσκευών Hik-Connect και iVMS, το AXHub ειδοποιεί τον τελικό χρήστη σε οποιοδήποτε συμβάν και παρέχει επαλήθευση βίντεο μέσω της επαναστατικής επαλήθευσης εισβολέα ως υπηρεσία (Intruder Verification as a Service - IVaaS).

Τι είναι πραγματικά έξυπνο ...στην Ασφάλεια!

Ο όρος “έξυπνος”, “ευφυής” και άλλοι συναφείς προσδιορισμοί, χρησιμοποιούνται συχνά τα τελευταία χρόνια για διάφορες τεχνολογίες, συστήματα, προϊόντα διαδικασίες ...ακόμα και για κτίρια ή πόλεις! Η χρήση των εννοιών Smart & Intelligent, θα λέγαμε ότι αρκετές φορές γίνεται και καταχρηστικά, εννοώντας με αυτό ότι είναι δεν αποτυπώνεται η πραγματική διάσταση του “έξυπνου”. Μιλάμε δηλαδή για ένα **“marketing buzzword”** που πολλές φορές απλά εξυπηρετεί την προσπάθεια να γίνει το εκάστοτε προϊόν πιο ελκυστικό και να δελεαστούν οι εν δυνάμει αγοραστές. Θα είχε ενδιαφέρον λοιπόν -και με αφορμή το κεντρικό άρθρο του τεύχους για την Τεχνητή Νοημοσύνη- να δούμε τι πραγματικά θα πρέπει να πρεσβεύει ο όρος έξυπνο στις **τεχνολογίες και τις διαδικασίες για την ασφάλεια**.

Καταρχήν η αποτύπωση του όρου έξυπνου για ένα τεχνολογικό προϊόν μπορεί να είναι δύσκολη. Αν θα επιχειρούσαμε να δώσουμε ένα ορισμό μελετώντας διάφορες διεθνείς πηγές, θα μπορούσαμε να προσδιορίσουμε ως ένα έξυπνο προϊόν αυτό που **υπερβαίνει την κανονική του αποστολή**, ενσωματώνοντας δυνατότητες -πέρα από τις παραδοσιακές- με κυριότερες την άμεση και πιο **εύκολη αλληλεπίδραση** με το χρήστη ή με άλλες συσκευές με πυρήνα τη **διασυνδεσιμότητα του στο Διαδίκτυο**. Θα μπορούσαμε να χαρακτηρίσουμε έξυπνο οποιοδήποτε σύστημα συνδέεται στο internet; Η απάντηση είναι πως όχι. Βασικό στοιχείο ευφυΐας, είναι η αυτοματοποίηση διαδικασιών και η ευελιξία λειτουργιών με **προσαρμοστικότητα σε διάφορες συνθήκες και σενάρια**. Προχωρώντας ένα βήμα παραπάνω και σε ότι αφορά το Artificial Intelligence θα προσθέταμε τη δυνατότητα **εκμάθησης από το γύρω περιβάλλον** και τη λήψη αποφάσεων που θα στηρίζονται στην αξιολόγηση των στοιχείων που συλλέγονται. Ένα ολοκληρωμένο σύστημα ασφάλειας, θα μπορούσαμε να το ορίσουμε ως έξυπνο όταν ενσωματώνει πολλαπλούς αισθητήρες που λαμβάνουν δεδομένα από το περιβάλλον (εικόνες, ήχους, κινήσεις κ.λπ.), διαθέτει προηγούμενους αλγόριθμους επεξεργασίας και ανάλυσης και έχει τη δυνατότητα σε πραγματικό χρόνο να επιτελεί διάφορες λειτουργίες, δίνοντας εντολές σε άλλα συστήματα και ενημερώνοντας άμεσα τους διαχειριστές για οποιαδήποτε συμβάν έχει ενδιαφέρον. Με βάση αυτό τον ορισμό, υπάρχουν σήμερα αρκετά συστήματα βιντεο-επιτήρησης, συναγερμού, ελέγχου πρόσβασης αλλά και πυρανίχνευσης που δικαιωματικά μπορούν να χαρακτηριστούν ως έξυπνα. Στο τομέα των κτιρίων αλλά των πόλεων, η έννοια του έξυπνου, αποτυπώνεται με βάση **το επίπεδο ενσωμάτωσης αυτών των τεχνολογιών**, έχοντας ως πυρήνα το Διαδίκτυο των Πραγμάτων (IoT - Internet of Things) και την ανάπτυξη υποδομών με διασυνδεδεμένους αισθητήρες και μηχανές. Η ασφάλεια αλλά και η πολιτική προστασία αποτελούν πλέον σημαντικές πτυχές σε ένα έξυπνο κτίριο ή μια έξυπνη πόλη, με στόχο τη διαχείριση των τεχνητών και φυσικών κινδύνων και τη έγκαιρη ενημέρωση και προληπτική προστασία από εγκληματικές δράσεις (π.χ. βομβιστικές ενέργειες) ή φυσικές καταστροφές (σεισμοί, πλημμύρες, πυρκαγιές). Σήμερα περισσότερο από ποτέ, **η ανθεκτικότητα των πόλεων και των κτιρίων** εξαρτάται από την ανοιχτή επικοινωνία, συνεργασία και διασύνδεση μεταξύ μιας ευρείας ποικιλίας συστημάτων, οργανισμών και ανθρώπων σε πραγματικό χρόνο ενημέρωσης, αξιολόγησης, λήψης απόφασης και ανάληψης δράσης. Οι προκλήσεις σε αυτό το τομέα είναι ανεξάντλητες και η δημιουργία ενός πραγματικά έξυπνου οικοσυστήματος αποτελεί τώρα και στο μέλλον ένα λαμπρό πεδίο δράσης για τους ανθρώπους της ασφάλειας.

Βλάσης Αμανατίδης

Περιοδικό για την ασφάλεια
security
manager

Εκδότης
Κώστας Νόσσης

Αρχισυντάκτης
Βλάσης Αμανατίδης v.amanatidis@smartpress.gr

Διεύθυνση Επικοινωνίας & Marketing
Ειρήνη Νόστη

Υπεύθυνος Διαφήμισης
Γιώργος Ιωσηφέλης

Συνεργάτες
Παρασκευάς Βερώνης
Δημήτρης Θωμαδάκης
Γιάννης Κανάλης
Σπύρος Κυριακάκης
Καίτη Κωνσταντάκου
Δημήτρης Λόγος
Αριστοτέλης Λυμπερόπουλος
Δημοσθένης Παναγιώτου
Γιάννης Ρούσσος
Δημήτρης Σκιάννης
Βασίλης Χαλβατζής

Σύμβουλος Έκδοσης
Νίκη Πανδη

Υπεύθυνη Παραγωγής
Ελένη Καπιτσάκη

DTP
Θοδωρής Παπουτσής
Νίκος Χαλκιαδάκης

Υπεύθυνος Ηλεκτρονικών Μέσων
Δημήτρης Θωμαδάκης

Υπεύθυνη Συνεδρίων
Αγγελική Νόστη

Φωτογράφος
Ιωάννης Μαρμαράς

Γραμματεία Εμπορικού
Έλλη Μαστρομανώλη

Λογιστήριο
Ανδρέας Λουλάκης

Consulting by
SPEG Co
τηλ.: 210 5238777, www.speg.gr, info@speg.gr

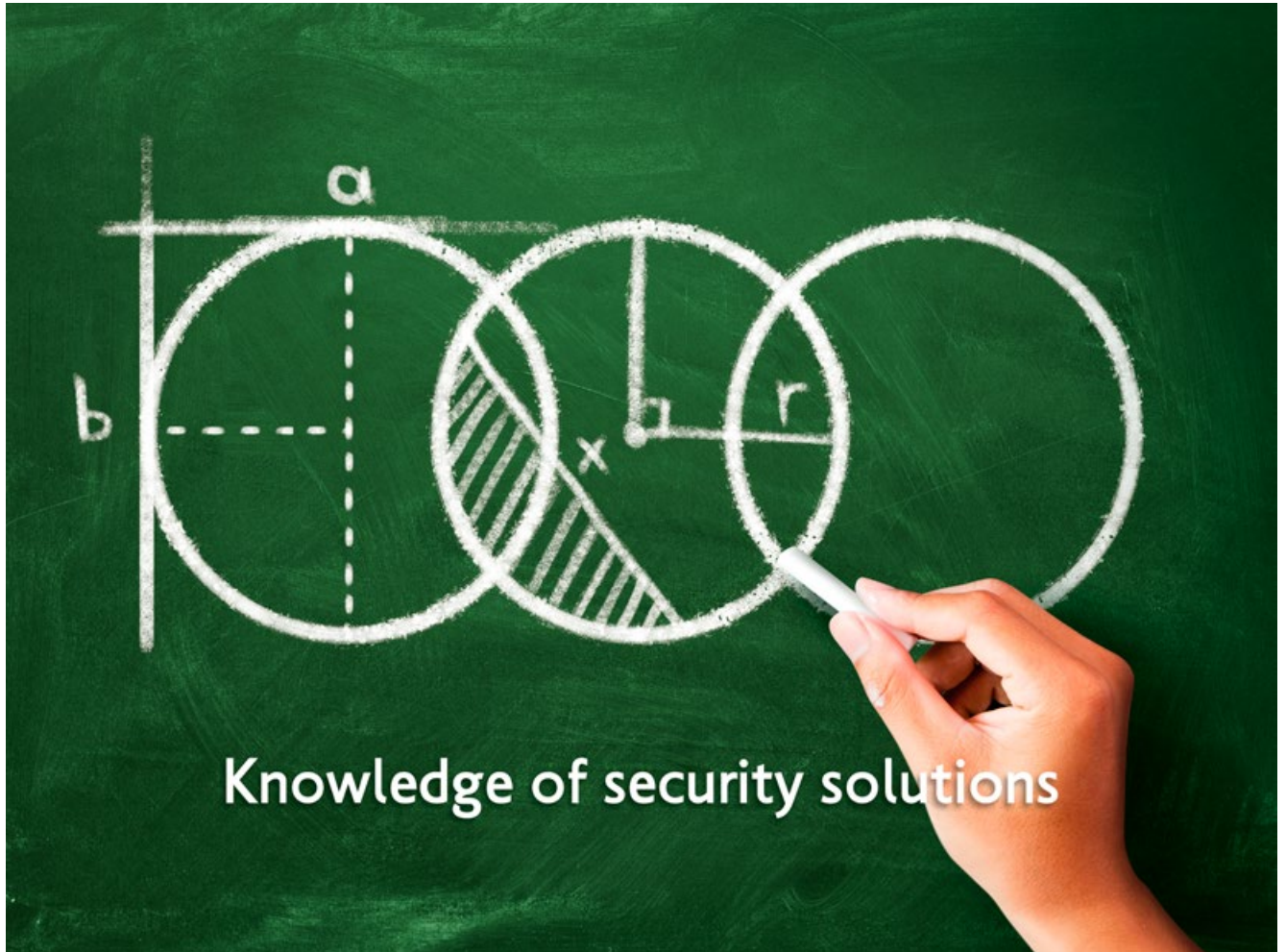
Ιδιοκτήτης
Smart Press
Μάγερ 11, 10438, Αθήνα
Τηλ.: 210 5201500, 210 5230000,
Fax: 210 5241900

Τμήμα συνδρομών
support@securitymanager.gr



SMART
PRESS
www.smartpress.gr
www.securitymanager.gr
info@securitymanager.gr

ΚΩΔΙΚΟΣ ΕΛΤΑ: 01-7627
ISSN: 2407-9413



security solutions

www.esasecurity.gr

2 Editorial

6 Market News

Feature Story

- 22 Θερμική απεικόνιση ανίχνευσης θερμοκρασίας ...και άλλα μέτρα προστασίας!
- 26 Η εξέλιξη της Europol στη Διεθνή Αστυνομική Συνεργασία
- 38 Η Ασφάλεια στην Περιφερειακή Ανάπτυξη

Management Analysis

- 48 "Διαχείριση Ποιότητας"... μια Σταθερά!
- 50 Διοίκηση διαφορετικότητας σε ιδιωτικές υπηρεσίες ασφαλείας
Η διαχείριση των δύο φύλων
- 54 Διαχείριση Κρίσης στα νερά του Ινδικού Ωκεανού
Μια βιωματική μελέτη περίπτωσης

Event Report

- 56 Νέες λύσεις Διαχείρισης Οχημάτων Vector Security και η Dahua Technology
"The Track Day"

Fire Safety

- 58 Νέα Πυροσβεστική Διάταξη
Χρήσιμες οδηγίες εφαρμογής για τις εγκαταστάσεις

Intrusion Alarm

- 62 Πρόβλημα επικοινωνίας σε συναγερμούς;
Υπάρχει Λύση!
- 64 Η εξέλιξη των συστημάτων συναγερμού ...προς το εξυπνότερο!

Video Surveillance

- 68 Μετάβαση σε Δικτυακές Πλατφόρμες
- 72 Το AI αλλάζει την Ασφάλεια

Security Installer

- 78 Συνέπεια, εξέλιξη και συνεχή εκπαίδευση
Συνέντευξη με την Ολιάντα Μπέλλα - Ιδιοκτήτρια Bella Security Group

80 Product Reviews

86 Products Update

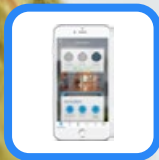
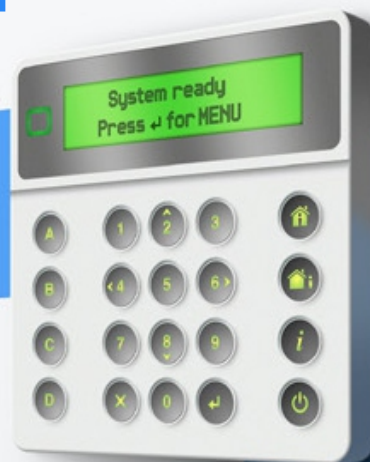
94 Ευρετήριο Εταιρειών





Έλεγχος με ένα Άγγιγμα!

Σας παρέχουμε την απλότητα,
και την ασφάλεια που χρειάζεστε.



*Τι γίνεται όταν ξεπερνάς
την ΚΟΡΥΦΗ !!!!*



G.I. SECURITY S.A.
SECURITY PRODUCTS-SYSTEMS

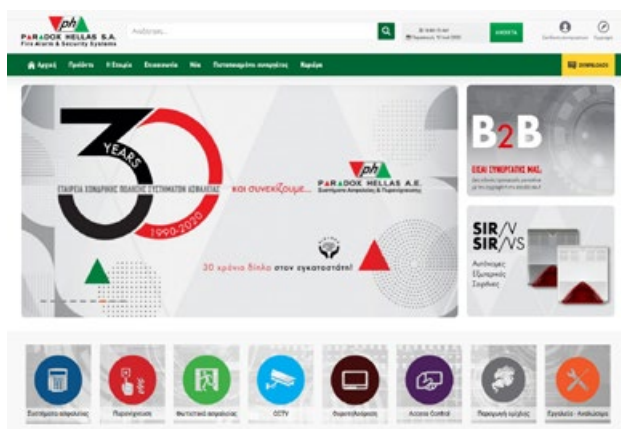
Μια στάση για όλες σου τις ανάγκες!

ΑΘΗΝΑ: 16ο χλμ. Λεωφ. Λαυρίου Παιανία,
Τηλ.: 210-604-0601, Fax: 210-665-8710,
e-mail: sales@gisecurity.gr,

www.gisecurity.gr

ΘΕΣ/ΝΙΚΗ: Προέκταση Μαϊάνδρου & Ελευθερίου
Ωραιόκαστρο, Θεσ/νίκη 570 13,
Τηλ.: 2310-020-150, Fax: 2310-688-284,
e-mail: ndc@gisecurity.gr

■ Το νέο **B2B site** της **Paradox Hellas: www.phs.gr** ...είναι γεγονός!



Στα πλαίσια της εξέλιξης των **30 χρόνων** εμπειρίας της στο χώρο της Χονδρικής Πώλησης Συστημάτων Ασφαλείας & Πυρανίχνευσης, η **Paradox Hellas** παρουσίασε με χαρά τη **νέα της πλήρη ηλεκτρονική πλατφόρμα B2B στη διεύθυνση: www.phs.gr**.

Η Paradox Hellas A.E. με σύμμαχο την εξέλιξη και την τεχνολογία, βελτιώνει την ήδη πετυχημένη συνεργασία της με τους επαγγελματίες του χώρου για να τους εξυπηρετήσει άμεσα και λειτουργικά σε πραγματικό χρόνο.

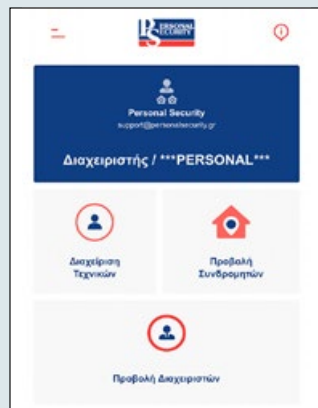
Με τη νέα πλατφόρμα η εταιρία επενδύει στην απευθείας και παραγωγική εξυπηρέτηση των συνεργατών της, μέσω του νέου B2B site, στηρίζοντας τους και εξοικονομώντας τους Χρόνο και Χρήμα.

Όπως μας ενημερώνει η εταιρεία, μπαίνοντας στο **www.phs.gr** κάνετε εγγραφή και είσοδο στο B2B, ώστε να δημιουργήσετε το δικό σας λογαριασμό πελάτη και να μπορείτε να βλέπετε όλα τα προϊόντα και τις προσφορές της εταιρείας! Με αυτό το τρόπο θα αποκτήσετε το δικό σας ιστορικό αγορών αναλυτικά και θα έχετε μια πλήρη εικόνα της επιχείρησής σας, σε σχέση με την συνεργασία με την Paradox Hellas, επιτρέποντας:

- Online παραγγελίες Online διαθεσιμότητα προϊόντων
- Πλήρες ιστορικό αγορών - Ειδικές προσφορές - Προσωποποιημένες τιμολογιακές πολιτικές - Φίλτρα επιλογής προϊόντων - Downloads

Για την καλύτερη εξυπηρέτησή σας, η παλιά ιστοσελίδα θα λειτουργεί έως 31 Οκτωβρίου χωρίς τη δυνατότητα εγγραφής νέων χρηστών. Νέες αιτήσεις εγγραφής θα πρέπει να γίνονται στο B2B. Μετά την παραπάνω ημερομηνία το νέο B2B θα λειτουργεί παράλληλα και στους δύο συνδέσμους (www.paradox.gr, www.phs.gr).

■ Αναβάθμιση της **υπηρεσίας PSView** από την **Personal Security** - Δωρεάν για όλους τους συνεργάτες της!



Η **Personal Security** ολοκλήρωσε την **αναβάθμιση** της υπηρεσίας **PSView** και την προσφέρει πλέον **δωρεάν** σε όλους τους **συνεργάτες** της!

Η νέα, εξελιγμένη έκδοση της εφαρμογής PSView, διαθέτει μια σειρά από πρωτοποριακές δυνατότητες, προσφέροντας

στους **επαγγελματίες εγκαταστάτες** χρηστικές πληροφορίες όπως:

- Άμεση πρόσβαση στα σήματα του συνδρομητή
- Αναλυτική οπτικοποίηση των ζωνών του συνδρομητή όπως έχουν δηλωθεί

- Πρόσβαση στην καρτέλα με όλα τα στοιχεία και τα τηλέφωνα ειδοποίησης συνδρομητή
- Αναλυτική πρόσβαση στα κανάλια επικοινωνίας του συστήματος συναγερμού
- Δυνατότητα ανάθεσης κάθε συνδρομητή σε συγκεκριμένους τεχνικούς με χρονικό περιορισμό
- Πρόσβαση σε μια μεγάλη βιβλιοθήκη με εγχειρίδια εγκαταστάτη αλλά και τελικού χρήστη

Η εφαρμογή **PSView** παρέχει πλήρη ασφάλεια δεδομένων καθώς είναι **GDPR Compliant & ISO 27001:2013 approved**, και υποστηρίζεται από **Windows, iOS** και **Android**. Για να εγγραφείτε στην υπηρεσία PSView, ακολουθήστε το σύνδεσμο: <https://psview.personalsecurity.gr/> και επικοινωνήστε με το τμήμα Τεχνικής Υποστήριξης ή το ΚΛΣ της Personal Security στο τηλ.: 210 8068675.



ΕΥΡΩΠΑΪΚΟ ΚΕΝΤΡΟ ΛΗΨΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΣΗΜΑΤΩΝ

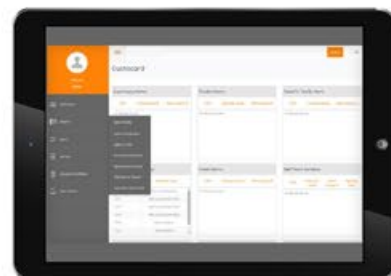


Web Dealer

Το νέο πρόγραμμα διαχείρισης που επιτρέπει στον επαγγελματία εγκαταστάτη πρωτοφανή διαχείριση του πελατολογίου του



Made in the U.S.A.



Παρακολουθήστε τα σήματα συναγερμού των πελατών σας



Δημιουργήστε νέες συνδρομές



Διαγράψτε συνδρομές



Προσθέστε περιγραφή ζωνών και προβείτε σε αλλαγές της λίστας των τηλεφώνων ειδοποίησης



Το πρόγραμμα διαχείρισης υποστηρίζεται από υπολογιστή και smartphone

Νέες δυνατότητες από κορυφαίους κατασκευαστές με την μέγιστη ασφάλεια δεδομένων.

SPEED • EFFECTIVENESS • TEAMWORK

ΑΘΗΝΑ: 210-602-8120 | ΘΕΣΣΑΛΟΝΙΚΗ: 231-111-7400

e-mail: info@hellasdms.com

www.hellasDMS.com

■ Η έκθεση **SECUREXPO** τον **Οκτώβριο του 2021**



Η διοργάνωση της έκθεσης SECUREXPO συμμεριζόμενη τη διάχυτη αβεβαιότητα που επικρατεί στην αγορά, εξαιτίας

των επιπτώσεων του COVID-19, αποφάσισε να μεταθέσει την έκθεση **SECUREXPO** για τον **Οκτώβριο του 2021**.

Η μετάθεση χρονικά της **SECUREXPO** ήταν αποτέλεσμα συζητήσεων με όλους τους εκθέτες ως η πιο ενδεδειγμένη επιλογή. Οι νέες ημερομηνίες διεξαγωγής της έκθεσης θα

ανακοινωθούν σύντομα. Η διοργάνωση διαβεβαιώνει ότι θα συνεχίσει να εργάζεται μεθοδικά και με υπευθυνότητα, προκειμένου να διασφαλίσει τις προϋποθέσεις για την επιτυχή έκβαση της **SECUREXPO 2021 ως το κορυφαίο ραντεβού του κλάδου**.

Πλήρης ενημέρωση θα πραγματοποιείται από το site της έκθεσης: www.secureexpo.eu

Η Διοργάνωση ευχαριστεί θερμά για τη κατανόηση και τη διαχρονική στήριξη των εταιρειών του κλάδου στην έκθεση SECUREXPO.

■ **LEXIS** και **KEDACOM** παρουσιάζουν τις **AI κάμερες 3ης γενιάς!**

Η **LEXIS** Πληροφορική και η **KEDACOM**, ένας από τους πλέον κορυφαίους κατασκευαστικούς οίκους AI συστημάτων απομακρυσμένης παρακολούθησης, παρουσιάζουν την **3η γενιά AI καμερών** με ανανεωμένο hardware και αναβαθμισμένο ισχυρό αλγόριθμο **Deep Learning** με **ακόμα μεγαλύτερες δυνατότητες**.

Οι νέες κάμερες αναγνώρισης της KEDACOM μπορούν να εκτελούν, ταυτόχρονα, **ανάλυση, ανθρώπου, οχήματος και πλήρους δομής με μεγαλύτερη ακρίβεια αναγνώρισης, ισχυρότερη προσαρμοστικότητα σκηνής και το πιο σημαντικό, να επιτυγχάνεται η απλοποίηση και διάδοση της Τεχνητής Νοημοσύνης (AI)**. Έχουν τη δυνατότητα ταυτόχρονης ανίχνευσης άνω των 100 προσώπων σε κάθε καρέ, όταν πραγματοποιούν σενάρια αναγνώρισης ανθρώπων σε μεγάλο πλήθος ατόμων. Επιπλέον, επιτυγχάνουν πλήρως δομημένη ανάλυση, βασισμένη στην εξαιρετικά υψηλής ευκρίνειας 4K, με περισσότερα από 30 χαρακτηριστικά μηχανοκίνητων και μη οχημάτων, καθώς και αναγνώρισης ανθρώπων.

Ανάμεσα στα πλούσια χαρακτηριστικά των καμερών περιλαμβάνονται η real-time σύγκριση, η διαχείριση ειδοποιήσεων και η δυνατότητα προσθήκης άνω των 50.000 προσώπων στη βιβλιοθήκη δεδομένων, αποτελώντας ιδανική λύση για αναγνώριση προσώπων σε χώρους με υψηλή συγκέντρωση ατόμων. Επιπλέον, οι κάμερες ελέγχου οχημάτων έχουν τη δυνατότητα ανίχνευσης 11 τύπων (αμάξι, pickup, λεωφορείο, βαν, φορτηγό, μίνι-βαν, μηχανή, ποδήλατο, ηλεκτρικό τρίκυκλο, τρίκυκλο και πεζών) ενώ



η σειρά trinocular καμερών συνδυάζει πανοραμικές λήψεις και κοντινά πλάνα παρέχοντας ένα εξαιρετικά ευρύ οπτικό πεδίο που φτάνει τα 10 μέτρα, καλύπτοντας τις πιο απαιτητικές λήψεις ανθρώπων και οχημάτων σε πολλαπλά σημεία (σκηνές).

Η σειρά 3ης γενιάς καμερών της KEDACOM είναι διαθέσιμη μέσα από το δίκτυο συνεργατών της LEXIS, καλύπτοντας ένα ευρύ πεδίο εφαρμογών, ξεκινώντας από την αναγνώριση ανθρώπων και οχημάτων μέχρι την παροχή ολοκληρωμένης ανάλυσης δεδομένων, χρησιμοποιώντας τους πλέον εξελιγμένους αλγόριθμους Deep Learning.

Περισσότερες πληροφορίες: email: lexis@lexis.gr, τηλ. Αθήνας: 210 6777007, τηλ. Θεσ/νίκης: 2310 329350-1.



Λύσεις στην αιχμή της τεχνολογίας

Ανιχνευτές κίνησης Επίσημος διανομέας



**FARO
IP PLUS**



**FARO
EXT**



**FARO
MINI**



**FARO
WINDO**



VENITEM

&

ΗΛΚΑ

*10 χρόνια
συνεργασίας*

Εξωτερικές σειρήνες*



DOGE



HOLA



MOSE



**ECO 800
METAL**



**ECO 800
INOX**



HEMA



RONDO

* Εγγύηση 5 έτη, πλακέτες με επιστροφή ρυτίνης, πιστοποιήσεις EN50131-4 Grade 3 & 4 σε ορισμένα μοντέλα.



ΗΛΚΑ Α.Ε.

Τεμπών 14, 153 42, Αγ. Παρασκευή Αττικής

T: 210-6071510, F: 210-6071599, E: sales@ilka.gr | www.ilka.gr

www.ilka.gr/products



[ilka.gr/facebook](https://www.facebook.com/ilka.gr)



[ilka.gr/twitter](https://www.twitter.com/ilka.gr)



[ilka.gr/linkedin](https://www.linkedin.com/company/ilka.gr)



[ilka.gr/instagram](https://www.instagram.com/ilka.gr)

■ Η **Dahua** καινοτομεί με τη λύση **Three-in-One Camera, TiOC**

Μια προηγμένη λύση για την αντιμετώπιση των ψευδών συναγερμών, την άμεση ανταπόκριση σε συμβάντα και την αξιόπιστη συλλογή αποδεικτικών στοιχείων παρουσίασε η Dahua.

Καθώς τα σενάρια εφαρμογής των συστημάτων ασφάλειας και των αντίστοιχων έργων γίνονται όλο και πιο απαιτητικά, τα παραδοσιακά συστήματα θα πρέπει να βρουν τρόπους να αντιμετωπίζουν τις διάφορες προκλήσεις με κυριότερη αυτή που αφορά τους ψευδείς συναγερμούς, που προκαλούνται από κατοικίδια ζώα, έντομα, φύλλα και άλλους παράγοντες. Προκειμένου να αντιμετωπίσει αυτά τα ζητήματα, η **Dahua Technology** λανσάρει την πρωτοποριακή και ισχυρή λύση ασφάλειας **Three-in-One Camera**, γνωστή και ως **TiOC**. Αυτή η αυτοματοποιημένη και ολοκληρωμένη λύση ασφάλειας προσφέρει:

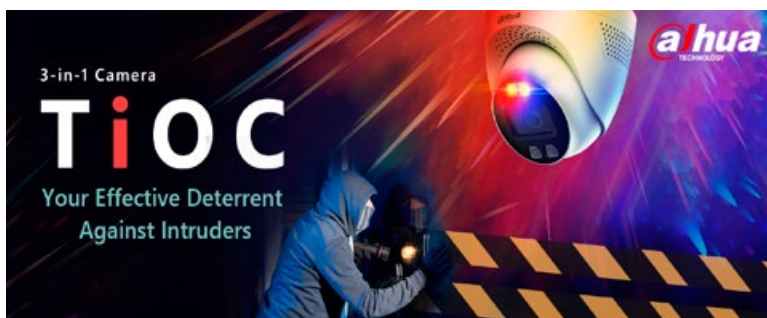
Συναγερμό με μεγάλη ακρίβεια. Ο ψευδής συναγερμός θεωρείται πάντα πονοκέφαλος για τους χρήστες όταν συμβαίνει. Με δυνατότητα περιμετρικής προστασίας, **βασισμένη σε Τεχνητή Νοημοσύνη (AI) και SMD Plus**,

η λύση Dahua TiOC παρέχει λειτουργία ενεργοποίησης συναγερμού με πολύ μεγάλη ακρίβεια στοχεύοντας άτομα και οχήματα, ενώ φιλτράρει αντικείμενα που δεν ενδιαφέρουν, όπως ζώα, φύλλα και προβολείς αυτοκινήτων. Ενώ διατηρούν το ποσοστό ψευδών συναγερμών κάτω από 2%, οι ισχυροί αλγόριθμοι AI παρέχουν επίσης ταχύτερη, ακριβέστερη και μεγαλύτερης εμβέλειας ανίχνευση κίνησης (η απόσταση ανίχνευσης αυξάνεται περισσότερο από 185%), βελτιώνοντας σημαντικά την αποτελεσματικότητα ολόκληρης της λύσης TiOC.

Συναγερμός ενεργής αποτροπής και πραγματικού χρόνου. Αντί οι διαχειριστές ενός συστήματος επιτήρησης να βασίζονται μόνο στα καταγεγραμμένα βίντεο ως αποδεικτικά στοιχεία μετά από ένα συμβάν, το TiOC καθιστά **δυνατή την απόκριση κατά τη διάρκεια του συμβάντος με τις λειτουργίες ενεργής αποτροπής**

και συναγερμού σε πραγματικό χρόνο που μπορούν να αποτρέψουν σημαντικά το συμβάν. Η ενεργή αποτροπή γίνεται πιο αποτελεσματική με το κόκκινο και το μπλε φως, το οποίο είναι πιο ευκρινές από το λευκό φως και είναι επίσης ορατό ακόμη και σε πυκνή ομίχλη και δυνατή βροχή. Ένα βελτιωμένο ηχείο παρέχει ήχους έως και 110 dB, με σειρήνα ή ηχογραφημένη φωνή.

Το **APP Alarm Push** παρέχει ειδοποιήσεις συναγερμού σε πραγματικό χρόνο, επιτρέποντας στους χρήστες να ανταποκρίνονται εγκαίρως, επιτρέποντας την αποστολή ηχητικών μηνυμάτων και λειτουργία αμφίδρομης ομιλίας. Επιπλέον, το σύστημα επιτρέπει επίσης προ-ηχογραφημένες ανακοινώσεις ή προσαρμοσμένες ηχογραφήσεις. Η εφαρμογή για κινητά υποστηρίζει επίσης λειτουργία οπλισμού / αφοπλισμού με ένα πάτημα που προσφέρει μεγάλη ευκολία στους χρήστες.



Πλήρης χρωματική απεικόνιση. Οι πολλές αξιόπιστες πληροφορίες αποτελούν το κλειδί κατά την ανάκτηση στοιχείων σε ένα συμβάν. Με την κορυφαία τεχνολογία

πλήρους χρώματος το Dahua TiOC προσφέρει έγχρωμες εικόνες μέρα και νύχτα, βελτιώνοντας σημαντικά την ικανότητα εντοπισμού υπόπτων, αυξάνοντας παράλληλα την ποιότητα των αποδεικτικών βίντεο.

Τρία σε ένα. Η TiOC ενσωματώνει 24/7 πλήρη έγχρωμη παρακολούθηση, ενεργή αποτροπή και AI σε μία έξυπνη, καινοτόμο λύση, εξοικονομώντας χρόνο και κόστος για διανομείς και εγκαταστάτες.

Σενάρια εφαρμογής. Το TiOC είναι κατάλληλο για όλους τους χώρους που απαιτείται ασφάλεια 24/7 και βρίσκονται απομακρυσμένα και όχι μόνο, παρέχοντας τη δυνατότητα άμεσης προειδοποίησης στους εισβολείς, όπως βίλες, αποθήκες, καταστήματα, μονάδες παραγωγής, αλλά και ειδικές εφαρμογές όπως η προστασία των δασικών ζωνών αποτροπής πυρκαγιάς κ.ά.



Η Personal Security ιδρύθηκε το 1978 και αποτέλεσε μία από τις πρώτες εταιρείες που οργάνωσαν και λειτούργησαν, με επιτυχία, ιδιόκτητο Κέντρο Λήψης Σημάτων συναγερμού.

Έκτοτε, διαθέτοντας συνέπεια, επαγγελματισμό και άριστη τεχνογνωσία, σε συνδυασμό με συνεχόμενες επενδύσεις, αποτελεί μία από τις πιο δυναμικές εταιρείες στον τομέα της ηλεκτρονικής ασφάλειας, παρέχοντας υψηλού επιπέδου υπηρεσίες σε 35.000 και πλέον συνδρομητές πανελλαδικά, σύμφωνα με τις αυστηρότερες προδιαγραφές ποιότητας που προβλέπονται από το **ISO 27001:2013, ISO 9001:2015, ISO 14001:2015 και ISO 45001:2018** του οίκου **TUV AUSTRIA HELLAS**.

Σε όλα αυτά τα χρόνια ανοδικής πορείας, η εταιρεία έχει καταφέρει να κερδίσει την εμπιστοσύνη 900 και πλέον επαγγελματιών εγκαταστατών - συνεργατών, ενώ συνεχίζει διαρκώς να αναβαθμίζει τις παρεχόμενες υπηρεσίες της, μέσα από ένα μακροχρόνιο επενδυτικό πλάνο και με συνεχή κατάρτιση και εκπαίδευση του προσωπικού της, διατηρώντας πάντα την ανθρωποκεντρική προσέγγιση τόσο στα θέματα εσωτερικής λειτουργίας, όσο και εξυπηρέτησης.

Διη/α 6ος... προβωηικά!
από το 1978

- 24ωρο Κέντρο Λήψης Σημάτων Συναγερμού
- Υπηρεσία Οπτικής Επιβεβαίωσης (Video Analytics)
- Άμεση Επέμβαση – Περιπολία
- Πλήρης Συμβατότητα Πρωτοκόλλων Επικοινωνίας (Tel.-IP-GPRS)
- Τεχνική Υποστήριξη Επαγγελματιών Εγκαταστατών
- Χονδρική Μεταπώληση Συστημάτων Ασφαλείας

PERSONAL SECURITY A.E. Οδός Μεσογείων 99, Μαρούσι, Τ.Κ. 15126, Αθήνα

☎ 210-8068675 📠 210-6122531 ✉ info@personalsecurity.gr 🌐 www.personalsecurity.gr 📱 personalsecurity

■ Νέα προϊόντα, νέες λειτουργίες, νέο firmware Ajax

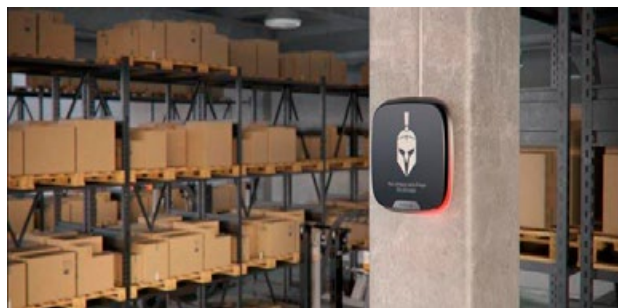
Η Ajax, σε πρόσφατη παρουσίασή της, ανακοίνωσε ότι το επόμενο διάστημα θα είναι διαθέσιμες νέες λύσεις που ενισχύουν σημαντικά την γκάμα των καταξιωμένων παγκοσμίως προϊόντων που διαθέτει. Συγκεκριμένα οι λύσεις αυτές είναι:

Hub 2 Plus



Το νέο Hub 2 Plus υποστηρίζει 4 ανεξάρτητα κανάλια επικοινωνίας (2xSIM 4G/3G/2G, Wi-Fi, Ethernet) και 200 συσκευές ενώ έχει δυνατότητα αποστολής στιγμιότυπου μέσα σε 9 δευτερόλεπτα ακόμα κι όταν λειτουργεί με κάρτα SIM (LTE).

StreetSiren DoubleDeck



Η StreetSiren DoubleDeck είναι μια εξωτερική σειρήνα με δυνατότητα εγκατάστασης προσαρμοσμένης πρόσοψης με το λογότυπό σας για να διαφημίζετε τις υπηρεσίες σας.

MultiTransmitter



Το MultiTransmitter είναι ένα νέο περιφερειακό που μπορεί να χρησιμοποιηθεί για την ενσωμάτωση 18 ενσύρματων

ζωνών. Αντικαθιστά τον παλιό πίνακα συναγερμού ενσωματώνοντας ενσύρματα περιφερειακά στον Ajax. Στον επαγγελματία δίνεται η δυνατότητα για απομακρυσμένη παραμετροποίηση περιφερειακών, ενώ οι χρήστες αποκτούν όλες τις δυνατότητες διαχείρισης του συστήματος μέσω της εφαρμογής για κινητό. Ενσωματώνονται συσκευές άλλων κατασκευαστών στον Ajax. Αυτό σημαίνει ότι μπορούν να προστεθούν ανιχνευτές αερίου, θερμοκρασίας, πλημμύρας, μπάρες υπερύθρων, κ.ά.

OS Malevich 2.9



Το νέο firmware OS Malevich 2.9 φέρνει σημαντικές αλλαγές για τους χρήστες αλλά και τους εγκαταστάτες. Στις κύριες αλλαγές περιλαμβάνονται:

- Δυνατότητα άμεσης αντικατάστασης ενός Hub με το νέο μενού εισαγωγής δεδομένων.
- Επιλογή για προσωρινή απενεργοποίηση ενός περιφερειακού που παρουσιάζει δυσλειτουργία χωρίς να αφαιρεθεί από το σύστημα.
- Λειτουργία παλμού σε Socket και Wall Switch για ενεργοποίηση συσκευών για ορισμένο χρονικό διάστημα.
- Προσαρμοσμένος τύπος συναγερμού για το Button και το Transmitter.
- Ενημέρωση για την τοποθεσία ενός χρήστη με το πάτημα του πανικού από την εφαρμογή.
- Επιπλέον προστασία για τυχαία πατήματα στο SpaceControl.
- Ρύθμιση φωτεινότητας στο πλαίσιο LED του Socket.
- Δυνατότητα απενεργοποίησης της φωτεινής ένδειξης ενός ανιχνευτή σε περίπτωση συναγερμού.
- Ειδοποίηση όταν ενεργοποιείται, απενεργοποιείται ή επαναφέρεται σε εργοστασιακές ρυθμίσεις ένα Hub.



**Security & Automation
Solutions**



Προτιμήστε προμηθευτές
που προσφέρουν άρτια
τεχνική υποστήριξη!

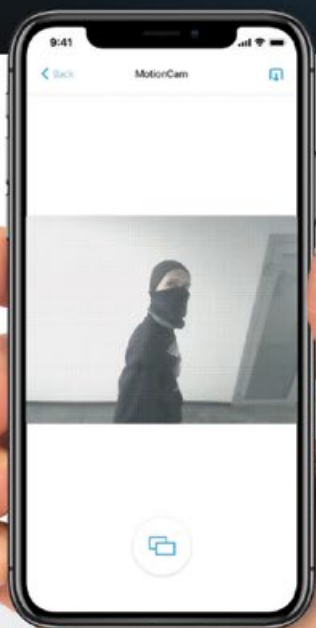


StarterKit Cam

Ολοκληρωμένη προστασία με
οπτική επιβεβαίωση συναγερμού

Το Ajax StarterKit Cam αποτελείται από:

- Κεντρική μονάδα Hub 2
- Ανιχνευτή MotionCam με ενσωματωμένη κάμερα
- Μαγνητική επαφή DoorProtect
- Τηλεχειριστήριο SpaceControl



Λεωφ. Βουλιαγμένης 262 Άγιος Δημήτριος, ΤΚ 17343
Τ 210 9640258 E sales@electrosystems.gr
www.electrosystems.gr



Βραβείο καλύτερου
συστήματος συναγερμού
της χρονιάς



Βραβείο καλύτερου
συστήματος συναγερμού
και πυρασφάλειας



Βραβείο καλύτερου
καινοτόμου
προϊόντος



Βραβείο καλύτερου
συστήματος ασφαλείας
της χρονιάς

■ Η Keeper Group διαθέτει τα συστήματα της DSC στην Ελλάδα με την ενδυνάμωση της συνεργασίας με την SDC

Η **KEEPER Group** ανακοίνωσε ότι εμβαθύνει τη μακροχρόνια συνεργασία της με την **Security Distribution Center S.D.C. Ltd (SDC)** και με την υποστήριξη της **Tyco/Johnson Controls** ανακοινώνουν Νέα Επίσημη Διάθεση των συστημάτων ασφαλείας DSC για την Ελληνική επικράτεια. Η αποτελεί για περισσότερο από 10 έτη επίσημο συνεργάτη της Tyco/Johnson Controls για την Κυπριακή αγορά, με δραστηριοποίηση στην Ελληνική και την Μαλτέζικη αγορά. Η KEEPER Group αποτελεί επίσημο διανομέα της Πυρανίχνευσης Fireclass του ομίλου Tyco/Johnson Controls, έχοντας υποστηρίξει κάποια από τα σημαντικότερα έργα των τελευταίων ετών. Από τον Ιούλιο του 2020, ανακοινώνεται και η επίσημη διάθεση των συστημάτων ασφαλείας του Παγκόσμιου Ηγέτη στην ηλεκτρονική ασφάλεια, DSC, για την Ελληνική αγορά. Ο συνδυασμός των ηγέτιδων εταιριών, έρχεται να αποτελέσει έναν ισχυρό πυλώνα διάθεσης προϊόντων, υποστήριξης, κατάρτισης, τεχνολογίας και καινοτόμων υπηρεσιών της DSC στην Ελληνική αγορά. Η υπεροχή των προϊό-



ντων DSC τόσο σε απόδοση όσο και σε αξιοπιστία την καθιστούν ως πρώτη επιλογή σε περισσότερες από 140 χώρες ανά τον κόσμο. Ο τομέας έρευνας και ανάπτυξης καθώς και οι υπερσύγχρονες μονάδες παραγωγής σε Ευρώπη και Αμερική, εξελίσσουν και παράγουν συνεχώς νέα προϊόντα υψηλής τεχνολογίας και υπεροχής. Η DSC θα διαθέσει μέσω της KEEPER Group στην Ελληνική αγορά τις σειρές Power, Neo, Pro και WP.

■ Analytics για την ασφαλή επιστροφή των θεατών σε γήπεδα και άλλες εκδηλώσεις

Η τεχνολογία venue optimization της SAS θα μπορούσε να φέρει τους θεατές πίσω στα γήπεδα, με την ασφάλεια που απαιτείται.



Τα περισσότερα ευρωπαϊκά πρωταθλήματα και διοργανώσεις επέστρεψαν στη δράση. Για την ώρα βλέπουμε κάτι μοναδικό, όλα τα παιχνίδια παίζονται σε άδεια γήπεδα. Όσοι σχετίζονται με το ποδόσφαιρο θέλουν την επιστροφή των φιλάθλων στα γήπεδα το γρηγορότερο δυνατό, ειδικά οι υπεύθυνοι των τηλεοπτικών καναλιών που βιώνουν από πρώτο χέρι την πτώση της τηλεθέασης, αλλά και οι ομάδες που βασίζονται στα τηλεοπτικά δικαιώματα και τις πωλήσεις εισιτηρίων για να καλύψουν μισθούς παικτών και μεταγραφικά έξοδα. Ωστόσο, δεν είναι μόνο το ποδόσφαιρο που χρειάζεται απεγνωσμένα τους θεατές πίσω. Είναι εφικτό να

επιτραπούν εκδηλώσεις με μαζική παρουσία κόσμου σε αυτούς τεράστιους χώρους και ταυτόχρονα τηρούνται τα 2 μέτρα που απαιτούνται για την κοινωνική αποστασιοποίηση; Αξιοποιώντας τα analytics, είναι εφικτό να βρούμε τη βέλτιστη ταξινόμηση θέσεων που επιτρέπει στους θεατές να γυρίσουν στα γήπεδα, τηρώντας ταυτόχρονα τις αποστάσεις ασφαλείας. Για παράδειγμα, σε μια κερκίδα 7 σειρών, όπου στην κάθε σειρά αντιστοιχούν 7 καθίσματα, μπορούμε να καθίσουμε 10 άτομα, όταν υπό κανονικές συνθήκες θα χωρούσε 49 άτομα, αφήνοντας 2 κενές θέσεις μεταξύ κάθε θεατή. Οι υπεύθυνοι των χώρων εκδηλώσεων όμως θέλουν να πάνε ένα βήμα παραπέρα καθώς με τον παραπάνω τρόπο η πληρότητα των χώρων δε μπορεί να ξεπεράσει το 20%. Με την καινοτόμα λύση Social Distancing Venue & Seat Optimisation η SAS, χρησιμοποιεί προηγμένα analytics και διαδικασίες βελτιστοποίησης για να βρει την καλύτερη διάταξη ανάλογα με τις ειδικές συνθήκες που επικρατούν στο χώρο.

Η τεχνολογική εξέλιξη...

στην φυσική της ΘΕΣΗ !



KEEPERGROUP
ΟΛΟΚΛΗΡΩΜΕΝΕΣ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

KEEPERGROUP
ΟΛΟΚΛΗΡΩΜΕΝΕΣ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

DSC

From Tyco Security Products

GETTING
STRONGER
AND STRONGER

■ Πραγματοποιήθηκε η έναρξη του ευρωπαϊκού προγράμματος “Be Secure Feel Secure” στο Δήμο Πειραιά

Με μεγάλη επιτυχία πραγματοποιήθηκε, στο Δημοτικό Θέατρο Πειραιά, η **εναρκτήρια εκδήλωση του ευρωπαϊκού προγράμματος «Be Secure Feel Secure»** στο οποίο ο Δήμος Πειραιά είναι συντονιστής εταίρος και υλοποιείται μέσω του Ευρωπαϊκού

Ταμείου Περιφερειακής Ανάπτυξης και του οργανισμού UIA (Urban Innovative Actions). Στόχος του προγράμματος «Be Secure Feel Secure» είναι η δημιουργία ενός ενιαίου πλαισίου φυσικής και ψηφιακής ασφάλειας που θα οδηγήσει στην μείωση της τοπικής εγκληματικότητας, ούτως ώστε ο Πειραιάς να γίνει μια πόλη ασφαλέστερη για τους δημότες και τους επισκέπτες του και να αποτελέσει έναν ελκυστικότερο τουριστικό προορισμό.

Οι δραστηριότητες του έργου επικεντρώνονται πέρα από την πρόληψη, στην εκπαίδευση των πολιτών, ώστε να είναι σε θέση να αποφύγουν ή να αντιμετωπίσουν με τον καλύτερο δυνατό τρόπο, μια ενδεχόμενη δύσκολη κατάσταση.

Στον τομέα της ψηφιακής ασφάλειας προβλέπεται από το έργο, η δημιουργία ενός συνεργατικού πληροφοριακού συστήματος διαχείρισης ρίσκου το οποίο θα μπορεί να συλλέγει και να επεξεργάζεται πληροφορίες από την τοπική Αστυνομία, το Λιμάνι, τις ανοιχτές πηγές (πχ social media, Pireapp) και από έξυπνους αισθητήρες. Αξιοποιώντας αυτές τις πληροφορίες, το σύστημα θα ενημερώνει τους αρμόδιους συνεργαζόμενους φορείς για το αίσθημα ασφάλειας των πολιτών, για πιθανά συμβάντα ασφάλειας και για δράσεις πρόληψης και ενίσχυσης της αστικής ασφάλειας (π.χ. ενίσχυση φωτισμού σε συγκεκριμένα σημεία).

Στο φυσικό Περιβάλλον και σε συνεργασία με το εργαστήριο Αστακής Εγκληματολογίας του Παντείου Πανεπιστημίου, τα αρμόδια τμήματα του Δήμου, την Αστυνομία και τους τοπικούς συνεργαζόμενους φορείς, θα οριστεί ένα αρχικό σύνολο δράσεων ενημέρωσης και ευαισθητοποίησης των πολιτών σε θέματα αστικής ασφάλειας.



Στην ομάδα του έργου μετέχουν εκτός από την Δημοτική Αρχή του Πειραιά, η EFUS (European Forum for Urban Security), η Space Hellas, η Singular Logic, το Πάντειο Πανεπιστήμιο, το Πανεπιστήμιο Πειραιά, το Υπουργείο Προστασίας του Πολίτη, καθώς και ευρύτερα ενδιαφερόμενα μέρη, όπως η Μητρόπολη Πειραιά, το Εμπορικό Επιμελητήριο, σχολικές επιτροπές κ.λπ.

Για την Τεχνολογία και την Αστική Ασφάλεια στην εκδήλωση μίλησαν:

- οι κ. κ. Σπύρος Παπαστεργίου και Δημήτρης Καλλέργης από το Κέντρο Ερευνών Πανεπιστημίου Πειραιά με θέμα: «Μεθοδολογία και Ανάπτυξη Συνεργατικής Πλατφόρμας Διαχείρισης Αστικών Κινδύνων».
- ο κ. Σωκράτης Κωστίκογλου από την Space Hellas με θέμα: «Αύξηση της αίσθησης ασφάλειας των πολιτών και η μείωση του φόβου εγκλήματος».
- ο Δρ Κώστας Δαβαράκης από την «Singular Logic S.A.» με θέμα: «SPIRIT Tools: Ανάπτυξη τεχνολογιών πρόληψης, έρευνας και μετριάσμου στο πλαίσιο της καταπολέμησης του εγκλήματος και της τρομοκρατίας».

«Το έργο Be Secure - Feel Secure προσεγγίζει το ζήτημα της αστικής ασφάλειας, με τρόπο καινοτόμο και σύγχρονο. Στόχος του έργου μέσω της πρόληψης, του συμβουλευτικού αλλά και ενημερωτικού του χαρακτήρα, η μείωση του αισθήματος φόβου, αλλά και η μείωση των ευκαιριών που ευνοούν τη δράση του παραβάτη, σε κάθε επίπεδο. Μια πόλη ασφαλέστερη για τους δημότες και τους επισκέπτες της, ένας ελκυστικότερος τουριστικός προορισμός.» Δήλωσε η Αντιδήμαρχος Επικοινωνίας-Προβολής και Μέσων Ενημέρωσης και Αξιοποίησης Ευρωπαϊκών και Εθνικών Πόρων, κα Ανδριάννα Ζαρακέλη.



AUTOMATIC ALARM

GRANDE[®]

Προϊόντα και Υπηρεσίες Ασφαλείας

Ο ΑΓΡΥΠΝΟΣ ΦΡΟΥΡΟΣ ΣΑΣ



Μια ζωή μαζί σας!



Συστήματα Ασφαλείας - Συναγερμοί

Συστήματα Πυρανίχνευσης - Κατάσβεσης - Ανίχνευσης Αερίων

Συστήματα Ελέγχου Πρόσβασης

Συστήματα Θυροτηλεόρασης - Ενδοεπικοινωνίας

Συστήματα Παρακολούθησης - Καταγραφής Εικόνας (Κλειστού Κυκλώματος Τηλεόρασης)

Περιφερειακά - Υποστηρικτικά Συστημάτων Ασφαλείας

Τεχνική Υποστήριξη

Υπηρεσίες Κέντρου Λήψης Σημάτων - Μεταφοράς Εικόνας (VIDEO VERIFICATION)

HIKVISION

OPTEX

AUS electronics
ITALIAN SECURITY MANUFACTURER

Honeywell

FIRECLASS

cofem, s.a.
1973

Focus[®]

ALEPH

videofied

KANTECH

SECUSYS

A.A.Systems

DSC

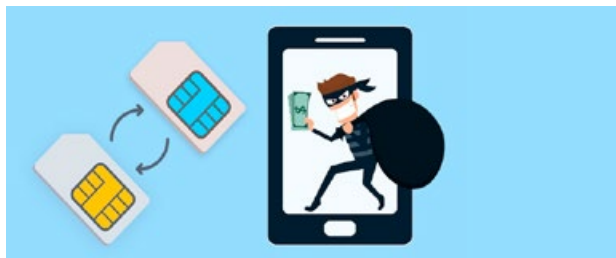
BENTEL
SECURITY

VENITEM

GRANDE SECURITY A.E.

Λεωφ. Πρωτοπαπαδάκη 83, Γαλάτσι Τ.Κ. 111 47 || Τηλ.: 210 21 39 999 - Fax: 210 29 22 148
www.grande.gr || email: grande@grande.gr

■ Απάτη **SIM swap**: τί είναι και πως να προστατευθείτε;



Γνωρίζετε ότι το κινητό σας τηλέφωνο μπορεί να παρέχει στους κυβερνοεγκληματίες τρόπο ώστε να έχουν πρόσβαση στους οικονομικούς λογαριασμούς σας. Πως? Μέσω του κινητού σας αριθμού. Η απάτη είναι γνωστή ως **SIM swap** και μπορεί να χρησιμοποιηθεί για την ανάληψη χρημάτων από τον λογαριασμό σας. Το **SIM swap** βασίζεται στον έλεγχο ταυτότητας μέσω τηλεφώνου. Σε μια επιτυχημένη απάτη ανταλλαγής SIM, οι εγκληματίες στον κυβερνοχώρο θα μπορούσαν να παραβιάσουν τον αριθμό του κινητού σας τηλεφώνου και να τον χρησιμοποιήσουν για να αποκτήσουν πρόσβαση στα ευαίσθητα προσωπικά δεδομένα και τους λογαριασμούς σας όπως μας ενημερώνει η **Bitdefender Greece**.

Πως δουλεύει; Μπορεί να προσπαθήσετε να αποκτήσετε πρόσβαση σε έναν από τους τραπεζικούς λογαριασμούς σας που χρησιμοποιεί έλεγχο ταυτότητας δύο παραγόντων. Αυτό σημαίνει ότι στην αρχή αποκτάτε πρόσβαση στον λογαριασμό σας εισάγοντας το όνομα χρήστη και τον κωδικό πρόσβασής σας. Στη συνέχεια, η τράπεζά σας στέλνει έναν κωδικό πρόσβασης στο κινητό σας για να ολοκληρώσετε τη διαδικασία σύνδεσης. Τι γίνεται όμως αν οι απατεώνες μπορούν να αλλάξουν την κάρτα SIM που είναι συνδεδεμένη στον αριθμό του κινητού σας; Αυτό θα τους έδινε τον έλεγχο αυτού του αριθμού - και αυτόματα θα λάβουν τον κωδικό πρόσβασης για τον λογαριασμό σας. **Πώς λειτουργεί η απάτη του SIM swap;** Μια απάτη SIM swap -επίσης γνωστή ως διαίρεση SIM, simjacking, sim hijacking ή port-out scamming- είναι μια απάτη που συμβαίνει όταν οι απατεώνες εκμεταλλεύονται μια αδυναμία ελέγχου ταυτότητας και επαλήθευσης δύο παραγόντων στην οποία το δεύτερο βήμα είναι ένα μήνυμα επαλήθευσης (SMS) ή κλήση στον αριθμό του κινητού σας τηλεφώνου. Οι απατεώνες καλούν τον πάροχο κινητής τηλεφωνίας σας, πλαστοπροσωπώντας σας και ισχυρίζονται ότι έχουν χάσει ή καταστρέψει την κάρτα SIM. Στη συνέχεια, ζητούν από τον αντιπρόσωπο εξυπηρέτησης πελατών να ενεργοποιήσει μια νέα κάρτα SIM

που βρίσκεται στην κατοχή του απατεώνα. Αυτό μεταφέρει τον αριθμό τηλεφώνου σας στη συσκευή του που περιέχει διαφορετική κάρτα SIM. Ή, μπορεί να ισχυριστούν ότι χρειάζονται βοήθεια για να τη μεταφέρουν σε νέο τηλέφωνο.

Πώς μπορούν όμως να απαντήσουν στις ερωτήσεις ασφαλείας σας; Εκεί γίνονται χρήσιμα τα δεδομένα που έχουν συλλέξει για εσάς μέσω phishing, κακόβουλου λογισμικού, ή των social media. Μόλις αποκτήσουν πρόσβαση και έχουν τη δυνατότητα να ελέγχουν τον αριθμό του κινητού τηλεφώνου σας, οι απατεώνες μπορούν στη συνέχεια να αποκτήσουν πρόσβαση στις τηλεφωνικές σας επικοινωνίες με τράπεζες και άλλους οργανισμούς και συγκεκριμένα, τα μηνύματα σας. Στη συνέχεια, μπορούν να λάβουν κωδικούς ή νέους κωδικούς πρόσβασης που αποστέλλονται σε αυτό το τηλέφωνο μέσω κλήσης ή κειμένου για οποιονδήποτε από τους λογαριασμούς σας. **Πώς παίρνουν τα χρήματά σας;** Ενδέχεται να δημιουργήσουν έναν δεύτερο τραπεζικό λογαριασμό στην τράπεζά σας και στο όνομά σας - όπου, επειδή είστε ήδη τραπεζικός πελάτης, ενδέχεται να υπάρχουν λιγότερο ισχυροί έλεγχοι. Οι μεταφορές μεταξύ αυτών των λογαριασμών στο όνομά σας ενδέχεται να μην προκαλούν δηλαδή συναγερμούς.

Τρόποι με τους οποίους μπορείτε να προστατευτείτε από το SIM swap

- **Διαδικτυακή συμπεριφορά:** προσοχή στα mail σας (phishing) και άλλους τρόπους με τους οποίους οι εισβολείς ενδέχεται να προσπαθήσουν να αποκτήσουν πρόσβαση στα προσωπικά σας δεδομένα για να τους βοηθήσουν να πείσουν την τράπεζά σας ή τον πάροχο κινητής τηλεφωνίας ότι είναι εσείς.
- **Ασφάλεια λογαριασμού:** ενισχύστε την ασφάλεια λογαριασμού του κινητού σας με έναν μοναδικό, ισχυρό κωδικό πρόσβασης και ισχυρές ερωτήσεις-απαντήσεις που μόνο εσείς γνωρίζετε.
- **Κωδικοί PIN:** εάν η εταιρεία κινητής τηλεφωνίας σας επιτρέπει να ορίσετε ξεχωριστό κωδικό πρόσβασης ή PIN για τις επικοινωνίες σας, εξετάστε το ενδεχόμενο να το κάνετε. Θα μπορούσε να παρέχει ένα επιπλέον επίπεδο προστασίας.
- **Εφαρμογές ελέγχου ταυτότητας:** μπορείτε να χρησιμοποιήσετε μια εφαρμογή ελέγχου ταυτότητας, όπως το Google Authenticator, η οποία σας παρέχει έλεγχο ταυτότητας δύο παραγόντων, αλλά συνδέεται με τη συσκευή σας και όχι με τον αριθμό τηλεφώνου σας.



24ωρο Κέντρο Λήψης Σημάτων



- ✓ 35.000 ενεργοί συνδρομητές
- ✓ 35 χρόνια εμπειρία & τεχνογνωσία στα συστήματα ασφαλείας
- ✓ Το μεγαλύτερο πιστοποιημένο Κέντρο Λήψης Σημάτων στην Ελλάδα

Το μοναδικό Κέντρο Λήψης Σημάτων με την
καινοτόμο υπηρεσία Ιατρικής Βοήθειας



Με την συνεργασία της  INTERAMERICAN

Μάθετε περισσότερα στο www.atlasecurity.gr



Λ. Βουλιαγμένης 85
Γλυφάδα



210 9600556
210 9646494

Ο συναγερμός σας
στα καλύτερα χέρια!

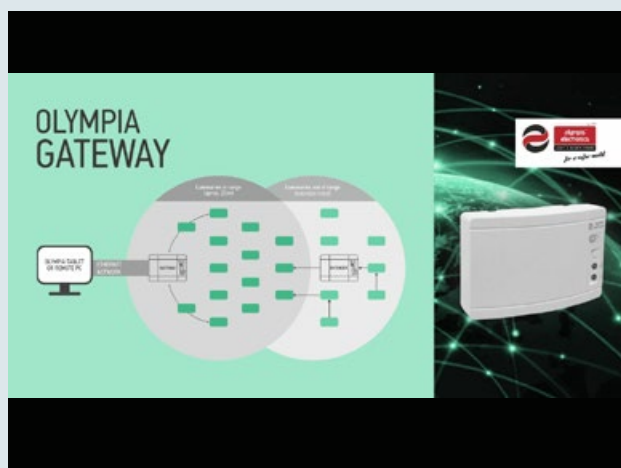
■ **Axxon Next 4** - Προηγμένη Διαχείριση **Video Wall**

Το Axxon Next έχει καταξιωθεί ως ένα από τα κορυφαία λογισμικά Video Management παγκοσμίως και ιδιαίτερα ως VMS με ειδικές λειτουργίες για Κέντρα Λήψης Εικόνων και Ελέγχου. Με το Axxon Next, οι χειριστές μπορούν να επιλέξουν-δημιουργήσουν μια συγκεκριμένη «διάταξη οθονών» που έχει δημιουργηθεί στο σύστημα και να την στείλουν στην οθόνη οποιουδήποτε άλλου υπολογιστή-client που είναι συνδεδεμένος με κάποιον server παρακολούθησης βίντεο. Αυτό προσφέρει άμεση και εύκολη μεταφορά πληροφορίας ανάμεσα σε χειριστές, επόπτες και υπεύθυνους ασφαλείας και ως εκ τούτου αποτελεί εξαιρετικά χρήσιμο εργαλείο για τον έλεγχο περιοχών, που απαιτούν σύνθετη παρακολούθηση όπως στρατιωτικές εγκαταστάσεις, γήπεδα, αεροδρόμια, λιμάνια, αποθήκες κ.λπ. Κάθε χρήστης με επαρκή δικαιώματα πρόσβασης θα μπορεί να διαχειριστεί το Video Wall και να «μεταφέρει» ένα συμβάν στην οθόνη κάποιου διαχειριστή στέλνοντας τη σχετική διάταξη οθονών σε ένα άλλο Video Wall. Να υπενθυμίσουμε ότι το Axxon Next θεωρείται ιδανικό για την ενοποίηση παλαιών και νέων καμερών κάθε κατασκευαστή, σε υφιστάμενες εγκαταστά-



σεις, αλλά και στην προσθήκη πολλών έξυπνων λειτουργιών, με προεξάρχουσα αυτή της Έξυπνης περιμετρικής φύλαξης με προηγμένα 3D Analytics με σύνθετους κανόνες. Για περισσότερες πληροφορίες επικοινωνήστε με την **Novo Technologies** (Τηλέφωνο: 2102723127 / Τρωάδος 15, Νέα Ιωνία / Web site: www.novo.gr)

■ **Έξυπνος απομακρυσμένος έλεγχος** συστημάτων ασφαλείας



Μετά από ανάγκη που προέκυψε στην αγορά, η Olympia Electronics ανέπτυξε το νέο προϊόν Olympia Gateway, προσφέροντας λύση με τεχνολογία IOT (Internet of things). Πρόκειται για μία έξυπνη συσκευή που σκοπό έχει τον απομακρυσμένο έλεγχο και την διαχείριση σε ένα

ενοποιημένο σύστημα παρακολούθησης των τοπικών συστημάτων ασφαλείας (πίνακες πυρανίχνευσης, φωτισμού ασφαλείας) μέσω θύρας Ethernet, παρέχοντας τα ακόλουθα πλεονεκτήματα:

- Εύκολη και ασφαλής πρόσβαση σε απομακρυσμένες συσκευές τύπου GR-6500, BSR-100X πίνακες
- Πρόσβαση στις σελίδες των πινάκων μέσω browser.
- Δυνατότητα εποπτείας πολλών πινάκων παράλληλα
- Δυνατότητα χρήσης τοπικά αλλά και απομακρυσμένα μέσω cloud
- Ενημέρωση μέσω gmail για συμβάντα alarm
- Ασφάλεια στην μετάδοση δεδομένων

Η OLYMPIA ELECTRONICS A.E. έχει υιοθετήσει στην παραγωγική της διαδικασία την καινοτομία και την εφαρμογή των νέων τεχνολογιών γιατί αυτοί οι δύο παράγοντες είναι καθοριστικοί για την ανάπτυξη της επιχείρησης, καθώς και για την διατήρηση του ανταγωνιστικού πλεονεκτήματος. Για περισσότερες πληροφορίες:

www.olympia-electronics.gr



vector security

Quality. No Surprises!



Greece



Cyprus



Australia



Romania

Agiou Savva 2
10447 Athens

T +30 210 49 25 473
E info@vectorsecurity.gr
W www.vectorsecurity.gr

Steliou Kazantzidi 2,
71408 Heraklion

T +30 28 10 37 0210
E creta@vectorsecurity.gr
W www.vectorsecurity.gr

Georgiou Neophytou 24
(Bridge House)

T +357 2503 0507
E info@vectorsecurity.com.cy
W www.vectorsecurity.com.cy

Θερμική απεικόνιση ανίχνευσης θερμοκρασίας ...και άλλα μέτρα προστασίας!

Τι πρέπει να προσέχουμε



Η ιστορία με τα μέτρα αντιμετώπισης της διασποράς του covid-19 συνεχίζεται και ένα από τα βασικά εργαλεία για αυτό το σκοπό, προέρχονται από τη βιομηχανία των ηλεκτρονικών συστημάτων ασφάλειας και είναι τα συστήματα θερμομέτρησης με τη χρήση θερμικών καμερών. Είναι λοιπόν η κατάλληλη στιγμή τώρα που ωρίμασαν κάπως οι συνθήκες και “έπεσε η σκόνη” των πρώτων ημερών να δούμε τι πρέπει λοιπόν να λάβουμε υπόψη κατά τη χρήση αυτών των συστημάτων και όχι μόνο.

Η υγειονομική κρίση σε παγκόσμιο επίπεδο που έχει επιφέρει η πανδημία του νέου κορωνοϊού, έχει οδηγήσει μεταξύ άλλων στην αναζήτηση τεχνολογικών λύσεων που θα βοηθήσουν στην προστασία της δημόσιας υγείας. Σε αυτές τις τεχνολογικές λύσεις για την αντιμετώπιση αυτής της πανδημίας, θα λέγαμε ότι έχουν πρωταγωνιστικό ρόλο τα συστήματα ελέγχου θερμοκρασίας μέσω καμερών θερμικής απεικόνισης. Τα ολοκληρωμένα αυτά συστήματα έχουν σχεδιαστεί και κατα-

σκευαστεί από μεγάλους αλλά και μικρότερους κατασκευαστές από τη βιομηχανία της ασφάλειας και απευθύνονται σε μια πληθώρα εγκαταστάσεων, από νοσοκομεία, σταθμούς μεταφοράς (αεροδρόμια, τρένα κ.λπ.) και δημόσια κτίρια, μέχρι ξενοδοχεία, εμπορικά κέντρα, μονάδες παραγωγής και γραφεία επιχειρήσεων.

Είναι αλήθεια πως το προηγούμενο διάστημα κατακλυστήκαμε από προωθητικές ενέργειες συστημάτων θερμομέτρησης

κάτι που ήταν αναμενόμενο, αφού η ζήτηση που προέκυψε ήταν μεγάλη από πολλές επιχειρήσεις και οργανισμούς. Ας δούμε λοιπόν, τι θα πρέπει να λάβουν υπόψη τους όσες οι εταιρίες επιθυμούν να αποκτήσουν και να χρησιμοποιούν τέτοιες συσκευές για τον έλεγχο της θερμοκρασίας σώματος μέσω θερμικές απεικόνισης αλλά και τι άλλο χρειάζεται συνδυαστικά για να μειώσουν τις πιθανότητες διάδοσης του ιού.

Βασικές παραδοχές

Καταρχήν οι τελικοί πελάτες - επιχειρήσεις που έχουν την ευθύνη διαχείρισης των κτιριακών εγκαταστάσεων, θα πρέπει να γνωρίζουν ότι υπάρχουν πολλοί και διαφορετικοί τύποι θερμικών καμερών για πολλές εφαρμογές ασφάλειας, στρατιωτικού σκοπού, βιομηχανίας κ.ά.

Στην προκειμένη περίπτωση μιλάμε για κάμερες ενσωματωμένες σε ολοκληρωμένα συστήματα που έχουν σχεδιαστεί για την ανίχνευση θερμοκρασίας σώματος και τη δυνατότητα παραγωγής ειδοποιήσεων και συναγερμών. Και σε αυτή τη κατηγορία, υπάρχουν όμως διαφοροποιήσεις στους τύπους συστημάτων, με διαφορετικά χαρακτηριστικά, για διαφορετικές εφαρμογές αλλά και απαιτήσεις. Στην αγορά θα δούμε αποκλίσεις στις τιμές, που σχετίζονται με τις δυνατότητες που υποστηρίζουν αλλά και το brand κατασκευής. Σε γενικές γραμμές, οι παράγοντες διαφοροποίησης των δυνατοτήτων αυτών των συστημάτων, περιλαμβάνουν την ακρίβεια στην μέτρηση θερμοκρασίας, την ταχύτητα ανίχνευσης αλλά και άλλα πρόσθετα χαρακτηριστικά, όπως η ανίχνευση πλήθους. Θα πρέπει εδώ να σημειωθεί, ότι οι θερμικές κάμερες έχουν σχεδιαστεί για να προσφέρουν μια ένδειξη της θερμοκρασίας του σώματος και σίγουρα δεν είναι μια μέθοδος ιατρικής διάγνωσης πυρετού και φυσικά διάγνωσης ασθένειας.

Για να γίνει ο μεμονωμένα σε ένα άνθρωπο ο έλεγχος της θερμοκρασίας του σώματος του σε ένα σημείο εισόδου και ελέγχου πρόσβασης σε μια εγκατάσταση, είναι πολύ πιθανόν να χρειαστεί μόνο ένα προϊόν που μπορεί να ανιχνεύσει τη θερμοκρασία ενός ατόμου που στέκεται σταθερά μπροστά

από το σημείο ελέγχου.

Ωστόσο, για την παρακολούθηση της θερμοκρασίας πολλών ανθρώπων στην είσοδο ή στο λόμπι ενός κτιρίου, οι διαχειριστές θα πρέπει να τοποθετήσουν ένα σύστημα κάμερας με δυνατότητα ανίχνευσης πλήθους και υψηλή ταχύτητα ανίχνευσης σε ένα κινούμενο πλήθος. Στην περίπτωση αυτή, είναι απαραίτητο να υπάρχει λειτουργία συναγερμού -όταν ξεπεραστεί κάποιο προκαθορισμένο όριο- για να ειδοποιείται το προσωπικό επιτόπου και να λαμβάνει τα αντίστοιχα μέτρα όταν ανιχνεύεται υψηλή θερμοκρασία.

Η ακρίβεια της μέτρησης που παρέχουν τα συστήματα θα πρέπει να είναι κάτω του +/- 0,5 βαθμού C προκειμένου να είναι αποτελεσματική και σίγουρα η προσθήκη επιπλέον εργαλείων όπως τεχνητή νοημοσύνη βοηθούν στην ελαχιστοποίηση των ψευδών συναγερμών.

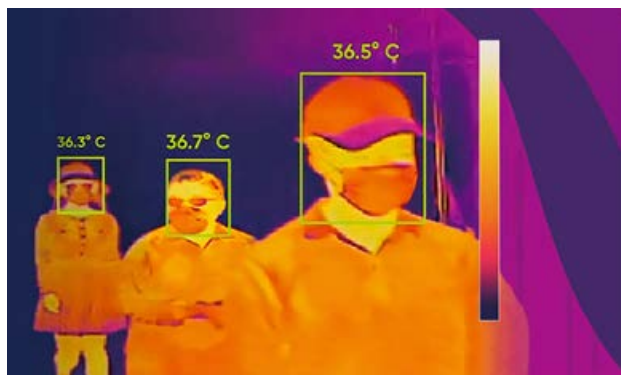
Υπάρχουν επίσης νέα προϊόντα που έρχονται στην αγορά και συνδυάζουν την ανίχνευση της θερμοκρασίας του σώματος και την αναγνώριση προσώπου. Δηλαδή, εκτός από τον έλεγχο της θερμοκρασίας του σώματος, το σύστημα μπορεί να ελέγξει την ταυτότητα ενός ατόμου εφόσον είναι καταγεγραμμένος σε μια βάση δεδομένων, καθώς και το αν φοράει μάσκα στο πρόσωπο. Η διεύθυνση αυτών των συνδυαστικών συστημάτων, είναι πολύ πιθανόν να αυξηθεί σε πολλές χώρες, από τη στιγμή που θα πρέπει μάθουμε να ζούμε με τον covid-19 για άγνωστο ακόμα χρονικό διάστημα.

Σημεία που χρήζουν προσοχής

Πριν την τοποθέτηση ενός συστήματος μέτρησης της θερμοκρασίας με τη χρήση θερμικών καμερών, είναι σημαντικό να αξιολογήσουμε σωστά το περιβάλλον όπου θα γίνει η εγκατάσταση του συστήματος και αυτό επειδή η θερμική κάμερα είναι πιθανόν να επηρεαστεί από τις συνθήκες περιβάλλοντος. Για παράδειγμα θα πρέπει να εξετάσουμε την περίπτωση όπου η θερμική κάμερα βλέπει στην είσοδο κτηρίου, όπου υπάρχει άμεσο φως του ήλιου από το εξωτερικό περιβάλλον. Σε αυτή την περίπτωση, η ευαισθησία της ανίχνευσης θερμοκρασίας είναι πιθανόν να έχει απόκλιση από +/- 0,3 βαθμό C σε +/- 0,5 βαθμό C.

Ένα άλλο σημαντικό ζήτημα που θα πρέπει να ληφθεί υπόψη -και δεν γίνεται συνήθως- είναι να εξεταστούν οι τοπικοί κανόνες και νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων. Το τοπίο σε πολλές χώρες είναι διαφορετικό σε ότι αφορά το συγκεκριμένο ζήτημα και επομένως η μέτρηση της θερμοκρασίας των εργαζομένων και επισκεπτών και η χρήση της τεχνολογίας αναγνώρισης προσώπου μπορεί να αγγίζει τα όρια της νομιμότητας.

Σε κάθε περίπτωση θα πρέπει οι επιχειρήσεις και οργανισμοί





να συζητούν με το προσωπικό τους να ενημερώνουν τους επισκέπτες, να ακούνε τις ανησυχίες τους και γενικότερα να επικοινωνούν τους λόγους για τους οποίους έχει αναπτυχθεί μια τέτοια λύση και τον τρόπο με τον οποίο εφαρμόζεται. Ακόμα και εάν μια λύση εγκαθίσταται με καλές προθέσεις, αλλά χωρίς ενημέρωση και διαφάνεια, τότε είναι πολύ πιθανόν οι άνθρωποι να μην ανταποκριθούν θετικά.

Επίσης οι οργανισμοί που θέλουν να επενδύσουν σε μια τέτοια λύση θα πρέπει να είναι πολύ προσεκτικοί στην επιλογή που θα κάνουν. Καλό θα ήταν να μην έχουν ως μοναδικό κριτήριο το κόστος αλλά να δούνε τη συνολική εικόνα. Δεν είναι κρυφό ότι πολλές εταιρίες με το που διέγνωσαν τη συγκεκριμένη ανάγκη έσπευσαν να αναπτύξουν προϊόντα και συστήματα θερμομέτρησης που δεν προσφέρουν την απαιτούμενη αξιοπιστία και απόδοση.

Ολιστική προσέγγιση ...για την επιστροφή στην “κανονικότητα” ή στη μετάβαση μιας νέας πραγματικότητας

Πολλοί μιλάνε για επιστροφή στην κανονικότητα στους χώρους εργασίας και άλλοι για μια νέα πραγματικότητα. Σε κάθε περίπτωση το μόνο σίγουρο είναι ότι για όσο διαρκεί αυτή η ιστορία, κάποια πράγματα δεν είναι ίδια. Το τοπίο είναι πολύ δυναμικό και σε αυτό το πλαίσιο η προσπάθεια λήψης μέτρων για την αντιμετώπιση της εξάπλωσης του ιού, δεν θα πρέπει να επικεντρώνετε μόνο σε μια λύση αλλά σε μια ολιστική προσέγγιση. Η ανίχνευση της θερμοκρασίας του σώματος θα πρέπει να είναι ένα μέρος του πρωτοκόλλου “μετάβασης στη νέα πραγματικότητα”.

Η συμβίωση με τον COVID-19, καθιστά τους εσωτερικούς χώρους και κυρίως τα κτίρια με μαζική παρουσία ανθρώπων, ως τα πλέον κρίσιμα σημεία για την ανάπτυξη μέτρων καταπολέμησης της εξάπλωσης του ιού. Σε αυτά τα πλαίσια λοιπόν θα πρέπει να εξετάσουμε τη χρήση τεχνολογιών για τη δημιουργία των συνθηκών που βοηθούν στην προστασία της υγείας και την ασφάλεια εργαζομένων και επισκεπτών, που

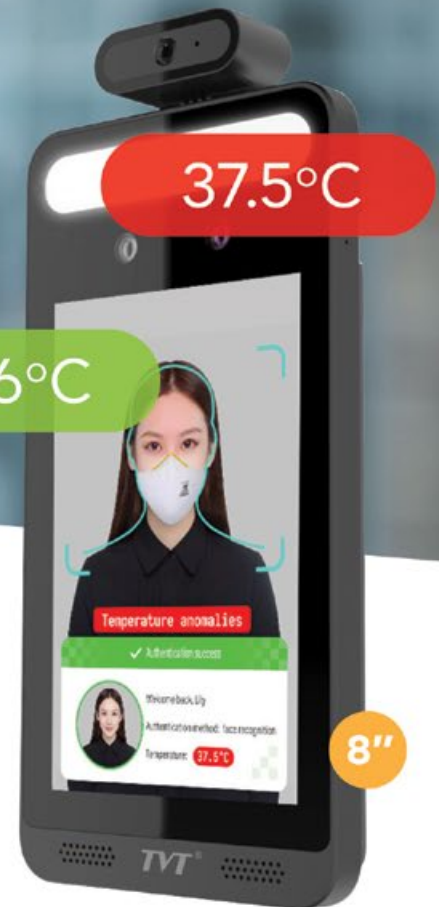
άλλωστε πάντα αποτελεί βασική μέριμνα κάθε οργανισμού. Επομένως, οι επιχειρήσεις θα πρέπει να εξετάσουν το ενδεχόμενο εφαρμογής λύσεων με βάση δυο πτυχές: πρώτον, μέτρα για τη μείωση ή τη διαχείριση των κινδύνων και τη δημιουργία ενός εσωτερικού περιβάλλοντος που θα υποστηρίζει την υγεία των εργαζομένων. Δεύτερον, την ανάγκη δημιουργίας του αισθήματος ασφάλειας στο εργασιακό του περιβάλλον για όλους.

Στο στάδιο της διαχείρισης και των προσπαθειών περιορισμού των κινδύνων, πολλές επιχειρήσεις έχουν εφαρμόσει νέες πολιτικές για το εργατικό δυναμικό τους, όπως για παράδειγμα είναι: ο διαχωρισμός των εργαζομένων σε ομάδες Α και Β, η χρήση μεθόδων περιορισμού των κινήσεων και του αυστηρότερου ελέγχου πρόσβασης και εσωτερικά σε ένα κτίριο για τους υπαλλήλους αλλά και τους επισκέπτες, αλλά και ευρύτερα η αναθεώρηση των πολιτικών για τη χωροθέτηση των θέσεων εργασίας και συνάθροισης σε κοινούς χώρους, όπως οι αίθουσες συσκέψεων, κυλικεία, τραπεζαρίες κ.λπ.

Οι πολιτικές αυτές αντικατοπτρίζονται στις προσαρμογές των υφιστάμενων συστημάτων ελέγχου πρόσβασης, διαχείρισης επισκεπτών και χρήσης των εγκαταστάσεων, καθώς και στην υλοποίηση νέων εφαρμογών. Σε αυτές μπορεί να περιλαμβάνονται η χρήση του κινητού τηλεφώνου ως διαπιστευτήριο ελέγχου πρόσβασης αντί για κάποια ταυτότητα ή διακριτικό σήμα, βοηθώντας στην υλοποίηση ανέπαφων εφαρμογών. Από την πλευρά της Διαχείρισης Εγκαταστάσεων, οι επιχειρήσεις θα πρέπει να μειώσουν τα σημεία επαφής μέσα στα κτίρια και να εφαρμόσουν έξυπνα συστήματα για να διασφαλίσουν ότι οι κοινόχρηστες εγκαταστάσεις και οι αίθουσες συσκέψεων καθαρίζονται μετά από κάθε χρήση.

Όπως είπαμε η αίσθηση της ασφάλειας που πρέπει να νιώσουν όσοι βρίσκονται σε ένα κτίριο -είτε είναι εργαζόμενοι σε αυτό είτε επισκέπτες- έχει μεγάλη σημασία σήμερα. Θα πρέπει λοιπόν όλοι αυτοί να βλέπουν τα μέτρα προστασίας και υγιεινής να «ξετυλίζονται» μπροστά τους. Να είναι δηλαδή τόσο εμφαντικές όλες οι διαδικασίες τήρησης των μέτρων υγιεινής, έτσι ώστε να δημιουργείται η επιθυμητή αίσθηση ασφάλειας. Σε αυτό μπορούν να βοηθήσουν μεταξύ άλλων και ψηφιακές σημάνσεις που θα ενημερώνουν τον κόσμο σε πραγματικό χρόνο, παρέχοντας πληροφορίες αλλά και συμβουλές.

Όπως αναλύσαμε σε άρθρο του προηγούμενου τεύχους ο ρόλος των Υπευθύνων Ασφάλειας επαναπροσδιορίζεται και προσαρμόζεται σε ένα ευρύτερο πλαίσιο που περιλαμβάνει πλέον και τη διαχείριση όλων των παραπάνω λύσεων και πολιτικών για την αντιμετώπιση της υγειονομικής κρίσης.



TD-E2128-T

Τερματικό ελέγχου πρόσβασης με αναγνώριση προσώπου, ανέπαφο έλεγχο θερμοκρασίας και έλεγχο μάσκας

Το τερματικό ελέγχου πρόσβασης **TD-E2128TM** ενσωματώνει την αιχμή της τεχνολογίας, προσφέροντας μια ολοκληρωμένη λύση στον έλεγχο πρόσβασης. Διαθέτει σύστημα αναγνώρισης προσώπου με ακρίβεια 99.7%, δυνατότητα ανέπαφης θερμομέτρησης από απόσταση, ενώ μπορεί να ανιχνεύσει αν ο εισερχόμενος φοράει μάσκα. Αποτελεί την πλέον ποιοτική λύση, για χώρους όπως νοσοκομεία, εμπορικά κέντρα, σχολεία, ξενοδοχεία και συγκροτήματα γραφείων, που έχουν μεγάλη προσέλευση επισκεπτών. Εγκαθίσταται εύκολα είτε σε τοίχους είτε σε διαδρόμους, από όπου διέρχονται οι επισκέπτες και ειδοποιεί ηχητικά σε περίπτωση που κάποιο άτομο δεν φοράει μάσκα ή έχει υψηλή θερμοκρασία σώματος.

Έξυπνα και γρήγορα, περισσότερο από ποτέ!

Δυνατότητα
στήριξης
στον τοίχο
ή σε στυλό



Ανέπαφη
θερμομέτρηση



Ακριβής αναγνώριση
προσώπου με τη μάσκα



Πολλαπλές επιλογές
ελέγχου πρόσβασης



Ηχητικός
συναγερμός



Η εξέλιξη της Europol στην καταπολέμηση του διεθνούς οργανωμένου εγκλήματος και της τρομοκρατίας*



Ενώ η Interpol κυριαρχούσε ανέκαθεν στη διεθνή αστυνομική συνεργασία, στις αρχές της δεκαετίας του 1990 αναδύεται η Europol διεκδικώντας ένα σημαντικό μέρος της συνεργασίας για την εφαρμογή του νόμου σε ευρωπαϊκό επίπεδο.

Έκτοτε, η Europol εξελίχθηκε σημαντικά τόσο στρατηγικά όσο και επιχειρησιακά, μέσα όμως σε ένα περίπλοκο και σύνθετο πολιτικό και νομικό πλαίσιο της ευρωπαϊκής αστυνομικής συνεργασίας.

Στην παρούσα μελέτη επιχειρείται μια εις βάθος ανάλυση της εξέλιξης της Europol εν μέσω σημαντικών πολιτικών αντιξοοτήτων και περιορισμών, που συνδέονται άρρηκτα με την έννοια της εθνικής κυριαρχίας. Στα συμπεράσματα της μελέτης περιλαμβάνονται συγκεκριμένες διαπιστώσεις και προβληματισμοί, σχετικά με την τρέχουσα κατάσταση της Europol και τις μελλοντικές δυνατότητές της στην καταπολέμηση του διεθνούς οργανωμένου εγκλήματος και της τρομοκρατίας.

Εισαγωγή

Ιστορικά, η συνεργασία της διεθνούς κοινότητας για την καταπολέμηση του εγκλήματος βασίστηκε στη σύναψη διμερών και πολυμερών συμφωνιών συνεργασίας, οι οποίες εξελίχθηκαν σε στρατηγικά και επιχειρησιακά δίκτυα συνεργασίας (Das & Kratcoki, 2001: 4-7). Η διεθνής αστυνομική συνεργασία, ωστόσο, ήταν πάντοτε ένα περίπλοκο εγχείρημα λόγω των διαφορετικών πολιτικών και των διαφορών στα εθνικά ποινικά και δικονομικά συστήματα (Deflem, 2002: 45). Στην Ευρωπαϊκή Ένωση (ΕΕ), τα πρώτα βήματα για την ενίσχυση της αστυνομικής συνεργασίας επικεντρώθηκαν στην ίδρυση της Ευρωπόλ. Από την ίδρυση της, στις αρχές της δεκαετίας του 1990, η Ευρωπόλ εξελίχθηκε στην πορεία του χρόνου ως ένας εξέχων ευρωπαϊκός οργανισμός στην καταπολέμηση του οργανωμένου εγκλήματος και της τρο-

* Η παρούσα μελέτη βασίζεται στην έρευνα του συγγραφέως για τη Europol:

Stergioulis, E. (2020). Past, present and future trends of Europol's evolution in the European law enforcement cooperation. European Law Enforcement Research Bulletin, [19], tbc. <https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/420>

**Ο κ. Ευάγγελος Στεργιούλης είναι Διδάκτωρ Κοινωνιολογίας του Παντείου Πανεπιστημίου και ε. α. Υποστράτηγος της Ελληνικής Αστυνομίας. Υπηρέτησε στην έδρα της Ευρωπαϊκής Αστυνομικής Υπηρεσίας-Europol, στη Χάγη, ως υπεύθυνος εξωτερικών και δημοσίων σχέσεων και διετέλεσε προϊστάμενος των Εθνικών Υπηρεσιών Interpol και Europol της Ελλάδας. Έχει διδάξει στις Ακαδημίες της Ελληνικής και Κυπριακής Αστυνομίας, καθώς και στο Ανοικτό Πανεπιστήμιο Κύπρου. Είναι μέλος της Ελληνικής Εταιρείας Εγκληματολογίας, του Ελληνικού Οργανισμού Πολιτικών Επιστημόνων και ερευνητής στο Ελληνικό Ινστιτούτο για τα Ηνωμένα Έθνη.



μοκρατίας και μάλιστα εν μέσω διαφορετικών ευρωπαϊκών νομικών και πολιτικών συστημάτων επιβολής του νόμου.

Ιστορικό και Πολιτικό Πλαίσιο

Η ίδρυση της Ευρωπόλ ήταν αντικείμενο συζητήσεων από τα μέσα της δεκαετίας του 1970 στην Ομάδα Εργασίας Trevi, όπου τα τότε 12 κράτη μέλη της ΕΕ συζητούσαν ένα ευρύ φάσμα θεμάτων επιβολής του νόμου σε διακυβερνητικό επίπεδο (Woodward, 1993, Bunyan, 1993). Οι κοινωνικοπολιτικές εξελίξεις σε ευρωπαϊκό επίπεδο εκείνη την περίοδο, επηρέασαν την πρόοδο των διαβουλεύσεων για την ίδρυση της Ευρωπόλ. Συγκεκριμένα, η κατάρρευση της Σοβιετικής Ένωσης και των πρώην ανατολικών καθεστώτων σε συνδυασμό με την ανησυχία που υπήρχε για παράνομο εμπόριο πυρηνικών υλικών, η αύξηση των ροών παράνομης μεταναστευσης από χώρες του ανατολικού μπλοκ προς χώρες της ΕΕ, η απειλή από την ταχεία διεθνοποίηση του εμπορίου ναρκωτικών για την οποία οι ιταλικές αρχές ανέφεραν αναδιοργάνωση και ανάπτυξη των δραστηριοτήτων της μαφίας στην Ευρώπη, ήταν μερικοί από τους κύριους λόγους που ώθησαν την συζήτηση για την ίδρυση της Ευρωπόλ (Στεργιούλης, 2003: 23-27).

Επιπλέον, η πρόταση για την ίδρυση της Ευρωπόλ υποβλήθηκε από τον Γερμανό καγκελάριο Helmut Kohl στη σύνοδο του Ευρωπαϊκού Συμβουλίου στις 28/29 Ιουνίου 1991, στο

Λουξεμβούργο, μαζί με μια Βρετανική πρόταση για τη δημιουργία μιας ευρωπαϊκής μονάδας πληροφοριών για τα ναρκωτικά (Woodward, 1993). Οι προτάσεις αυτές εγκρίθηκαν στην επόμενη Σύνοδο Κορυφής του Μάαστριχτ, στις 09/10 Δεκεμβρίου 1991, και τελικά ενσωματώθηκαν στις διατάξεις της Συνθήκης του Μάαστριχτ, άρθρο Κ.1.9. Στις 2 Ιουνίου 1993, στην Κοπεγχάγη, οι υπουργοί Δικαιοσύνης και Εσωτερικών Υποθέσεων αποφάσισαν τη σύσταση της Ευρωπαϊκής Μονάδας Ναρκωτικών (European Drugs unit-EDU) που αποτέλεσε τον πρόδρομο της ίδρυσης της Ευρωπόλ (Rauchs & Koenig, 2001: 43). Οι αρμοδιότητες της EDU, με έδρα τη Χάγη, περιορίστηκαν σε εγκλήματα που σχετίζονταν με τη διακίνηση ναρκωτικών και τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες σχετικές με το εμπόριο ναρκωτικών (Ministerial Agreement, 1993).

Παράλληλα, τα κράτη μέλη συνέχισαν τις προσπάθειές τους για την κατάρτιση της Σύμβασης Ευρωπόλ, η οποία θα επέτρεπε στην Ευρωπόλ να αναλάβει πλήρως τις δραστηριότητές της. Ωστόσο, η Σύμβαση Ευρωπόλ έπρεπε να επικυρωθεί από όλα τα κοινοβούλια των κρατών μελών, μια μακρά διαδικασία που διήρκεσε περισσότερα από πέντε χρόνια λόγω του σκεπτικισμού και της απροθυμίας των κρατών μελών να παραχωρήσουν μέρος της εθνικής τους κυριαρχίας στην Ευρωπόλ για θέματα της εσωτερικής τους ασφάλειας. Τελικά, η Σύμβαση Ευρωπόλ επικυρώθηκε από όλα τα κράτη μέλη και τέθηκε σε ισχύ την 1η Οκτωβρίου 1998 (OJEU, 1998).

Η ίδρυση της EDU ήταν η πρώτη προσπάθεια στην ιστορία της Ευρώπης να δημιουργήσει μια κοινή ευρωπαϊκή δομή για επιχειρησιακή συνεργασία στον τομέα της επιβολής του νόμου. Ωστόσο, αυτή η πρώτη προσπάθεια δεν έτυχε της δέουσας προσοχής. Η αρχική φάση της Ευρωπόλ χρειαζόταν μια αποτελεσματική στρατηγική, καθώς και μια ισχυρή πολιτική υποστήριξη που δεν υπήρχε τότε, ενώ τα κράτη μέλη ήταν επιφυλακτικά και απρόθυμα να παράσχουν στην Ευρωπόλ ένα ευρύ πλαίσιο αρμοδιοτήτων για την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας. Αναφορικά, τέλος, με την ιδέα της ίδρυσης της Ευρωπόλ ως ένα ευρωπαϊκό FBI (Occhipinti, 2003, Bruggeman, 2007, De Moore, Vermeulen, 2010a: 63-66), το θεσμικό πλαίσιο της ΕΕ δεν είχε ποτέ προβλέψει μια ευρωπαϊκή ομοσπονδιακή δομή επιβολής του νόμου. Στην πραγματικότητα, η ίδρυση της Ευρωπόλ δεν έγινε ποτέ αντιληπτή στο πλαίσιο ενός ευρωπαϊκού FBI και κανένα από τα κράτη μέλη, το Συμβούλιο της ΕΕ ή η Ευρωπαϊκή Επιτροπή, δεν είχαν υποβάλει μία τέτοια πρόταση. Έτσι, ο ρόλος της Ευρωπόλ στην ευρωπαϊκή συνεργασία επιβολής του νόμου, συμπεριλαμβανομένης

και της συμμετοχής της στις Κοινές Ομάδες Ερευνών (OJEU, 2002), προβλέπονταν πάντα με υποστηρικτικούς όρους, όπως η ανταλλαγή και ανάλυση πληροφοριών. Σε αυτό το πλαίσιο, η αρχή της εθνικής κυριαρχίας επί θεμάτων εσωτερικής ασφάλειας επισκίαζε συνεχώς τον τομέα της Δικαιοσύνης και Εσωτερικών Υποθέσεων της ΕΕ, περιορίζοντας τις επιχειρησιακές δραστηριότητες της Ευρωπόλ.

Νομική Βάση

Η Σύμβαση της Ευρωπόλ σηματοδότησε την έναρξη μιας μακροπρόθεσμης διαδικασίας για τη λεγόμενη κοινοτικοποίηση της συνεργασίας επιβολής του νόμου στην Ευρωπαϊκή Ένωση (Fijnaut, 1993). Ωστόσο, η Σύμβαση Ευρωπόλ αποδείχθηκε συχνά ένα άκαμπτο νομικό εργαλείο για την αντιμετώπιση των νέων προκλήσεων στην καταπολέμηση του διεθνούς εγκλήματος και της τρομοκρατίας. Για κάθε τροποποίηση των διατάξεών της, ένα πρωτόκολλο έπρεπε να εκπονηθεί και να επικυρωθεί από όλα τα κράτη μέλη, σύμφωνα με τις εθνικές τους κοινοβουλευτικές διαδικασίες, δημιουργώντας έτσι μεγάλες καθυστερήσεις και τεράστιες δυσκολίες στην έγκαιρη προσαρμογή των καθηκόντων της Ευρωπόλ για την αντιμετώπιση των εγκληματικών και τρομοκρατικών απειλών (European Commission, 2008). Αυτή η περίπλοκη πολιτική διαδικασία κατέδειξε μια σοβαρή έλλειψη σχεδιασμού και ανάπτυξης, καθώς επίσης και έλλειψη εμπιστοσύνης των κρατών μελών προς την Ευρωπόλ (Benyon, 1996, Rozée, et al. 2013). Η Ευρωπόλ λειτούργησε σε διακυβερνητικό πλαίσιο στον αποκαλούμενο κοινό χώρο ελευθερίας, ασφάλειας και δι-

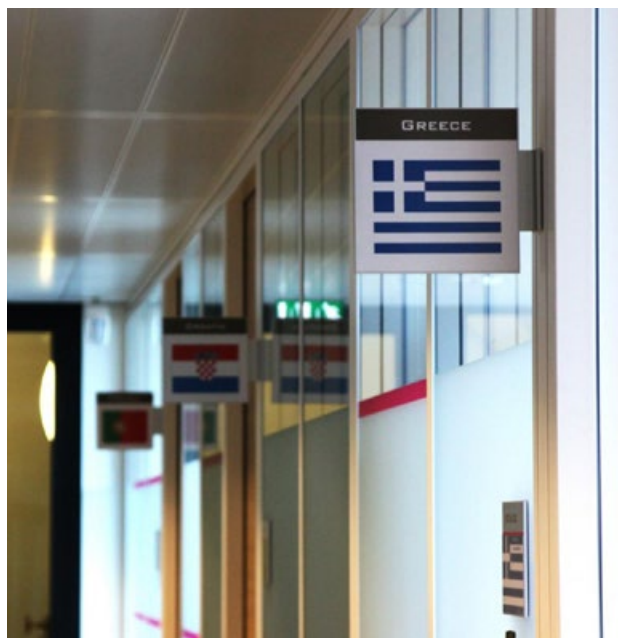
καιοσύνης (Fijnaut, 1999) μέχρι το 2009, όταν η Σύμβαση Ευρωπόλ αντικαταστάθηκε με Απόφαση του Συμβουλίου (OJEU, 2009) που τέθηκε σε ισχύ την 1η Ιανουαρίου 2010. Αυτή η σημαντική νομική τροποποίηση διέυρυνε την εντολή της Ευρωπόλ, έτσι ώστε να καλύπτει κάθε μορφή σοβαρού εγκλήματος, απελευθερώνοντας έτσι τις δυνατότητες της στην καταπολέμηση του οργανωμένου εγκλήματος χωρίς περιορισμούς. Πράγματι, η απόφαση του Συμβουλίου ήταν ένα σημαντικό βήμα προόδου στη συνεργασία των κρατών μελών της ΕΕ για την επιβολή του νόμου, καθώς η Ευρωπόλ κατέστη οργανισμός της ΕΕ, αποκτώντας ένα νέο νομικό καθεστώς μετά από λειτουργία ως διακυβερνητικός οργανισμός για περισσότερο από μια δεκαετία.

Τέλος, το 2013, η Ευρωπαϊκή Επιτροπή ανέλαβε μια νέα πρωτοβουλία για να αντικαταστήσει την προαναφερθείσα απόφαση του Συμβουλίου του 2009 με έναν Κανονισμό που τέθηκε σε ισχύ την 1η Μαΐου 2017 (OJEU, 2016). Αυτή η νέα και τρέχουσα νομική βάση επιτρέπει στην Ευρωπόλ να αντιμετωπίζει τις απειλές για την ασφάλεια της ΕΕ δημιουργώντας εξειδικευμένες εσωτερικές δομές, όπως το Ευρωπαϊκό Κέντρο Αντιτρομοκρατίας (Moor & Vermeulen, 2010β). Συγχρόνως, ενίσχυσε το καθεστώς προστασίας δεδομένων, καθώς η Ευρωπόλ είναι πλέον υπόλογη στην Αρχή Προστασίας Δεδομένων της ΕΕ, επιλύοντας έτσι ένα κρίσιμο και ευαίσθητο θέμα για την επεξεργασία προσωπικών δεδομένων που εκκρεμούσε από την ίδρυσή της (Boehm, 2012: 292, OJEC, 2001). Ωστόσο, το ερώτημα της προστιθέμενης αξίας της νέας νομικής βάσης στο επιχειρησιακό έργο της Ευρωπόλ, παραμένει ακόμη αναπάντητο (Busuioc & Groenleer, 2013).

Κύριες Αρμοδιότητες

Ανταλλαγή Πληροφοριών

Ελλείψει εκτελεστικών αρμοδιοτήτων, η Ευρωπόλ εξελίχθηκε εστιάζοντας στην ανάπτυξη υποστηρικτικών υπηρεσιών προς τις αρχές επιβολής του νόμου των κρατών μελών (Anderson, 1989: 13). Από την αρχή της λειτουργίας της, η Ευρωπόλ είχε επενδύσει στον τομέα της ανταλλαγής πληροφοριών, παρέχοντας σε κάθε κράτος μέλος ένα γραφείο συνδέσμου στην έδρα της. Εκείνη την περίοδο, η έννοια του δικτύου αξιωματικών συνδέσμων στα κεντρικά γραφεία της Ευρωπόλ θεωρούνταν ως μία καινοτόμος ιδέα για την ενίσχυση της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και της Ευρωπόλ, μέσω των άμεσων διαπροσωπικών επαφών. Ωστόσο, οι αποσπασμένοι αξιωματικοί σύνδεσμοι στην Ευρωπόλ λειτουργούσαν και συνεχίζουν να λειτουργούν σύμφωνα με το εθνικό τους νομικό πλαίσιο, οι πληροφορίες που ανταλλάσσονται υπόκεινται στον έλεγχο των





24 ωρο ΚΕΝΤΡΟ
ΛΗΨΗΣ
ΣΗΜΑΤΩΝ & ΕΙΚΟΝΑΣ

η ασφαλής επιλογή

- ✓ Νέες εφαρμογές διαχείρισης σημάτων για τελικούς χρήστες.
- ✓ Νέες εφαρμογές διαχείρισης πελατών για τους εγκαταστάτες.
- ✓ Ενημέρωση με Push Notification.
- ✓ APS (Panic) μέσω smartphone.

Η εταιρεία μας δεν αναλαμβάνει εγκαταστάσεις

αντίστοιχων εθνικών αρχών και η Ευρωπόλ δεν έχει καμία αρμοδιότητα για το έργο και τα καθήκοντα των αξιωματικών συνδέσμων, οι οποίοι, ως εθνικοί εκπρόσωποι, λαμβάνουν εντολές μόνο από τις εθνικές τους αρχές. Με την πάροδο του χρόνου, το δίκτυο αξιωματικών συνδέσμων της Ευρωπόλ επεκτάθηκε με τη συμμετοχή επίσης αξιωματικών συνδέσμων από τρίτα κράτη, με τα οποία η Ευρωπόλ έχει υπογράψει διμερείς συμφωνίες συνεργασίας (Eurropol, 2016a: 7).

Η συνεχώς διευρυνόμενη δομή των αξιωματικών συνδέσμων συνδέεται άμεσα με τις εθνικές πολιτικές των κρατών μελών, διασφαλίζοντας και προωθώντας την εκπροσώπηση διαφορετικών υπηρεσιών επιβολής του νόμου (αστυνομία, χωροφυλακή, τελωνεία, λιμενική αστυνομία κλπ.) στην έδρα της Ευρωπόλ. Ωστόσο, το δίκτυο σχετίζεται άμεσα και με τον προϋπολογισμό της Ευρωπόλ που καλύπτει ένα ευρύ φάσμα λειτουργικών δαπανών, εκτός από τις αμοιβές των αξιωματικών συνδέσμων που καλύπτονται από τις εθνικές τους αρχές. Εναλλακτικά, το δίκτυο αξιωματικών συνδέσμων της Ευρωπόλ θα μπορούσε να λειτουργήσει αποτελεσματικά και μέσω της έδρας των κρατών μελών δεδομένης της ήδη υπάρχουσας προηγμένης τεχνολογίας επικοινωνιών, αποφεύγοντας έτσι τη γραφειοκρατία και το αυξημένο κόστος των αποσπάσεων υπαλλήλων στην έδρα της Ευρωπόλ. Στην πραγματικότητα, θα μπορούσε να εφαρμοστεί από το 2009, όταν η πλατφόρμα ανταλλαγής πληροφοριών της Ευρωπόλ που ονομάζεται SIENA (Secure Information Exchange Network Application) έγινε λειτουργική με τεχνολογία αιχμής επιτρέποντας όχι μόνο στις εθνικές μονάδες των κρατών μελών να χρησιμοποιούν την πλατφόρμα, αλλά και των αξιωματικών συνδέσμων της Ευρωπόλ, το σύνολο του προσωπικού της Ευρωπόλ, καθώς και των αρμοδίων αρχών τρίτων κρατών και οργανισμών που υπέγραψαν συμφωνίες συνεργασίας με την Ευρωπόλ (Eurropol, 2018). Λαμβάνοντας υπόψη τις απειλές για την ασφάλεια της ΕΕ και τις γεωπολιτικές εξελίξεις στην ευρύτερη περιοχή της Ευρώπης, θα μπορούσε να αντικατασταθεί η δομή και λειτουργία του δικτύου αξιωματικών συνδέσμων της Ευρωπόλ από περιφερειακά γραφεία της Ευρωπόλ (Regional Offices) που θα ιδρυθούν σε ευαίσθητες περιοχές του ευρωπαϊκού χώρου, όπως για παράδειγμα η περιοχή των Βαλκανίων, για την προώθηση της συνεργασίας με αυτές τις χώρες στην καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας.

Ανάλυση Πληροφοριών & Βάσεις Δεδομένων

Η ίδρυση της Ευρωπόλ βασίστηκε σε μεγάλο βαθμό στην ανάλυση εγκληματολογικών πληροφοριών, ως μία υπηρε-



σία υψηλής προστιθέμενης αξίας από επιχειρησιακής και στρατηγικής πλευράς για τις έρευνες των κρατών μελών. Πράγματι, η Ευρωπόλ εισήγαγε στην πρώτη της λειτουργική δομή το 1993, ένα τμήμα ανάλυσης του εγκλήματος με την πρόκληση των πρώτων αναλυτών από κράτη μέλη των οποίων οι αρχές επιβολής του νόμου είχαν ένα ορισμένο επίπεδο γνώσεων και εμπειρίας στην εγκληματολογική ανάλυση. Παράλληλα, η Ευρωπόλ διέδωσε την εμπειρογνωμοσύνη της στην ανάλυση του εγκλήματος, εκπαιδεύοντας προσωπικό των κρατών μελών και ενθαρρύνοντας τις εθνικές αρχές να δημιουργήσουν μονάδες ανάλυσης πληροφοριών. Για το σκοπό αυτό, η Ευρωπόλ εξέδωσε τις πρώτες κατευθυντήριες γραμμές και κανόνες στην ευρωπαϊκή κοινότητα (Eurropol, 2000a), η οποία μάλιστα κέρδισε βραβείο από τη Διεθνή Ένωση Αναλυτών Επιβολής του Νόμου (Eurropol, 2000b: 10). Έκτοτε, η Ευρωπόλ δεν έπαψε ποτέ να επενδύει συστηματικά στην ανάλυση πληροφοριών, θεωρώντας την ως ένα πολύτιμο και αποτελεσματικό εργαλείο για την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας, παρά το σκεπτικισμό ορισμένων κρατών μελών να τροφοδοτούν την Ευρωπόλ με πληροφορίες (Fägersten, 2010). Σήμερα, η Ευρωπόλ διαθέτει και λειτουργεί ένα υπερσύγχρονο κεντρικό σύστημα ανάλυσης, το οποίο καλύπτει όλες τις μορφές σοβαρού οργανωμένου εγκλήματος και τρομοκρατίας και ο οργανισμός αναγνωρίζεται ευρέως ως το ευρωπαϊκό κέντρο ανάλυσης πληροφοριών (Brady, 2008, Bureš, 2016).

Σε αντίθεση με το δίκτυο αυτόνομων βάσεων δεδομένων της Ιντερπόλ, η Ευρωπόλ είχε από ιδρύσεως της προγραμματίσει τη δημιουργία μίας ενιαίας και πολύγλωσσης βάσης δεδομένων, όπως προβλέπονταν από τη Σύμβαση Ευρωπόλ του 1998 (άρθρα 7, 8 & 9). Η πρόοδος, ωστόσο, των εργασιών του Συστήματος Πληροφοριών Ευρωπόλ (EIS) ήταν εξαιρετικά αργή λόγω της πολιτικής γραφειοκρατίας των κρατών μελών, αλλά και λόγω του αυστηρού νομικού πλαισίου της ΕΕ για την προστασία των δεδομένων, συμπεριλαμβανομένης, βεβαίως, και της πολυπλοκότητας των τεχνικών πτυχών του συστήματος. Το EIS άρχισε τελικά να λειτουργεί το 2005 (Eurropol,



24ΩΡΟ ΚΕΝΤΡΟ ΛΗΨΗΣ ΣΗΜΑΤΩΝ
ΣΥΣΤΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ



Ολοκληρωμένες Λύσεις



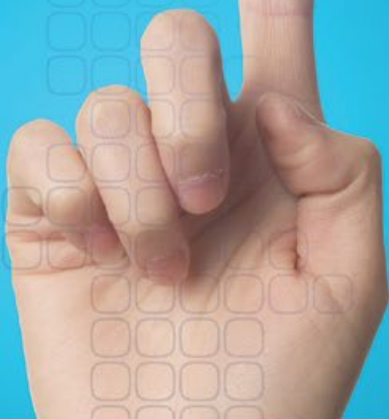
Σύγχρονες Υπηρεσίες



Τεχνογνωσία & Εμπειρία



Αξιόπιστες Συνεργασίες



security

ΜΕΝΕΛΑΟΥ 32 & ΠΛΑΤΩΝΟΣ, Ν.ΗΡΑΚΛΕΙΟ Τ.Κ. 141 22
ΤΗΛ.: 210 28 41 680 FAX: 210 28 41 872 ΚΙΝ.: 6979 72 37 12
E-mail: info@planet-security.gr

Η Planet
δεν δραστηριοποιείται
στην πώληση
συστημάτων ασφαλείας



2013) και έκτοτε έχει εξελιχθεί σημαντικά περιλαμβάνοντας όλους τους τύπους εγκληματικών πληροφοριών που αφορούν πρόσωπα, αντικείμενα, ακόμη και δομές εγκληματικών οργανώσεων. Η προστιθέμενη αξία του EIS έγκειται στην τεχνική δυνατότητα διασύνδεσης όλων των σχετικών εγκληματολογικών δεδομένων κατά τη διεξαγωγή μιας αναζήτησης. Είναι προσβάσιμο από όλες τις εθνικές αρχές επιβολής του νόμου μέσω του SIENA συμπεριλαμβανομένων και των αντιτρομοκρατικών μονάδων, αξιωματικών συνδέσμων και εμπειρογνομόνων της Ευρωπόλ. Επιπροσθέτως, όλα τα δεδομένα που εισάγονται στο σύστημα ελέγχονται αυτόματα έναντι των δεδομένων των αρχείων ανάλυσης πληροφοριών που διατηρεί η Ευρωπόλ για όλες τις μορφές οργανωμένου εγκλήματος, υποστηρίζοντας έτσι ένα ευρύτερο φάσμα συνεργασίας για τη διεξαγωγή ερευνών κατά του οργανωμένου εγκλήματος και της τρομοκρατίας σε ολόκληρη την Ευρώπη.

Συμπεράσματα & Διαπιστώσεις

Η ίδρυση της EDU το 1993 και εν συνεχεία η επικύρωση της Σύμβασης Eurapol το 1998, ήταν τα πρώτα βήματα στην ευρωπαϊκή ιστορία για τη δημιουργία μιας θεσμοθετημένης κοινής δομής ευρωπαϊκής συνεργασίας για την εφαρμογή του νόμου. Ωστόσο, η λειτουργία αυτή της πρώτης δομής αποδείχθηκε με την πάροδο του χρόνου ότι δεν ήταν ιδιαίτερα επιτυχής. Για μία περίοδο άνω των δέκα ετών, η Ευρωπόλ λειτουργήσε υπό εκτεταμένους περιορισμούς που έθετε η Σύμβαση Ευρωπόλ, η φιλοσοφία της οποίας βασίζονταν στην αρχή της διακυβερνητικής συνεργασίας (Boer & Walker,

1993). Η αρχή της εθνικής κυριαρχίας, σύμφωνα με την οποία τα θέματα εσωτερικής ασφάλειας υπάγονται στην αποκλειστικά αρμοδιότητα των κρατών, που εν πολλοίς συνοδεύονταν και από έλλειψη εμπιστοσύνης των κρατών μελών προς την Ευρωπόλ, υπήρξε από τους κυριότερους αποτρεπτικούς παράγοντες προκαλώντας σοβαρές καθυστερήσεις στις διαβουλεύσεις για τη στρατηγική και επιχειρησιακή εξέλιξη του οργανισμού (Rozée, et al., 2013).

Τα πρώτα σημάδια της θετικής αλλαγής στην εξέλιξη της Ευρωπόλ, έγιναν εμφανή όταν η Σύμβαση Ευρωπόλ αντικαταστάθηκε με την Απόφαση του Συμβουλίου της ΕΕ του 2009. Από εκείνη τη στιγμή, η Ευρωπόλ, ως οργανισμός πλέον της ΕΕ, εξήλθε από το άκαμπτο πλαίσιο της διακυβερνητικής συνεργασίας που απέρρεε από τις διατάξεις της Σύμβασης Ευρωπόλ και άρχισε μια νέα εποχή στην ευρωπαϊκή αστυνομική συνεργασία, με την επέκταση των αρμοδιοτήτων της Ευρωπόλ σε όλες τις μορφές του οργανωμένου εγκλήματος. (Paterson & Pollock, 2011: 137). Ο Κανονισμός της ΕΕ του 2017 που αντικατέστησε την Απόφαση του Συμβουλίου του 2009 και αποτελεί σήμερα τη νομική βάση της Ευρωπόλ, ενίσχυσε τον επιχειρησιακό και στρατηγικό ρόλο της Ευρωπόλ στο πλαίσιο της πολύπλευρης και σύνθετης ευρωπαϊκής αστυνομικής συνεργασίας και παράλληλα αύξησε τη διαφάνεια στους τομείς της λογοδοσίας και της προστασίας των προσωπικών δεδομένων που τηρεί και επεξεργάζεται ο οργανισμός από ίδρύσεώς του. Η ανταλλαγή πληροφοριών αποτελούσε ανέκαθεν τον ακρογωνιαίο λίθο της διεθνούς

ΧΟΝΔΡΙΚΗ ΠΩΛΗΣΗ
ΣΥΣΤΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Tiandy

SUPER STARLIGHT

24-hour color surveillance



NOVO

TECHNOLOGIES



Naked eye

Super Starlight

axxi4next

Experience The Next®

ΤΟ ΚΟΡΥΦΑΙΟ ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ
ΜΕ VIDEO ANALYTICS



AUTOZOOM



TIME COMPRESSOR



MOMENTQUEST



ΔΙΑΔΡΑΣΤΙΚΟΣ ΤΡΙΣΔΙΑΣΤΑΤΟΣ ΧΑΡΤΗΣ



ΚΑΤΑΓΡΑΦΗ ΠΙΝΑΚΙΔΩΝ ΚΥΚΛΟΦΟΡΙΑΣ



ΑΝΑΓΝΩΡΙΣΗ ΠΡΟΣΩΠΩΝ

www.novo.gr

Τρωάδος 15
Νέα Ιωνία, Αθήνα
Τηλ: 210 27 231 27
info@novo.gr



συνεργασίας για την επιβολή του νόμου. Η Ευρωπόλ είχε επενδύσει εξαρχής στη δημιουργία ενός δικτύου αξιωματικών συνδέσμων, το οποίο αποδείχθηκε εξαιρετικά χρήσιμο στην αρχή της λειτουργίας της ως διακυβερνητικός οργανισμός. Με την πάροδο του χρόνου, αυτό το δίκτυο επεκτάθηκε υπερβολικά, ειδικά μετά τη διεύρυνση της ΕΕ αλλά και των συμφωνιών συνεργασίας της Ευρωπόλ με τρίτες χώρες και διεθνείς οργανισμούς. Δεδομένης, ωστόσο, της προηγμένης τεχνολογίας που χρησιμοποιείται από την Ευρωπόλ από το 2009 όταν το SIENA τέθηκε σε λειτουργία, θα μπορούσε σήμερα να εξετασθεί το ενδεχόμενο της αντικατάστασης του υφιστάμενου δικτύου αξιωματικών συνδέσμων με την ίδρυση περιφερειακών υπηρεσιών της Ευρωπόλ στον ευρωπαϊκό χώρο. Συγκεκριμένα, η Ευρωπόλ θα μπορούσε να δημιουργήσει περιφερειακές υπηρεσίες σε κρίσιμες ευρωπαϊκές περιοχές, όπως στα δυτικά Βαλκάνια ή και σε άλλες γεωγραφικές περιοχές, ώστε να υποστηρίξει καλύτερα τη συνεργασία με αυτά τα κράτη, αλλά και μεταξύ των κρατών μελών της, στην καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας.

Κατά την τελευταία δεκαετία, η Ευρωπόλ έχει εξελιχθεί σημαντικά αποδεικνύοντας την προστιθέμενη αξία της στην ευρωπαϊκή αστυνομική συνεργασία, με απτά αποτελέσματα που παρουσιάζονται μέσω των εκθέσεων της για την εκτίμηση απειλής του σοβαρού οργανωμένου εγκλήματος και της τρομοκρατίας. Έχοντας ολοκληρώσει την ανάπτυξη της πλατφόρμας SIENA στον τομέα της ανταλλαγής πληροφο-

ριών, μαζί με το EIS ως πανευρωπαϊκή βάση δεδομένων για εγκληματικές δραστηριότητες και με ένα προηγμένο σύστημα ανάλυσης πληροφοριών, η Ευρωπόλ δημιούργησε με επιτυχία μια ολοκληρωμένη επιχειρησιακή δομή που επιτρέπει στον οργανισμό να λειτουργεί αποτελεσματικότητά στην υποστήριξη των ερευνών όλων των αρχών επιβολής του νόμου των κρατών μελών. Σήμερα, ο πρωταγωνιστικός ρόλος της Ευρωπόλ στην καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας, αναγνωρίζεται μέσω της ολοκληρωμένης στρατηγικής της ως μέρος της αρχιτεκτονικής ασφάλειας της ΕΕ, αλλά και του πρωτεύοντος ρόλου της στην υλοποίηση του κύκλου πολιτικής της ΕΕ που εστιάζει σε επιχειρησιακά σχέδια για την καταπολέμηση σοβαρών μορφών οργανωμένου εγκλήματος (Council of EU, 2014 & Europol, 2016b: 19).

Η αρχή της εθνικής κυριαρχίας έχει επηρεάσει σημαντικά την αποτελεσματικότητα των επιχειρησιακών δραστηριοτήτων της Ευρωπόλ, καθόσον περιορίζει δραστικά το ρόλο της στην υποστήριξη των ερευνών των κρατών μελών μέσω της διευκόλυνσης της ανταλλαγής πληροφοριών και της παροχής ανάλυσης πληροφοριών. Μια πολύ ισχυρή ένδειξη του αντίκτυπου της εθνικής κυριαρχίας στον τομέα της δικαιοσύνης και των εσωτερικών υποθέσεων της ΕΕ, ήταν η πρόσφατη αποχώρηση της Δανίας από μέλος της Ευρωπόλ (Μάιος 2017), μετά από ειδικό προς τούτο δημοψήφισμα της χώρας. Παρομοίως, οι προσεχείς μελλοντικές συνέπειες που θα προκύψουν από το Brexit, το οποίο αναπόφευκτα

SAFETY THAT MEETS YOUR STANDARDS!



**ΑΠΟΛΥΤΟΣ ΕΛΕΓΧΟΣ
ΠΑΡΑΚΟΛΟΥΘΗΣΗ & ΚΑΤΑΓΡΑΦΗ
ΧΡΗΣΗΣ ΚΛΕΙΔΙΩΝ**



**ΑΥΤΟΜΑΤΑ ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΚΛΕΙΔΙΩΝ & ΕΞΟΠΛΙΣΜΟΥ.**



**ΠΡΟΣΤΑΤΕΥΣΤΕ ΤΑ ΠΕΡΙΟΥΣΙΑΚΑ ΣΑΣ ΣΤΟΙΧΕΙΑ
& ΤΟΥΣ ΠΟΡΟΥΣ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΣΑΣ.
ΜΕΤΑΤΡΕΨΤΕ ΣΕ «ΕΞΥΠΝΑ» ΤΑ ΣΥΜΒΑΤΙΚΑ ΣΑΣ ΚΛΕΙΔΙΑ!**



**ΑΔΙΑΠΕΡΑΣΤΗ
ΟΜΙΧΛΗ
ΑΣΦΑΛΕΙΑΣ**



**ΣΥΣΤΗΜΑ ΠΑΡΑΓΩΓΗΣ ΑΝΤΙΚΛΕΠΤΙΚΗΣ ΟΜΙΧΛΗΣ
ΚΑΝΕΙΣ ΔΕΝ ΜΠΟΡΕΙ ΝΑ ΚΛΕΨΕΙ ΚΑΤΙ ΠΟΥ ΔΕΝ ΒΛΕΠΕΙ!**



**ΑΣΙΟΠΙΣΤΟ, ΚΑΤΑΛΛΗΛΟ ΓΙΑ ΧΩΡΟΥΣ ΦΥΛΑΞΗΣ & ΑΠΟΘΗΚΕΥΣΗΣ
ΕΜΠΟΡΕΥΜΑΤΩΝ, ΠΙΣΤΟΠΟΙΗΜΕΝΟ ΚΑΤΑ EN 50131-8,
5 ΧΡΟΝΙΑ ΕΓΓΥΗΣΗ.**



**ΠΡΟΣΤΑΤΕΨΤΕ Ο,ΤΙ ΑΞΙΖΕΙ
ΟΠΟΥ ΚΑΙ ΑΝ ΒΡΙΣΚΕΤΑΙ!**



ΧΡΗΜΑΤΟΚΙΒΩΤΙΑ



ΘΗΣΑΥΡΟΦΥΛΑΚΙΑ



**ΔΙΑΧΕΙΡΙΣΗ
ΧΡΗΜΑΤΟΣ**



**ΜΗΧΑΝΕΣ ΚΑΤΑΜΕΤΡΗΣΗΣ &
ΑΝΙΧΝΕΥΣΗΣ ΓΝΗΣΙΟΤΗΤΑΣ**

traka
ASSA ABLOY

PROTECT

Wertheim

KABA

GLORY

θα καταλήξει στην αποχώρηση του Ηνωμένου Βασιλείου από μέλος της Ευρωπόλ, εγείρουν σοβαρές ανησυχίες για τη μελλοντική εξέλιξη του οργανισμού, αν και προβλέπεται να υπάρξουν διμερείς συμφωνίες στρατηγικής και επιχειρησιακής συνεργασίας προκειμένου να καλυφθούν τα κενά που θα δημιουργηθούν από μια τόσο ανησυχητική απώλεια δύο ισχυρών κρατών μελών της Ευρωπόλ. Τίθεται, τέλος, το ερώτημα εάν και κατά πόσο είναι εφικτή η περαιτέρω στρατηγική και επιχειρησιακή εξέλιξη της Ευρωπόλ εντός του ισχύοντος νομικού πλαισίου της ΕΕ, σύμφωνα με το οποίο (άρθρο 88 της Συνθήκης για τη λειτουργία της ΕΕ & άρθρο 4.2 της Συνθήκης της ΕΕ) ορίζεται κατηγορηματικά ότι τα θέματα εσωτερικής ασφάλειας και δημόσιας τάξης υπάγονται αποκλειστικά στην εθνική κυριαρχία των κρατών μελών (Guyomarch, 1994, European Commission, 2017).-

Παραπομπές

Benyon, J. (1996) "The politics of police cooperation in the European Union", *International Journal of the Sociology of Law*, 14 (4):353-379.
Boehm, F. (2012) *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards a harmonised data protection principles for information exchange at EU level*. Berlin: Springer.
Boer, M. & Walker, N. (1993) *European Policing after 1992*, *Journal of Common Market Studies*, 31(1):3-28.
Brady, H. (2008) "Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime", *Policing: A Journal of Policy and Practice*, 2(1):103-109.
Bruggeman, W. (2007) *The future of Europol and its limits*, http://www.europol.europa.eu/hearings/20070410/libe/bruggeman_en.pdf (accessed on 18.9.2019).
Bunyan, T. (1993) "Trevi, Europol and the European State", in Bunyan, T. (ed) *State watching the New Europe: A handbook on the European State*, London: Statewatch.
Bureš, O. (2016) "Intelligence sharing and the fight against terrorism in the EU: Lessons learned from Europol", *European View*, 15(1):57-66.
Busuic, M. & Groenleer, B. (2013) "Beyond design: The evolution of Europol and Eurojust", *Perspectives on European Politics and Society*, 14(3):285-304.
Council of the European Union (2014) *The EU Policy Cycle to tackle organized and serious international crime*, EU Publications Office.
Deflem, M. (2002) *Policing World Society: Historical Foundations of International Police Cooperation*. Oxford, UK: Oxford University Press.
Das, D & Kratcoski, P. (2001) "International Police Cooperation: A World Perspective" in Koenig, D & Das, D. (eds.), (2001), *International Police Cooperation. A world Perspective*, Oxford: Lexington Books.
European Commission (2008) "Europol to become EU agency in 2010", Press Release, Brussels, 18.4.2008.
European Commission (2013) "Europol: The EU hub for support to law enforcement cooperation and training", Press Release, Brussels, 27 March 2013, http://europa.eu/rapid/press-release_IP-13-284_en.htm (accessed on 16.7.2019).
European Commission (2017) "Commission welcomes Europol's new mandate and cooperation agreement with Denmark", Brussels, 29 April 2017, http://europa.eu/rapid/press-release_STATEMENT-17-1169_en.htm (accessed on 17.8.2019).
Europol (1998) Press Release, "Official Opening of Europol", 1.10.1998.
Europol (2000a) *Europol Analytical Guidelines*, EU Publications Office.
Europol (2000b) *Annual Report 2000*, EU Publications Office.
Europol, (2013) *Europol Information System*, EU Publications Office.

Europol (2016a) *Europol Review 2015*, EU Publications Office.
Europol (2016b) *Europol Strategy 2016-2020*, EU Publications Office.
Europol (2017) Press Release "Today, on 1 May 2017, Europol's new Regulation enters into force and takes effect in all EU Member States" <https://www.europol.europa.eu/newsroom/news/europol-s-new-regulation> (accessed on 20.6.2019).
Europol (2018) Press Release, "In 2017 more than one million messages were exchanged between the users of SIENA and more than 66,000 cases were initiated in 2017, an increase of 42% compared to 2016", 11.1.2018.
<https://www.europol.europa.eu/newsroom/news/more-one-million-operational-messages-shared-between-europol-member-states-and-third-parties-in-2017> (accessed on 14.5.2019).
Fägersten, B. (2010) "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol", *Intelligence and National Security*, 25(4): 500-520.
Fijnaut, C. (2004) *Police cooperation and the area of freedom, security and justice*, in Walker, N. (ed.), *Europe's area of freedom, security and justice*. Oxford: Oxford University Press, p. 241-282.
Fijnaut, C. (1993) "The Communitization of police cooperation in Western Europe", in Schermers H, (et.al.) (eds) *Free movement of persons in Europe: Legal problems and experiences*. Dordrecht: Martinus Nijhoff, p. 75-92.
Guyomarch, A. (1994) *Problems and prospects for European police cooperation after Maastricht*, *Policing and Society*, 5 (3):249-261.
Ministerial Agreement (1993) *Establishment of the Europol Drugs Unit*, Copenhagen, 2 June 1993.
Moore, A. & Vermeulen, G. (2010a) *Shaping the competence of Europol. An FBI perspective in Cools, M.et. al. (eds.) (2010) EU and international crime control: Topical Issues*, Antwerpen: Maklu.
Moor, A. & Vermeulen, G. (2010b), *The Europol Council Decision: A new legal basis for Europol*, *New Journal of European Criminal Law*, (1) 2:178-198.
Occhipinti, J. (2003) *The politics of EU Police Cooperation. Toward a European FBI?* London: Lynne Rienner Publishers.
OJEU (1995) *Joint Action of 10 March 1995 adopted by the Council on the basis of article K.3 of the treaty on European Union concerning the Europol Drugs Unit*, 95/73/JHA, L 062, 20.3.1995.
OJEU (1996) *Joint Action of 16 December 1996 adopted by the Council on the basis of article K.3 of the Treaty on European Union extending the mandate given to the Europol Drugs Unit*, 96/748/JHA, L 342 (39), 31.12.1996.
OJEU (1998) *Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)*, C 316, 27.11.1995.
OJEU (1999) *Council Communication concerning the taking up of activities of Europol*, C185/01, 1.7.1999.
OJEU (2001) *Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, L 8/1, 12.01.2001.
OJEU (2002) *Council Framework Decision of 13 June 2002 on joint investigations teams*, (2002/465/JHA), L 162/1, 20.6.2002.
OJEU (2009) *Council Decision of 6 April 2009 establishing the European Police Office (Europol)*, (2009/371/JHA), L 121/37, 15.5.2009.
OJEU (2016) *EU Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)*, L 135/53, 24.5.2016.
Paterson, C. & Pollock, E. (2011), *Policing and Criminology*, UK: Learning Matters.
Rauchs, G. / Koenig, D. (2001) "Europol" in Koenig, D & Das, D. (eds.), (2001), *International Police Cooperation. A world Perspective*, Oxford: Lexington Books.
Rozée, S., Kaunert, C., & Léonard, S., (2013) "Is Europol a Comprehensive Policing Actor?", *Perspectives on European Politics and Society*, 14(3): 372-387.
Stergioulis, E. (2003) *The European Police Office-Europol*. Athens: Nomiki Vivliothiki (in Greek).
Woodward, R. (1993) *Establishing Europol*, *European Journal of Criminal Policy and Research*. 1(4):7-33.



PROVISION-ISR IP TECHNOLOGY

- Ισραηλινή τεχνολογία, αξιοπιστία και υποστήριξη
- Πλήρης σειρά προϊόντων για επαγγελματίες
- Πλήρης συμβατότητα με όλες τις σύγχρονες τεχνολογίες τρίτων κατασκευαστών
- Απλές χρηστικές εφαρμογές λογισμικού και API
- Λύσεις "Value for Money"

IP TECHNOLOGY
SMART SOLUTIONS THROUGH THE NETWORK

SIGNAL
ELECTRONICS SECURITY



Η Ασφάλεια στην Περιφερειακή Ανάπτυξη

Οικονομική επίδοση και επιχειρησιακή
ετοιμότητα του χώρου



Η υψηλή οικονομική επίδοση και η επιχειρησιακή ετοιμότητα του χώρου αποτελούν εγγυητές της ασφάλειας και επιταχυντές της ανάπτυξης, είτε πρόκειται για γειτονιά είτε για χωριό είτε για την πρωτεύουσα είτε για μια περιφέρεια είτε για κράτη ή ομοσπονδίες κρατών. Ασφαλές σύστημα είναι το ανεπτυγμένο σύστημα.

Κατά το παρελθόν, η **σχέση της ασφάλειας με την ανάπτυξη** προσδιοριζόταν από τη θωράκιση ή επέκταση μιας εδαφικής ή λειτουργικής ενότητας (πόλη, περιφέρεια, κράτος, ομοσπονδία ή συνομοσπονδία κρατών) με στρατιωτικά μέσα και συμβατικά όπλα σκληρής ισχύος. Ο εχθρός των πόλεων αποτελούσε μια **ορατή και υπολογίσιμη απειλή**. Σήμερα, και ενώ ο κίνδυνος είναι αόρατος και αδιαίρετος, η χωρική διάσταση της προστασίας μαλακής ισχύος (οικονομική, διπλωματική, πολιτισμική) έχει τώρα το προβάδισμα: υπολογίζεται ως (α) η **ανταγωνιστική οικονομική επίδοση** και (β) η **επιχειρησιακή ετοιμότητα και επάρκεια των κοινωνιών** σε ψηφιακές και υγειονομικές δομές, καθώς και στην πολιτική

και ατομική προστασία. Μια συσχέτιση ανάμεσα στην αστική ασφάλεια και την αστική ανάπτυξη φαίνεται ότι υπάρχει.

Εισαγωγή

Ποιο είναι το **κοινό σημείο** ανάμεσα στην άτρωτη **Navy SEAL Team 6** και το **Firewall της Fortinet με την πόλη του Τόκιο**; Η ασφάλεια: ως το αδιόρατο αλλά αδιαπέραστο στρώμα προστασίας του συστήματος από τον κίνδυνο ή την απώλεια. Στη θετική της διάσταση, συμβάλλει στην αποτροπή και αποφυγή του κινδύνου με ενίσχυση της άμυνας και στην αρνητική της διάσταση επιτυγχάνει την αποτροπή πολέμου μέσω της εξάλειψης μιας απειλής.

Περιφερειακή Επιστήμη, Κυβερνητική & Ασφάλεια

Πολλά έχουν ειπωθεί και άλλα τόσα έχουν διατυπωθεί στην ακαδημαϊκή συζήτηση γύρω από τη **σχέση της ανάπτυξης με την έννοια της ασφάλειας**. Και οι δύο δυνάμεις είναι στενά συνδεδεμένες με τη διαμόρφωση των τάσεων στο χώρο, η οποία όμως σε πολλές περιφερειακές οικονομίες δεν είναι ομαλή, λόγω κάποιας οικονομικής ή/και πολιτικής αστάθειας. Τα υπερμεγέθη οικονομικά συστήματα δείχνουν να αντιμετωπίζουν μεγαλύτερη ανασφάλεια από αυξημένο κίνδυνο αποσταθεροποίησης σε σχέση με τα μικρότερα όπου είναι πιο εύκολο να ελεγχθούν. Ωστόσο, ορισμένες φορές φαίνεται ότι υπάρχει θετική συσχέτιση ανάμεσα στο βαθμό συγκέντρωσης της ανάπτυξης σε ένα οριοθετημένο χώρο, το μεγάλο μέγεθος του συστήματος και στην ασφαλή λειτουργία του. Ας δούμε:

Σύμφωνα με το θεμελιώδες αξίωμα της Περιφερειακής Επιστήμης, κάθε οικονομική δραστηριότητα εξελίσσεται μέσα στο χώρο και ο χώρος επιδρά στην οικονομική δραστηριότητα: (α) ως **επιφάνεια του εδάφους**: η στενότητα διαμορφώνει τις συγκεντρώσεις ή τη διασπορά - διαχύσεις πόρων και δραστηριοτήτων όπως και τις συγκρούσεις των ατόμων για τις χρήσεις γης, (β) ως **γεωγραφική απόσταση** και (γ) ως **επιλογή του τόπου εγκατάστασης των παραγωγικών και καταναλωτικών** δραστηριοτήτων λόγω της γεωγραφικής απόστασης. Η άνιση κατανομή των πόρων και δραστηριοτήτων στο χώρο είναι γνωστή ως περιφερειακό πρόβλημα και διαταράσσει την ισορροπία δυνάμεων σε κάθε είδους σχέση δράσης και αντίδρασης που αναπτύσσεται εντός κάθε λειτουργικής περιοχής, η οποία αποτελεί ένα σύστημα. Στην Περιφερειακή Επιστήμη ως **ασφάλεια νοείται η ομαλή λειτουργία του χωρικού συστήματος**, είτε πρόκειται για ένα χωριό είτε για μια ήπειρο.

Επομένως, δεν είναι δυνατόν η μεταβλητή του χώρου να μην υπολογίζεται στις μεταβολές στην κατάσταση όλων των φυσικών και ανθρωπογενών συστημάτων που πρέπει να λειτουργούν με ασφάλεια. Ως τέτοιες μεταβολές λογίζονται:

1) Η παγκοσμιοποίηση στις τέσσερις διαστάσεις της:

(α) Χωροταξική, (β) γεωπολιτική, (γ) ανάπτυξη υψηλής τεχνολογίας, (δ) διαμόρφωση τεσσάρων επιπέδων χωρικών συγκεντρώσεων: (i) Μεγάλα Διεθνή Λιμάνια, (ii) Διεθνή Κέντρα Ευρύτερης Χωρικής Ζώνης, (iii) Περιφερειακά Κέντρα Αναδυόμενης Επιρροής, (iv) Τοπικά ή Πολικά Αστικά Κέντρα.

2) Η ενεργοποίηση των γεωπολιτικών μονάδων:

οι σχηματισμοί γεωπολιτικών αντιλήψεων για αμφισβητήσεις των εθνικών συνόρων και οικονομιών εκκινεί περιφερεια-

κές συμμαχίες ως διεθνείς συνασπισμούς με οργανωτική δομή, επιχειρησιακή ισχύ και αποστολή τη διατήρηση της διεθνούς ειρήνης και ασφάλειας.

3) Η αστικοποίηση: ο πληθυσμός και οι οικονομικές δραστηριότητες τείνουν να συγκεντρώνονται στα αστικά κέντρα, διαταράσσοντας τη χωροταξική ισορροπία· ο αστικός συνωστισμός δημιουργεί χωρικά δίπολα δύο ταχυτήτων με διωνυμική κατανομή πόρων (οι ανεπτυγμένοι τόποι μόνο αντλούν και οι υπανάπτυκτοι μόνο δίνουν).

4) Η ρύπανση του περιβάλλοντος: η διαδικασία της ανάπτυξης εκκινεί αντιοικονομίες και εξωτερικές επιβαρύνσεις, δηλαδή πρόσθετη ζημία στην υγεία των ατόμων που δεν την προκαλούν, η οποία αντανακλάται και στην τιμή των αγαθών και υπηρεσιών που κάνουν χρήση.

Σύμφωνα με την **Επιστήμη Συστημάτων και την Κυβερνητική** (Cybernetics), κάθε φυσικό, μηχανικό, κοινωνικό ή οικονομικό σύστημα είναι μια σύνθετη πληροφοριακή δομή, αποτελούμενη από αυτόνομα δομικά μέρη με υλική και χωρική υπόσταση που αλληλεπιδρούν μεταξύ τους και με το εξωτερικό περιβάλλον. Κατά την αλληλεπίδραση, η αλλαγή που συντελείται σε έναν κόμβο δομικών μερών επηρεάζει και τους υπόλοιπους, ενώ η συνολική δράση του συστήματος προκαλεί αντίδραση στο περιβάλλον· η οποία ανάπαλιν αντικατοπτρίζεται στο σύστημα με κάποιο τρόπο και ενεργοποιεί μια αλλαγή του συστήματος. Η αλλαγή μπορεί να είναι προβλέψιμη ή απρόβλεπτη. Και όταν είναι προβλέψιμη, το σύστημα είναι ασφαλές.

Ένα τέτοιο σύστημα είναι και μια περιφερειακή οικονομία [μια πόλη ή περιφέρεια, ένα κράτος (και) ως τμήμα μιας ένωσης κρατών, μια ομοσπονδία ή συνομοσπονδία κρατών], **η οποία είναι ασφαλής όταν είναι σταθερή**· όταν οι αλλαγές που συντελούνται σε ένα από τα δομικά μέρη του συστήματος δεν επηρεάζουν τα υπόλοιπα. Ως εκ τούτου, ένα **περιφερειακό οικονομικό σύστημα πρέπει να σέβεται και να ικανοποιεί έξι κανόνες για να βρίσκεται σε ασφαλή κατάσταση**:

- **Μέγεθος περιοχής.** Όσο μικρότερη μια περιφερειακή οικονομία, τόσο πιο προβλέψιμη και ελατή (σφυρηλατήσιμη), άρα πιο εύκολη είναι η αλλαγή και το αντίστροφο. Το μικρού μεγέθους (και) ενιαίο σύστημα αξιών είναι πιο δεκτικό στην υιοθέτηση νέων προτύπων και παρέχει μεγαλύτερη ελαστικότητα πρόσβασης σε νέους κανόνες (τα αντανακλαστικά της Ελλάδας στην εμφάνιση της πανδημίας Covid-19 είναι το τέλειο παράδειγμα).
- **Σταθερότητα οικονομίας.** Τα μέσα άσκησης της περιφερειακής δημοσιονομικής πολιτικής πρέπει να είναι αποτελεσματικά για τη σταθεροποίηση των οικονομικών

διαταραχών (πληθωρισμού και ανεργίας) και των εισοδηματικών ανισοτήτων (αμοιβών εργασίας και συγκέντρωσης πλούτου).

- **Σταθερότητα πολιτικού συστήματος.** Η θεσμική οντότητα πρέπει να έχει συνέχεια και να μην αμφισβητείται η προγραμματική στρατηγική έπειτα από κάθε αλλαγή κυβέρνησης, αλλά να δίδεται ο απαραίτητος χρόνος στις δημόσιες πολιτικές να ωριμάζουν ώστε να αρχίσουν να αποδίδουν.
- **Σταθερότητα σχέσεων με τους γείτονες και θεσμοποίηση των εξωτερικών σχέσεων.** Η περιφερειακή οικονομία πρέπει να συνάπτει περιφερειακές συνεργασίες και να προτάσσει θεσμικές νόρμες, βασισμένες σε κοινά αποδεκτές αρχές στις διεθνείς σχέσεις (ανθρώπινα δικαιώματα, δημοκρατικό πολίτευμα, κράτος δικαίου).
- **Ανθεκτικότητα συστήματος.** Πρέπει να διαθέτει την ικανότητα να αντιστέκεται στις εσωτερικές και εξωτερικές μεταβολές και την ταχύτητα να επαναφέρει όλα τα χαρακτηριστικά του (πληθυσμό, οικονομική δραστηριότητα, δομημένο περιβάλλον) στα επίπεδα ισορροπίας τους πριν την εμφάνιση μιας διαταραχής.
- **Άνοιγμα οικονομίας.** Η φυγόκεντρος κατανομή της ανάπτυξης προς τις όμορες περιοχές συντελεί στην καλλιέργεια αμοιβαίων χωρικών συμφερόντων.

Αντίθετα, τα **συστήματα αβεβαιότητας** κινδυνεύουν από:

- υψηλά επίπεδα ανεργίας,
- οργανωμένο έγκλημα,
- περιβαλλοντικές καταστροφές,
- μαζικές μετακινήσεις πληθυσμών από χώρες με αποσταθεροποιημένη οικονομία.

Για τις ανάγκες του παρόντος, θα σταθούμε στην παγκοσμιοποίηση ως μεταβολή στην κατάσταση του χώρου και τη θετική κατ'εξάιρεση **συσχέτιση της ανάπτυξης ως μεγέθυνση με την αστική ασφάλεια.**



Οι 33 megacities με βάση την πληθυσμιακή κατάταξη του Οργανισμού Ηνωμένων Εθνών.

Αστικοποίηση & Ασφάλεια: οι Σύγχρονες Πόλεις - Κράτη

Τα τελευταία εκατόν είκοσι χρόνια ο πληθυσμός της γης αυξήθηκε κατά 4,6 δις, όσο δηλαδή δεν έχει αυξηθεί από κτήσεις κοινωνιών. Αυτή τη στιγμή, το 55% του παγκόσμιου πληθυσμού ζει σε αστικές περιοχές, το οποίο εκτιμάται ότι θα αυξηθεί σε 68% έως το 2050. Ο υψηλός ρυθμός αστικοποίησης των περιοχών που όλο και μεγεθύνονται ή πολλαπλασιάζονται δημιουργήσε νέες κατηγορίες πόλεων. Πρώτα τις **mega πόλεις** (megapolis ή megacities ή supercities ή hypercities ή city states ή metropoles: πόλεις με πληθυσμό άνω των 10 εκατ. κατοίκων), έπειτα τις **meta πόλεις** (metacities: σπάνε το όριο των 20 εκατ. κατοίκων, τόσο μεγάλες που ενώνονται μεταξύ τους) και τώρα τις **mega περιφέρειες** [megaregions: δίκτυα μεγαπόλεων συνεχούς ηλεκτροδότησης με βάση τις τελευταίες νυχτερινές δορυφορικές εικόνες που λειτουργούν ως σταθμοί παραγωγής οικονομικής δύναμης άνω των \$300 δις (light-based regional product - LRP)· ο νυχτερινός φωτισμός δείχνει την κατανάλωση ενέργειας, η οποία αντιστοιχεί στην περιφερειακή οικονομική δραστηριότητα].



Οι 29 megaregions από το δορυφόρο της Εθνικής Υπηρεσίας Ωκεανών και Ατμόσφαιρας (NOAA) των ΗΠΑ με βάση την κατάσταση του ΑΕΠ (σε μονάδες αγοραστικής δύναμης).

Από το δορυφόρο διακρίνονται 29 megaregions (11 στην Αμερική, 10 στην Ασία, 5 στην Ευρώπη και 3 στην τομή Μέσης Ανατολής και Βόρειας Αφρικής). Δέκα από αυτές παράγουν τα \$28 τρις της παγκόσμιας οικονομικής και ενεργειακής μηχανής. Μέχρι το 2030, αναμένεται να σχηματισθούν 39 συνολικά megacities, όπου θα καταλαμβάνουν το 3% της επιφάνειας της γης, θα φιλοξενούν το 9% του ανθρώπινου πληθυσμού και θα παράγουν το 15% του παγκόσμιου ΑΕΠ.

Δεν είναι, λοιπόν, τα εθνικά κράτη, ούτε και οι διακρατικές ενώσεις οι ηγέτιδες δυνάμεις που κατευθύνουν την παγκόσμια οικονομία, αλλά οι σύγχρονες πόλεις - κράτη και οι μεγαπεριφέρειες ως περίπλοκα οικονομικά και τεχνολογικά συστήματα συγκέντρωσης της πληροφορίας που τραβούν περισσότερο βάρος από άλλες.

Κατ'ακολουθίαν, θα πίστευε κανείς, ότι λόγω του μεγέθους

ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΣΥΣΚΕΥΩΝ ΙΟΤ / Μ2Μ ΕΙΝΑΙ ΕΔΩ...



Νέα γενιά συσκευών τεχνολογίας LTE-M

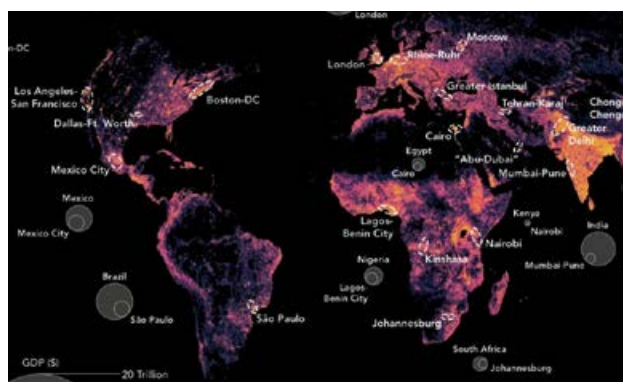


- Σύνδεση μέσω Bus (για πίνακες DSC PC series)
- Σύνδεση μέσω TIP/RING (για όλους τους πίνακες)
- Ενσωματωμένη GLOBAL e-SIM
- Ασφαλές ιδιωτικό δίκτυο VPN
- AES κωδικοποίηση αποστολής σημάτων
- Μεγαλύτερη εμβέλεια και διείσδυση έως 30 dB
- Χαμηλή κατανάλωση
- CE, EN50136/ATS5 (Grade 4)





και της εγγύτητας των συνδέσεων μεταξύ τους (ως οικιστικά, εμπορικά, βιομηχανικά, πολιτικά κέντρα και κόμβοι συνδυσμένων μεταφορών), πρόκειται για **γίγαντες με πηλίνα πόδια**, που είναι δύσκολο να διατηρήσουν τον έλεγχό τους: και **ανά πάσα στιγμή διατρέχουν τον κίνδυνο κυβερνο-και-τρομοκρατικών επιθέσεων, φυσικών καταστροφών ή πανδημιών** και να συμπαρασυρθούν σε οικονομική κατάρρευση. Κάθε άλλο.



Connectography > connectivity + geography, όπου η νέα κατανομή του παγκόσμιου πληθυσμού προκύπτει από τη συνδεσιμότητα των συγκεντρώσεων οικονομικής δραστηριότητας στο χώρο (παγκόσμιοι κόμβοι) παρά τα εθνικά σύνορα των κρατών.

Megacities, οι Ασφαλέστερες Πόλεις στον Κόσμο

Από τις 33 πρώτες supercities, οι **20 θεωρούνται οι πιο ασφαλείς πόλεις στον κόσμο, με ασφαλέστερη το Τό-**

κυο της Ιαπωνίας. Και αν δεν είναι η υπ' αριθμόν ένα, σίγουρα θα βρίσκεται σταθερά μέσα στις δέκα πρώτες. Το Τόκυο (ή Greater Tokyo) αποτελεί τη μεγαλύτερη megacity και την τέταρτη κατά σειρά megaregion με βάση τις τελευταίες νυχτερινές δορυφορικές λήψεις και την παγκόσμια κατάταξη της οικονομικής δραστηριότητας. Έχει πληθυσμό ≈ 38 εκατ. κατοίκους συγκεντρωμένους σε μια έκταση 13.500 km² και συνολικό ετήσιο ΑΕΠ \$1,8 τρις ή \$46.000 μέσο ετήσιο κατά κεφαλήν εισόδημα.



Greater Tokyo, NASA Earth Observatory (νυχτερινή δορυφορική λήψη).

Αυτή η hypercity:

- έχει **υψηλή οικονομική επίδοση**, ούσα ικανή να αξιοποιεί όλους τους παραγωγικούς συντελεστές της με αρκετά υποκατάστατα ώστε να εξακολουθεί να λειτουργεί ομαλά σε περίπτωση εμφάνισης διαταραχής· είναι και ευσταθής, αφού αντιμετωπίζει την υπάρχουσα παγκό-



Σταθερός Αριθμός Τηλεφώνου με μόνο €1 το μήνα!



Αξιοπιστία



Ποιότητα



Ασφάλεια



Οικονομία



Διαθεσιμότητα

supervoice

www.supervoice.eu

210 710 7000

Η τιμή συμπεριλαμβάνει ΦΠΑ 24% και Τέλος Συνδρομητών Σταθερής Τηλεφωνίας 5%.
Η προσφορά αφορά το κόστος του παγίου του τηλεφωνικού αριθμού ανά μήνα και απαιτεί εφάπαξ πληρωμή των παγίων για 12 μήνες.
Ισχύουν όροι και προϋποθέσεις στο www.supervoice.eu



σμια αβεβαιότητα χωρίς να υποβαθμίζει το βιοτικό της επίπεδο·

- διαθέτει **επινοητικότητα με σχέδιο επιχειρησιακής ετοιμότητας και συνέχειας**, σύστημα πρόβλεψης και παρακολούθησης των κινδύνων, με δομές (υποδομή και ανωδομή) σχεδιασμένες ώστε να αντέχουν σε οικονομικούς και φυσικούς κραδασμούς·
- διακρίνεται από **συνεκτικότητα στην υγειονομική φροντίδα** και ταχύτητα ανταπόκρισης των υπηρεσιών έκτακτης ανάγκης, παρέχοντας πρόσβαση και περιορίζοντας τις απώλειες με τα αντανakλαστικά της να είναι σε εγρήγορση (χαρακτηριστικό είναι ότι παρουσιάζει ένα από τα χαμηλότερα ποσοστά ημερήσιων κρουσμάτων της πανδημίας Covid-19 σε σχέση με άλλες αστικές περιοχές)·
- προάγει την **καινοτόμα μάθηση με τεχνολογική διαφοροποίηση** από άλλες αστικές οικονομίες, επιτυγχάνοντας υψηλό ποσοστό ψηφιακού αλφαριθμητισμού

και πρόσβασης στο διαδίκτυο και ταυτόχρονα χαμηλή κυβερνο-διαπερατότητα σε κακόβουλα λογισμικά·

- εφαρμόζει **σύγχρονη κοινοτική αστυνόμευση**: ανιχνεύεται ότι επιβλέποντας τις κατοικημένες περιοχές σε κλίμακα γειτονιάς, αντισταθμίζεται η έννοια της παγκόσμιας πόλης, οι άνθρωποι αναγνωρίζουν ο ένας τον άλλον, θέλουν να βρίσκονται στην περιοχή και η ασφάλεια αυξάνεται.

Δεν πρόκειται βεβαίως για μια κοινωνία αγέγων ή κάποια εξιδανικευμένη κοινωνική μηχανή. Πρόκειται απλώς για μια πόλη που κατανοεί πώς να χρησιμοποιεί τα φυσικά και τα δομικά περιουσιακά στοιχεία της (πληθυσμό, οικονομική δραστηριότητα, δομημένο περιβάλλον) ως **εργαλεία μεγιστοποίησης της αστικής ασφάλειας** και ανάλογα με τις δυνατότητές της. Και ο βαθμός της συνεκτικής συμπεριφοράς του τοπικού πληθυσμού δείχνει, ότι οι άνθρωποι συνδέονται και συνεργάζονται κάτω από ένα κοινό θέμα συσπείρωσης: το να νιώθουν και να είναι ασφαλείς.

Παραδείσου 29 και Ζαγοράς /
Παράδεισος Αμαρουσίου, 15125
Email: eo.a.sec@gmail.com
Τηλ.: 210 6851086



Satel[®]



Intelligent
security
solutions



Έξυπνα Συστήματα
Ασφαλείας

INTERTECH S.A.
International Technologies

Αφροδίτης 24, 167 77 Ελληνικό
Τηλ. κέντρο: 210 96 92 300
satelsales@intertech.gr
www.intertech.gr

Συμπεράσματα

Από τα προεκτεθέντα γίνεται φανερό, ότι οι υψηλότερες οικονομικές επιδόσεις σχετίζονται με τη μεγαλύτερη λογοδοσία, που σχετίζεται με τον καλύτερο σχεδιασμό, που σχετίζεται με την μεγαλύτερη ετοιμότητα, που σχετίζεται με την αστική ασφάλεια. Ακαδημαϊκές μελέτες δείχνουν ότι **ο τρόπος που είναι σχεδιασμένη μια πόλη μπορεί να προλάβει την εγκληματικότητα**: από την οικοδόμηση **ασφαλέστερων κτιρίων** έως την ανάπτυξη της κοινωνικής αλλά και της **κυβερνο-εμπιστοσύνης** μεταξύ των εμπλεκόμενων μερών που ανταλλάσσουν πληροφορίες. Για παράδειγμα, οι συμμετοχικές διαδικασίες, όπως η δημόσια διαβούλευση των πολιτών για τη διάθεση του προϋπολογισμού σε έργα ή δράσεις με κριτήριο κατανομή τις ανάγκες προστασίας, συμβάλλουν περισσότερο στην ευαισθητοποίηση και την ενίσχυση της υπευθυνότητάς τους απέναντι στις τοπικές υποθέσεις. Ο **κοινός σκοπός της ασφάλειας** τους δίνει έναν ισχυρότερο λόγο να αναπτύξουν μια ανταποδοτική σχέση με τη μητροπολιτική διοίκηση και την επιχειρησιακή ετοιμότητα που χρειάζονται σε ενδεχόμενες εγκληματικές, περιβαλλοντικές, ψηφιακές και υγειονομικές απειλές. Άρα, η διαφάνεια είναι εξίσου σημαντική με το

κατά κεφαλήν εισόδημα. Διότι ελλείψει λογοδοσίας, όσοι είναι επιφορτισμένοι με την παροχή υπηρεσιών ασφάλειας αντιμετωπίζουν μεγαλύτερους πειρασμούς να τη θυσιάσουν για τα δικά τους ιδιωτικά συμφέροντα και οι απλοί πολίτες είναι λιγότερο πρόθυμοι να συμμετάσχουν ακόμη και σε καλοπροαίρετες προσπάθειες για την ενίσχυση της προστασίας τους.

Άλλωστε, η έντιμη κυβέρνηση δεν χρειάζεται να είναι δαπανηρή: για αρκετά χρόνια, η Γαλλία και τα Μπαρμπέντος είχαν παρόμοιες και σχετικά καλές βαθμολογίες στο Δείκτη Αντίληψης Διαφθοράς της Διεθνούς Διαφάνειας, αλλά το κατά κεφαλήν ΑΕΠ των δεύτερων είναι μικρότερο από το ήμισυ της πρώτης...

Θα λέγαμε, συγκεφαλαιωτικά, ότι **μια megacity δεν είναι απλώς ανθεκτική (resilient)** για τον εαυτό της και τους κατοίκους της, αλλά ότι εξελίσσεται ως μια **αυτοδύναμη και αξιόπιστη (self-reliant) περίβολος**, δηλαδή σταδιακά ικανή να βοηθά και άλλες περιοχές. Μια υπολογίσιμη περιφερειακή δύναμη που δεν απειλείται με μεταβολή ισχύος από εξωτερικές αλλαγές, όπου και δεν μπορεί να ελέγξει. Και από αυτό το σημείο αρχίζει πραγματικά η έννοια της αστικής ασφάλειας (urban safety).

Βιβλιογραφία

- Bouchet, M., Liu, S., Parilla, J. and Kabbani, N., (2018), Global Metro Monitor, Metropolitan Policy Program, Brookings Institute.
- Economist, (2019), Safe Cities Index: Urban Security and Resilience in an Interconnected World, Report.
- European Strategy and Policy Analysis System (ESPAS), (2015), Global Trends to 2030: Can the EU meet challenges ahead ? Report.
- Florida, R., (2019), The Real Powerhouses That Drive the World's Economy, Bloomberg City Lab.
- Ghosh, I., (2019), Ranked: The Megaregions Driving the Global Economy, Data Visualization, Visual Capitalist.
- Gottmann, J., (1957), Megalopolis. The Urbanized Northeastern seaboard of the United States, New York: The Twentieth Century Fund.
- Khanna, P., (2016), Connectography: Mapping the Future of Global Civilization, New York: Random House.
- McGrath, B., and Pickett, S.T.A., (2011), The Metacity: A Conceptual Framework for Integrating Ecology and Urban Design, Challenges, 2, 55-72.
- NASA Earth Observatory, (2015), The World's Largest Urban Area, Satellite Data.
- National Oceanic and Atmospheric Administration (NOAA), (2020), Megacities, Global Monitoring - Data Visualization.
- Oxford Economics, (2017), Cities and Regions in the Global Economy, Analysis.
- Retter, L., Frinking, E., Hoorens, S., Lynch, A., Nederveen, F., and Phillips, W., (2020), Relationships between the economy and national security: Analysis and considerations for economic security policy in the Netherlands, RAND Europe.
- Tokyo Metropolitan Government, (2020), Assessment.
- United Nations, Department of Economic and Social Affairs, Population Division, (2018), The World's Cities in 2018 - Data Booklet (ST/ESA/ SER.A/417).
- United Nations Habitat, (2006), Urbanization: Mega & Metacities, New City States? State of the World's Cities 2006/7, New York.
- Zukrowska, K., (2020), The Link Between Economics, Stability and Security in a Transforming Economy, Institute of Development and Strategic Studies, Warsaw.

Το Νέο **securitymanager.gr** είναι γεγονός
Με Ανανεωμένο Σχεδιασμό, Φιλικό στη Χρήση
...και πάντα με το πιο Πλούσιο Περιεχόμενο!

Νέα της Αγοράς

Αναφορές

Απόψεις

Λύσεις

Συνεντεύξεις



Εξελίξεις

Αναλύσεις

Ρεπορτάζ

Case Studies

Παρουσιάσεις

- Management Υπηρεσίες Εκπαίδευση Τεχνολογία Αγορά
- Video Surveillance Intrusion Alarm Access Control
- Fire Safety Smart Home Drones

Το Σημείο Αναφοράς και στην Ηλεκτρονική Ενημέρωση
για την Ασφάλεια



“Διαχείριση Ποιότητας”... μια Σταθερά!



Σε πρώτη φάση αναφέροντας τον όρο ‘διαχείριση’ ή ‘μánaτζμεντ καταλήγουμε σε μια ατέρμονη διαδικασία των βασικών λειτουργιών της Ηγεσίας, της Οργάνωσης, του Σχεδιασμού και του Ελέγχου.

Σε δεύτερη φάση ο ορισμός της ποιότητας ποικίλει, χωρίς αναπόφευκτα να καταλήγει η συζήτηση ότι κάποιος ορισμός είναι σωστός και κάποιος είναι λάθος (σημαντική εδώ είναι η αναφορά στη διαφορετική οπτική γωνία που ο κάθε επαγγελματίας/επιστήμονας ορίζει την ποιότητα).

Κάτι που βρίσκει σύμφωνα όλα τα μέρη, είναι ότι η **έννοια της ποιότητας** είναι ‘ζωντανή’ και ατέρμονα μεταβάλλεται. Επίσης, χαρακτηριστική είναι η εξέλιξη του όρου της ποιότητας ξεκινώντας από τη σύνδεση και το χαρακτηρισμό ενός προϊόντος στη δεκαετία του 50-60 μέχρι τη μετεξέλιξη της σήμερα ως έννοια που έχει να κάνει με διαδικασίες διοίκησης καθιστώντας αυτές σημαντικές, ώστε ένας οργανισμός να έχει σημαντικό προβάδισμα στο ανταγωνιστικό περιβάλλον.

Κάποιοι βασικοί ορισμοί που παρουσιάζονται έντονα στη βιβλιογραφία είναι:

- Ποιότητα σημαίνει **να ταιριάζει το προϊόν ή η υπηρεσία** στον σκοπό ή τη χρήση για την οποία προορίζεται (Juran, 1950).

- Ποιότητα σε ένα προϊόν ή σε μια υπηρεσία δεν είναι αυτό που βάζει ο προμηθευτής. Είναι **αυτό που παίρνει ο πελάτης** και για το οποίο είναι διατεθειμένος να πληρώσει. Αυτό που προσδίδει ποιότητα σε ένα προϊόν δεν είναι ούτε η δυσκολία κατασκευής του ούτε το μεγάλο κόστος του, όπως πιστεύουν συνήθως οι κατασκευαστές. Οι πελάτες πληρώνουν μόνο γι’ αυτό που είναι χρήσιμο σ’ αυτούς και προσφέρει σε αυτούς αξία. Τίποτε άλλο δεν αποτελεί ‘ποιότητα’ (Drucker, 1985).
- Ποιότητα είναι η **φιλοσοφία εργασίας** μέσα από την οποία μπορούμε να πραγματοποιήσουμε το όραμα μας και να εκπληρώσουμε την αποστολή μας με τρόπο πλήρως συμβατό με τις αξίες μας και υποστηριζόμενο από αυτές (Alderman, 1996).

Ο κομβικός ρόλος της ποιότητας στις υπηρεσίες ασφάλειας

Αν θεωρηθεί ως δεδομένο το πιο πάνω θα λέγαμε ότι οι οργανισμοί που αναγνωρίζουν τη μεγάλη σημασία της ποιότη-

τας θα είναι αυτοί που θα έχουν ένα σημαντικό βήμα στην αγορά εργασίας. Σε ένα τομέα όπως είναι η **παροχή υπηρεσιών ασφαλείας όπου ο ανταγωνισμός είναι ένα από τα κύρια θέματα που αντιμετωπίζει ο κλάδος**, χωρίς αυτό να είναι πάντα αναπόφευκτα κακό... η παροχή ποιοτικών υπηρεσιών ασφαλείας σύμφωνα με ένα δομημένο σύστημα εσωτερικού ποιοτικού ελέγχου, επιθεωρήσεων, διαδικασιών διοίκησης σε πρότυπα για παράδειγμα ISO 9001, με ασφάλεια των πληροφορικών συστημάτων σύμφωνα με πρότυπα για παράδειγμα ISO 27001, με προστασία και επεξεργασία των προσωπικών δεδομένων σύμφωνα με τους ανάλογους κανονισμούς αποδεικνύεται μια σταθερά.

Μια σταθερά που καθιστά τον οργανισμό παροχής υπηρεσιών ασφαλείας **ανθεκτικό** ακόμα και σε μια πανδημία. Ο Covid-19 ξέβρασε διάφορα προβλήματα όπως έφερε και πολλές «αναγκαιότητες» όπως η απομακρυσμένη εργασία (για το διοικητικό προσωπικό), προστασία των προσωπικών δεδομένων των πελατών και του προσωπικού.

Ως τομέας έχουμε να προστατεύσουμε την ανθρώπινη ζωή, περιουσιακά στοιχεία και άλλα, αναπόφευκτα πρέπει πλέον να μιλάμε για ένα **καταρτισμένο και ορθά προετοιμασμένο κλάδο**, έτοιμο να ανταπεξέλθει σε πολυσύνθετους κινδύνους.

Σύμφωνα με την τελευταία αναφορά της **Europol**, λόγω Covid-19 οι κυβερνοεπιθέσεις με χαρακτηριστικά τις επιθέσεις **“phishing”** μέσω ηλεκτρονικού ταχυδρομείου αυνανένεται να ανεβούν αισθητά. Θεωρούμε ως δεδομένο ότι λόγω της φύσης της δουλειάς μας ένα γραφείο παροχής υπηρεσιών ασφαλείας αποθηκεύει και διαφυλάσσει διάφορων τύπων προσωπικά δεδομένα, από τα δεδομένα του προσωπικού του, των πελατών του, των συνεργατών του και η λίστα μπορεί να μεγαλώσει περισσότερο. Άρα εδώ τίθενται σημαντικά θέματα όπως η κατάλληλη διοικητική οργάνωση της εταιρείας σύμφωνα με τα πλαίσια του GDPR, η προστασία του πληροφορικού δικτύου με τα ανάλογα συστήματα ή ενημέρωση του προσωπικού ώστε να καταλήξουμε σε ικανοποιητικό επίπεδο ‘επίγνωσης’ των κινδύνων που μπορεί να αντιμετωπίσουν αν ανοίξουν ένα **«μολυσμένο email»**, για παράδειγμα, και πως να το αποφύγουν.

Τα «standards» ποιότητας και η κατοχύρωση!

Όπως αναφέρθηκε και πιο πάνω η **ανθεκτικότητα είναι το ζητούμενο**. Τα «standards» ορίζονται ως οι δράσεις που επικεντρώνονται όχι αποκλειστικά και μόνο στην «απλή» απόδοση αλλά στην ποιοτική απόδοση των υπηρεσιών ασφα-



λείας. Στόχος είναι η ολιστική προσέγγιση, δημιουργώντας έτσι παράλληλα με το αίσθημα ασφάλειας, μια ανεμπόδιστη «εμπειρία» μέσω των υπηρεσιών παροχής ασφαλείας. Τα «standards» ποιότητας μετρούνται! Οπότε αναπόφευκτα δημιουργούν μια ξεκάθαρη εικόνα της κατάστασης. Οι δείκτες απόδοσης (Key Performance Indicators) με τους οποίους υπάρχει η πλήρης απεικόνιση ώστε να ανευρεθεί το θέμα (Εύρημα) και να διορθωθεί (Διορθωτική Ενέργεια): Στόχος σε αυτό τον αέναο κύκλο από διαδικασίες, ελέγχους και παρατηρήσεις είναι η συνεχόμενη βελτίωση!

Τρόποι κατοχύρωσης της ποιότητας είναι τα ανάλογα συστήματα επικεντρωμένα στις ανάλογες απαιτήσεις «ποιότητας στην εργασία», «ασφάλειας και υγείας», «πληροφορικής ασφάλειας», «εταιρικής κοινωνικής ευθύνης» και φυσικά τα πιο επίκαιρα που έχουν να κάνουν με τον περιορισμό εξάπλωσης πανδημίας, καθώς επίσης και πολλά άλλα. Σαφέστατα, βασικά βήματα είναι η ενημέρωση του προσωπικού αναφορικά με τις διαδικασίες, τις απαιτήσεις των προτύπων ώστε να επιτευχθεί η συνεργασία και η δημιουργία των ανάλογων εγχειριδίων, πολιτικών και εγγράφων. Η συνεργασία μεταξύ των τμημάτων, του προσωπικού του οργανισμού και της διοίκησης παίζει εξίσου σημαντικό ρόλο. Στα προαναφερθέν «πρότυπα» ποιότητας οι αναφορές (reports), η ορθή συμπλήρωση των ανάλογων εγγράφων, η χρησιμοποίηση των πάντα ανανεωμένων εγγράφων είναι κάποιες από τις παραμέτρους της βάσης του τι ορίζεται ως εφαρμογή ‘standards’ ποιότητας. Άρα εκπαίδευση = επίγνωση = συνεργασία = απόδοση = ανταγωνιστικό πλεονέκτημα!

Έχοντας διασφαλίσει σε διοικητικό και επιχειρησιακό επίπεδο την ποιότητα των παρεχόμενων υπηρεσιών μέσω των ανάλογων προτύπων και διαδικασιών, ο οργανισμός αποκτά ανθεκτικότητα. Μέσω της ανθεκτικότητας κλειδώνεται έμπρακτα και ο απαιτούμενος επαγγελματικός δεσμός μεταξύ οργανισμού και προσωπικού/προσωπικού και οργανισμού.



Διοίκηση διαφορετικότητας σε ιδιωτικές υπηρεσίες ασφαλείας

Η διαχείριση των δύο φύλων



Στη διοίκηση διαφορετικότητας σημαντική είναι η κατανόηση των διαφορών ανάμεσα στα μέλη μιας επιχείρησης, η σωστή διαχείριση τους, η ίδια εκπαίδευση και ευκαιρίες εξέλιξης. Οι διαφορές αυτές αφορούν χαρακτηριστικά όπως φύλο, ηλικία, εθνικότητα, θρησκεία, πολιτικές πεποιθήσεις, πολιτισμικές διαφορές κ.ά.

Ο τομέας της ασφάλειας ήταν μέχρι πρότινος ανδροκρατούμενος, όμως τα τελευταία χρόνια η παρουσία των γυναικών στον τομέα είναι δυναμική. Στην Ελλάδα με τους δείκτες εγκληματικότητας να είναι στα ύψη και τις δημόσιες δυνάμεις με ελλείψεις σε ανθρώπινο δυναμικό και οικονομικούς πόρους, δόθηκε χώρος στις ΙΕΠΥΑ να ανθίσουν και στις θέσεις εργασίας σε αυτές να αυξηθούν. Παρόλο που οι εργαζόμενοι έχουν την ίδια άδεια εργασίας, διαφοροποιούνται σε πολλούς τομείς όπως φύλο, ηλικία, μόρφωση, εκπαίδευση, σωματική διάπλαση κ.ά.

Άνδρες και γυναίκες στο Security

Οι γυναίκες έχουν να αντιμετωπίσουν στερεότυπα στο χώρο της ασφάλειας. Για αυτό **πρέπει πρώτα οι ίδιες να κατανοήσουν πως ο κλάδος είναι και δική τους υπόθεση**. Καθώς λοιπόν πλέον αριθμητικά δεν υστερούν έναντι των ανδρών, το πρώτο βήμα που πρέπει να γίνει είναι να έχουν

περισσότερες γυναίκες το ρόλο του εκπαιδευτή του αντικειμένου. Έτσι μελλοντικά θα αναλάβουν και νευραλγικές θέσεις στο χώρο.

Η λέξη ασφάλεια είναι συνυφασμένη με τον άνδρα. Στο άκουσμα της λέξης “security” δημιουργείται η εικόνα ενός μυώδη άνδρα με αρρενωπά χαρακτηριστικά και αυστηρό βλέμμα. Η αλήθεια είναι ότι η ασφάλεια δε χρειάζεται μόνο αυτό. Άλλωστε ιστορικά, **η γυναίκα έχει δείξει ότι μπορεί να σταθεί στην πρώτη γραμμή, ακόμη και σε συνθήκες πολέμου.**

Η άδεια εργασίας του προσωπικού ασφαλείας και η εκπαίδευση έγιναν υποχρεωτικές και αυτό ώθησε στην αύξηση του ποσοστού των γυναικών που εργάζονται ως security. Σημαντικό είναι πως οι γυναίκες μπαίνουν στο επάγγελμα συνειδητοποιημένες και δεν το βλέπουν σαν κάτι ευκαιρικό. Έτσι πολλές γυναίκες μετά την είσοδο στο επάγγελμα άρχισαν να φροντίζουν για τη φυσική τους κατάσταση και

την επέκταση των γνώσεων τους. Η γυναίκα έχει κάποια **έμφυτα χαρακτηριστικά που είναι σημαντικότερα για τον κλάδο:**

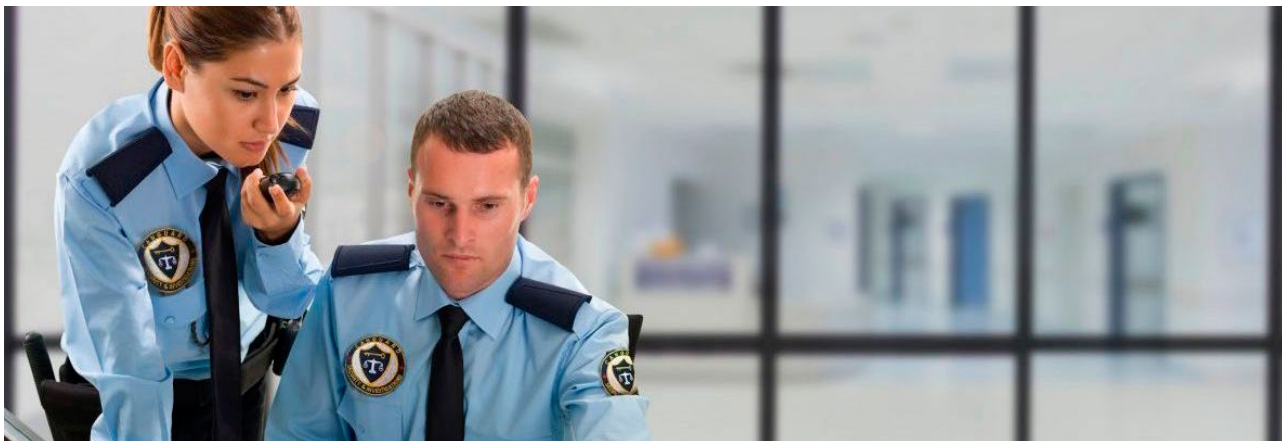
- Αναγνωρίζουν τον κίνδυνο από τα πολύ πρώιμα σημεία του, ικανότητα που έχουν έμφυτη για να προστατεύσουν τα (νεογέννητα) παιδιά τους με τη λεγόμενη έκτη αίσθηση. Είναι δηλαδή πιο παρατηρητικές από τους άνδρες.
- Ιστορικά έχουν αποδείξει ότι μπορούν να διοικήσουν και να προστατεύσουν την οικογένειά τους. Δεν ήταν λίγες οι χήρες πολέμου που στάθηκαν μάνα και πατέρας ακόμη και σε πολύτεκνες οικογένειες.
- Είναι καχύποπτες και δύσκολα θα κερδίζουν την εμπιστοσύνη τους.
- Κερδίζουν την εμπιστοσύνη ευκολότερα. Μια γυναίκα είναι ή απλά φαίνεται πιο στοργική από έναν άνδρα και έτσι ο εκάστοτε πελάτης θα μπορούσε να δεθεί ευκολότερα μαζί της.
- Μπορούν να προσαρμοστούν ευκολότερα σε νέο περιβάλλον αφού είναι πιο δεκτικές και ομιλητικές.
- Είναι λιγότερο επιθετικές και αφήνουν πίσω το "εγώ" τους σε διάφορες καταστάσεις. Έτσι μπορούν ευκολότερα να αποκλιμακώσουν μια ένταση σε σχέση με έναν άνδρα φύλακα που λόγω του αυξημένου εγωισμού του μπορεί να δημιουργήσει ένταση ακόμα και εκεί που δεν υπάρχει. Αυτό τις κάνει καλύτερες στις διαπραγματεύσεις.
- Διαβάζουν καλύτερα τη γλώσσά του σώματος και έτσι καταλαβαίνουν γρηγορότερα έναν επίδοξο ληστή.
- Ένα άλλο σημαντικό στοιχείο των γυναικών στις security είναι η συνεχής επαγρύπνησή τους λόγω του ότι έχουν πιο ανεπτυγμένο το αίσθημα της αυτοσυντήρησης σε σχέση με τον άνδρα. Αυτό στην ασφάλεια είναι πολύ σημαντικό προσόν αφού όταν χρειαστεί να επέμβουν θα είναι έτοιμες. Ο εφησυχασμός είναι ένας από τους μεγα-

λύτερους εχθρούς των επαγγελματιών της ασφάλειας.

- Μεγάλο ενδιαφέρον παρουσιάζει η περίπτωση των γυναικών σωματοφυλάκων. Οι γυναίκες ειδικά όταν εργάζονται με πολιτική αμφίεση δε γίνονται εύκολα αντιληπτές διότι το μυαλό του υποψήφιου επιτιθέμενου δεν αντιλαμβάνεται εύκολα ότι οι γυναίκες που περιστοιχίζουν ένα επίσημο είναι σωματοφύλακες και όχι γραμματείς κτλ. Έναν σωματώδη άνδρα με γυαλιά ηλίου και αυστηρό βλέμμα θα τον καταλάβαινε αμέσως. Τέλος, είναι σύνηθες, γυναίκες VIP να προσλαμβάνουν γυναίκες σωματοφύλακες διότι δένονται ευκολότερα μαζί τους και μπορούν να τους ανοιχτούν πιο εύκολα!

Από την άλλη, **ο άνδρας, έχει τα δικά του δυνατά χαρτιά** όσον αφορά στο αντικείμενο:

- Κυριότερο προτέρημα των ανδρών είναι η φυσική τους δύναμη. Ο άνδρας γεννιέται ισχυρότερος μυϊκά και ψυχολότερος.
- Είναι πιο προστατευτικοί. Υπάρχει η γνώμη ότι σταδιοδρομούν στο επάγγελμα, άτομα που σε μικρή ηλικία προστάτευαν τα αδύναμα παιδιά.
- Είναι τολμηροί. Ένα χαρακτηριστικό της αρρενωπότητας είναι και η τόλμη άρα όταν χρειαστεί φροντίζει να το δείχνει. Έτσι είναι ευκολότερο για αυτούς να εργαστούν νύχτα και μοναχικά.
- Εμπνέουν περισσότερο φόβο. Αν και αυτό έχει να κάνει με την εμφάνιση και την προσωπικότητα του καθενός είναι σίγουρο ότι η παρουσία ενός άνδρα σε ένα φυλασόμενο μέρος ή πρόσωπο θα ήταν μεγαλύτερος αποτρεπτικός παράγοντας για κάποιο επίδοξο ληστή, από τη γυναικεία παρουσία.
- Είναι ψυχραιμότεροι. Την ώρα που θα χρειαστεί να επέμβει, διαχειρίζεται καλύτερα την αδρεναλίνη και το



φόβο ενώ η γυναίκα δυσκολεύεται να ενεργήσει όταν οι καρδιακοί παλμοί ανέβουν.

- Είναι λιγότερο ανταγωνιστικοί μεταξύ τους σε σχέση με τις γυναίκες, έτσι δημιουργούνται λιγότερες εντάσεις μεταξύ τους.

Υπάρχουν όμως και άλλες βασικές διαφορές που αφορούν τον τρόπο αντίδρασης των δυο φύλων και μάλιστα επιστημονικά τεκμηριωμένες.

Μια μεγάλη διαφορά είναι στη **διαχείριση του θυμού**. Η Legato, μια ειδικός στην κατά φύλο ιατρική, υποστηρίζει ότι η γυναίκα αργεί περισσότερο να ξεπεράσει το θυμό της απ' ό,τι ο άνδρας. Όταν ο άνθρωπος θυμώνει ο εγκέφαλος απελευθερώνει ορμόνες στο αίμα και αυτά τα επίπεδα ορμονών στη γυναίκα, αργούν να επανέλθουν στο φυσιολογικό. Άρα ακόμα και αν το θέμα έχει λήξει, η γυναίκα θα αργήσει να ξεπεράσει το θυμό της.

Επίσης διαφορά υπάρχει στη **διαχείριση του άγχους**. Οι γυναίκες είναι επιστημονικά τεκμηριωμένο ότι αγχώνονται περισσότερο από τους άνδρες και για διαφορετικές αφορμές. Αυτό οφείλεται σε ορμονικές και βιολογικές διαφορές. Στη διάρκεια ενός στρεσογόνου γεγονότος, τα οιστρογόνα ενεργοποιούν ένα ευρύτερο πεδίο νευρώνων στο μπροστινό μέρος του εγκεφάλου. Τα επίπεδα οιστρογόνων στις γυναίκες, είναι υψηλότερα και τυγχάνει να έχουν περισσότερη φαιά ουσία στο τμήμα του εγκεφάλου που ρυθμίζει το άγχος. Έτσι ένα γεγονός που θα τις ταράξει, θα το βιώσουν εντονότερα. Όταν αγχώνονται οι γυναίκες παράγουν περισσότερη κορτιζόλη από τους άντρες και για περισσότερη ώρα. Οι γυναίκες διαθέτουν την προγεστερόνη, η οποία εμποδίζει την απενεργοποίηση της κορτιζόλης. Η κορτιζόλη με τη σειρά της συμβάλλει στη λειτουργία της μνήμης. Αυτά τα υψηλά επίπεδα σημαίνουν ότι οι γυναίκες όχι μόνο ζουν εντονότερα ένα δυσάρεστο συμβάν, αλλά το θυμούνται και περισσότερο καιρό. Αντιθέτως, η αρσενική γεννητική ορμόνη, η τεστοστερόνη, εμποδίζει τη δράση της κορτιζόλης. Έτσι οι άνδρες ξεχνούν ευκολότερα τις δυσάρεστες καταστάσεις. Οι άνδρες όταν αγχώνονται κλείνουν στον εαυτό τους και δύσκολα θα εκφράσουν το συναίσθημα τους ενώ οι γυναίκες, γεμάτες από συναισθήματα, θέλουν να τα εξωτερικεύσουν για να νιώσουν καλύτερα και μάλιστα όταν το κάνουν, η περιγραφή του δυσάρεστου γεγονότος γίνεται με έμφαση. Οι άνδρες από την άλλη, όταν πάρουν την απόφαση να μιλήσουν είναι για να συμβουλευτούν κάποιο έμπιστο άτομο.

Η Legato υποστηρίζει πως η γυναίκα **μπορεί να ανακαλέσει στη μνήμη της ένα παλιό γεγονός σε ανύποπτη στιγμή**. Αυτό συμβαίνει γιατί υπάρχει περισσότερη παρο-



χή αίματος σε ορισμένα σημεία του εγκεφάλου. Η γυναίκα επίσης έχει μεγαλύτερη συγκέντρωση σε οιστρογόνα, μια ομάδα ορμονών που θωρακίζει τη λειτουργία του εγκεφάλου και είναι υπεύθυνα για την επισκευή και τη λειτουργία των νευρώνων.

Υποστηρίζει επίσης πως σε μια δυσάρεστη κατάσταση, λόγω του ότι η γυναίκα γεμίζει από συναίσθημα, δε μπορεί να συμπεριφερθεί ψύχραιμα και να την αντιμετωπίσει εύκολα, ενώ ο άνδρας σκέφτεται πιο λογικά και ψύχραιμα. Αυτό συμβαίνει, σύμφωνα με τα αποτελέσματα της μελέτης που δημοσιεύονται στην επιστημονική επιθεώρηση «Neuroscience and Biobehavioral Reviews», διότι οι γυναίκες έχουν πιο ανεπτυγμένη τη δομή του εγκεφάλου που ονομάζεται αριστερός μετωπιαίος πόλος (λοβός). Ο εγκέφαλος των ανδρών έχει σχεδιαστεί για να εκτελεί καλύτερα ενιαία καθήκοντα δηλαδή ένα συγκεκριμένο πράγμα ενώ των γυναικών είναι φτιαγμένος για πολλαπλές εργασίες. Έτσι η γυναίκα μπορεί να ασχολείται με πολλά πράγματα ταυτόχρονα (multitasking).

Η θέση του manager

Ένας σύγχρονος security manager, οφείλει να βλέπει και να κατανοεί τις διαφορές των δυο φύλων, να τις σέβεται και να διανέμει αρμοδιότητες δίκαια δίνοντας ευκαιρίες σε όλους. Ο manager οφείλει να μη διαχωρίζει τα δύο φύλα αλλά να τα καθοδηγήσει έτσι ώστε να συνεργάζονται και να αλληλοσυμπληρώνονται. Εφόσον μάθουν όλοι να σέβονται την ιεραρχία, είναι πλέον υποχρέωση του η εξασφάλιση του σεβασμού των υφισταμένων του και η δημιουργία ομαδικού πνεύματος και αλτρουισμού. Ο υπάλληλος κρίνεται βάση προσόντων έτσι το φύλο θα πρέπει να λαμβάνεται υπόψιν μόνο προς γνώση και προσαρμογή σε ειδικές καταστάσεις. Οι σύγχρονες απειλές είναι διαφορετικές και με τη συνδρομή της τεχνολογίας έχει αλλάξει η αντιμετώπιση τους στην οποία όλοι πρέπει να έχουν ενεργό ρόλο.

Η online έκδοση του μοναδικού περιοδικού στην Ελλάδα για το **Business IT** και την **Ασφάλεια Πληροφοριών**



- Αναλύσεις για τις ψηφιακές απειλές
- Τεχνολογίες Προστασίας
- Στρατηγικές & Πολιτικές
- Λύσεις Διαχείρισης IT
- Νέα της αγοράς

- Τάσεις
- Απόψεις
- Αναφορές
- Παρουσιάσεις
- Συνεντεύξεις
- Ρεπορτάζ

itsecuritypro.gr

Με ανανεωμένο σχεδιασμό και πλούσιο περιεχόμενο αποτελεί
κορυφαία πηγή ενημέρωσης για τους επαγγελματίες IT

Στο **www.itsecuritypro.gr** υπάρχουν σε μορφή **e-book** τεύχη των περιοδικών του
IT Security Professional, όπου μπορείτε **να τα διαβάσετε online**
όπως ακριβώς εκδόθηκαν σε έντυπη μορφή.

Διαχείριση Κρίσης στα νερά του Ινδικού Ωκεανού

Μια βιωματική μελέτη περίπτωσης



Ένα πραγματικό περιστατικό παρατιθέμενο σε πρώτο πρόσωπο, αφού ο συγγραφέας αναδείχθηκε σε ένα από τους κεντρικούς παίκτες, της κατάστασης. Χρήσιμο ως μελέτη περίπτωσης, σε σχετικές εκπαιδεύσεις.

Έπρεπε να συνοδέψω ένα bulkcarrier (φορτηγό πλοίο) το οποίο κατευθυνόταν από την Κίνα προς το Ισραήλ με στάση στη Sri Lanka για να μας παραλάβει. Η ομάδα μου αποτελούνταν από 4 μέλη: εμένα ως team leader, δύο Έλληνες, και έναν από την Sri Lanka. Μάθαμε ότι το πλοίο είχε ως πλήρωμα Φιλιππινέζους που ταξίδευαν για πρώτη φορά στην επικίνδυνη ζώνη του Ινδικού Ωκεανού.

Η αποστολή μας ήταν να περάσουμε με ασφάλεια το πλοίο από τα επικίνδυνα νερά του Ινδικού Ωκεανού (HRA - high risk area) και **ειδικότερα από τις ακτές της Σομαλίας**, όπου και διεξάγονται πειρατείες τα τελευταία χρόνια.

Πλησιάζοντας στο βαπόρι, είδα αρκετό κόσμο να μας περιμένει επάνω στο κατάστρωμα. Η ανεμόσκαλα έπεσε και ανεβήκαμε όλη η ομάδα με τον εξοπλισμό. Χαιρέτησα το πλήρωμα αντιλαμβανόμενος ανησυχία, αγωνία και φόβο. Προσπάθησα να τους καθησυχάσω λέγοντάς τους: **«ο καιρός είναι θαυμάσιος για μια υπέροχη κρουαζιέρα»**.

Ξεκινήσαμε **συμβούλιο** με τη συμμετοχή του καπετάνιου, του υποπλοίαρχου, του πρώτου και του δεύτερου μηχανικού. Εκεί τους ανέλυσα την κατάσταση της περιοχής, το πως πρέπει να οχυρώσουμε το βαπόρι, το πως πρέπει να κινείται το πλήρωμα καθώς και τις **καταστάσεις εκτάκτου ανάγκης**. Αμέσως μετά ξεκινήσαμε να βάζουμε συρματοπλέγμα γύρω από το βαπόρι. Στη συνέχεια τοποθετήσαμε μάνικες οι οποίες ρίχνουν νερό με υψηλή πίεση και ρίξαμε σχοινιά από το πίσω μέρος του πλοίου στη θάλασσα, ούτως ώστε να μπερδευτεί η προπέλα οποιουδήποτε σκάφους πλησιάσει κοντά μας. Μετά κατευθυνθήκαμε στο εσωτερικό του πλοίου όπου και **φτιάξαμε δωμάτιο ασφαλείας** με ενισχυμένη πόρτα, φάρμακα, τρόφιμα, νερό, επικοινωνίες σε περίπτωση που δεν θα μπορούσαμε να αποτρέψουμε την επίθεση ώστε να είμαστε ασφαλείς και να επικοινωνήσουμε με φίλιες δυνάμεις για βοήθεια. Οι μέρες κυλούσαν ομαλά μέχρι την στιγμή που αφήσαμε το convoy και τα πολεμικά συνοδείας



και κατευθυνθήκαμε **προς τα στενά του Bab El Mandeb** για να μπούμε στην Ερυθρά Θάλασσα όπου αυτό είναι και το πιο επικίνδυνο τμήμα. Ο καιρός ήταν θαυμάσιος κάτι που με ανησυχεί πάντα, διότι **διευκολύνει την επίθεση**. Γι' αυτόν τον λόγο είχα σε ετοιμότητα όλη την ομάδα στη γέφυρα και αναπτυγμένη δεξιά και αριστερά του πλοίου.

Κατά το μεσημεράκι **διέκρινα με τα κιάλια κάποια μικρά σκάφη στον ορίζοντα**. Ανέπτυξα την ομάδα στις θέσεις της και κάλεσα τον πλοίαρχο στη γέφυρα.

Σε απόσταση περίπου 6 μιλίων υπήρχαν τέσσερα ταχύπλοα σκάφη σαν και αυτά που χρησιμοποιούνται σε επιθέσεις. Συμβούλεψα τον καπετάνιο να στρίψει το πλοίο αριστερά για να τους έχω από μια μεριά καθώς έδειχναν ότι μας περίμεναν. Η απάντηση του ήταν ότι είναι ψαράδες και δεν συντρέχει κανένας λόγος αλλαγής πορείας. Επέμεινα **λέγοντάς τους πως οι πειρατές είναι ψαράδες και οι ψαράδες πειρατές**. Εκείνος επέμεινε στο ότι πρέπει να παραμείνει στην πορεία του και εφόσον δεν μου έδινε περιθώρια, του ζήτησα να απομακρύνει όλο το πλήρωμα στο δωμάτιο ασφαλείας, να θέσει το πλοίο σε έκτακτη ανάγκη και να επικοινωνήσει με τις αρχές. Ο πλοίαρχος μου αρνήθηκε λέγοντάς μου ότι δεν συντρέχει λόγος να γίνουν όλα αυτά επειδή βρισκόμαστε στα νερά της Υεμένης και όχι της Σομαλίας. Τον ενημέρωσα πως **η Υεμένη δεν επιτρέπει πρόσβαση σε πολεμικά πλοία και έτσι οι πειρατές κάνουν τη δουλειά τους ανενόχλητοι**. Εκείνος επέμεινε στην άποψή του. Τότε και καθώς έβλεπα ύποπτες κινήσεις, ζήτησα να χτυπήσει γενικός συναγερμός με δική μου ευθύνη και να ενημερωθούν η εταιρεία, το NATO, το UKMT0 και το MSCHOA όπως και έγινε.

Βγαίνω στο φτερό της γέφυρας και ρίχνω την πρώτη προειδοποιητική φωτοβολίδα. Εκείνη την ώρα και ενώ η απόστασή μας είναι γύρω στο 1.5 nm διακρίνω το ένα ταχύπλοο με τρία άτομα να κατευθύνεται προς το άλλο και να παίρνει άλλα τέσσερα άτομα. Αμέσως μετά αρχίζει να πλησιάζει με περίπου 25 κόμβους το βαπόρι μας από την αριστερή

πλευρά. Δίνω εντολή **στην ομάδα να κάνει επίδειξη των όπλων καθώς ρίχνω και την δεύτερη προειδοποιητική φωτοβολίδα**, ενώ εκείνοι συνεχίζουν να πλησιάζουν και φροντίζω όλο το πλήρωμα να μπει στο δωμάτιο ασφαλείας. Έχω δώσει εντολή στην ομάδα να με καλύψει ενώ ήδη έχουν φτάσει από κάτω και βλέπω πλέον καθαρά τη σκάλα που χρησιμοποιούν για να ανέβουν στα πλοία, όπλα καθώς και έναν με **Ρουκετοβόλο (RPG)** να με σημαδεύει κρατώντας το με το ένα χέρι, πράγμα που σημαίνει ότι δεν θέλει να με πυροβολήσει παρά μόνο να με τρομοκρατήσει.

Ακούγονται έντονες φωνές από τους πειρατές. Μου φωνάζουν να σταματήσω το πλοίο. Τους δείχνω το όπλο μου τους λέω ότι δεν πρόκειται, για κανένα λόγο, να σταματήσει το πλοίο και **τους καλώ να απομακρυνθούν από την περίμετρό μου, διαφορετικά θα εμπλακούμε όπως ακριβώς απαιτούν οι διεθνείς κανονισμοί**.

Συνεχίζουν επιτακτικά να φωνάζουν να σταματήσω το πλοίο, ενώ ο χειριστής του RPG έχει βάλει και τα δυο του χέρια στο όπλο, πράγμα που σημαίνει πως θα πυροδοτήσει, ενώ παράλληλα από το δεύτερο ταχύπλοο που βρίσκεται πιο μακριά ακούγονται πυροβολισμοί, προφανώς εκφοβισμού μιας και ήταν αρκετά μακριά (πάνω από 500 μέτρα) και εκτός βολής. Υπολογίζω αστραπιαία την κατάσταση όπως το που βρίσκονται τα υπόλοιπα ταχύπλοα, εάν η ομάδα μου είναι καλυμμένη και παράλληλα με καλύπτει και αποφασίζω να προβώ σε προειδοποιητικές βολές. Με μια αστραπιαία κίνηση σηκώνομαι και **πυροβολώ με ψυχραιμία 2 φορές μπροστά από την πλώρη του ταχυπλόου**. Κάτι που προφανώς **δεν περίμεναν οι πειρατές καθώς ξαφνιάστηκαν, φοβήθηκαν και έπεσαν μες το ταχύπλοο για κάλυψη ενώ άρχισαν να απομακρύνονται**.

Έχω αλλάξει θέση και προσπαθώ να απεμπλακώ παρακολουθώντας ταυτόχρονα και τις κινήσεις των τεσσάρων ταχυπλόων. Βρίσκομαι σε συνεχή επικοινωνία με την ομάδα μου ενώ τα ταχύπλοα (2 αριστερά και 2 δεξιά) βρίσκονται στο πίσω μέρος του πλοίου μας καθώς εμείς συνεχίζουμε την πορεία μας. **Δεν δείχνουν πλέον σημάδια νέας επίθεσης**.

Η ομάδα συνεχίζει να παρακολουθεί την δραστηριότητα των ταχυπλόων ενώ εγώ με τον πλοίαρχο ξεκινάμε τη διαδικασία απεμπλοκής: Να δώσουμε αναφορά σε NATO, UKMT0, MSCHOA, την ναυτιλιακή εταιρεία και την εταιρεία ασφαλείας.

Οι βάρδιες συνεχίζονται κανονικά μέχρι και την επόμενη μέρα που θα βγαίναμε εκτός της επικίνδυνης ζώνης, ενώ εγώ έκανα ένα καφέ και βγήκα έξω από τη γέφυρα να κάνω την αυτοκριτική μου την αυτοαξιολόγησή μου και να περιχαρακώσω το "Lesson Learned"...

Νέες λύσεις Διαχείρισης Οχημάτων παρουσίασαν Vector Security και Dahua Technology



Στο επιτυχημένο και μοναδικό για τα ελληνικά δεδομένα event “The track Day” που πραγματοποιήθηκε σε πίστα καρτ στην Αττική, η Vector Security παρουσίασε σε live δοκιμές όλες τις σύγχρονες νέες λύσεις διαχείρισης και ελέγχου πρόσβασης χώρων στάθμευσης και εισόδου parking της Dahua Technology.

Η **Vector Security** μας έχει συνηθίσει σε πρωτοποριακές εκδηλώσεις όπως αυτή που πραγματοποιήθηκε πρόσφατα σε συνεργασία με την ομάδα της Dahua στην Ελλάδα με αφορμή την παρουσίαση αλλά και δοκιμή κάτω από πραγματικές συνθήκες των καμερών για τη διαχείριση οχημάτων. Οι κάμερες των δοκιμών ήταν:

- **Dahua ANPR Parking control (ITC215-PW4I-IRLZF AI 2MP)**
- **Dahua Parking Management (ITC314-PH2A-TF2)**

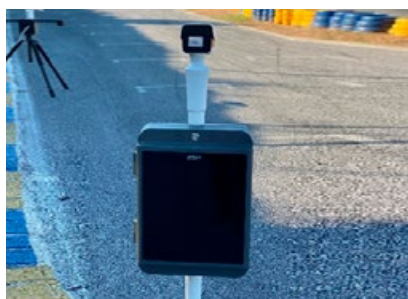
Αρχικά και όπως μας ανέλυσαν οι δυο εισηγητές -**Βασίλης Δέδες (Product Manager για την Vector Security)** και **Γιάννης Χατζής (Dahua Project**

Manager)- οι κάμερες Parking control της Dahua προσφέρουν υψηλό επίπεδο ασφάλειας στον έλεγχο οχημάτων κατά την είσοδο και έξοδο από οποιοδήποτε χώρο. Μία λύση που ήταν ευρέως γνωστή μέχρι τώρα και πλέον έρχεται με αναβαθμισμένες δυνατότητες και **AI λειτουργίες**. Πλέον η διαχείριση ενός χώρου πάρκινγκ, αλλά και της πρόσβασης σε αυτόν γίνεται ευκολότερη μέσω της εγκεκριμένης λίστας οχημάτων (βάσει πινακίδας). Με αυτό τον τρόπο αυτοματοποιείται μία διαδικασία που μέχρι τώρα μπορεί να δημιουργούσε προβλήματα, καθυστερήσεις και μπερδέματα στην καταγραφή της λίστας των εισερχόμενων και εξερχόμενων οχημάτων.

Ενδιαφέρον έχουν επίσης και οι white/black lists όπου μπορούμε να χρησιμοποιήσουμε στους χώρους αυτούς, καθώς με αυτό τον τρόπο δίνουμε ή αποτρέπουμε πρόσβαση σε συγκεκριμένα οχήματα αποφεύγοντας την είσοδο μη εξουσιοδοτημένου οχήματος. Η κάμερα **ITC215-PW4I-IRLZF** εκτός των άλλων, χρησιμοποιεί τον εξελιγμένο **αλγόριθμο AI της Dahua** και μέσω της **τεχνητής νοημοσύνης**, μας δίνει επιπλέον πληροφορίες για τα οχήματα όπως το χρώμα τους, τη μάρκα και τον τύπο οχήματος βάσει μεγέθους (van, φορτηγό, λεωφορείο). Έτσι η αναζήτηση συμβάντων γίνεται πιο γρήγορη κατά 85% χρησιμοποιώντας τα παραπάνω κριτήρια αναζήτησης.



Στην εκδήλωση έδωσαν το παρόν οι Βασίλης Δέδες (Product Manager για την Vector Security) και Γιάννης Χατζής (Dahua Project Manager) - που ήταν και οι δυο εισηγητές των παρουσιάσεων (σχετική φωτογραφία) και άλλα στελέχη των δυο εταιριών όπως οι Μανώλης Μανδαλάκης (Τεχνικός Διευθυντής για την Vector Security), Ηλίας Αθανασόπουλος (Tech expert για την Vector Security), Emma Palova (Dahua Marketing Manager).



Η αποθήκευση της λίστας των πινακίδων μπορεί να γίνει μέσω της on board micro SD card slot ή σε καταγραφικό της Dahua (προαιρετικά σειρά NVR5XXX-4KS2). Μέσω των εξόδων alarm in/out, relay out και σε συνδυασμό με μία θυροτηλεόραση της Dahua μπορούμε να έχουμε αυτοματοποιημένη διαδικασία ανοίγματος μίας πόρτας εισόδου, live επικοινωνία με τον διαχειριστή σε περίπτωση κάποιου προβλήματος και ενημέρωση του συστήματος συναγερμού σε περίπτωση event. Τέλος, μπορούμε να συνδυάσουμε την κάμερα με το μοντέλο δοκιμής του event, δηλαδή κάμερα και LED οθόνη με stand. Μέσω της οθόνης μπορούμε να προβάλλουμε στον χώρο οποιοδήποτε μήνυμα θέλουμε κατά την είσοδο ή έξοδο από τον χώρο, μπορούμε επίσης να απευθύνουμε και ειδικό χαιρετισμό καθώς φέρει και ενσωματωμένο ηχείο.

Η **δεύτερη λύση** αφορά στον **έλεγχο θέσεων parking** μέσω καμερών indicator της Dahua.

Οι ειδικές κάμερες τις Dahua φέρουν ειδική λυχνία ένδειξης και μπορεί να ελέγχει έως 6 θέσεις parking ταυτόχρονα. Με αυτό το τρόπο ο διαχειριστής του συστήματος αλλά και οι χρήστες μπορούν να δουν ανά πάσα στιγμή πόσες και ποιες θέσεις είναι κενές αποφεύγοντας άσκοπους «κύκλους», καθυστερήσεις και συνωστισμό στους χώρους στάθμευσης. Επιπλέον, με την λειτουργία VIP, ο διαχειριστής μπορεί από πριν να κλείσει θέση για κάποιο όχημα και η λυχνία της κάμερας να δείχνει κόκκινο ή δεσμευμένη την συγκεκριμένη θέση. Οι κάμερες ελέγχου θέσεων προσφέρουν επίσης ευκολία στην εγκατάσταση τους καθώς με ένα καλώδιο UTP μπορούν να συνδεθούν έως 10 κάμερες μειώνοντας έτσι το κόστος εγκατάστασης και συντήρησης σε πολύ σημαντικό βαθμό. Τέλος μέσα από ειδικές οθόνες ενδείξεων στους χώρους μπορούμε μεταφέρουμε κάποια μηνύματα ηχητικά ή ο χρήστης μπορεί να αναζητήσει το όχημα του σε περίπτωση που έχει ξεχάσει που βρίσκεται πατώντας αναζήτηση της πινακίδας του στην ειδική touch οθόνη.



Σε **πραγματικές δοκιμές** που έγιναν στο χώρο της πίστας καρτ, είδαμε στη πράξη τα αποτελέσματα και την απόδοση των συστημάτων. Χρησιμοποιήσαμε την ITC215-PW4I-HRLZF AI 2MP για να κάνουμε αναγνώριση πινακίδας οχήματος. Στήσαμε τη κάμερα μπροστά στη πίστα και είδαμε ότι ακόμη και με ταχύτητα 60 χλμ η κάμερα κατάφερε να ανιχνεύσει τον αριθμό της πινακίδας της McLaren Mercedes που είχαμε για τις δοκιμές μας. Στο **τέλος του event** οι συμμετέχοντες είχαν την ευκαιρία να κάνουν ερωτήσεις, να πειραματιστούν με τις κάμερες να κάνουν μία βόλτα εντός πίστας με το «θηρίο» των 1.280 ίππων McLaren Mercedes, αλλά και να διαγωνιστούν σε ένα αγώνα ταχύτητας με καρτ.



Νικητές και μη το απόλαυσαν, αυτό είναι το μόνο σίγουρο. Μάθετε περισσότερα για τις νέες λύσεις AI parking solutions της **Dahua στη Vector Security** και ζητήστε τη υποστήριξη έργων από την έμπειρή τεχνική ομάδα της Vector. (Αγίου Σάββα 2, Αθήνα, 210-4925473 - www.vectorsecurity.gr)



Νέα Πυροσβεστική Διάταξη

Χρήσιμες οδηγίες εφαρμογής για τις εγκαταστάσεις



Η Πυροσβεστική Διάταξη 19/2020 «Διαδικασία επιβολής διοικητικών προστίμων για παραβάσεις επί κανονιστικών διατάξεων νομοθεσίας πυροπροστασίας» αποκτά ιδιαίτερη σημασία για αυτό και αξίζει να δούμε τις διαδικασίες και τις οδηγίες εφαρμογής.

Δημοσιεύτηκε στην Εφημερίδα της Κυβερνήσεως (ΦΕΚ τ Β 2233 / 11 Ιουνίου 2020) η Κοινή Απόφαση των Υφυπουργών Οικονομικών και Προστασίας του Πολίτη με την οποία εγκρίνεται η υπ' αριθμό 19/2020 Πυροσβεστική Διάταξη με θέμα «Διαδικασία επιβολής διοικητικών προστίμων για παραβάσεις επί κανονιστικών διατάξεων νομοθεσίας πυροπροστασίας». Συγκεκριμένα:

- **Ταξινομούνται τα διοικητικά πρόστιμα, καθορίζεται το ύψος και προβλέπεται η διαδικασία βεβαίωσης και είσπραξης αυτών**, ανά κατηγορία και είδος παράβασης, από τα αρμόδια ελεγκτικά όργανα του Πυροσβεστικού Σώματος (Π.Σ.) στο πλαίσιο άσκησης της εποπτείας των οικονομικών δραστηριοτήτων, επιχειρήσεων και εγκαταστάσεων, κατόπιν διαπίστωσης μη τήρησης των απαιτούμενων από τις κείμενες διατάξεις πυροπροστασίας:
 - α) προληπτικών και κατασταλτικών μέσων, μέτρων και συστημάτων ενεργητικής πυροπροστασίας,
 - β) στοιχείων δομικής (παθητικής) πυροπροστασίας,
 - γ) τυπικών προϋποθέσεων ως μέρος διοικητικών διαδικασιών,
 - δ) μέριμνας για την πρόληψη και αντιμετώπιση πυρκαγιών σε οικοπεδικούς και ακάλυπτους χώρους, αγροτικές και δασικές εκτάσεις.

- **Καθορίζονται τα κριτήρια προσδιορισμού του ύψους των διοικητικών προστίμων τα οποία είναι:**

- α) η εγγενής επικινδυνότητα της δραστηριότητας, επιχείρησης - εγκατάστασης,
- β) το μέγεθος της δραστηριότητας, επιχείρησης - εγκατάστασης,
- γ) το είδος και ο βαθμός επικινδυνότητας σε περίπτωση εκδήλωσης πυρκαγιάς,
- δ) η κατηγορία (ομάδα) και ο αριθμός χρηστών της δραστηριότητας, επιχείρησης - εγκατάστασης,
- ε) ο βαθμός υπαιτιότητας των ιδιοκτητών και
- στ) οι περιπτώσεις υποτροπής τους εντός διαστήματος ενός (1) έτους από τη βεβαίωση της προηγούμενης παράβασης.

- **Καθορίζεται ο τρόπος Υπολογισμού των προστίμων** με συγκεκριμένο μαθηματικό τύπο με συντελεστή βαρύτητας προστίμου ανά κατηγορία κινδύνου.

- **Καθορίζονται τα όργανα ελέγχου και επιβολής των προστίμων**

Η δημοσίευση της παραπάνω Πυροσβεστικής Διάταξης ουσιαστικά δημιουργεί έναν **μηχανισμό ελέγχου εφαρμογής** της Πυροσβεστικής Νομοθεσίας και διαβαθμίζει τα επιβαλ-

λόμενα προστίμου ανάλογα προς τη σοβαρότητα, το είδος της παράβασης και πιθανή υποτροπή.

Ιδιαίτερα για την πρόληψη και αντιμετώπιση πυρκαγιών σε οικοπεδικούς και ακάλυπτους χώρους, αγροτικές και δασικές εκτάσεις, καθορίζονται οι συντελεστές βαρύτητας προστίμου και προσαύξησης σε περίπτωση υποτροπής, σύμφωνα με τον ημερήσιο δείκτη επικινδυνότητας, όπως αυτός εκδίδεται από την αρμόδια Διεύθυνση της Γενικής Γραμματείας Πολιτικής Προστασίας (Γ.Γ.Π.Π.). Κατά τη χρονική περίοδο όπου δεν εκδίδεται από τη Γ.Γ.Π.Π. Ημερήσιος Χάρτης Πρόβλεψης Κινδύνου Πυρκαγιάς, ως συντελεστής βαρύτητας λαμβάνεται η μονάδα. Θα πρέπει να επισημάνουμε ότι ήδη έχουν καταλογιστεί τα πρώτα διοικητικά πρόστιμα, πέρα και πλέον ποινικών ευθυνών, για μελισσοκομικές εργασίες (κάπνισμα μελισσών), καύση υπολειμμάτων καλλιεργειών και δενδροκομίας κ.λπ.

Στην περίπτωση αυτή, ειδικά για την αντιμετώπιση πυρκαγιών σε οικοπεδικούς και ακάλυπτους χώρους, αγροτικές και δασικές εκτάσεις, είναι σημαντική η συμβολή των αρμοδίων οργάνων πολιτικής προστασίας των Οργανισμών Τοπικής Αυτοδιοίκησης καθώς έχουν την υποχρέωση για ενημέρωση, σχετικά με τον δείκτη επικινδυνότητας, αλλά και την πραγματοποίηση αυτοψιών και ελέγχων για την επικινδυνότητα των οικοπεδικών χώρων που προκύπτει από την μη αποψίλωση των ξηρών χόρτων.

Είναι σημαντικό η συγκεκριμένη Πυροσβεστική Διάταξη να έρθει σε γνώση των Τεχνικών Ασφαλείας και των υπευθύνων πυρασφαλείας των εγκαταστάσεων, των επιχειρήσεων, των οργανισμών και όλων των υπόχρεων να λαμβάνουν μέτρα πυροπροστασίας, ώστε να λαμβάνουν υπόψη, κατά τον έλεγχο των εγκαταστάσεων, τα κριτήρια της Π.Δ 19/2020 και να προβαίνουν έγκαιρα στην αναφορά αυτών για την αποκατάσταση των προβλημάτων και την εφαρμογή της Νομοθεσίας.

Επίσης θα πρέπει να γίνεται μνεία της Πυροσβεστικής Διάταξης στους **συντηρητές και στους εγκαταστάτες των πυροσβεστικών μέτρων,** μέσων και συστημάτων για την αυτονόητη υποχρέωση τους, για την καλή λειτουργία καθώςον πλέον είναι βέβαιο ότι θα ενταθούν οι έλεγχοι και κατά



συνέπεια δεν δικαιολογούνται αμέλειες, καθυστερήσεις και μικρές παραλήψεις που ενδεχόμενα πίστευαν ότι δεν θα γίνονταν αντιληπτές.

Θεωρούμε ότι είναι αναγκαίο οι μεγάλες επιχειρήσεις και οι αντίστοιχες εγκαταστάσεις (Βιομηχανίες, Εμπορικά και Ψυχαγωγικά Κέντρα, Μονάδες Υγείας, Εκπαιδευτικές Μονάδες, Αθλητικές εγκαταστάσεις κ.λπ.) να προβαίνουν στην Αξιολόγηση των υφιστάμενων και εγκατεστημένων μέτρων, μέσων και συστημάτων πυρασφάλειας και πυροπροστασίας (FIRE AUDIT) από εξειδικευμένους επιστήμονες.

Με τον όρο αξιολόγηση μέτρων, μέσων και συστημάτων πυρασφάλειας και πυροπροστασίας (FIRE AUDIT) εννοούνται μια σειρά από διαδικασίες, ενέργειες, δράσεις και έλεγχοι (tests) που έχουν ως στόχο και σκοπό να διαπιστώσουν την επάρκεια, την ετοιμότητα και το βαθμό αντίδρασης αυτών και του μηχανισμού σε πιθανούς κινδύνους πυρκαγιών και συμβάντων πολιτικής προστασίας γενικότερα, όπως είναι πυρκαγιές, σεισμοί, τρομοκρατικά χτυπήματα, παρουσία ή με χρήση φωτιάς κ.λπ., ώστε με τις κατάλληλες παρεμβάσεις και συμπληρώσεις να βελτιωθεί η αποτελεσματικότητα των μέτρων και να εξασφαλιστεί με τον καλύτερο δυνατό τρόπο η πυρασφάλεια των εγκαταστάσεων. Συγκεκριμένα η αξιολόγηση της εγκατάστασης μπορεί να περιλαμβάνει:

GQ★TECH S.A.
DIGITAL PRODUCTS
www.GQtechgr.com

NEW
2020

WXS

OPTEX
Sensing Innovation

2.0m

0.8 - 1.2m



5 years
warranty

Anti-Masking • PIR • Microwave



1. Ισχύουσα Νομοθεσία πυρασφάλειας εγκατάστασης.

- Νομοθετικές Διατάξεις.
- Ερμηνευτικές οδηγίες.
- Πεδίο εφαρμογής.

2. Έλεγχος μελέτης πυρασφάλειας της εγκατάστασης.

- Συμφωνία αυτής με την κείμενη νομοθεσία.
- Ταυτοποίηση αυτής με την υφιστάμενη κατάσταση.
- Βεβαιώσεις - πιστοποιητικά πυροπροστασίας.

3. Επικινδυνότητα της εγκατάστασης από κίνδυνο πυρκαγιάς και συμβάντα πολιτικής προστασίας.

- Καθορισμός επικινδυνοτήτων.
- Ανάλυση εσωτερικών και εξωτερικών κινδύνων, των παραμέτρων επιρροής και παραδοχές για την επιτυχία και αποτελεσματική αντιμετώπισή τους.
- Ανάλυση διακινδύνευσης πληθυσμού.

4. Εφαρμογή μελέτης πυροπροστασίας στην εγκατάσταση.

- Ύπαρξη των προβλεπόμενων μέτρων και μέσων.
- Έλεγχος (test) δοκιμής καλής λειτουργίας και ανταπόκρισης.
- Τεχνική περιγραφή μέσων και συστημάτων.

5. Ανασκόπηση και καταγραφή των υφιστάμενων προληπτικών ενεργειών και διαδικασιών πυροπροστασίας της εγκατάστασης. Ενδεικτικά:

- Τεχνικοί έλεγχοι των δομών και έλεγχοι οδεύσεων διαφυγής.
- Συντήρηση, οπτικοί έλεγχοι, δοκιμαστική λειτουργία εξοπλισμού πυρασφάλειας. Κατάθεση προτάσεων αναβάθμισης και βελτίωσης των διαδικασιών όπου αυτό κρίνεται.

6. Τρωτότητα εγκατάστασης (υφιστάμενη κατάσταση) από κίνδυνο πυρκαγιάς και συμβάντα πολιτικής προστασίας.

- Επιχειρησιακός σχεδιασμός εγκατάστασης.
- Τρόπος αντίδρασης και άμεση ανταπόκριση.
- Διατιθέμενοι πόροι (προσωπικό, μέσα, εξοπλισμός).

Είναι αναγκαίο να γίνεται επαναξιολόγηση του κινδύνου πυρκαγιάς και έλεγχος ορθής λειτουργίας των μέτρων, μέσων και συστημάτων πυροπροστασίας, όχι μόνο για την αποφυγή των προστίμων, όπως αυτά καθορίζονται από την Πυροσβεστική Διάταξη 19/2020, αλλά και για την βέλτιστη της αποτελεσματικότητας των μέτρων και μέσων πυρασφάλειας στην αντιμετώπιση των συμβάντων πυρκαγιάς. Επιπλέον είναι σημαντικό να ελέγχονται σε τακτά χρονικά διαστήματα τα μέτρα και μέσα πυρασφάλειας και να γίνεται επικαιροποίηση του σχεδιασμού όταν έχουν γίνει σημαντικές αλλαγές.

NEW 2020

XTLplus

η No1 ασύρματη μονάδα είναι MADE IN USA

3 years warranty



DMP

GQ★TECH S.A.
DIGITAL PRODUCTS

www.GQtechgr.com

Εκδόσεις για την Ασφάλεια

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
(IT SECURITY)

ΝΕΟ
30€



ΕΓΚΥΚΛΟΠΑΙΔΙΚΟ ΕΓΧΕΙΡΙΔΙΟ
ΤΟΥ SECURITY MANAGER

ΒΙΟΜΗΧΑΝΙΚΗ ΚΑΤΑΣΚΟΠΙΑ -
ΥΠΟΚΛΟΠΗ ΠΛΗΡΟΦΟΡΙΩΝ και
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ και ΑΝΤΙΜΕΤΡΑ

Πληροφορίες: support@securitymanager.gr

Τηλ.: 210 5225479



SMART PRESS

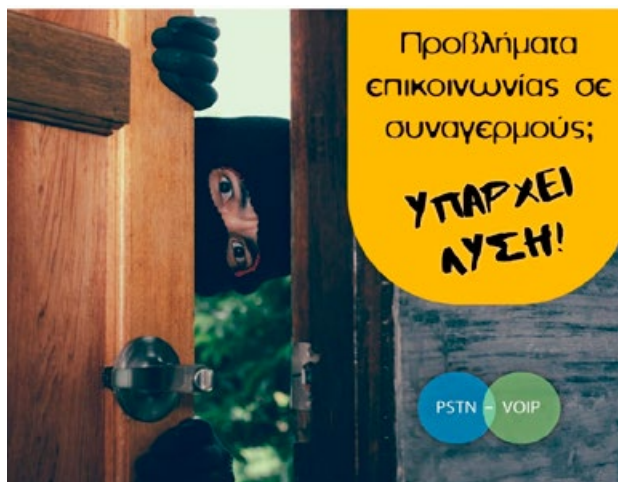
SMART PRESS A.E.
Μόλυβη 11, 10438, Αθήνα

T. 210.5201500, 210.5231555
F. 210.5241900

www.smartpress.gr
support@smartpress.gr

Πρόβλημα επικοινωνίας σε συναγερμούς;

Υπάρχει Λύση!



Στα συστήματα ασφάλειας και ειδικότερα στα συστήματα συναγερμού, η αδιάλειπτη επικοινωνία είναι κομβικής σημασίας και τα όποια προβλήματα προκύπτουν σχετικά θα πρέπει να επιλύονται άμεσα.

Οι αναφορές σχετικά με προβλήματα επικοινωνίας που συναντώνται στα συστήματα ασφάλειας δεν είναι λίγες και απασχολούν έντονα τους εγκαταστάτες των έργων και φυσικά τους τελικούς πελάτες. Σχετικά πρόσφατα και ο Σύνδεσμος Αδειοδοτημένων Επιχειρήσεων Εγκατάστασης Συστημάτων Ασφαλείας Ελλάδος (Σ.Α.Ε.Ε.Σ.Α.Ε.) είχε αναρτήσει διεξοδικό άρθρο, όπου ενημερώνει για την πηγή και τη φύση αυτών των προβλημάτων. Η Keeper Group διαθέτει και προτείνει λύσεις για το συγκεκριμένο ζήτημα που είναι κατάλληλες για όλα τα συστήματα της αγοράς.

Τα συνήθη προβλήματα επικοινωνίας

Οι συνεχόμενες αλλαγές και αναβαθμίσεις των τηλεφωνικών παρόχων, μπορεί από την μια να προσφέρουν μεγαλύτερες ταχύτητες στο internet, αλλά από την άλλη καθιστούν πιο ευάλωτα τα συστήματα ασφάλειας, όσον αφορά τον τομέα της επικοινωνίας.

Πλέον όλη η διαδικασία της επικοινωνίας του συναγερμού με τους Κεντρικούς Σταθμούς ή τον τελικό χρήστη περνάει μέσα από το router, με αποτέλεσμα να δημιουργούνται συχνά προβλήματα που οφείλονται συνήθως σε: διακοπές ρεύματος, κακό συγχρονισμό, επανεκκινήσεις του router, φθορές των router από υπερθέρμανση κ.λπ.

Επίσης παρατηρούνται συχνά υπερβάσεις του χρόνου ομιλίας των σταθερών συνδέσεων επικοινωνίας voice, ιδιαίτερα σε παλιά συστήματα συναγερμού. Αυτό συμβαίνει λόγω της μετάβασης των εταιρειών τηλεπικοινωνιών, αποκλειστικά σε νέες ψηφιακές πλατφόρμες (Voip).

Το βασικότερο πρόβλημα λοιπόν είναι ότι ενδέχεται σε μια περίπτωση πραγματικής διάρρηξης το σύστημα μας να μην καταφέρει να στείλει το σήμα του στον κεντρικό σταθμό και η εγκατάσταση να βρεθεί εκτεθειμένη.

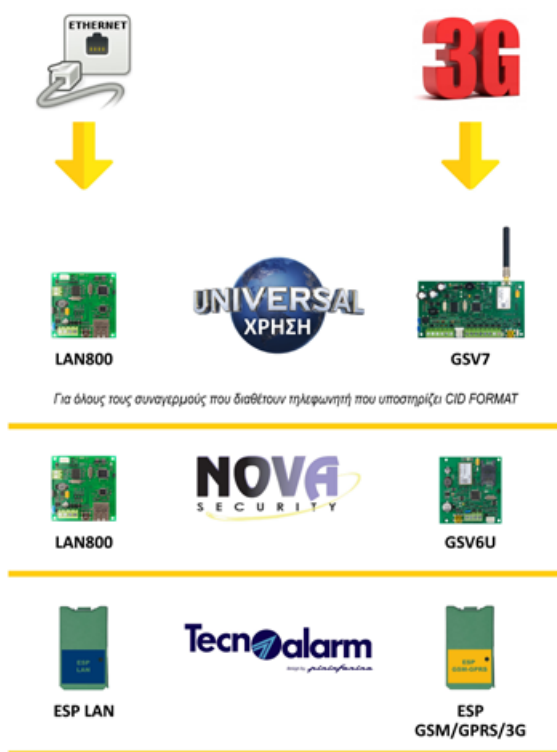
Τι επιλογές έχει ο εγκαταστάτης;

Τα νέα συστήματα συναγερμού διαθέτουν τη δυνατότητα αντιμετώπισης τέτοιων προβλημάτων επικοινωνίας μέσω δικτυακής επίγειας (TCP/IP) ή GPRS/3G/4G επικοινωνίας. Οφείλουμε λοιπόν να συμβουλευτούμε τον τελικό μας πελάτη για τις επιλογές που μπορεί να έχει και να επιλέξει τι θέλει. Η καλύτερη επιλογή είναι πάντα αυτή που προβλέπει την περίπτωση αποτυχίας της πρωτεύουσας γραμμής επικοινωνίας με την ύπαρξη back up λύσης. Αυτό σημαίνει το λιγότερο δύο διαφορετικούς τρόπους επικοινωνίας.



Λύσεις από την Keeper Group

Η Keeper Group διαθέτει μια σειρά από λύσεις με μια ολοκληρωμένη γκάμα Universal ή Bus προϊόντων σε συνδυασμό φυσικά με τις αξιόπιστες υπηρεσίες του Κέντρου Λήψης Σημάτων **TecnoHellas**.



Πιο αναλυτικά προτείνεται η μονάδα **LAN 800 IP MODULE NOVA** που αποτελεί ένα Universal IP Module με δυνατότητα αναφορών σε ΚΛΣ Contact ID μέσω TCP/IP με iPhone application για τη διαχείριση του συστήματος μέσω smartphone. Το iPhone application είναι συμβατό με πίνακες NOVA Alarm και με πίνακες DSC, εφόσον το LAN800 συνδεθεί στο DSC Keybus.

Επίσης διατίθεται το **GSV7** από τη **Nova** ένα UNIVERSAL GSM/GPRS 3G SIGNAL με κουτί που είναι συμβατό με συστήματα άλλων κατασκευαστών που διαθέτουν PSTN dialer με format επικοινωνίας CID. Διαθέτει 6 εισόδους (NC/NO) με ξεχωριστή ευαισθησία η κάθε μία, με δυνατότητα αποστολής επιλέξιμου CID σήματος ή οποιαδήποτε φράση επιθυμείτε μέσω SMS αλλά και 2 εξόδους PGM οι οποίες μπορούν να χρησιμοποιηθούν για την όπλιση ή αφόπλιση του συναγερμού (με χρήση ζώνης κλειδοδιακόπτη) ή για να ελέγξουν από απόσταση ηλεκτρικές συσκευές, φώτα, καλοριφέρ, γκαρα-



ζόπορες κ.λπ.! Επίσης έχει τη δυνατότητα να ειδοποιεί τους χρήστες με τηλεφωνική κλήση, μιλώντας τους στα ελληνικά. Υποστηρίζει έως και 10 χρήστες ταυτόχρονα, με διαφορετικές επιλογές ειδοποιήσεων και είναι συμβατό με Global Sim, ελληνικών παρόχων. Παρέχει ακόμα δυνατότητα αναφοράς στο ΚΛΣ μέσω GPRS με 2 κανάλια επικοινωνίας και είναι πλήρως συμβατό με πολλά συστήματα DSC & PARADOX με σύνδεση μέσω SERIAL καλωδίου.

Στις λύσεις περιλαμβάνεται και η μονάδα **GSV6U GSM/GPRS AUDIO της NOVA**, μια πλακέτα GSM με εσωτερική κεραία για πίνακες σειράς PAS. Προσφέρει Back-up για την επικοινωνία με το 24ωρο ΚΛΣ μέσω GPRS και δυνατότητα αποστολής sms στα Ελληνικά. Επίσης υποστηρίζει τηλεφωνική στα ελληνικά και δυνατότητα χειρισμού του συστήματος μέσω κλήσης ή sms.

Από την **TecnoAlarm** προτείνεται η ethernet μονάδα επέκτασης multifunction TCP/IP "ESP LAN" που προσφέρει δυνατότητα αποστολής σημάτων στο Κ.Λ.Σ μέσω TCP/IP και παράλληλης σύνδεσης του χρήστη μέσω της εφαρμογής MyTecnoalarm από κινητά android/ios.

Επίσης από την TecnoAlarm συναντάμε την μονάδα επέκτασης GSM/GPRS, **ESP GSM-GPRS 3G** με δυνατότητα αποστολής σημάτων σε Κ.Λ.Σ, αποστολή μηνυμάτων στο προσωπικό τηλέφωνο του χρήστη και δυνατότητα κλήσης στο κινητό του πελάτη με φωνητικό μενού καθώς επίσης και δυνατότητα όπλισης /αφόπλισης του συστήματος αλλά και ενεργοποίησης/απενεργοποίησης τηλεφωνικών εντολών (π.χ. φώτα, θέρμανση).

Για περισσότερες πληροφορίες μπορείτε να απευθυνθείτε στην Keeper Group (www.keeper.gr) επικοινωνώντας στο τηλέφωνο 210 2025705.

Η εξέλιξη των συστημάτων συναγερμού ...προς το εξυπνότερο!



Για πολλά χρόνια ο τομέας των συστημάτων συναγερμού θεωρούνταν ένα «συντηρητικό» πεδίο εφαρμογής νέων τεχνολογιών. Τα τελευταία χρόνια όμως, πληθώρα νέων χαρακτηριστικών και λειτουργιών έχουν προσδώσει στα συστήματα συναγερμού δυνατότητες που θα μπορούσαμε να τις χαρακτηρίσουμε έξυπνες. Τι προσφέρουν λοιπόν τα νέα έξυπνα συστήματα συναγερμού; Τι πρέπει να προσέξουμε κατά την επιλογή τους και ποιος ο ουσιαστικός ρόλος των επαγγελματιών του κλάδου στην επιλογή και την τοποθέτησή τους;

Τη στιγμή που θα κληθούμε να επιλέξουμε ένα σύστημα συναγερμού θα διαπιστώσουμε πλέον ότι υπάρχει πλήθος νέων χαρακτηριστικών και δυνατοτήτων στα καινούργια συστήματα, κάτι που καθιστά αυτή την επιλογή ως μια δύσκολη απόφαση ορισμένες φορές. Μπορεί τα βασικά χαρακτηριστικά τους να παραμένουν τα ίδια -με κύριο ρόλο να ανιχνεύουν

εισβολές και να παράγουν ειδοποιήσεις συναγερμού- πλέον όμως οι δυνατότητες τους είναι τέτοιες που υπερβαίνουν τις απλές λειτουργίες ασφάλειας και αποκτούν ένα πιο πολυχρηστικό ρόλο. Αυτές οι καινούριες δυνατότητες που κάνουν τα συστήματα πιο έξυπνα και πιο λειτουργικά προσφέρουν **νέες ευκαιρίες στους εγκαταστάτες αλλά και πλεονεκτήματα για τους τελικούς χρήστες**. Ας δούμε όμως πως φτάσαμε σε αυτό το σημείο.

Η εξέλιξη

Σίγουρα ο βασικός παράγοντας ενσωμάτωσης των νέων δυνατοτήτων στα συστήματα συναγερμού όπως είναι: οι εφαρμογές απομακρυσμένης διαχείρισης μέσω cloud από smartphone, η βελτιστοποίηση της ασύρματης τεχνολογίας, η συνεργασία με άλλα συστήματα ασφάλειας ή αυτοματισμούς ήταν αποτέλεσμα της **εξέλιξης της τεχνολογίας** που επέτρεπε την αναβάθμιση της απόδοσης και αποτελεσματικότητάς τους. Όμως υπεισέρχεται και ένας ακόμα παράγοντας.

Ο επαγγελματικός κλάδος της φυσικής ασφάλειας, αλλά κυρίως ο κλάδος καθαρά των συστημάτων συναγερμού βρίσκεται τα τελευταία χρόνια μπροστά σε ένα έντονο ανταγωνιστικό περιβάλλον, στο οποίο συμμετέχουν πλέον και κατασκευαστές **από άλλους παρεμφερείς κλάδους**. Για παράδειγμα οι ολοκληρωμένες λύσεις διαχείρισης κτιρίων (building management systems) αλλά και των έξυπνων σπιτιών και κτιρίων (smart homes & buildings) υπόσχονται ότι μπορούν να προσφέρουν ότι μέχρι προσέφεραν τα απλά συστήματα συναγερμού, αλλά εμπλουτισμένα με πολλές άλλες δυνατότητες. Οπότε, επανερχόμενοι σε αυτά που αναφέραμε στην αρχή του κειμένου είναι λογικό η παραδοσιακή αγορά των κατασκευαστών συστημάτων συναγερμού, να προσπαθεί κάνει βήματα προς τα εμπρός ώστε να αποκτήσει ξανά το ανταγωνιστικό πλεονέκτημα σε σχέση με την αναδυόμενη αγορά που έχει δημιουργηθεί

Αυτή η εξέλιξη -δηλαδή η εισδοχή των κατασκευαστών εξοπλισμού smart home και smart building και στην αγορά των συστημάτων συναγερμού- έχει αλλάξει σε ένα βαθμό στο καταναλωτικό κοινό τον τρόπο προσέγγισης απέναντι στα

συστήματα συναγερμού σε σχέση με περασμένες δεκαετίες. Μέχρι πριν από λίγα χρόνια, τα συστήματα συναγερμού αποτελούσαν μια ξεχωριστή αυτόνομη κατηγορία σε σχέση με άλλες εφαρμογές του ευρύτερου ηλεκτρονικού κλάδου. Αυτό οφείλονταν σε δύο βασικούς λόγους. Πρώτον διότι υπήρχαν συγκεκριμένα πρότυπα βάσει των οποίων υλοποιούνταν η κατασκευή, η εγκατάσταση αλλά και η λειτουργία ενός συστήματος συναγερμού. Τα πρότυπα αυτά ήταν απαιτητά κυρίως από τις ασφαλιστικές εταιρείες τις οποίες τις καλούσαν οι ιδιοκτήτες για να ασφαλίσουν τις ιδιοκτησίες τους. Ο δεύτερος βασικός λόγος είναι οι απαιτήσεις των αστυνομικών αρχών ή των κέντρων λήψης σημάτων που καθόριζαν συγκεκριμένες προδιαγραφές για τη διασύνδεση στα συστήματα τους.

Όσο όμως αλλάζει η τεχνολογία και εξελίσσεται τόσο μεταβάλλονται και οι παραπάνω πρακτικές. Υπάρχουν ακόμα φυσικά τελικοί χρήστες που επιθυμούν την εναρμόνιση και προσήλωση με αυτές τις παραδοσιακές αρχές. Αλλά και χρήστες που επιθυμούν να χρησιμοποιούν συστήματα πιο ευέλικτα και με πιο ανοικτές με πλατφόρμες και τα οποία να μπορούν να συνεργασθούν με άλλες εφαρμογές. Αυτή η συγκεκριμένη κατηγορία χρηστών -που με την πάροδο του χρόνου αυξάνεται- δεν βασίζεται σε καθιερωμένες πρακτικές για την υλοποίηση ενός συστήματος συναγερμού. Καθορίζει τα επιθυμητά επίπεδα προστασίας χρησιμοποιώντας δικές τους μεθόδους εκτίμησης κινδύνου (risk assessment). Θέλει ευελιξία, επεκτασιμότητα και διασύνδεση με άλλες εφαρμογές. Δηλαδή επιθυμούν κάτι περισσότερο από καλή απόδοση, μειωμένη συχνότητα εμφάνισης λανθασμένων συναγερμών και σταθερότητα. Θέλουν τα συστήματα που επιλέγουν να έχουν έναν πολυδιάστατο ρόλο.

Εδώ θα πρέπει να τονίσουμε όμως ότι από άποψη ποιότητας και αξιοπιστίας της καθαυτού λειτουργίας ανίχνευσης εισβολής δεν τίθεται θέμα σύγκρισης με τα συστήματα των παραδοσιακών κατασκευαστών να υπερτερούν σε πολύ μεγάλο βαθμό.

Οπότε και οι "παραδοσιακοί παίκτες" συνεχώς αναπτύσσουν καινούρια σύγχρονα συστήματα συναγερμού που ικανοποιούν απόλυτα τις απαιτήσεις των έξυπνων κτιρίων αλλά και του Internet of Things και μπορούν να καλύψουν πολλές και διαφορετικές συνδυαστικές ανάγκες όπως συνεργασία με εξοπλισμό διαχείρισης βίντεο, αυτοματισμούς εγκαταστάσεων, εξ αποστάσεως αναφορές, άμεσες ενημερώσεις (push notifications) κ.λπ. Όλα αυτά προσφέρονται σε μια ενιαία πλατφόρμα η οποία μπορεί να έχει τις αυστηρές προδιαγραφές λειτουργίας ενός συμβατικού συστήματος συναγερμού, αλλά όπως είναι φανερό προσφέρει πολύ μεγαλύτερη ευχρη-

 **GeoVision**



 **Milesight**



 **Visional**



 **FORCE**
GROUP OF COMPANIES

Θεσσαλονίκη:
Ηλέκτρας 5,
τ.κ. 551 34 Καλαμαριά
Τηλ.: 2310 805.180-1
Fax: 2310 805.387

Αττική:
Στ. Σαράφη 15,
τ.κ. 122 41 Αιγάλεω
Τηλ.: 210 57.57.227
Fax: 210 57.87.342

Κύπρος:
Αγαπήνωρος 12,
τ.κ. 8049 Πάφος
Τηλ.: 00357 26945221

info@force.gr

www.force.gr

cypus@force-security.com
www.force-security.com

στία στον τελικό χρήστη. Εδώ υπεισέρχεται ο σημαντικός ρόλος των μελετητών και των εγκαταστατών που οφείλουν να αντιληφθούν τις πραγματικές ανάγκες του χρήστη. Οφείλουν δηλαδή να κατανοήσουν αν οι τελικοί πελάτες κερδίσουν κάτι από τα νέα έξυπνα συστήματα τα οποία δεν ανήκουν μεν στη κατηγορία των συμβατικών συστημάτων προσφέρουν όμως πολλές από τις προαναφερθείσες δυνατότητες όπως ασύρματη διασύνδεση, ενοποίηση με άλλες εφαρμογές, push notifications και ανταλλαγή δεδομένων. Ίσως ένα συμβατικό σύστημα συναγερμού να μην προσφέρει αυτές τις δυνατότητες, αλλά το ερώτημα που θα πρέπει να απαντηθεί από όλους τους εμπλεκόμενους είναι κατά πόσο χρειάζεται ο τελικός χρήστης όλες αυτές τις δυνατότητες.

Νέες τάσεις

Η ενσωμάτωση πολλών συστημάτων συναγερμού με τις τεχνολογίες βίντεο επιτήρησης είναι ίσως μια από τις σημαντικότερες τάσεις και μάλλον από τις πιο χρήσιμες. Ο λόγος της χρησιμότητας είναι προφανής. Η δυνατότητα λήψης εικόνας από ένα σημείο στο οποίο υπάρχει ένδειξη συναγερμού -η λεγόμενη **οπτική επιβεβαίωση**- είναι πάντα χρήσιμη. Δεν είναι λίγες οι φορές που έχουμε μια ένδειξη συναγερμού ή μια ενημέρωση από το κέντρο λήψης σημάτων χωρίς όμως να έχουμε μια σαφή εικόνα του τι έχει γίνει. Αν είχαμε οπτική επιβεβαίωση από το συγκεκριμένο σημείο θα μπορούσαμε αμέσως να έχουμε μια καλύτερη εικόνα της κατάστασης. Εάν λοιπόν χρειάζεται και η ενσωμάτωση βίντεο τότε θα πρέπει να εξετασθούν συστήματα συναγερμού που να υποστηρίζουν αυτή τη δυνατότητα. Πολλοί χρήστες δεν είναι ίσως απόλυτα ενημερωμένοι για τα πλεονεκτήματα αυτής της λειτουργίας. Άλλοι φοβούνται ότι ίσως αν επιλέξουν αυτή τη δυνατότητα θα επιβαρυνθεί σημαντικά ο προϋπολογισμός τους. Η αλήθεια είναι ότι τα σύγχρονα συστήματα προσφέρουν αυτές τις δυνατότητες χωρίς σημαντική μεταβολή στο κόστος. Το ζητούμενο είναι να ξέρει αυτός που θα αναζητήσει μια λύση που θα κάνει την αναζήτηση. Η καλή γνώση των συστημάτων και των λύσεων που παρουσιάζονται συνεχώς από τις εταιρείες είναι εκείνη που μπορεί να βοηθήσει τον εγκαταστάτη να προσφέρει μια **αξιόπιστη και οικονομική πρόταση στον πελάτη του** (value engineering).

Η διασύνδεση με συσκευές που υποστηρίζουν την τεχνολογία **Internet of Things** είναι άλλη μια τάση που μπορεί να συμβάλει στην ακόμα μεγαλύτερη διεύθυνση ενός συναγερμού στην αγορά. Είναι μια δυνατότητα που θα επιτρέψει στους χρήστες να έχουν τον έλεγχο σε ακόμα μεγαλύτερο αριθμό συσκευών οι οποίες δεν ανήκουν στα συστήματα ασφαλείας. Φυσικά, αυτή η λειτουργία υπήρχε ακόμα και



πριν την εμφάνιση του Internet of Things απλώς με την εμφάνιση μιας ενιαίας πλατφόρμας γίνεται ακόμα απλούστερη και πιο προσιτή στον απλό χρήστη. Εφαρμοσμένες λύσεις IoT υπάρχουν σήμερα αρκετές και οι περισσότερες δίνουν τη δυνατότητα του ελέγχου συστημάτων φωτισμού, συστημάτων ελέγχου πρόσβασης, μεγαφωνικών συστημάτων, κλιματισμού, θέρμανσης και παραγωγής ζεστού. Πρόκειται ουσιαστικά για αυτό που αναφέραμε στην αρχή ότι τα σύγχρονα συστήματα συναγερμού μπορούν να επιτελέσουν το ρόλο μιας εφαρμογής BMS (Building Management System). Το ερώτημα όμως και πάλι είναι τι ακριβώς θέλει ο χρήστης και πως αυτές οι διαθέσιμες λύσεις παρουσιάζονται σε αυτό από τους μελετητές και εγκαταστάτες.

IFTTT ...μια νέα έξυπνη προσέγγιση!

Αν θέλουμε να αναδείξουμε όμως μια νέα τάση που αναδύεται στο χώρο των συστημάτων συναγερμών, αλλά και γενικότερα στον χώρο των έξυπνων εφαρμογών κτιριακού αυτοματισμού, θα εστιάζαμε στην επανομαζόμενη **IFTTT (if this, then that)**. Είναι μια τάση/ υπηρεσία που ακούγεται πολύ συχνά τον τελευταίο καιρό. Οι πηγές της συγκεκριμένης προσέγγισης πηγάζουν από τις πρώιμες ημέρες του προγραμματισμού των υπολογιστών και η απόδοση της στην Ελληνική γλώσσα είναι «Εάν ισχύει αυτό τότε κάνει το άλλο». Για όσους είχαν ή έχουν εντρυφήσει στον προγραμματισμό είναι εξοικειωμένοι με τη συγκεκριμένη λογική καθώς αυτή η εντολή δίνει τη δυνατότητα σε έναν υπολογιστή να εκτελέσει κάποιες λειτουργίες σύμφωνα με κάποιες παραμέτρους και εντολές που δίνει ο προγραμματιστής. Η τάση λοιπόν IFTTT ξεκίνησε πριν κάποια χρόνια στο Internet και επιτρέπει στους χρήστες να δημιουργούν συσχετισμένες ενέργειες μεταξύ των διαδικτυακών υπηρεσιών. Χαρακτηριστικό παράδειγμα αποτελεί η εντολή που μπορεί να δώσει ένας χρήστης όταν αλλάξει η φωτογραφία του στο Facebook να αλλάξει και η φωτογραφία σε έναν άλλο κοινωνικό δίκτυο. Πρόκειται για

ένα απλουστευμένο παράδειγμα πως λειτουργεί η υπηρεσία IFTTT (εάν συμβεί αυτό τότε κάνε το άλλο).

Είναι γνωστό ότι οι κλάδοι της πληροφορικής και των συστημάτων ασφαλείας αν και ξεκίνησαν από διαφορετικές αφητηρίες, τη τελευταία δεκαετία στο πλαίσιο της γενικότερης σύγκλισης των τεχνολογιών έχουν βρει πολλά κοινά σημεία επαφής. Η υπηρεσία IFTTT δεν θα μπορούσε να αποτελεί εξαίρεση. Πολλά συστήματα συναγερμού κάνουν πλέον χρήση της συγκεκριμένης τεχνολογίας. Η κυριότερη διαφορά μεταξύ των γενικών εφαρμογών IFTTT και των έξυπνων συστημάτων συναγερμού είναι ότι τα πρώτα προσφέρουν λύσεις που σχετίζονται κυρίως με την καθημερινότητα όπως την αυτοματοποίηση συσκευών καθημερινής χρήσης και τον έλεγχο λειτουργιών χωρίς όμως κάποια διαβάθμιση ασφάλειας. Αντίθετα οι επαγγελματικές λύσεις συστημάτων συναγερμού που χρησιμοποιούν την τεχνολογία IFTTT προσφέρουν μεν όλα τα παραπάνω αλλά με μια σημαντική διαφοροποίηση: Ότι έχει να κάνει με τις λειτουργίες ασφάλειας είναι πιστοποιημένο, σωστά εγκατεστημένο και συντηρημένο και έχει δοκιμαστεί ώστε να διασφαλίζεται η αξιόπιστη λειτουργία του. Αυτή η διαφοροποίηση είναι πολύ σημαντική όμως για το τελικό χρήστη. Είναι το στοιχείο που θα τον κατευθύνει να επιλέξει μια επώνυμη και αξιόπιστη λύση ενός συστήματος συναγερμού η οποία θα έχει υλοποιηθεί και από έναν πιστοποιημένο εγκαταστάτη από το να επιλέξει μια γενική λύση οικιακού αυτοματισμού που μπορεί μεν να προσφέρει και λειτουργίες επιτήρησης χωρίς όμως να είναι πιστοποιημένη για τη συγκεκριμένη εργασία.

Τα σύγχρονα συστήματα συναγερμού προσφέρουν μια ευρεία γκάμα δυνατοτήτων. Δεν υπάρχει καμία σύγκριση με την εικόνα που είχαμε στο νου μας μέχρι πριν λίγα χρόνια. Ίσως το μόνο σημαντικό μειονέκτημα τους σε σχέση με άλλες λύσεις πιο εμπορικές είναι στο πως γίνεται το marketing των συστημάτων συναγερμού καθώς οι περισσότεροι τελικοί χρήστες δεν γνωρίζουν αυτές τις λειτουργίες.

Είναι πολύ σημαντικό λοιπόν οι επαγγελματίες του χώρου να έχουν εξοικειωθεί με όλο αυτό το φάσμα των νέων δυνατοτήτων ώστε να μπορούν να το επικοινωνούν στους πελάτες τους. Πολύ σημαντικό επίσης είναι να είναι σε θέση να αξιολογήσουν τις πραγματικές ανάγκες ενός χρήστη και να του προτείνουν το κατάλληλο σύστημα. Κάθε εφαρμογή έχει τις δικές της απαιτήσεις και το να προτείνουμε συστήματα τα οποία είτε υπερβαίνουν κατά πολύ τις προδιαγραφές είτε δεν τις καλύπτουν δημιουργεί ένα σημαντικό έλλειμμα εμπιστοσύνης και αποτρέπει τους χρήστες από το να δοκιμάσουν τις νέες λύσεις και στρέφονται σε πιο παλιές συμβατικές προτάσεις.



Honeywell

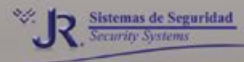


TAKEX

JAPAN



alhua
TECHNOLOGY



FORCE S.A.
GROUP OF COMPANIES

Θεσσαλονίκη:
Ηλέκτρας 5,
τ.κ. 551 34 Καλαμαριά
Τηλ.: 2310 805.180-1
Fax: 2310 805.387

Αττική:
Στ. Σαράφη 15,
τ.κ. 122 41 Αιγάλεω
Τηλ.: 210 57.57.227
Fax: 210 57.87.342

Κύπρος:
Αγαπήνωρος 12,
τ.κ. 8049 Πάφος
Τηλ.: 00357 26945221

info@force.gr

www.force.gr

cyprus@force-security.com
www.force-security.com

Μετάβαση σε Δικτυακές Πλατφόρμες



Τα οφέλη υιοθέτησης μίας δικτυακής προσέγγισης στα έργα των συστημάτων ασφαλείας είναι γνωστά εδώ και χρόνια. Το ζητούμενο πλέον σήμερα, είναι οι εταιρίες που υλοποιούν μεγάλα έργα, αλλά και οι εγκαταστάτες συστημάτων, να προσαρμόσουν ακόμα καλύτερα τις προτάσεις τους στο τομέα της δικτυακής τεχνολογίας ως τη μοναδική ρεαλιστική επιλογή, προκειμένου να τους προσφέρουν έξυπνες λύσεις ασφαλείας και οικονομικά αποδοτικές. Ας δούμε λοιπόν τι γίνεται σήμερα σε ότι αφορά τη μετάβαση από τα παλαιά αναλογικά συστήματα σε δικτυακές πλατφόρμες.

Όταν τα δικτυακά συστήματα ασφαλείας πρωτοεμφανίστηκαν πριν αρκετά χρόνια και άρχισαν να εφαρμόζονται στα αντίστοιχα τεχνολογικά έργα και ειδικότερα στο τομέα της βίντεο-επιτήρησης, η άφιξη τους, δεν θα λέγαμε ότι συνοδεύτηκε με μια "θριαμβευτική υποδοχή" ούτε ότι προκάλεσε κάποια πολύ σημαντική αλλαγή τότε στον τρόπο υλοποίησης των εγκαταστάσεων. Ο λόγος ήταν ότι τότε, πολλοί από τους κατασκευαστές συστημάτων ασφαλείας, είχαν εξελίξει αρκετά τις δυνατότητες του composite βίντεο σε νέα επίπεδα, με καινοτόμες τεχνολογίες. Ως αποτέλεσμα, οι τότε λύσεις IP στην πρώτη μορφή τους από την μια πλευρά δεν είχαν να προσφέρουν πολλά περισσότερα όσον αφορά τις επιδόσεις και από την άλλη επιβάρυναν σημαντικά τον απαιτούμενο προϋπολογισμό. Φυσικά θα πρέπει να σημειώσουμε ότι και οι απαιτήσεις των παλαιότερων εποχών καλύπτονταν με τις τότε

υπάρχουσες λύσεις των Κλειστών Κυκλωμάτων Τηλεοράσεων CCTV.

Με την πάροδο των χρόνων, οι επιδόσεις των λύσεων IP ενισχύθηκαν σημαντικά, οι δυνατότητες τους επέτρεπαν περισσότερες λειτουργίες και το κόστος προμήθειας των σχετικών συστημάτων άρχισε να γίνεται ακόμα πιο προσιτό.

Σήμερα, οι λόγοι και τα επιχειρήματα υπέρ της μετάβασης σε μια δικτυακή πλατφόρμα ασφαλείας, ισχυροποιούνται χρόνο με το χρόνο. Οι πρόσφατες τεχνολογικές εξελίξεις έχουν αλλάξει σημαντικά το τοπίο σε ότι αφορά τα έργα των συστημάτων ασφαλείας, σε σημείο ώστε οι εγκαταστάτες και οι εταιρίες υλοποίησης μεγάλων έργων, να έχουν ως μονόδρομο **ρεαλιστικής επιλογής τα δικτυακά συστήματα βίντεο-επιτήρησης**, αν θέλουν να παραμείνουν ανταγωνιστικοί στην αγορά και να πετυχαίνουν συμφέρουσες εμπορικές συμφωνίες.

Παρόλα αυτά, ακόμα και σήμερα τα συστήματα που χρησιμοποιούν παλαιές αναλογικές πλατφόρμες υπάρχουν ακόμα σε πολλές εγκαταστάτες. Αυτό που συνήθως γίνεται είναι κάποιες σταδιακές αναβαθμίσεις, με πιο διαδεδομένες τα προηγούμενα χρόνια τις λύσεις HD μέσω ομοαξονικού, που προσφέρουν πολλοί κατασκευαστές με μεγάλη θα λέγαμε επιτυχία τα προηγούμενα χρόνια, τουλάχιστον εμπορικά. Είναι επίσης αλήθεια ότι και για αυτές τις λύσεις αναβάθμισης με την αξιοποίηση τεχνολογικών προτύπων HD μέσω αναλογικού, έχει επέλθει κάποιος κορεσμός. Μια τέτοια λύση -που σίγουρα απαιτεί και κάποια επένδυση από πλευράς του πελάτη- δεν μπορεί να είναι για πάντα βιώσιμη, ειδικά σήμερα, όπου οι αναλύσεις συνεχώς αυξάνονται και παράλληλα υπεισέρχονται πολλές σύγχρονες τεχνολογίες που δημιουργούν ακόμα μεγαλύτερη προστιθέμενη αξία στα έργα.

Υπερύψηλες αναλύσεις, ευέλικτες λύσεις VMS, έξυπνη ανάλυση βίντεο και ήχου, τεχνητή νοημοσύνη και βαθιά εκμάθηση, επιχειρηματική ευφυΐα, σύγχρονα γραφικά περιβάλλοντα, λύσεις ενοποίησης με άλλες υποδομές, έξυπνα κτίρια και οικιακοί αυτοματισμοί, είναι μερικές μόνο από τις εξελίξεις όπου έχουν δημιουργήσει μεγαλύτερες απαιτήσεις από τους τελικούς πελάτες προς τους εγκαταστάτες. **Ο μόνος τρόπος αποτελεσματικής διαχείρισης αυτών των απαιτήσεων είναι η σχεδίαση και υλοποίηση μιας καθολικά δικτυακής πλατφόρμας.**

Ακόμα και αν δεν υπάρχει η γνώση των πλεονεκτημάτων που πηγάζουν από τη μετάβαση σε IP υποδομές στους τελικούς χρήστες θα πρέπει οι εταιρίες προμήθειας εξοπλισμού και εγκαταστάσεων να ενημερώνουν τους πελάτες τους για τα πρόσθετα οφέλη που θα προκύψουν μεταβαίνοντας σε δικτυωμένη πλατφόρμα.

Σχεδιάζοντας τη μετάβαση

Η υλοποίηση μετάβασης μιας πλατφόρμας ασφάλειας σε μια πλήρως δικτυακή αρχιτεκτονική, μπορεί να επιτευχθεί με διάφορους τρόπους. Σε πολλές από τις εφαρμογές, η επιθυμητή προσέγγιση είναι να ολοκληρωθεί η μετάβαση βάσει ενός προγράμματος πολλαπλών φάσεων, σύμφωνα πάντα με τη διαθεσιμότητα προϋπολογισμού αλλά και των υφιστάμενων υποδομών. Ένα σημαντικό πλεονέκτημα του πολυφασικού μοντέλου μετάβασης στο IP, είναι ότι οι τερματικές συσκευές μπορούν να αντικατασταθούν οικονομικά, είτε σταδιακά μία-μία, είτε ομαδικά, ανάλογα με τις ανάγκες.

Υπάρχουν σήμερα διαθέσιμες αρκετές τεχνολογίες που μπορούν να αξιοποιήσουν οι εγκαταστάτες και οι εταιρίες υλοποίησης έργων κατά τη μετάβαση σε μια απόλυτα ψηφιακή τεχνολογία, χρησιμοποιώντας σε κάποιο βαθμό και τις υπάρ-



Νέο Ασύρματο Σύστημα Οικιακού Συναγερμού - Αυτοματισμού

- Έξυπνη Παρακολούθηση - Υψηλή Αξιοπιστία
- Εύκολη Χρήση - Απομακρυσμένη Διαχείριση
- Ιδανικό για σπίτια, διαμερίσματα και συγκροτήματα κατοικιών
- Δυνατότητα Σύνδεση με Κεντρικό Σταθμό

DINSAFER NOVA PRO



FORCE
GROUP OF COMPANIES

Θεσσαλονίκη:

Ηλέκτρας 5,
τ.κ. 551 34 Καλαμαριά
Τηλ.: 2310 805.180-1
Fax: 2310 805.387

Αττική:

Στ. Σαράφη 15,
τ.κ. 122 41 Αιγάλεω
Τηλ.: 210 57.57.227
Fax: 210 57.87.342

Κύπρος:

Αγαπήνωρ 12,
τ.κ. 8049 Πάφος
Τηλ.: 00357 26945221

info@force.gr

www.force.gr

cypus@force-security.com
www.force-security.com



χουσες υποδομές. **Το πλεονέκτημα αυτής της προσέγγισης είναι ότι δεν απαιτείται νέα καλωδίωση** για πολλές από τις συνδέσεις των συστημάτων.

Αυτό αποφέρει σίγουρα οφέλη για τον τελικό χρήστη, όπως για παράδειγμα: λιγότερες επεμβάσεις στο χώρο, εκτεταμένη απόδοση των επενδύσεων για υπάρχουσες υποδομές και κάποια τερματικά, δυνατότητα παράλληλης χρήσης της νέας συνδεσιμότητας και για άλλα συστήματα, όπως VoIP και διαδικασίες, κ.ά. Επίσης, αποφέρει οφέλη για τον εγκαταστάτη όπως, μειωμένο χρόνο εγκατάστασης των καλωδίων (μία από τις πιο χρονοβόρες εργασίες της εγκατάστασης), ενώ δεν τίθεται θέμα περιορισμού για το μήκος των δικτυακών καλωδίων και γενικότερα οι όλες εργασίες πραγματοποιούνται ταχύτερα. Κατά το πρώτο στάδιο μίας βασικής εγκατάστασης, συνήθως **αποφασίζουμε αν θα χρησιμοποιήσουμε EoC** (Ethernet over Coax - ομοαξονικό Ethernet) ή κάποια παρόμοια συσκευή. Όταν κάποιο αναλογικό ή AHD σύστημα αντικαθίσταται, μία τέτοια συσκευή τοποθετείται κανονικά στο κέντρο ελέγχου. Αυτό γίνεται επειδή οι περιορισμοί του ομοαξονικού καλωδίου στα παραδοσιακά συστήματα, δεν επιτρέπουν την κοινή χρήση του καλωδίου και για άλλες λειτουργίες. Έτσι, κάθε τερματική συσκευή είχε αποκλειστική σύνδεση με το σύστημα κεντρικής διαχείρισης και καταγραφής.

Αξίζει να σημειώσουμε ότι όταν χρησιμοποιείται ομοαξονική σύνδεση για συστήματα EoC, το ίδιο το γεγονός ότι λειτουργεί ως δικτυακή σύνδεση, σημαίνει ότι πακέτα δεδομένων από πολλαπλές συσκευές μπορούν να μοιραστούν το διαθέσιμο bandwidth. Αυτό συνεπάγεται **αυξημένη ευελιξία κατά τον σχεδιασμό ενός αναβαθμισμένου συστήματος**. Για παράδειγμα, αν ένα παραδοσιακό καλωδιακό σύστημα έχει μία μόνο κάμερα στην άκρη ενός parking, μπορεί να αντικατασταθεί μόνο με άλλη μεμονωμένη κάμερα. Ωστόσο η ομοαξονική σύνδεση μπορεί μέσω ενός EoC switch να επιτρέψει σε πολλαπλές συσκευές να συνδεθούν στο δίκτυο, χωρίς την ανάγκη επιπλέον καλωδίωσης.

Το EoC switch ουσιαστικά κωδικοποιεί τα πακέτα δεδομένων

δικτύου, ώστε να μπορούν να μεταδίδονται μέσω ομοαξονικών μέσων και στην άλλη άκρη της σύνδεσης μετατρέπεται τα πακέτα ξανά στην αρχική μορφή τους, ώστε να μεταδοθούν μέσω καλωδίωσης LAN και WAN. Σε κάθε περίπτωση, η λειτουργία των συσκευών EoC και των συνδέσεων που χρησιμοποιούν ομοαξονικό εξοπλισμό, παραμένει αόρατη και απρόσκοπτη.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι **μπορούν να προστίθενται συσκευές σε δικτυακά συστήματα με ελάχιστο επιπλέον κόστος για hardware ή software**, εκτός από το EoC switch. Σε κάποιες εφαρμογές, το switch μπορεί επίσης να χρησιμοποιηθεί για να τροφοδοτήσει μέσω PoE (Power over Ethernet) τις τερματικές συσκευές.

Οι εφαρμογές από κτίριο προς κτίριο, όπου πρέπει να μεταδίδονται πολλαπλές ροές IP streams μεταξύ τους, μπορούν να επιτευχθούν με τη χρήση EoC, όπου υπάρχει παλαιότερη καλωδίωση. Πολλοί κατασκευαστές προσφέρουν επίσης συστήματα παρόμοια με το EoC, που μπορούν να χρησιμοποιήσουν τις υπάρχουσες συνδέσεις UTP επίσης.

Κάτι τελευταίο που πρέπει να λάβουμε υπ' όψη κατά τη σχεδίαση ενός συστήματος που κάνει χρήση EoC switches, είναι ότι αυτή η προσέγγιση επιτρέπει τη δημιουργία ενός LAN υψηλών επιδόσεων, χωρίς να χρειάζεται να χρησιμοποιήσουμε το εταιρικό LAN μας. Μπορεί να δημιουργηθεί ένα αυτόνομο δίκτυο που να χρησιμοποιεί παλαιότερη υποδομή. Έπειτα, μπορεί να τοποθετηθεί ένα gateway για να επιτρέψει την πρόσβαση από το εταιρικό δίκτυο στο δίκτυο της ασφάλειας, εξασφαλίζοντας ότι στο σύστημα ασφαλείας μπορούν να έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα, χωρίς να το εκθέτουμε σε πιθανές ευπάθειες που ίσως υπάρχουν στο εταιρικό δίκτυο.

Αυτή η προσέγγιση όχι μόνο απλοποιεί τη συνεργασία με το τμήμα πληροφορικής, καθώς εξαλείφονται οι φόβοι για καταπόνηση του δικτύου από τα δεδομένα βίντεο και ασφάλειας, αλλά επίσης **βοηθάει στη δημιουργία μίας πιο ισχυρής πολιτικής κυβερνοασφάλειας**.





Μεγαλύτερη κάλυψη

Ένας από τους ελάχιστους περιορισμούς που σχετίζονται με τη δικτυακή μετάδοση είναι η εμβέλεια μετάδοσης των 100 μέτρων. Κάθε δίκτυο που θέλει να λειτουργεί ξεπερνώντας αυτή την απόσταση, απαιτεί συσκευές που ονομάζονται repeaters (επαναλήπτες). Αν και αυτό το πρόβλημα δεν είναι αξεπέραστο, περιλαμβάνει επιπλέον καλωδίωση και κόστος για συμπληρωματικές συσκευές. Πάντως, το θέμα της απόστασης μπορεί να αντιμετωπιστεί χρησιμοποιώντας συγκεκριμένα EoC switches.

Πολλά LAN είναι σχεδιασμένα για να κάνουν χρήση συμβατικών LAN switches, μαζί με τους εγγενείς περιορισμούς αποστάσεων. Γι' αυτό και πολλοί εγκαταστάτες που πραγματοποιούν μεταβάσεις συστημάτων σε δικτυακή λογική, πιστεύουν ότι η μόνη επιλογή είναι να ξηλώσουν τελείως την παλαιότερη υποδομή και να εγκαταστήσουν νεότερα PoE switches, συγκεκριμένων προδιαγραφών.

Το θέμα που προκύπτει είναι ότι εξ αιτίας των εξόδων που προκαλεί η ανάγκη διπλασιασμού της υπάρχουσας υποδομής, αυτή η προσέγγιση μπορεί να αποτελέσει το κύριο εμπόδιο ώστε να μη συμφωνήσουν οι τελικοί χρήστες για τη μετάβαση σε μία αποκλειστικά IP πλατφόρμα.

Η χρήση της υπάρχουσας υποδομής επιτρέπει στην πραγματικότητα τη χρήση switches PoE μεγάλης εμβέλειας, που επιτρέπουν στους πελάτες να μετατρέψουν την υποδομή UTP παλαιού τύπου, τηλεφωνίας ή πολλαπλών ζευγών, σε μια ισχυρή πλατφόρμα IP. Τα switches είναι ιδανικά για πολλές συμβατικές τερματικές συσκευές, όπως κάμερες, αποκωδικοποιητές, ελεγκτές θυρών και άλλες συσκευές ασφαλείας. Ωστόσο θα υποστηρίξουν επίσης συγκεκριμένες συσκευές πληροφορικής και τηλεπικοινωνιών.

Η τοποθέτηση τέτοιων switches εξαλείφει την ανάγκη ξηλώματος της υποδομής, προσφέροντας έναν διακριτικό και

οικονομικό τρόπο μετάβασης σε IP, χωρίς θέμα περιορισμού αποστάσεων. Αυτό ισχύει γιατί τα switches μεγάλων αποστάσεων προσφέρουν ανώτερη δυνατότητα μετάδοσης χωρίς ανάγκη για repeaters.

Η εξοικονόμηση κόστους γίνεται εμφανής όταν διαπιστώσετε ότι τα switches μπορούν να υποστηρίξουν τη **λειτουργία τερματικών συσκευών σε δίκτυο έως και 700 μέτρων**, ακόμα και όταν χρησιμοποιούν υπάρχουσα ομοαξονική καλωδίωση. Η εναλλακτική προσέγγιση, όπου γίνεται χρήση καθιερωμένων LAN switches, απαιτεί έξι καμπίνες εξοπλισμού, repeaters, και εγκατάσταση νέας καλωδίωσης Ethernet.

Η χρήση switches μεγάλων αποστάσεων καθιστά ένα μεγάλο εύρος εργασιών εγκατάστασης **πιο απλές και ευέλικτες, κατά τη μετάβαση σε IP**. Αυτή η προσέγγιση απλοποιεί πολύ την ολοκλήρωση πλήρους ή μερικής μετάβασης. Το κάθε switch μεγάλων αποστάσεων συνδέεται στον server, και η λύση IP τοποθετείται δίπλα στην παλαιότερη λύση. Η μετάβαση από μερική σε πλήρη μετάβαση, προϋπολογισμού επιτρεπόντος και η κίνηση από ένα εκτεταμένο LAN σε κάποιο ξεχωριστό, είναι έτσι επίσης πολύ απλές εργασίες για εγκαταστάτες και ενσωματωτές.

Εν κατακλείδι

Η δυνατότητα αξιοποίησης της υπάρχουσας υποδομής είναι ιδανική για πολλές εφαρμογές και απλοποιεί σημαντικά τη μετάβαση σε ψηφιακή πλατφόρμα. Το PoE μεγάλων αποστάσεων επιτρέπει στους εγκαταστάτες να κάνουν ομαλά τη μετάβαση, δημιουργώντας μία ξεχωριστή ή ενσωματωμένη τοπολογία LAN.

Κατά τη μετάβαση αναλογικών συστημάτων, ή την αντικατάσταση AHD με μία ευέλικτη και ωφέλιμη λύση, η μετάβαση σε δικτυωμένη πλατφόρμα είναι αναγκαία για τους μηχανικούς που σκέφτονται μακροπρόθεσμα.



Η Τεχνητή Νοημοσύνη -Artificial Intelligence (AI)- βρίσκεται σήμερα στην κορυφή της ατζέντας των συζητήσεων παγκοσμίως ως μια τεχνολογική επανάσταση που επηρεάζει καθοριστικά τις εξελίξεις σε επιστημονικό, επαγγελματικό, οικονομικό και κοινωνικό επίπεδο. Αξίζει λοιπόν μια ιδιαίτερη ανάλυση προκειμένου αποτυπώσουμε πώς το AI επιδρά ευρύτερα στο τομέα της φυσικής ασφάλειας και ειδικότερα στις υποδομές βιντεο-επιτήρησης.

Τεχνητή Νοημοσύνη - AI - Artificial Intelligence. Δυο λέξεις, μια συντομογραφία που σίγουρα συναντάμε όλο και πιο συχνά θα λέγαμε σε κάθε πτυχή της ζωής. Στην ειδησεογραφία, σε επαγγελματικές αναφορές, σε επιστημονικές αναλύσεις, σε συνέδρια, σε εμπορικές προβολές, αλλά θα λέγαμε και στη καθημερινότητα μας. Άλλες φορές τρομάζει, ενώ άλλες προκαλεί ενθουσιασμό! Υπάρχουν οι ένθερμοι υποστηρι-

κτές, αλλά και οι σκεπτικιστές σε ότι αφορά την ευρεία υιοθέτηση της Τεχνητής Νοημοσύνης.

Το σίγουρο είναι ότι το AI δεν αποτελεί σήμερα, απλά και μόνο ένα “buzzword” ή ένας marketing όρος χωρίς πρακτικό αντίκρισμα – όπως μπορεί να συνέβαινε τα παλαιότερα χρόνια – αλλά αποτελεί, μια **κυρίαρχη τεχνολογική τάση που μετουσιώνεται σε πρακτικές εφαρμογές**, μέσα από ένα πλήθος συστημάτων προϊόντων και ολοκληρωμένων λύσεων σε πολλές κάθετες αγορές και βιομηχανίες. Σε όλο αυτό το περιβάλλον όπως διαμορφώνεται σταδιακά με την καθολική επίδραση του AI, **ο τομέας της ασφάλειας στην ευρύτερη διάσταση** του δεν θα μπορούσε να μείνει ανεπηρέαστος.

Και στους δυο κόσμους της ασφάλειας λοιπόν, τον φυσικό και τον ψηφιακό κόσμο, διαπιστώνουμε ενσωμάτωση της τεχνητής νοημοσύνης σε πολλές λειτουργίες των συστημάτων που αναπτύσσονται και σε πολλές πτυχές των έργων και των εφαρμογών που υλοποιούνται. Θα μπορούσαμε να ισχυριστούμε ότι για το AI υπάρχει ακόμα πεδίο δόξης λαμπρό στον ευρύτερο χώρο της ασφάλειας και όχι μόνο για την κάλυψη υψηλών απαιτήσεων σε κρίσιμης σημασίας έργα, αλλά και για πιο καταναλωτικές εφαρμογές.

Η τεχνητή νοημοσύνη μπορεί να μετατοπίσει το σύγχρονο τοπίο της ασφάλειας να έχει καταλυτικό ρόλο στον τομέα

της επιτήρησης και γενικότερα να **αλλάξει δραματικά τον τρόπο με τον οποίο οι χρήστες αλληλεπιδρούν με τα συστήματα ασφαλείας.**

Σε κάθε περίπτωση όμως απαιτείται μια σύνθεση και μια ρεαλιστική προσέγγιση μέσα από μια ορθολογιστική αξιολόγηση της κάθε προτεινόμενης λύσης με Τεχνητή Νοημοσύνη και των αναγκών που καλύπτει. Θα πρέπει να είμαστε σίγουροι για το πότε χρησιμοποιείται, από ποιους και για ποιο λόγο. Επίσης απαιτείται και καλύτερη κατανόηση των όρων που συνοδεύουν το AI όπως είναι το Deep Learning (βαθιά εκμάθηση) και Machine Learning (μηχανική εκμάθηση).

Όλες αυτές τις πτυχές του AI που εξακολουθεί να είναι μια αναδυόμενη τεχνολογία με πολλά περιθώρια εξέλιξης, θα επιχειρήσουμε να αναδείξουμε μέσα από το συγκεκριμένο άρθρο.

Τί προσφέρει η τεχνητή νοημοσύνη;

Η ανίχνευση σεναρίων υψηλού κινδύνου πριν κλιμακωθούν είναι ένα από τα βασικά κίνητρα πίσω από την ανάπτυξη της τεχνητής νοημοσύνης (AI) για εφαρμογές ασφαλείας. Με την τεχνητή νοημοσύνη στη φαρέτρα τους, οι διαχειριστές συστημάτων επιτήρησης μπορούν πέρα από μια απλή παρακολούθηση να αξιοποιούν κάθε καρέ βίντεο και σύνολο δεδομένων που είναι διαθέσιμα για τον εντοπισμό απειλών και την αντιμετώπιση καταστάσεων έκτακτης ανάγκης.

Η τεχνητή νοημοσύνη, μεταξύ άλλων, θα λέγαμε ότι συνιστά μια ισχυρή μέθοδο συλλογής, αξιολόγησης, επεξεργασίας και ανάλυσης δεδομένων κάθε μορφής, με κύριο στόχο την εξαγωγή ουσιαστικών συμπερασμάτων, που θα μπορούν να βοηθήσουν να καταλήξουμε σε αποφάσεις πιο γρήγορα, αλλά και πιο σωστά, ή ακόμα και να αυτοματοποιήσουμε διαδικασίες στο μέγιστο βαθμό. Το AI ως ορισμός, είναι μεταγενέστερος του Machine Learning (μηχανική εκμάθηση) ή του machine processing, ενώ το Deep Learning «βαθιά εκμάθηση» θα λέγαμε πως είναι μια εξέλιξη του AI.

Ειδικότερα τώρα σε ότι αφορά στην εφαρμογή του όρου του



Η Τεχνογνωσία μας Προνόμιό μας!



Η Ασφάλεια

Η Επιτήρηση

Ο Έλεγχος

Η Ποιότητα

Η Αξιοπιστία

Η Προστασία

Η Τεχνογνωσία

έχουν κοινό συνώνυμο!



www.techforall.gr

TECHFORALL™
Η Τεχνογνωσία μας Προνόμιό μας!



AI στη βιομηχανία της ασφάλειας και πιο συγκεκριμένα στον τομέα της βιντεο-επιτήρησης, θα λέγαμε ότι συνιστά αρχικά τη δυνατότητα των συστημάτων αυτών να λαμβάνουν και να επεξεργάζονται σημαντικές πληροφορίες και δεδομένα από τις κάμερες ασφάλειας και άλλους διασυνδεδεμένους αισθητήρες σε ταχύτατους χρόνους, που πριν μερικά χρόνια δεν θα μπορούσαμε καν να φανταστούμε, όχι μόνο στους “αναλογικούς καιρούς” αλλά και κατά τον πρώτο ψηφιακό μετασχηματισμό των συστημάτων ασφάλειας.

Στη συνέχεια η κυριότερη εφαρμογή του AI είναι στα λογισμικά συστήματα διαχείρισης βίντεο, τα γνωστά σε όλους μας VMS: Video Management Software. Εδώ θα πρέπει να επισημάνουμε ότι λειτουργίες που συναντάμε στα VMS όπως: αναζήτηση αντικειμένου, αφαίρεση αντικειμένου, ανίχνευση κίνησης, παραβίαση χώρου και γραμμής και άλλα εργαλεία που γνωρίζουμε από τα video analytics δεν πρέπει να συγχέονται άμεσα με το AI. Όλες αυτές οι λειτουργίες που προϋπήρχαν της ενσωμάτωσης της Τεχνητής Νοημοσύνης, είναι analytics τα οποία τώρα δουν υποστηρικτικά προς το AI, αλλά δεν είναι από μόνα τους AI.

Η τεχνητή νοημοσύνη σίγουρα έχει καταφέρει να βελτιστοποιήσει την αξιοπιστία των μοντέλων και των παραπάνω σεναρίων σε απόλυτο βαθμό, αλλά κάνει και περισσότερα πράγματα με κυριότερο να μαθαίνει από το περιβάλλον.

Αλληλεπίδραση με τους χρήστες

Είναι γεγονός ότι ο ανθρώπινος εγκέφαλος έχει πεπερασμένα όρια στην ικανότητα συλλογής και επεξεργασίας δεδομένων σε συγκεκριμένη χρονική περίοδο. Αυτοί οι περιορισμοί ισχύουν φυσικά και για τους επαγγελματίες χειριστές καμερών ασφάλειας σε ένα κεντρικό σταθμό, που εποπτεύουν ζωντανά αλλά και διαχειρίζονται σε πραγματικό χρόνο μια πληθώρα καμερών από πολλαπλά σημεία εγκαταστάσεων. Το AI όμως θα λέγαμε ότι είναι μια τεχνολογία που δεν έχει όρια, δεν κουράζεται, δεν εφρυσχάζει και μπορεί ταυτόχρονα να αναλύσει τεράστιο όγκο δεδομένων, υπερκαλύπτοντας τις όποιες ανθρώπινες αδυναμίες.

Θα πρέπει εδώ να επισημάνουμε όμως, ότι η τεχνολογία AI

για εφαρμογές ασφάλειας δεν έχει σχεδιαστεί με στόχο να αντικαταστήσει τον ανθρώπινο παράγοντα, αλλά κυρίως για **να ενισχύσει την αντίληψη και διορατικότητα** του και να τον βοηθήσει να εντοπίσει γρήγορα ένα πιθανό συμβάν, να το αξιολογήσει και να πάρει τις σωστές αποφάσεις στο σωστό χρόνο.

Η βασική ιδέα του AI στο τομέα της βιντεο-επιτήρησης είναι να στρέψει την προσοχή των ανθρώπων που έχουν την ευθύνη διαχείρισης των συστημάτων ασφάλειας στα σημεία που χρίζουν άμεσης ανταπόκρισης, να επικεντρωθούν δηλαδή στα πιθανά συμβάντα απειλής της ασφάλειας έγκαιρα και αποτελεσματικά, με αξιοπιστία και ακρίβεια.

Προκειμένου να επιτευχθεί αυτό, οι μηχανισμοί που συνιστούν το AI σε ένα σύστημα ασφάλειας, τροφοδοτούνται συνεχώς από πληροφορίες που περιέχουν χρήσιμα δεδομένα από το περιβάλλον και συμπεριφορές μεμονωμένων ατόμων αλλά και ενός πλήθους. Αναλύοντας αυτές τις πληροφορίες, μπορούν να εξαχθούν αξιόπιστα συμπεράσματα για πιθανές κακόβουλες ενέργειες πριν αυτές εκδηλωθούν, έτσι ώστε έπειτα από την κατάλληλη ενημέρωση το προσωπικό ασφάλειας -ιδιωτικής αλλά και δημόσιας δύναμης- να αναλάβει δράση επιχειρώντας στο πεδίο δράσης για το έλεγχο και την αποτροπή αυτών των ενεργειών.

Με την τεχνητή νοημοσύνη οι κάμερες επιτήρησης δεν έχουν απλά ένα παθητικό ρόλο ως μέσο παρακολούθησης εικόνων, αλλά παράλληλα αποκτούν λειτουργίες ενός αισθητήρα συλλογής σημαντικών δεδομένων αναγνώρισης και ανίχνευσης προσώπων, συμπεριφορών και άλλων χρήσιμων στοιχείων με αυτοματοποιημένες διαδικασίες σε πραγματικό χρόνο που επιτρέπουν στο επιχειρησιακό προσωπικό ασφάλειας, αλλά και τους υπεύθυνους διαχειριστές και διοικητές έργων, να λάβουν τις σωστές αποφάσεις.

Η ανάλυση συμπεριφοράς μπορεί επίσης να χρησιμοποιηθεί για τη διασφάλιση της ασφάλειας στο χώρο εργασίας.

Ειδικά σε ό,τι αφορά στην **ανίχνευση και ανάλυση ανθρώπινης συμπεριφοράς** και ειδικότερα την αναγνώριση προσώπων ως μέρος του AI σε συνδυασμό με τη δημιουργία βάσεων δεδομένων, γίνεται μεγάλη συζήτηση παγκοσμίως, ως ένα εργαλείο που μπορεί πραγματικά να δώσει θετικά αποτελέσματα στην πρόληψη και αποτροπή βαριάς εγκληματικότητας, όπως είναι οι τρομοκρατικές ενέργειες, ενώ από την άλλη πλευρά εγείρονται και αρκετές αντιδράσεις σχετικά με την προστασία προσωπικών δεδομένων σε δημόσιους χώρους.

Βαθιά Εκμάθηση - Deep Learning

Το επόμενο επίπεδο του AI είναι το Deep Learning AI, που επιτρέπει μέσα σε ένα διασυνδεδεμένο οικοσύστημα βίντεο

επιτήρησης και άλλων αισθητήρων, μια συγκριτική ανάλυση μεγάλου όγκου δεδομένων σε βάθος με πληροφορίες που έχουν συλλεχθεί από πολλαπλές πηγές ίσως και σε διαφορετικά σημεία. Μια ανάλυση με βάση νευρωνικά δίκτυα που προσδίδει στο σύστημα ασφάλειας τη δυνατότητα να εκπαιδεύεται και να προσαρμόζεται συνεχώς σε νέα δεδομένα, να αναγνωρίζει μοτίβα και να εντοπίζει πιθανές απειλές.

Με μια ευρύτερη διάσταση λοιπόν, η τεχνητή νοημοσύνη σε μια πλατφόρμα ασφάλειας, θεωρείται ως η βάση για την αξιοποίηση ενός συστήματος μηχανών με στόχο τη συλλογή, επεξεργασία, ανάλυση και παραγωγή πληροφοριών, που λαμβάνονται από τη λήψη βίντεο ή τις προηγμένες δυνατότητες των video analytics.

Το τι μαθαίνουν οι μηχανές αυτές, εξαρτάται από το τι τους ζητείται. Η αλήθεια είναι, πως ο μόνος τρόπος προκειμένου η Τεχνητή Νοημοσύνη να παράγει τα επιθυμητά αποτελέσματα, είναι να υπάρχουν πολλές και επαρκείς πληροφορίες που θα βοηθήσουν το εκάστοτε σύστημα να μάθει αυτά που χρειάζεται.

Αν δεν υπάρχουν αρκετές πληροφορίες, τότε πρέπει θα πρέπει να εμβαθύνουμε ακόμα περισσότερο σε κάποιες από αυτές ή να μάθουμε στο σύστημα περισσότερα πράγματα κάτι που αποτυπώνει ο όρος Deep Learning «βαθιά εκμάθηση» AI. Πρακτικά, αυτό σημαίνει ότι πρέπει να μάθουμε περισσότερα και σε βαθύτερο επίπεδο, προκειμένου να λάβουμε τις συνδυασμένες πληροφορίες που είναι απαραίτητες για την επίτευξη του επιθυμητού αποτελέσματος.

Η «βαθιά εκμάθηση» μπορεί να μας δώσει τη δυνατότητα να κατανοήσουμε περισσότερα για τα χαρακτηριστικά και τις συμπεριφορές των προσώπων. Η εφαρμογή αυτών των πληροφοριών μπορεί στη συνέχεια να εφαρμοστεί περαιτέρω για να κατανοήσουμε τον τρόπο ερμηνείας των προτύπων συμπεριφοράς με τελικό στόχο την πρόβλεψη συμπεριφοράς. Αυτή η πρόβλεψη απαιτεί κάποιο βαθμό ανθρώπινης ερμηνείας, έτσι ώστε να είμαστε σε θέση να ερμηνεύσουμε πρότυπα ύποπτης συμπεριφοράς ή απλά να αναζητήσουμε

άτομα ενδιαφέροντος με βάση αυτά τα πρότυπα.

Αυτά τα ίδια πρότυπα εξελίσσονται σε τεχνητή νοημοσύνη η οποία με την πάροδο του χρόνου αυξάνει την ικανότητα της μηχανής να προβλέπει με μεγαλύτερη ακρίβεια συμπεριφορές που οδηγούν στη λήψη αποφάσεων για την προστασία προσώπων και την ασφάλεια εγκαταστάσεων.

Αυτή η τεχνολογία συνιστά μια ολιστική αξιοποίηση των δεδομένων, συνδέοντας μεμονωμένα σημεία συλλογής για να εντοπίσει τι ακριβώς συμβαίνει, προκειμένου να εντοπίσει γρήγορα καταστάσεις υψηλού κινδύνου πριν κλιμακωθούν. Στον τομέα της παρακολούθησης βίντεο, ξεχωρίζουν πολλές εφαρμογές που μπορούν να επωφεληθούν από τη βαθιά εκμάθηση.

Αναγνώριση προσώπου

Η τεχνολογία βαθιάς εκμάθησης έχει βελτιώσει σημαντικά το ποσοστό ακρίβειας της αναγνώρισης προσώπου. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ διενήργησε δοκιμές για την αναγνώριση προσώπου (Face Recognition Vendor Test (FRVT) FRVT) κατά την τελευταία δεκαετία. Οι βελτιώσεις τα τελευταία χρόνια είναι πολύ σημαντικές και τα ποσοστά σφάλματος αναγνώρισης προσώπων έχουν μειωθεί σε πολύ μεγάλο βαθμό. Τα περισσότερα από τα σημερινά εμπορικά προϊόντα αναγνώρισης προσώπου που παρουσιάζουν κορυφαία απόδοση βασίζονται στη βαθιά εκμάθηση. Η ακρίβεια έχει φτάσει το 99,9% για ελεγχόμενα περιβάλλοντα όπως εφαρμογές αναγνώρισης προσώπων σε διαδικασίες ελέγχου αεροδρομίου, σύμφωνα με έρευνα του Πανεπιστημίου του Τελ Αβίβ.

Ταχύτερη αναζήτηση

Αξίζει επίσης να σταθούμε στη λειτουργία αναζήτησης, η οποία επιτυγχάνεται με πολύ ταχύτερο και αποτελεσματικό τρόπο μέσα από τους μηχανισμούς που προσφέρει το AI. Οι διαχειριστές των συστημάτων έχουν πλέον στα χέρια τους εργαλεία με τεχνητή νοημοσύνη, που έχουν σχεδιαστεί για να κάνουν την αναζήτηση αρχείων βίντεο με ιδιαίτερο ενδιαφέρον τόσο εύκολη, όσο η αναζήτηση σε μια μηχανή στο διαδίκτυο. Πρόκειται για εργαλεία με εξελιγμένη βαθιά εκμάθηση AI, που καθιστούν εφικτή μια μηχανή αναζήτησης βίντεο που επιτρέπει πολύ γρήγορα τον εντοπισμό συγκεκριμένων προσώπων ή οχημάτων από όλες τις κάμερες σε μια περιοχή με την εισαγωγή εύκολων κριτηρίων και χαρακτηριστικών.

Όταν ο διαχειριστής ασφαλείας διαθέτει για παράδειγμα περιγραφές φυσικών χαρακτηριστικών ενός ατόμου που πιθανώς να εμπλέκεται σε ένα συμβάν, **η τεχνολογία AI**





του επιτρέπει να ξεκινήσει μια αναζήτηση επιλέγοντας απλώς ορισμένα στοιχεία, όπως το φύλο, την ηλικία, το ύψος ή το χρώμα του ρουχισμού. Κατά τη διάρκεια κρίσιμων ερευνών, όπως στην περίπτωση ενός αγνοούμενου ή ύποπτου για μια εγκληματική ενέργεια σε ένα προκαθορισμένο πεδίο θέασης ή ένα πολυσύχναστο δημόσιο χώρο, αυτή η δυνατότητα είναι ιδιαίτερα πολύτιμη, καθώς με βάση απλές περιγραφές καθίσταται εφικτή η εξαγωγή συμπερασμάτων σε πολύ σύντομα χρονικά διαστήματα.

Εστιασμένη προσοχή

Η δυνατότητα της τεχνητής νοημοσύνης να επιτυγχάνει σημαντική μείωση του χρόνου της απόλυτης προσοχής που πρέπει να επιδεικνύουν οι ελεγκτές στην επιτήρηση εικόνων από κάμερες ασφάλειας, είναι πολύ σημαντική και χρήσιμη, αν αναλογιστούμε ότι κατά το χρόνο αυτής της εργασίας, υπάρχει όπως προαναφέρθηκε σταδιακή μείωση της ικανότητας και της προσοχής των χειριστών στη κάθε λεπτομέρεια και πληροφορία ως απόρροια των φυσικών ανθρώπινων χαρακτηριστικών.

Ο κάθε ελεγκτής σε ένα κέντρο ελέγχου καμερών από ένα σημείο και μετά μπορεί να εστιάζει μόνο σε πληροφορίες ή γεγονότα που του προκαλούν ενδιαφέρον ή είναι ασυνήθιστα. Το εύρος της προσοχής του μειώνεται σημαντικά έπειτα από κάποιο χρονικό διάστημα και η πιθανότητα να του ξεφύγει κάτι που μπορεί να αποτελέσει γενεσιουργό αιτία μιας ενδεχόμενης απειλής δεν είναι μικρή. Εδώ έρχεται και πάλι το AI **να βοηθήσει τους ελεγκτές να εστιάζουν σε συμβάντα που χρήζουν περαιτέρω διερεύνησης.**

Μια αλλαγή ή μια ασυνήθιστη διεργασία σε μια τυπική δραστηριότητα σε μια περιοχή ανιχνεύεται άμεσα και με αυτοματοποιημένο τρόπο ενημερώνεται ο χειριστής προκειμένου άμεσα να εστιάσει τη προσοχή του εκεί. Στην ουσία μιλάμε για ένα αυτοματοποιημένο επίπεδο ανίχνευσης συμβάντων στην επιτήρηση, που βασίζεται όχι μόνο σε προκαθορισμένα σενάρια όπως γίνεται στα συμβατικά video analytics, αλλά

και στην ανίχνευση δραστηριότητας που το ίδιο το σύστημα εντοπίζει και προέρχονται από αλλαγές στο περιβάλλον από το οποίο συλλέγει και επεξεργάζεται συνεχώς δεδομένα.

Μιλάμε για ένα δυναμικό περιβάλλον που εξελίσσεται διαρκώς και συμβάλει στην ενίσχυση της απόδοσης της προσοχής των χειριστών και στην βελτιστοποίηση των αποφάσεων που λαμβάνει. Δεν καταργείται φυσικά η ανάγκη συνεχούς παρακολούθησης των καμερών από τους χειριστές αλλά τους βοηθάει να εστιάζουν σε σημεία ενδιαφέροντος καθώς και να επαληθεύουν αξιόπιστα κάποια γεγονότα έτσι ώστε η ανάληψη της όποια δράσης να είναι προς τη σωστή κατεύθυνση και στο σωστό χρόνο.

Εφαρμογές πέρα από την ασφάλεια

Η τεχνητή νοημοσύνη ως μέρος ενός συστήματος ασφάλειας και ειδικότερα της βίντεοεπιτήρησης, θα μπορούσε να προσφέρει σημαντικά οφέλη στους οργανισμούς όχι μόνο στις εφαρμογές που είναι αποκλειστικά για την ασφάλεια, αλλά και σε άλλους τομείς όπως για παράδειγμα στην καλύτερη διαχείριση του πλήθους σε μεγάλους εμπορικούς χώρους για τη συλλογή δεδομένων που σχετίζονται με τη συμπεριφορά των πελατών ή ακόμα και σε άλλους χώρους μαζικής παρουσίας, όπως μια έκθεση ή μια εκδήλωση για την ανάλυση της κίνησης των επισκεπτών.

Αυτό εμφανίζεται συνήθως με τη μορφή χαρτογράφησης θερμότητας του πλήθους των ατόμων σε αυτούς τους χώρους και η ανάλυση όλων αυτών των στοιχείων μπορούν να οδηγήσουν σε χρήσιμα συμπεράσματα και αποφάσεις όπως οι αλλαγές των σημάτων της χωροθέτησης προϊόντων με απώτερο σκοπό την βελτίωση της εμπειρίας των πελατών και των επισκεπτών αλλά και την αύξηση των πωλήσεων και των εσόδων.

Επίσης οι έξυπνες πόλεις έχουν τη δυνατότητα να αξιοποιούν δίκτυα έξυπνων αισθητήρων για τη λήψη δεδομένων και με τη βοήθεια της τεχνητής νοημοσύνης σε πλατφόρμες βίντεοεπιτήρησης να βελτιστοποιούμε διαδικασίες όπως η ροή της κυκλοφορίας.

Ειδικότερα την εποχή των μέτρων για την αντιμετώπιση της διασποράς του covid-19 τα εργαλεία τεχνητής νοημοσύνης θα αποδειχτούν ιδιαίτερα χρήσιμα στις προσπάθειες για τη διαχείριση πλήθους και τον περιορισμό σημείων συνωστισμού.

Το AI έχει έρθει για να μείνει και είναι σίγουρο ότι τα επόμενα χρόνια θα έχει καταλυτικό ρόλο στη βιομηχανία των συστημάτων ασφάλειας και ακόμα μεγαλύτερη επιρροή στην υλοποίηση των έργων, μιας και τα πλεονεκτήματα είναι ιδιαίτερα σημαντικά.

it **PROFESSIONAL** security

ΣΗΜΕΙΟ
ΑΝΑΦΟΡΑΣ
ΣΤΗΝ ΕΝΗΜΕΡΩΣΗ
ΓΙΑ ΤΟ CYBER SECURITY ΚΑΙ ΤΟ BUSINESS IT



ΚΥΚΛΟΦΟΡΕΙ
ΤΟ ΝΕΟ ΤΕΥΧΟΣ!!!

www.itsecuritypro.gr



SMART PRESS
Μάγερ 11, 10438, Αθήνα

T. 210.5201500, 210.5231555
F. 210.5241900

www.smartpress.gr
smart@smartpress.gr

Συνέπεια, εξέλιξη και συνεχή εκπαίδευση!

Η συνέντευξη με τους επαγγελματίες εγκαταστάτες συστημάτων ασφαλείας έχει σε αυτό το τεύχος “άρωμα γυναίκας” αφού συναντήσαμε την κυρία Ολιάννα Μπέλλα - Ιδιοκτήτρια και υπεύθυνη της Bella Security Group με έδρα την Μεσσηνία.



Συνέντευξη με την Ολιάννα Μπέλλα – Ιδιοκτήτρια της Bella Security Group

Κυρία Μπέλλα είστε η πρώτη γυναίκα στην Ελλάδα, που διαθέτει τις απαραίτητες και νόμιμες άδειες που πρέπει να έχει ένας επαγγελματίας εγκαταστάτης συστημάτων ασφαλείας. Πείτε μας λίγα λόγια για το πώς ξεκινήσατε και πως εξελιχθήκατε στο συγκεκριμένο επάγγελμα που μέχρι στιγμής είναι ανδροκρατούμενο!

Καταρχήν θα ήθελα να σας ευχαριστήσω για την φιλοξενία σας στο περιοδικό Security Manager και για την ευκαιρία που μου δίνεται να παρουσιάσω και να αναφερθώ στις δυνατότητες και στα πλεονεκτήματα που παρέχει η εταιρεία μου.

Η εταιρεία μας διαθέτει: Άδεια Λειτουργίας Ιδιωτικής Επιχείρησης Υπηρεσιών Παροχής Υπηρεσιών Ασφάλειας (ΙΕΠΥΑ) - Τύπου Α για Παροχή Υπηρεσιών Φύλαξης - Τύπου Β Άρθρο 3 για Εγκαταστάσεις Συστημάτων Ασφάλειας.

Το επαγγελματικό μου ξεκίνημα έγινε το 2015 στην Πύλο Μεσσηνίας, ιδρύοντας την δική μου επιχείρηση. Αρχικά δραστηριοποιήθηκα στο χώρο των φυλάξεων με στατική φύλαξη και περιπολίες, η φύλαξη είναι αναμφισβήτητα ένας ιδιαί-

τερος επαγγελματικός κλάδος. Με την πάροδο των χρόνων και δειλά δειλά μετά από πολύ διάβασμα, πολλά σεμινάρια και εκπαίδευση ασχολήθηκα με τον τομέα των συστημάτων ασφαλείας, το οποίο εξακολουθεί μέχρι τώρα να είναι ανδροκρατούμενη ειδικότητα. Σίγουρα η αρχή ήταν αρκετά δύσκολη και χρειάστηκε χρόνος, κόπος και αρκετή θέληση και προσπάθεια από την πλευρά μου προκειμένου να γίνει αποδεκτή και στη συνέχεια να καθιερωθεί φυσιολογικά ευρύτερα στη περιοχή η επαγγελματική μου δραστηριότητα.

Ποιες είναι οι σημαντικότερες απαιτήσεις για την ασφάλεια στην περιοχή που δραστηριοποιήστε, τι έργα κυρίως καλείστε να αναλάβετε ως εταιρεία ;

Στο νομό Μεσσηνίας και πιο συγκεκριμένα στην περιοχή της Πύλου όπως και στις γύρω περιοχές, τα τελευταία χρόνια έχει παρατηρηθεί αυξημένη παραβατικότητα όπως κλοπές, ληστείες και διαρρήξεις σε επαγγελματικούς χώρους και μόνιμες ή εξοχικές κατοικίες. Η ανοδική πορεία της τοπικής εγκληματικότητας καθιστά λοιπόν επιτακτική την ανάγκη φύλαξης και τη λήψη μέτρων προστασίας όπως είναι η εγκατάσταση συστημάτων ασφαλείας.

Οι πελάτες που προσεγγίζουν την BELLA SECURITY GROUP, αναζητούν από εμάς τη συνέπεια που μας διέπει και κυρίως τη σιγουριά και ασφάλεια, όχι μόνο για την περιουσία τους, αλλά και σε προσωπικό και οικογενειακό επίπεδο. Για να προσφέρουμε το υψηλότερο επίπεδο προστασίας στους πελάτες μας, επιλέγουμε τα καλύτερα συστήματα ασφαλείας, πραγματοποιώντας παράλληλα οικονομοτεχνικές μελέτες και επιτυγχάνοντας βέλτιστες εγκαταστάσεις. Η επιχείρησή μας μπορεί να καλύψει όλων των ειδών τα έργα έχοντας πραγματοποιήσει με επιτυχία μελέτες και εγκαταστάσεις σε οικίες, καταστήματα, δημόσια κτίρια, εργοτάξια, φωτοβολταϊκά πάρκα, αγροκτήματα και άλλους χώρους. Ταυτόχρονα προσφέρουμε υπηρεσίες φύλαξης, περιπολίες και ασφάλεια σε συναυλίες και σε ομιλίες επισήμων. Εξίσου χρήσιμη, είναι και η σύνδεση των εγκαταστάσεων των πελατών μας με το

Κέντρο Λήψης Σημάτων καθώς η υπηρεσίας της Άμεσης Επέμβασης συνθέτοντας ένα σύνολο ολοκληρωμένων υπηρεσιών ασφάλειας.

Πως αξιολογείτε την τεχνολογική εξέλιξη των συστημάτων ασφάλειας σήμερα;

Για εμένα η εξέλιξη είναι τρόπος ζωής, για αυτό και ως εταιρία παρακολουθούμε συνεχώς τις τάσεις στη βιομηχανία των προϊόντων ασφάλειας. Είμαστε συχνά σε επικοινωνία με κατασκευαστικούς οίκους και τους προμηθευτές τους, παρακολουθούμε διαρκώς σεμινάρια για νέα προϊόντα, με στόχο να βαδίζουμε παράλληλα με τις νέες τεχνολογικές προκλήσεις. Μια από τις επικρατούσες τάσεις που απασχολεί σίγουρα, είναι ο συνδυασμός ασφάλειας και αυτοματισμού που καθιστά ευκολότερη τη λειτουργία πολλών υποδομών γενικότερα. Ένα απλό ενδεικτικό σενάριο αυτού του συνδυασμού, είναι για παράδειγμα όταν ενεργοποιηθεί ο συναγερμός να ανοίγει ταυτόχρονα ο εσωτερικός και ο περιμετρικός φωτισμός μιας εγκατάστασης και να αποστέλλει push notification με το συμβάν στο διαχειριστή, μεταδίδοντας live video ή φωτογραφίες από το σημείο που γίνεται το συμβάν. Αυτή η δυνατότητα δημιουργεί συνθήκες υψηλότερης προστασίας αλλά και ευκολίας στη διαχείριση.

Τί χρειάζεται σήμερα μια εταιρία εγκατάστασης προκειμένου να ανταποκριθεί με επιτυχία στο κρίσιμο ρόλο που έχει στη κοινωνία;

Για να σταθεί σήμερα αποτελεσματικά μια εταιρία στο χώρο των συστημάτων ασφάλειας θα πρέπει τα στελέχη της να διαθέτουν άριστη τεχνογνωσία, να ενημερώνονται και να εκπαιδεύονται πάνω στις νέες τεχνολογίες. Επίσης θα πρέπει να υπάρχει συνεχή επαφή με τον πελάτη και να διακρίνεται από εχεμύθεια, συνέπεια και αποτελεσματικότητα, προσφέροντας πρακτικές και αξιόπιστες λύσεις.

Από την πλευρά τους οι πελάτες θα πρέπει να επιλέγουν αδειούχους και πιστοποιημένους εγκαταστάτες και όχι απρόσωπες εταιρείες. Σήμερα παρατηρείται συχνά το φαινόμενο κάποιοι καταναλωτές να καταφεύγουν στο Internet για την αγορά συστημάτων ασφαλείας. Η επιλογή αυτή μπορεί να αποδειχτεί πολύ προβληματική, αφού τη σωστή και αξιόπιστη ασφάλεια με πιστοποιημένα συστήματα και προδιαγραφές, δεν μπορείς να τη βρεις σε ράφι στο σούπερ μάρκετ ή στο internet. Η BELLA SECURITY GROUP είναι μέλος του Συνδέσμου Αδειοδοτημένων Επιχειρήσεων Εγκατάστασης Συστημάτων Ασφαλείας Ελλάδος (Σ.Α.Ε.Ε.Σ.Α.Ε.) και όλοι μαζί προσπαθούμε να ενώσουμε τις δυνάμεις μας να αντιμετωπίσουμε τις παθογένειες που προκύπτουν από μη νόμιμους

εγκαταστάτες και τις εταιρείες χωρίς άδεια.

Γνώμονας για όλες τις εταιρίες πρέπει να είναι η σωστή πώληση των συστημάτων και η προσεκτική και αποτελεσματική εγκατάσταση και γενικότερα η εξυπηρέτηση και η υποστήριξη κάθε πελάτη. Δεν πρέπει ποτέ να ξεχνάμε ότι κάποιοι άνθρωποι εμπιστεύονται σε εμάς το υπέρτατο αγαθό της ασφάλειας τους, για αυτό και οφείλουμε όλοι μας να ανταποδίδουμε αυτή την εμπιστοσύνη με το καλύτερο δυνατό τρόπο.



Λίγα λόγια για την BELLA SECURITY GROUP



Η BELLA SECURITY GROUP ιδρύθηκε το 2015 με έδρα την Πύλο Μεσσηνίας και αποτελεί μια δυναμική εταιρία που ασχολείται με την φύλαξη και εγκατάσταση συστημάτων ασφάλειας σε κάθε τομέα (Συναγερμοί, CCTV, Access Control, Πυρασφάλεια) και BMS (Building Management Systems),

Με βασικά κριτήρια την συνέπεια, τον επαγγελματισμό, την αφοσίωση και την υψηλή ποιότητα υπηρεσιών στελεχώνεται από ανθρώπους με πολυετή εμπειρία και τεχνογνωσία στην ασφάλεια που συνεχώς βελτιώνονται με τη συνεχή παρακολούθηση εκπαιδεύσεων, σεμιναρίων και εκθέσεων.

Η εταιρεία προσφέρει ένα συνολικό φάσμα υπηρεσιών ασφάλειας (Total Security Package) επιλέγοντας για τους πελάτες της τα καλύτερα υλικά με υψηλές προδιαγραφές από τις μεγαλύτερες Αμερικανικές και Αγγλικές εταιρείες συστημάτων ασφαλείας.

ADESCO MQ03-LTE-M

Προσθέτει ευφυΐα σε κάθε απλό
DSC και Honeywell σύστημα συναγερμού

Μια νέα συσκευή της Adesco που υιοθετεί ότι πιο σύγχρονο τεχνολογικά, ήρθε και επιτρέπει σε όσους επαγγελματίες τοποθετούν συστήματα DSC και Honeywell να μεταμορφώσουν τους απλούς πίνακες των δυο αυτών σημαντικών brand σε ένα έξυπνο, λειτουργικό και εντελώς νέο σύστημα ασφάλειας!



Οι μονάδες **MQ03-LTE-M / MN02-LTE-M series** που συνδυάζονται άψογα με τους πίνακες των DSC και Honeywell, προσφέρουν με μια απλή κίνηση τα παρακάτω χαρακτηριστικά.

Διαχρονική τεχνολογία επικοινωνίας LTE-M - Όταν οι άλλοι θα τρέχουν να αλλάξουν συσκευές εσείς θα είστε από τώρα έτοιμοι για την κατάργηση των δικτύων 3G / 2G!!!

Σύνδεση μέσω BUS - Με αυξημένες λειτουργίες απομακρυσμένης διαχείρισης για DSC (PC series), HONEWELL (Vista): πλήρης & μερική όπλιση, αφόπλιση, bypass & real status ζωνών.

Universal συσκευές GLOBAL

sim - IoT - Ακόμα και για εγκαταστάσεις που δεν έχουν DSC ή HONEYWELL, είναι συμβατές με όλα τα συστήματα ασφαλείας. Διαθέτουν Dial capture

interface που υποστηρίζει πρωτόκολλα Contact ID & SIA.

Γενικές Λειτουργίες - Απομακρυσμένη όπλιση / αφόπλιση (μέσω κλειδοδιακόπτη) του συστήματος συναγερμού, αποστολή push notifications & emails, έλεγχος τάσης λειτουργίας και κατάστασης σύνδεσης στο δίκτυο.

Επιτήρηση επικοινωνίας - Ανά 3min για σύνδεση μέσω GPRS/ανά 20sec για σύνδεση μέσω LAN.

Web portal - Διαχείριση εγκαταστάτη - Αποκτήστε τον έλεγχο και την online διαχείριση όλων των συσκευών σας 365 ημέρες τον χρόνο, 24/7!!!

Σχετικά με τις **Διαδραστικές λειτουργίες** των συσκευών, υποστηρίζουν εφαρμογές smartphone app Ios & Android για τον τελικό πελάτη και admin για τον εγκαταστάτη καθώς και απομακρυσμένο έλεγχο και διαχείριση, ενημερώσεις Real-time με push notifications και email.

Ο κάθε επαγγελματίας τεχνικός εγκαταστάτης συστημάτων ασφαλείας που θα αξιοποιήσει τις νέες συσκευές της Adesco θα αποκτήσει **σημαντικά ανταγωνιστικά πλεονεκτήματα** όπως: **Προστιθέμενη αξία και smart χαρακτηριστικά** στις παλιές εγκαταστάσεις προσφέροντας σύγχρονες λύσεις στον τελικό πελάτη σου σε πολύ προσιτή τιμή - **Διαφοροποίηση από τον ανταγωνισμό** σε νέες προσφορές.

Ευελιξία στην επιλογή του κέντρου λήψης σημάτων και απόλυτος έλεγχος του πελατολογίου με δυνατότητα up/downloading μέσω της συσκευής. Πρόσθετη **διπλή πηγή εσόδων**. **Εύκολη πώληση συσκευής και υπηρεσίας** αφού ο τελικός πελάτης αντιλαμβάνεται εύκολα και άμεσα τα οφέλη και τα πλεονεκτήματα. **Ολοκληρωμένη υπηρεσία** με μια συσκευή πιστοποιημένη βάσει διεθνών standards με ενσωματωμένη κάρτα sim Global, απόλυτη ασφάλεια συνδεσιμότητας VPN και πιστοποίηση ISO 27001 για την ασφάλεια διαχείρισης πληροφοριών.



Provision-ISR Easy-check EC-001

Η Provision-ISR παρουσίασε το νέο Easy-check EC-001 που αποτελεί ένα εξελιγμένο σύστημα ελέγχου πρόσβασης υψηλής ποιότητας. Με έρευνα και ανάπτυξη στο Ισραήλ, έχει σχεδιαστεί ώστε να αποτρέπει τη διασπορά ιών όπως ο COVID-19.



Η συσκευή Provision-ISR Easy-check EC-001 υποστηρίζει έλεγχο πρόσβασης με αναγνώριση προσώπου, εντοπισμό για μάσκα προστασίας και θερμομέτρηση σύμφωνα με τις πρόσφατες οδηγίες για την ασφάλεια και την πρόληψη κινδύνων από τον COVID-19.

Στις βασικές λειτουργίες του Easy-check, περιλαμβάνεται η **εύκολη ενσωμάτωση** με ηλεκτρονικά ελεγχόμενες θύρες, τουρνικέ κ.λπ., η **βέλτιστη λειτουργία** σε σύνθετα περιβάλλοντα φωτισμού, η **ακρίβεια μέτρησης** θερμοκρασίας καθώς και **οι φωνητικές εντολές**. Διαθέτει σύστημα αναγνώρισης προσώπου με **ακρίβεια 99.7%** και δυνατότητα δημιουργίας βάσης δεδομένων με επιτρεπόμενα ή αποκλεισμένα πρόσωπα. Το Easy-check θα μπλοκάρει τον χρήστη που δεν θα φοράει προστατευτική μάσκα. Στον χρήστη θα γίνεται παρατήρηση να φορέσει προστατευτικό εξοπλισμό για να του δοθεί πρόσβαση.

Το Easy-check βασίζεται στους πιο **πρόσφατους αλγόριθμους αναγνώρισης προσώπου**, που επιτρέπουν στη συσκευή να αναγνωρίζει ένα πρόσωπο ακόμα και όταν ο χρήστης φοράει προστατευτική μάσκα, καθώς αναγνωρίζει τα χαρακτηριστικά του προσώπου που δεν

καλύπτονται από την μάσκα. Κάθε χρήστης θα μπορεί να διατηρεί τη μάσκα στο πρόσωπό του, ενώ εξακολουθεί να έχει πρόσβαση στις εγκαταστάσεις, χωρίς να απαιτείται η αφαίρεση αυτής.

Η μονάδα μέτρησης θερμοκρασίας επιτρέπει στο Easy-check να εκτελεί μια **γρήγορη και ακριβή μέτρηση θερμοκρασίας** σώματος. Όταν η θερμοκρασία του σώματος του χρήστη είναι πάνω από την κανονική, το Easy-check θα ενεργοποιήσει συναγερμό ή θα στείλει φωνητική ειδοποίηση στον διαχειριστή ελέγχου πρόσβασης ή στο κέντρο ελέγχου.

Το EC-001 μπορεί να λειτουργήσει και ως **αυτόνομο σύστημα ελέγχου πρόσβασης**, υποστηρίζοντας πρωτόκολλο Wiegand για τη διασύνδεση με εξωτερικό καρταναγνώστη, που επιτρέπει στον χρήστη να εισέλθει χρησιμοποιώντας μια κάρτα ελέγχου πρόσβασης. Για την έξοδο του χρήστη, υπάρχει η δυνατότητα διασύνδεσης κομβίου που τοποθετείται από την εσωτερική πλευρά του σημείου πρόσβασης.

Το Easy-check διαθέτει ελληνική γλώσσα, δυνατότητα διασύνδεσης με το λογισμικό Ossia CMS v1.2.1 για τη ρύθμιση της μονάδας επιτρέποντας μεταξύ άλλων τη βασική διαμόρφωση συσκευής, τη διαχείριση βάσης δεδομένων καθώς και την ανίχνευση/αναγνώριση προσώπου.

Λαμβάνοντας υπόψη όλες τις ανωτέρω προδιαγραφές έχει τη δυνατότητα να επιτρέψει ή να απαγορεύσει την πρόσβαση και παράλληλα να ενεργοποιήσει οπτικό και ηχητικό συναγερμό στο ενσωματωμένο ηχείο και την έγχρωμη οθόνη 8" ή να ενεργοποιήσει έξοδο συναγερμού. Παράλληλα έχει δυνατότητα εγγραφής φωτογραφιών και video είτε τοπικά σε κάρτα SD ή στο απομακρυσμένο λογισμικό διαχείρισης OSSIA CMS.

Η συσκευή μπορεί να εγκατασταθεί σε **νοσοκομεία, σχολεία, λεωφορεία, κυβερνητικές εγκαταστάσεις, εταιρείες, λόμπι ξενοδοχείων** και σε οποιοδήποτε μέρος απαιτεί μέτρα πρόληψης κινδύνων.

CADDX xGen Connect

Έλεγχος με ένα άγγιγμα

Η CADDX διευρύνει τη γκάμα συστημάτων στο τομέα του συναγερμού που διαθέτει στην Ελλάδα η G.I. SECURITY SA, προσθέτοντας τη νέα σειρά μονάδων με την ονομασία xGen Connect.



Οι πίνακες της νέας σειράς διαθέτουν έως 8 ενσωματωμένες ζώνες, έως 8 partitions και υποστηρίζουν μέχρι 48 ζώνες. Επίσης κάθε μονάδα στη νέα σειρά, θα διαθέτει ενσωματωμένο IP και προαιρετικά δέκτη Zwave για υποστήριξη όλων των Zwave συσκευών, WiFi-4G και δέκτη LoNa. Αξίζει να επισημανθεί η πλήρη συμβατότητα της νέας σειράς με την σειρά της CADDX NetworX. Επίσης διαθέτει 2 ξεχωριστά bus για σύνδεση συμβατών περιφερειακών συσκευών της σειράς NetworX και της σειράς xGen. Οι διαστάσεις της πλακέτας είναι ίδιες με της πλακέτας NX-4BO και NX-8BO (Σειρά NetworX) ώστε να διευκολυνθεί η αναβάθμιση της υπάρχουσας εγκατάστασης.

Πολλά από τα παρελκόμενα της CADDX, της οικογένειας networX μπορούν να συνεργαστούν με τη σειρά xGen Connect καθώς διαθέτει εκτός από 4-wire RS-485 xGen BUS επικοινωνίας (για περιφερειακά της σειράς NXG) και 3-wire BUS επικοινωνίας (της σειράς networX). Τα περισσότερα πληκτρολόγια και οι επεκτάσεις ζωνών από την υφιστάμενη σειρά της CADDX μπορούν να λειτουργήσουν και στο καινούργιο xGen Connect αποδεικνύοντας για ακόμα μια φορά το βάρος που δίνει η CADDX στη συμβατότητα των περιφερειακών της και δίνοντας πλήρη ευελιξία στον τρόπο εγκατάστασης που θα επιλέξει ο εγκαταστάτης.

Το νέο xGen Connect

Ως μέρος της οικογένειας της CADDX, η σειρά xGen Connect προσφέρει ένα νέο σύστημα που προσφέρει επεκτασιμότητα, ευελιξία και το πιο σημαντικό, συμβατότητα, κάτι το οποίο ξεχωρίζει τα CADDX από τα άλλα συστήματα συναγερμού, επιτρέποντας στους επαγγελματίες εγκαταστάτες να αξιοποιούν μια ενιαία πλατφόρμα για νέες εγκαταστάσεις, συνδυάζοντας όλη την γκάμα της CADDX με τις πιο σύγχρονες τεχνολογίες που απαιτεί η νέα εποχή.

Το xGen Connect είναι ένας έξυπνος υβριδικός πίνακας συναγερμού που είναι ιδανικός για κατοικίες ή βιομηχανικές εφαρμογές. Με την ικανότητα να ελέγχει μέχρι 48 ζώνες, 8 partitions και μέχρι 100 χρήστες, έχει την ευελιξία να ανταποκριθεί άμεσα στις σύγχρονες απαιτήσεις ασφάλειας. Η ενσωματωμένη θύρα ethernet επιτρέπει μια ασφαλή σύνδεση με το UltraSync, προσφέροντας πρόσβαση σε ένα ευρύ φάσμα υπηρεσιών, συμπεριλαμβανομένων τις αναφορές συναγερμών και απομακρυσμένη συνδεσιμότητα. Μια προαιρετική μονάδα 4G & Wi-Fi router plug-in είναι διαθέσιμη για backup ή για πρωτεύουσα συνδεσιμότητα με το Cloud UltraSync. Την ίδια στιγμή, η μονάδα 4G & Wi-Fi μπορεί να συνδεθεί με το router των πελατών μέσω δικτύου Wi-Fi. Αυτό αποτρέπει την ανάγκη να εγκαταστήσετε ένα καλώδιο ethernet μεταξύ του πάνελ και του router όπου δεν είναι εφικτό. Το Wi-Fi Module διαθέτει επίσης



μια θύρα Ethernet σε περίπτωση που το σύστημα ασφαλείας απαιτεί κάμερες UltraSync για βίντεο επιτήρηση. Η σειρά xGen Connect υποστηρίζει το πρότυπο αυτοματισμού κατοικίας Z-Wave®, επιτρέποντας στους χρήστες να χειρίζονται χειροκίνητα τα φώτα Z-Wave, τους θερμοστάτες και πολλά άλλα, μέσω της εφαρμογής κινητής τηλεφωνίας



UltraSync+. Ταυτόχρονα, μπορούν να δημιουργήσουν καθορισμένα σενάρια στο πάνελ, ώστε να εκτελούνται αυτοματοποιημένες λειτουργίες στην οικεία τους.

Εύκολος έλεγχος και παρακολούθηση

Το σύστημα ασφαλείας xGen Connect μπορεί να ελέγχεται από το πληκτρολόγιο, από ασύρματη οθόνη αφής Wi-Fi και απομακρυσμένα μέσω της εφαρμογής UltraSync+.

Η εφαρμογή UltraSync+ επιτρέπει στο χρήστη να ελέγχει το σύστημα ασφαλείας από συσκευή Apple® iPhone / iPad ή Google Android. Ο χρήστης μπορεί να έχει την πλήρη διαχείριση του συστήματός του, μέσω του πληκτρολογίου, είτε μέσω smartphone ή tablet, καθώς και να παρακολουθήσει ζωντανά ή να αναπαράγει το εγγεγραμμένο βίντεο. Η ίδια εφαρμογή θα επιτρέψει στον εγκαταστάτη να εκτελέσει το προγραμματισμό του συστήματος.

Εύκολος προγραμματισμός

Μόλις όλα τα περιφερειακά του συστήματος συνδεθούν με το xGen Connect χρησιμοποιώντας τη λειτουργία αυτόματης εγγραφής, ο πίνακας μπορεί να προγραμματιστεί από το τοπικό πληκτρολόγιο, από έναν επιτραπέζιο υπολογιστή που συνδέεται με τον ενσωματωμένο web server του πίνακα ή μέσω του λογισμικού διαχείρισης DLX900 που όλοι γνωρίζετε.

Νέα πληκτρολόγια xGen NXG-183X

Μαζί με τις νέες μονάδες η CADDX σας παρουσιάζει και τα νέα πληκτρολόγια LCD NXG-1830 (Λευκό χωρίς

proximity), NXG-1831 (Ανθρακί χωρίς Proximity), NXG-1832 (Λευκό με proximity) και NXG-1833 (Ανθρακί με proximity). Τα νέα πληκτρολόγια της CADDX NXG-183X με ή χωρίς proximity αναγνώστη για xGen NXG-4, NXG-8, NXG-9, NXG-64, NXG-256 και NXG-512 θα είναι σύντομα διαθέσιμα. Υποστηρίζουν πολλαπλές γλώσσες και 3 δυνατότητες όπλισης (Arm Away, Arm Stay και Arm Stay Night (Instant) καθώς και 4 προγραμματιζόμενα πλήκτρα (A/B/C/D) για γρήγορο Chime, Bypass ζωνών καθώς και για λειτουργία σεναρίων που έχουμε ορίσει.

NXG-1830



NXG-1833



Τα βασικά χαρακτηριστικά των μοντέλων που περιλαμβάνονται στη σειρά.

Χαρακτηριστικά	NXG-4	NXG-8	NXG-9
Ενσωματωμένες ζώνες	4	α	8
Μέγιστες Ζώνες	4 ενσύρματες ή 16 ασύρματες	48 ενσύρματες ή ασύρματες	48 ενσύρματες ή ασύρματες
Partitions	4	8	8
Χρήστες	40	100	100
Τηλεχειριστήρια	8	16	16
Πληκτρολόγια	16	24	24
Μέγιστος αριθμός Modules	24	32	32
Ενσωματωμένες έξοδοι	3 OC, BELL	4OC, BELL, Smoke	4OC, BELL, Smoke
Events	1024	1024	1024

Grandstream GSC3610 και GSC3615

Η οικογένεια Facility Management μεγαλώνει!

Δύο νέα μέλη και συγκεκριμένα δύο νέες IP κάμερες απέκτησε πρόσφατα η οικογένεια λύσεων Facility Management Solution της Grandstream.

Η ασφάλεια των κτιρίων είναι σαν την ασφάλιση, είναι κάτι που όλοι ελπίζουμε να είναι αχρείαστο, αλλά μπορεί να έρθει μια μέρα όπου θα είμαστε ευγνώμονες **που έχουμε εφαρμόσει μέτρα ασφαλείας**. Η τεχνολογία που υπάρχει για την προστασία των κτιριακών υποδομών μπορεί να προσφέρει σε οποιονδήποτε ιδιοκτήτη επιχείρησης τα εργαλεία, ώστε να διαχειριστεί με τον καλύτερο δυνατό τρόπο την οποιαδήποτε πιθανή απειλή που προκύπτει, είτε πρόκειται για αποτέλεσμα ζημιάς σε περιουσιακά στοιχεία, διάρρηξη, εσωτερική απειλή ή άλλη απειλή κτιρίου είτε σε άυλα περιουσιακά στοιχεία.

Η **Grandstream**, ο βραβευμένος κατασκευαστής τηλεπικοινωνιακού υλικού για επιχειρήσεις, έχει αναπτύξει μια **ολοκληρωμένη οικογένεια προϊόντων που προσφέρουν φυσική ασφάλεια στις κτιριακές υποδομές** των επιχειρήσεων με τίτλο **Facility Management Solution**. Η λύση αυτή απαρτίζεται από κάμερες, συστήματα πρόσβασης και ελέγχου, διασυνδέονται με υπάρχουσες υποδομές επιτήρησης ενώ ταυτόχρονα ενσωματώνονται στις τηλεπικοινωνιακές υποδομές του υπόλοιπου οικοσυστήματος της Grandstream, προσφέροντας ενοποιημένη εμπειρία και ασφάλεια στις επιχειρήσεις που τα αξιοποιούν. Η οικογένεια του Facility Management Solution πρόσφατα απέκτησε **δύο νέα μέλη, τις IP κάμερες GSC3610 και GSC3615**.

Η GSC3615 είναι επιτοίχια κάμερα IP bullet και η GSC360 τοποθετείται στην οροφή και είναι fixed dome IP κάμερα.

Οι κάμερες διαθέτουν υπέρυθρες (IR) με φακό 3,6mm. Υποστηρίζουν ανίχνευση κίνησης και έξυπνη τεχνολογία υπερέυθρων για ισορροπία λευκού και έκθεση στην παρακολούθηση της δραστηριότητας τη νύχτα σε εξωτερικούς ή σκοτεινούς κλειστούς χώρους. Η διαχείριση τους μπορεί να γίνει με το GSURF Pro, το δωρεάν λογισμικό διαχείρισης βίντεο της Grandstream, μαζί με άλλα συστήματα διαχείρισης βίντεο συμβατά με ONVIF. Συνδυάζεται με τα IP video phones της Grandstream με το intercom GSC3570



HD (ενδοεπικοινωνία) και το facility control station (σταθμό ελέγχου εγκαταστάσεων) για την ενεργή παρακολούθηση τελικού σημείου και τον έλεγχο των εγκαταστάσεων. Διαθέτουν ενσωματωμένο PoE για τροφοδοσία των συσκευών & για την παροχή σύνδεσης στο δίκτυο και υποστηρίζει ειδοποιήσεις για εξερχόμενη φωνητική κλήση ή βιντεοκλήση & email screenshot,

Η ανθεκτικότητά τους στις καιρικές συνθήκες (IP66-level αδιάβροχη προστασία) τις καθιστούν τις ιδανικές συσκευές για την διαχείριση των εγκαταστάσεων και την αύξηση της ασφάλειας σε οποιονδήποτε εσωτερικό ή εξωτερικό χώρο. Ιδανική πρόταση για την ευρεία παρακολούθηση του περιβάλλοντος χώρου σε επιχειρήσεις όπως τράπεζες, ξενοδοχεία, καταστήματα λιανικής, γραφεία, αποθήκες και είσοδοι κτιρίων.

Τα προϊόντα της Grandstream αντιπροσωπεύονται στην Ελλάδα από την εταιρεία Partnernet, www.partnernet-ict.com, τηλ.: 210 7100000, sales@partnernet-ict.com

HIKVISION DS-PDP18-EG2

Νέος ενσύρματος παθητικός ανιχνευτής
κίνησης εμβέλειας 18μ

Η HIKVISION, κορυφαίος κατασκευαστής συστημάτων ασφαλείας στον κόσμο, παρουσίασε πρόσφατα ένα νέο οικονομικό παθητικό ανιχνευτή κίνησης υπέρυθρων, που συνδυάζει μοντέρνα σχεδίαση, υψηλή αξιοπιστία και προηγμένες τεχνολογίες.



Πρόκειται για το μοντέλο **DS-PDP18-EG2**, το οποίο διαθέτει μικρό μέγεθος, μοντέρνο σχεδιασμό και διακριτικό φινίρισμα, παρέχοντας μια κομψή λύση ανίχνευσης για κάθε εσωτερικό χώρο.

Ο ανιχνευτής είναι εξοπλισμένος με διπλό πυροηλεκτρικό στοιχείο και φακό τεχνολογίας 3D Fresnel 52 ζωνών με κάθετη προστασία. Η τεχνολογία αυτή, βελτιώνει την ανίχνευση κινούμενων στόχων, διασφαλίζοντας την λήψη σημάτων μεγαλύτερης ακρίβειας από το PIR, με αποτέλεσμα την τέλεια εστίαση του υπέρυθρου σήματος στο πυρο-ηλεκτρικό αισθητήριο. Τα σήματα αυτά στη συνέχεια, αναλύονται από ειδικό αλγόριθμο, που υπάρχει σε μικροεπεξεργαστή και φιλτράρονται κατάλληλα, έτσι ώστε να ενεργοποιείται συναγερμός, μόνο στην περίπτωση που εντοπίζονται κινούμενα αντικείμενα στην περιοχή ανίχνευσης.

Παρέχεται ανοσία σε μικρά ζώα και πουλιά μέχρι 10 κιλά, με τη χρήση προαιρετικής μάσκας pet. Για την ευαισθησία, διαθέτει ρύθμιση με επιλογή αυτόματη, High ή Low

και λειτουργία αυτόματης προσαρμογής σε μεταβαλλόμενες περιβαλλοντικές συνθήκες. Επίσης, διαθέτει τεχνολογία ψηφιακής αντιστάθμισης θερμοκρασίας, η οποία προσαρμόζει ψηφιακά την ευαισθησία του ανιχνευτή για να διατηρήσει το καθορισμένο εύρος ανίχνευσης, όταν η θερμοκρασία στο χώρο είναι κοντά στη θερμοκρασία του σώματος.

Ο ειδικά σχεδιασμένος φακός καλύπτει και την περιοχή των τυφλών σημείων, ακριβώς κάτω από τον ανιχνευτή, αποτρέποντας τον εισβολέα να προσπαθήσει να εισέλθει στον χώρο έρποντας. Η ειδική σχεδίαση του ανιχνευτή με σφραγισμένα οπτικά που αποκλείουν την είσοδο εντόμων και εμποδίζει την κίνηση του αέρα μπροστά από τον πυρο-ηλεκτρικό αισθητήρα και προστατεύει από τις τυχόν ανακλάσεις από το εσωτερικό του περιβλήματος του ανιχνευτή. Διαθέτει ενσωματωμένες τερματικές αντιστάσεις (EOL) συναγερμού 1K, 2K2, 4K7, 5K6 και 8K2 καθώς και EOL αντιστάσεις για το tamper 1K, 2K2, 4K7 και 5K6, οι οποίες επιλέγονται κατά προτίμηση καλύπτοντας τους περισσότερους πίνακες συναγερμούς της αγοράς. Διαθέτει tamper, για προστασία σε περίπτωση αφαίρεσης του καλύμματος.

Προαιρετικά παρέχονται βάσεις στήριξης τοίχου και οροφής. Οι ανιχνευτές μπορούν να τοποθετηθούν σε ύψος από 1,8 έως 2,4 μέτρα. Το εύρος ανίχνευσης μπορεί να φτάσει έως τα 18 μέτρα και η γωνία κάλυψης τις 85.9°. Μπορεί να τροφοδοτηθεί με 9 έως 16 VDC (standard: 12 VDC). Διαθέτει πιστοποίηση EN50131 Security Grade 2. Λειτουργεί χωρίς πρόβλημα σε θερμοκρασίες από -10 °C έως 40 °C, ενώ οι διαστάσεις του ανιχνευτή είναι 65.4mm x 86.8mm x 45.5mm (ΠxΥxΒ).

Hikvision DS-D6022FN-B

Digital Signage Monitors



Πρόκειται για τη συσκευή της **HIKVISION**, ένα Android digital Signage monitor 22" Wide (16:9) LED που χρησιμοποιείται για αναπαραγωγή διαφημίσεων, εφαρμογές καταμέτρησης και ελέγχου ροής ατόμων, ελέγχου πυρετού, κ.λπ. Με ανάλυση full HD 1920x1080 και industrial A+ panel, είναι κατάλληλο για λειτουργία 7 x 24 h. Διαθέτει λειτουργικό σύστημα Android 6.0.1, επεξεργαστή CPU 4-core Cortex-A17 1.8 GHz, μνήμη RAM 2 GB, Flash 8 GB, υποδοχή TF Card, Ethernet, Wi-Fi, 2 x USB, ενσωματωμένα ηχεία και εισόδους audio in/out. Υπάρχει δυνατότητα για επίτοιχη

οριζόντια ή κάθετη τοποθέτηση (portrait ή landscape) ενώ στην συσκευασία περιλαμβάνονται βάση και τηλεχειριστήριο. Η κατανάλωση της συσκευής είναι 10~40 W και οι διαστάσεις της (Π×Β×Υ) 517 x 47 x 320 mm. Υποστηρίζει εμφάνιση στατικού και δυναμικού περιεχομένου, συμπεριλαμβανομένων εφαρμογών, εικόνων, ήχου, video, PDF, streaming media, ιστοσελίδων, live video (αποκωδικοποίηση IP καμερών), third-party data, κ.λπ. Εύκολη διαχείριση με το δωρεάν λογισμικό FocSign Lite. Αποτελεί επίσης ιδανική λύση και για δικτυακή παρακολούθηση καμερών μέσω της εφαρμογής Hik-connect. Το αντίστοιχο μοντέλο 32" **DS-D6032FN-B** διαθέτει ενσωματωμένα ηχεία 2 x 2 W, κατανάλωση 10~75 W και διαστάσεις (Π×Β×Υ) 723 x 62 x 423 mm ενώ τα λοιπά τεχνικά χαρακτηριστικά είναι τα ίδια με προηγούμενο monitor. Όλες οι συσκευές Digital Signage της HIKVISION, σε συνδυασμό με τις κατάλληλες κάμερες, μπορούν να χρησιμοποιηθούν επίσης σε εφαρμογές Health & Safety, υποστηρίζοντας τις παρακάτω λειτουργίες:

- Καταμέτρηση και έλεγχο ροής ατόμων. Εμφανίζεται ο αριθμός των ατόμων που είναι εντός του καταστήματος και ο αριθμός των ατόμων που μπορούν ακόμη να εισέλθουν. Δίνεται ειδοποίηση, αν υπάρχει υπέρβαση του μέγιστου αριθμού ατόμων.
- Έλεγχος πυρετού. Εμφανίζεται η εικόνα των αποτελεσμάτων ανίχνευσης της θερμικής κάμερας.
- Διαφήμιση. Αναπαραγωγή διαφημιστικών εικόνων ή βίντεο σε βρόγχο επανάληψης. Το περιεχόμενο των διαφημίσεων μπορεί να προετοιμασθεί με το δωρεάν λογισμικό FocSign Information Release.

ΗΛΚΑ Α.Ε | www.ilka.gr | τηλ.: 210 6071510

KEDACOM IPC2860-HN-PIR15-L0185

Εξωτερικού χώρου πανοραμική 8-Megapixel IP κάμερα, H.265

Το μοντέλο IPC2860-HN-PIR15-L0185 της KEDACOM αποτελεί μια εξωτερικού χώρου fish-eye IP κάμερα με αισθητήρα 8-Megapixel, απόδοση 3072x3072 στα 25fps και συμπίεση εικόνας H.265 για εξοικονόμηση bandwidth και αποθηκευτικού χώρου. Διαθέτει φακό 1.85mm για πανοραμική θέαση και ενσωματωμένους προβολείς IR εμβέλειας 15 μέτρων, ενώ με τη λειτουργία Smart IR αποφεύγεται η υπερέκθεση σε περίπτωση που τα αντικείμενα/άτομα βρίσκονται σε πολύ κοντινή απόσταση από την κάμερα. Στα χαρακτηριστικά της κάμερας περιλαμβάνονται οι λειτουργίες WDR, 3DNR, Auto iris, HLC και Digital Defog, το ενσωματωμένο μικρόφωνο, η υποδοχή για κάρτα Micro SD (max. 128GB) και η τροφοδοσία μέσω Ethernet (PoE) αλλά και DC12V. Το περίβλημα της κάμερας είναι αντιβανδαλιστικό (IK10) και προτύπου IP67 για προστασία από νερό και σκόνη, ενώ η κάμερα λειτουργεί σε θερμοκρασίες -40°C ~ 70°C. Όπως όλες οι κάμερες της KEDACOM, η IPC2860-HN-PIR15-L0185 είναι πρωτοκόλλου ONVIF.



Lexis Πληροφορική | www.lexis.gr | τηλ.: 210 6777007

Tiandy TC-NCL514S

5MP Starlight IR Bullet

Μια Starlight κάμερα που ξεχωρίζει στα 5 Megapixel (2592x1944) και στα 0.002 Lux στην έγχρωμη και 0.001 Lux στην ασπρόμαυρη λειτουργία συναντάμε στη συλλογή της Tiandy. Είναι μια κάμερα πολύ υψηλής ποιότητας κατασκευής, με πολύ όμορφο σχεδιασμό non-screw design δηλαδή χωρίς βίδες και είναι IP67. Τα συγκεκριμένα μοντέλα είναι κατασκευασμένα από ένα ειδικό πολυανθρακικό πολυμερές, που ονομάζεται Makrolon®. Το Makrolon, είναι σκληρότερο από το μέταλλο, και το καθιστά πρακτικά άθραυστο και έτσι είναι ιδανικό για αντιβανδαλιστικές εφαρμογές (Vandal Resistant). Επίσης το υλικό αυτό δεν αποχρωματίζεται από τον ήλιο όπως το κοινό πλαστικό που χρησιμοποιούν κάμερες άλλων κατασκευαστών και δεν διαβρώνεται από το αλάτι (Salt-Corrosion Proof). Έτσι, οι κάμερες είναι κατάλληλες για εγκαταστάσεις σε παραθαλάσσιες περιοχές. Τέλος, η αντοχή του σε υψηλές θερμοκρασίες είναι πολύ μεγάλη ενώ ταυτόχρονα θεωρείται επιβραδυντικό κατά της φωτιάς. Οι κάμερες αυτές λειτουργούν σε ακραίες θερμοκρασίες από -35 έως +60 βαθμούς Κελσίου. Επιπλέον η κάμερα ενσωματώνει 50m Smart IR, είναι True WDR 120dB, PoE και πρωτόκολλο συμπίεσης S+265 για πολύ γρήγορη μετάδοση μέσω δικτύων. Επίσης υποστηρίζει 3D DNR, HLC, Smart Defog, OSD. Είναι FULL ONVIF, Triple Stream, ενώ ενσωματώνει προστασία από υπερτάσεις (TVS protection) μέχρι 6.000 Volt. Η σειρά της Tiandy ενσωματώνει αλγόριθμους Video Analytics, για την διαφύλαξη περιμέτρου όπως Perimeter, Double Tripwire και Tripwire, ανίχνευσης πλήθους (Crowd), απωλεσθέντος αντικειμένου (Missing Object), ανίχνευση ανθρώπου που τρέχει (running), εγκαταλελειμμένου αντικειμένου, παράνομου παρκαρίσματος, αντικειμένου που κινείται γρήγορα (Fast Moving), αλλά και Loitering, Blur Image, Scene Change.



G.I Security S.A | www.gisecurity.gr | τηλ.: 210 6040601

Provision-ISR Sirius-Starlight

Εξαιρετική έγχρωμη εικόνα όλο το 24ωρο

Η Provision-ISR παρουσιάζει την νέα σειρά καμερών Sirius, που προσφέρει άριστη φωτεινότητα, ευκρίνεια και ζωντανές χρωματικές εικόνες ακόμα και κατά τη διάρκεια της νύχτας. Οι νέες κάμερες Sirius είναι σχεδιασμένες για να ενισχύουν τις δυνατότητες παρακολούθησης στο σκοτάδι και να προσφέρουν 24 ώρες εξαιρετική έγχρωμη εικόνα. Η συγκεκριμένη σειρά διαθέτει δύο μοντέλα καμερών, που περιλαμβάνει μια τύπου Dome DVL-391AS36 & και μια τύπου Bullet TVL-391AS36. Πιο αναλυτικά, οι κάμερες διαθέτουν ανάλυση 1945(H) x 1097(V) (τεχνολογίες AHD/TVI/CVI) ή 960(H) σε λειτουργία CVBS. Ο ενσωματωμένος φακός 3.6mm F1.0 επιτρέπει πεδίο θέασης στις 87ο ενώ τα ενσωματωμένα LED φωτισμού ενεργοποιούνται αυτόματα, όταν οι συνθήκες το απαιτούν. Στα επιπρόσθετα χαρακτηριστικά συγκαταλέγονται το CoC, το OSD, καθώς και το 3D-DNR. Οι μονάδες παρέχουν στεγανότητα IP66 και χρειάζονται παροχή 12 VDC. Γενικότερα οι κάμερες με τεχνολογία Sirius είναι κατάλληλες για εφαρμογές σε δημόσιους χώρους, βιομηχανικά συγκροτήματα, διασταυρώσεις κυκλοφορίας και γενικότερα σε περιβάλλοντα χαμηλού φωτισμού.



Signal Electronics Security | www.signalsecurity.gr | τηλ.: 210 9576351

Tiandy TC-C34LP

Κάμερα θερμογραφίας με Blackbody



Η θερμογραφική κάμερα της Tiandy TC-C34LP ενσωματώνει αισθητήρα Vanadium Oxide Uncooled Focal Plane Arrays ανάλυσης 256x192, αλλά και ένα οπτικό αισθητήρα 1/1.8" CMOS με ανάλυση 2560x1440. Ο θερμικός αισθητήρας επιτρέπει στην κάμερα να ανιχνεύει αυτόματα τη θερμοκρασία του ανθρώπινου σώματος παρουσιάζοντας ακρίβεια έως και $\pm 0.3^{\circ}\text{C}$ (με τη χρήση της συσκευής blackbody) και έρχεται με NETD (Noise Equivalent Temperature

Difference) στα $<50\text{mk}$ για να διακρίνει μεταξύ πολύ μικρών διαφορών στη θερμική ακτινοβολία μίας εικόνας. Διαθέτει ένα White LED, τεχνολογία WDR στα 120dB και το εξαιρετικό πρότυπο συμπίεσης της Tiandy S+265. Η πατενταρισμένη τεχνολογία S+265 που συναντάμε τόσο στα καταγραφικά όσο και στις κάμερες της Tiandy, μειώνει έως και 70% το bandwidth σε σχέση με άλλες IP της αγοράς (εξαιρετικά χρήσιμο στην Ελλάδα που έχουμε αργό Internet) και ως 8 φορές χαμηλότερες απαιτήσεις αποθήκευσης σε σκληρούς δίσκους. Η TC-C34LP διαθέτει ενσωματωμένο μικρόφωνο και ηχείο, με τεχνολογίας PoE, ενώ πιστοποιείται και με βαθμό στεγανότητας IP67 για να αντέχει στο νερό και τη σκόνη. Η κάμερα της Tiandy είναι κατάλληλη για τοποθέτηση σε εισόδους οργανισμών, εμπορικά καταστήματα, αεροδρόμια, σιδηροδρομικούς σταθμούς, μετρό κ.ά.

Novo Technologies | www.novo.gr | τηλ.: 210 2723127

Dahua DMSS v1.2!

Κυκλοφόρησε η νέα έκδοση!



Η Keeper Group μας ενημερώνει για την νέα έκδοση Dahua DMSS v1.2 καθώς και για την πρόταση της εταιρίας προς όλους τους υπάρχοντες χρήστες να κάνουν λήψη της νέας εφαρμογής, προκειμένου να ωφεληθούν από τα νέα χαρακτηριστικά της - μια και η

έκδοση iDMSS plus και gDMSS plus πρόκειται να σταματήσουν να υποστηρίζονται πλέον. Στα **νέα χαρακτηριστικά** της εφαρμογής συναντάμε: Νέο περιβάλλον χρήστη - Διαμοιρασμός συσκευών μέσω email - Νέο User Interface/User Experience - Υποστήριξη πανοραμικής κάμερας - Υποστήριξη Alarm θερμοκρασίας σώματος - Alarm Face Detection από τη βάση δεδομένων - Ρύθμιση περιόδου υποστήριξης μηνυμάτων με τοπικές συσκευές - Εργαλείο περιόδου υποστήριξης μηνυμάτων με τοπικές συσκευές - Εργαλείο δοκιμής Wi-Fi - Λοιπές Βελτιώσεις.

Keeper | www.keeper.gr | τηλ.: 210 2025705

Vivotek FD9166-HN

Στα 2MP με H.265 και IoT Security



Μια από τις νεότερες προτάσεις στο τομέα των δικτυακών καμερών από την Vivotek, είναι το μοντέλο με κωδικό ονομασίας FD9166-HN που ανήκει στη κατηγορία των fixed dome καμερών με ανάλυση στα 2 MP (30 fps @1920x1080)

με φακό 2.8/3.6mm και τεχνολογία συμπίεσης H.265. Διαθέτει πολλές προηγμένες λειτουργίες υψηλής απόδοσης, όπως WDR Pro για εξαιρετική ορατότητα σε περιβάλλοντα υψηλής αντίθεσης φωτισμού, αλλά και λειτουργία Smart Stream III, για βελτιστοποίηση της απόδοσης εύρους ζώνης. Επίσης ενσωματώνει IR φωτισμό με εμβέλεια 10 μέτρων και υποστηρίζεται από 802.3af Compliant PoE δυνατότητα. Η καλαίσθητη και διακριτική σχεδίαση της κάμερας σε συνδυασμό με το συμπαγές μέγεθος την καθιστούν ιδανική για πάρα πολλές εγκαταστάσεις. Φυσικά θα πρέπει να επισημάνουμε ότι όπως όλες οι δικτυακές κάμερες της Vivotek προστατεύεται από κυβερνοεπιθέσεις με λύσεις ασφάλειας IoT από την Trend Micro.

Lexis Πληροφορική

www.lexis.gr | τηλ.: 210 6777007

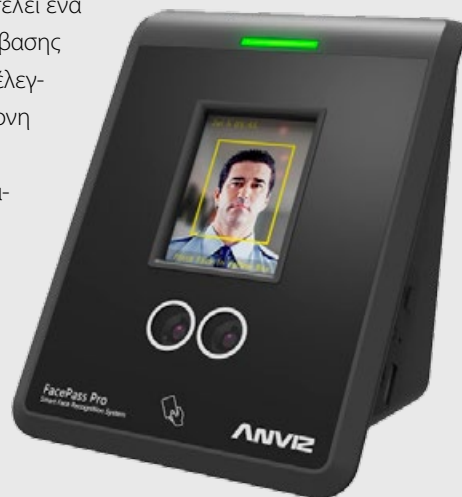
ANVIZ FACEPASS 7 IRT

Αναγνώριση προσώπου και ανέπαφη θερμομέτρηση



Η Anviz σχεδίασε και διαθέτει και στην Ελληνική αγορά μέσω της Sigma το FacePass 7 IRT που αποτελεί ένα τερματικό σύστημα ανέπαφου ελέγχου πρόσβασης και καταγραφής παρουσίας εργαζομένων με έλεγχο και ταυτοποίηση προσώπου και ταυτόχρονη ανέπαφη μέτρηση θερμοκρασίας.

Πρόκειται για ένα σύγχρονο τεχνολογικά σύστημα που διαθέτει λειτουργίες αναγνώρισης προσώπου μέσω διπλής κάμερας και θερμομέτρηση υψηλής ακριβείας, υποστηρίζοντας τεχνητή νοημοσύνη. Ο βασικός ρόλος του FacePass 7 IRT είναι να παρέχει 24/7 ταυτοποίηση με ακρίβεια και να αποτρέπει αποτελεσματικά την πρόσβαση σε μη εξουσιοδοτημένα άτομα. Το σύστημα υποστηρίζει δυνατότητα καταχώρησης 3000 χρηστών (με δακτυλικό αποτύπωμα αλλά και κάρτα) και διαχείρισης 100.000 εγγραφών. Διαθέτει αναγνώστη RFID τεχνολογίας EM ή εναλλακτικά Mifare και η αλληλεπίδραση με το χρήστη γίνεται μέσω οθόνης αφής HD 3.2" με φιλικό μενού χρήσης αλλά και παραμετροποίησης. Η αναγνώριση προσώπου είναι εφικτή σε απόσταση 0.3~0.8 μέτρα με γωνία +/-20ο ενώ η μέτρηση θερμοκρασίας με ακρίβεια 0.3οC με απόσταση μέτρησης 0,3~0,5 μέτρα. Οι μέθοδοι επικοινωνίας είναι μέσω TCP/IP, Wifi, RS-485 και προαιρετικά 4G ενώ παράλληλα ενσωματώνει Web Interface και δωρεάν λογισμικό παρουσίας εργαζομένων.



Sigma Security | www.sigmassec.gr | τηλ.: 210 9716046

Venitem STOP&GO 19 & LED 19

Πινακίδες φωτεινών ενδείξεων ελέγχου πρόσβασης



Η Ιταλική Venitem λανσάρει στην αγορά δύο νέα προϊόντα που έρχονται να δώσουν μία οικονομική λύση σε περιπτώσεις που θέλουμε να έχουμε οπτική και ηχητική σηματοδότηση για την πρόσβαση σε ελεγχόμενους χώρους. Πρόκειται για το μοντέλο VENITEM STOP&GO 19 και το VENITEM LED 19. Το πρώτο μοντέλο είναι μία ιδιαίτερα κομψή πινακίδα 3 φωτεινών ενδείξεων: STOP (κόκκινη), WAIT (πορτοκαλί) και GO (πράσινη), που μιμεί-

ται τη λειτουργία φωτεινού σηματοδότη, για άμεση οπτική επικοινωνία και ελεγχόμενη πρόσβαση. Για την ένδειξη GO μπορεί να επιλεγεί να ηχεί ενσωματωμένος βομβητής για τα πρώτα 2 sec. Κάθε ένδειξη μπορεί να είναι σταθερή ή να αναβοσβήνει (χωριστή επιλογή που μπορεί να γίνει μέσω dip-switch) και ελέγχεται από χωριστή είσοδο 12~28 VDC & 85 mA (max). Συνοδεύεται από 2 films ενδείξεων για κάθετη ή οριζόντια τοποθέτηση. Οι διαστάσεις της πινακίδας είναι (ΠxΒxΥ) 307x44x117mm. Το δεύτερο μοντέλο είναι επίσης μία κομψή μεταλλική πινακίδα 2 φωτεινών ενδείξεων: STOP (κόκκινη) και GO (πράσινη), που μιμείται και αυτή τη λειτουργία φωτεινού σηματοδότη, για άμεση οπτική επικοινωνία και ελεγχόμενη πρόσβαση. Είναι κατάλληλη και για εξωτερική τοποθέτηση (IP 54). Οι ενδείξεις μπορεί να είναι σταθερές ή να αναβοσβήνουν σε συχνότητα 1~3 Hz (ρυθμιζόμενη από ποτενσιόμετρο) και ελέγχονται από 2 χωριστές εισόδους με τάση 11 ~ 28 VDC & 50 mA. Οι διαστάσεις της πινακίδας είναι (ΠxΒxΥ) 65x35x109 mm.

ΗΛΚΑ Α.Ε. | www.ilka.gr | τηλ.: 210 6071510

Garrier NXG-8-BO

Αναβάθμιση του συστήματος ασφάλειας με μία μόνο πλακέτα



Η μονάδα NXG-8-BRO του κατασκευαστή Carrier ως μέλος της νέας οικογένειας UltraSync xGenConnect, προσφέρει επεκτασιμότητα, ευελιξία και συμβατότητα για κάθε τωρινή και μελλοντική ανάγκη. Επιτρέπει στους επαγγελματίες εγκαταστάτες να αναβαθμίσουν τα συστήματα ασφάλειας παλαιότερου τύπου, διαθέτοντας για αυτό το σκοπό 2 ξεχω-

ριστά bus για σύνδεση συμβατών περιφερειακών συσκευών της σειράς NetworX και της σειράς xGen. Η μονάδα συνιστά ένα έξυπνο υβριδικό πίνακα 8 ζωνών με δυνατότητα επέκτασης έως 48 ζώνες και 8 partitions, υποστηρίζοντας 100 χρήστες, όπου κάθε χρήστης μπορεί να έχει 4 προφίλ. Να αναφέρουμε επίσης τον προαιρετικό ασύρματο δέκτη 868MHz ή 433MHz όπου μπορεί να δεχθεί έως 48 ασύρματα αισθητήρια και 16 keyfobs. Η ενσωματωμένη θύρα Ethernet 10/100Base-T IP/LAN, επιτρέπει τη σύνδεση με κέντρο λήψης σημάτων, αλλά και την ασφαλή σύνδεση με το UltraSync+, παρέχοντας πρόσβαση σε αναφορές συναγερμών και απομακρυσμένη συνδεσιμότητα. Κάθε σύστημα συναγερμού xGenConnect μπορεί να ελεγχθεί επιτόπου από πληκτρολόγιο, αλλά και εξ αποστάσεως μέσω της εφαρμογής UltraSync+. Ο ενσωματωμένος web server επιτρέπει στον εγκαταστάτη να έχει πρόσβαση στο σύστημα και να προγραμματίζει κάθε λειτουργία από υπολογιστή, tablet ή smartphone. Διαθέτει 4 εξόδους ανοικτού συλλέκτη, 1 έξοδο για σειρήνα (Bell) και μία για τροφοδοσία πυρανιχνευτών SMOKE καθώς και δυνατότητα ενσωμάτωσης IP καμερών οι οποίες είναι συμβατές με την εφαρμογή UltraSync+. Οι διαστάσεις της πλακέτας είναι ίδιες με της πλακέτας NX-8BO (Σειρά NetworX) ώστε να διευκολυνθεί η αναβάθμιση μια υπάρχουσας εγκατάστασης.

GQ Tech | www.gqtechgr.com | τηλ.: 210 6640025

Satel ACU-220

Universal ασύρματα περιφερειακά και με πιστοποίηση Grade 2



Μια νέα πρόταση στα πιστοποιημένα με GRADE 2 universal ασύρματα συστήματα παρουσιάστηκαν από την Πολωνική εταιρεία SATEL. Σε αυτά συναντάμε τον universal ασύρματο δέκτη ACU-220 καθώς και μια μεγάλη ποικιλία ασύρματων περιφερειακών εσωτερικού και εξωτερικού χώρου. Ο ασύρματος δέκτης, υποστηρίζει αμφίδρομη επικοινωνία στα 868MHz με εμβέλεια μέχρι και 2km σε ανοικτό χώρο και 8 εξόδους για σύνδεση με οποιονδήποτε ενσύρματο πίνακα συναγερμού, καθώς και 4 προγραμματιζόμενες εισόδους, έξοδο χαμηλής μπαταρίας, έξοδο αντί-jamming



Η γκάμα των περιφερειακών περιλαμβάνει: ασύρματες μαγνητικές επαφές - ασύρματους απλούς και

PET ανιχνευτές εσωτερικού χώρου - ασύρματους PET ανιχνευτές εξωτερικού χώρου - ασύρματους ανιχνευτές κουρτίνας - ασύρματους πυρανιχνευτές, καθώς και ασύρματους ανιχνευτές θραύσης κρυστάλλων.

Η εξαιρετική ποιότητα των universal ασυρμάτων SATEL, καθώς και οι οικονομικές τιμές τους, δίνουν στον επαγγελματία εγκαταστάτη τη δυνατότητα κάλυψης των αναγκών των πελατών του με γρήγορη, ποιοτική και οικονομική εγκατάσταση.

Όλα τα προϊόντα προσφέρονται από την Artion Security Systems AE με εγγύηση 5 ετών. Μπορείτε να δηλώσετε συμμετοχή στα σεμινάρια που διοργανώνονται ανά τακτά διαστήματα και γνωρίστε τις εξαιρετικές λύσεις που προσφέρουν τα προϊόντα SATEL.

Artion Security Systems | www.artion-sec.gr | τηλ.: 210 5712000

DefenderTech DT400/800/1600

Συστήματα παραγωγής ομίχλης με ποιότητα και αξιοπιστία



Η Paradox Hellas A.E. ανακοινώνει την αντιπροσώπευση και υποστήριξη των Ιταλικών συστημάτων παραγωγής ομίχλης της εταιρείας DefenderTech (DT) στην Ελλάδα. Η DT είναι μία εταιρεία με μεγάλη εμπειρία στη κατασκευή συστημάτων παραγωγής ομίχλης εστιάζοντας στη ποιότητα και την αξιοπιστία, κάτι που αποδεικνύεται από την αποκλειστική κατασκευή των προϊόντων στην Ιταλία. Τα διάφορα συστήματα παραγωγής ομίχλης διαθέτουν λειτουργία με ή χωρίς τη χρήση κεντρικής μονάδας συναγερμού και πολλαπλά επίπεδα προστασίας από εσφαλμένες ρίψεις, ενώ υπάρχουν επεκτάσεις για δυνατότητα ρίψης από το πίσω μέρος των συστημάτων.

Επιπλέον, υπάρχουν διαθέσιμα συστήματα με δυνατότητα διασύνδεσης δικτύου και ολοκληρωμένη παρακολούθηση κατάστασης / συντήρησης. Διατίθεται λογισμικό κεντρικής διαχείρισης & προβολής κατάστασης όλων των εγκατεστημένων συστημάτων (εφόσον διαθέτουν τη λειτουργία δικτύου). Διαθέτουν αυτονομία ικανότητας ρίψης για 60 δευτερόλεπτα ακόμα και μετά τη διακοπή τροφοδοσίας. Ο μέγιστος χρόνος ρίψης / δημιουργίας ομίχλης υψηλής πυκνότητας, είναι 7 λεπτά με γεμάτο δοχείο. Το δοχείο είναι αφαιρούμενο, δεν είναι υπό πίεση και γεμίζει ξανά εξοικονομώντας σε οικονομία από την αντικατάσταση φιαλών και δοχείων. Επίσης ακόμα μία μεγάλη καινοτομία της DT είναι το υγρό παραγωγής ομίχλης το οποίο είναι απόλυτα ακίνδυνο στο περιβάλλον, τα αντικείμενα και τους ανθρώπους. Δεν είναι τοξικό, εύφλεκτο, εκρηκτικό, δεν διαβρώνει επιφάνειες, δεν είναι αγωγίμο, ενώ είναι από τα λίγα στην αγορά που πληροί όλες αυτές τις προδιαγραφές με πιστοποιητικό από επίσημους φορείς πιστοποίησης. Η σειρά συστημάτων παραγωγής ομίχλης DT400/800/1600 διατίθενται σε τέσσερα διαφορετικά χρώματα (κατόπιν παραγγελίας), ώστε να εναρμονίζονται με το χώρο εγκατάστασης και να δίνουν ένα ωραίο αισθητικό αποτέλεσμα (λευκό, ανθρακί, χρυσό, ασημένιο).

Paradox Hellas | www.paradox.gr | τηλ.: 210 2855000

Carrier NXG-7002

4G/Wi-Fi περιφερειακό GSM για NXG-Connect



Η NXG-7002 είναι μια πλακέτα 4G/WiFi τύπου modular, η οποία προστίθεται και ενσωματώνεται στο σύστημα ασφαλείας xGenConnect. Μπορεί να προγραμματιστεί ως βασικός τρόπος επικοινωνίας (με ΚΛΣ/Push/email) ή ως Backup για την περίπτωση που υπάρχει διαθέσιμη σύνδεση Ethernet ή Wifi. Εάν χαθεί η βασική σύνδεση θα γίνει αυτόματη μετάβαση σε 4G (κινητή). Εάν το 4G δεν είναι διαθέσιμο, η μονάδα θα αλλάξει σε 2G ανάλογα με τα τοπικά δίκτυα των παρόχων ή την κάλυψη. Υποστηρίζοντας έως και 2 συνδέσεις κεραίας τόσο για κινητά όσο και για WiFi, η μονάδα διασφαλίζει μια αξιόπιστη ασύρματη σύνδεση. Ο ενσωματωμένος δρομολογητής WiFi μπορεί να συνδεθεί ασύρματα με το

Router του πελάτη για κύρια πρόσβαση στο Διαδίκτυο. Αυτό αποφεύγει την εγκατάσταση καλωδίου Ethernet μεταξύ του πίνακα xGenConnect και του Router. Ο δρομολογητής WiFi παρέχει επίσης ενσύρματο LAN Ethernet σε περίπτωση που υπάρχει ανάγκη για ενσύρματη σύνδεση μίας ή περισσότερων κάμερες UltraSync.

GQ Tech | www.gqtechgr.com | τηλ.: 210 6640025

VENITEM HEMA

Grade 3 και 4! Ιταλική φινέτσα και αξιοπιστία.



Ο όμιλος Venitem είναι γνωστός ως ένας από τους κορυφαίους κατασκευαστές στον τομέα των συστημάτων ασφάλειας, με πάνω από 40 χρόνια εμπειρίας, που μεταξύ άλλων ειδικεύεται στην παραγωγή σειρήνων με κομψό και εκλεπτυσμένο σχεδιασμό και άψογη ποιότητα. Από τις νέες προτάσεις της εταιρίας, ξεχωρίζει η σειρά HEMA η οποία συνοδεύεται με λειτουργία 2πλου LED σε αναμονή, 5 χρόνια εγγύηση καλής λειτουργίας και 10 χρόνια εγγύηση χρώματος - διατίθεται και σε CHROME. Πρόκειται για αυτόνομη ενσύρματη εξωτερική μαγνητοδυναμική σειρήνα, με λευκό, ασημί, νίκελ ακόμα και μαύρο ματ περίβλημα και μπλε, πορτοκαλί ή γκρι φλας. Διαθέτει πιστοποίηση INCERT Security Grade 3 ή 4 (HEMA-WB-4) και ξεχωρίζει για το μοναδικό Ιταλικό design και την εξαιρετική ποιότητα κατασκευής. Επίσης διακρίνεται για το μεγάλο δυνατό ηχείο με πραγματική ακουστική ισχύ 111dB @ 3m ενώ το φλας με LEDs υψηλής φωτεινότητας και έλεγχο από μικροεπεξεργαστή διαθέτει διπλό tamper, εσωτερικό μεταλλικό κάλυμμα, προστασία από υγρασία με εμβάπτιση πλακέτας σε ρητίνη. Για τις σειρήνες HEMA

προβλέπεται επιλογή τρόπου ενεργοποίησης / ήχου σειρήνας / διάρκειας ενεργοποίησης / αριθμού συναγερμών την ημέρα / λειτουργίας flash / reset flash αλλά και αυτόματος έλεγχος μεγαφώνου (διακοπή πηνίου, ηλεκτρονικά οδήγησης του) και μπαταρίας (ρεύμα φόρτισης, ασύνδετη, χαμηλής τάσης, βλάβης της) με ενεργοποίηση τεχνικής εξόδου, και εσωτερικές οπτικές ενδείξεις σε περίπτωση προβλήματος. Επίσης διαθέτει δυνατότητα προαιρετικής τοποθέτησης εξαρτήματος ανίχνευσης αφρού και κραδασμού (Venitem HEMA-KIT) ενώ δέχεται μπαταρία 12VDC 1.2 ή 2.2Ah (δεν περιλαμβάνεται).

G.I Security S.A | www.gisecurity.gr | τηλ.: 210 6040601

Ajax MotionCam

Ασύρματος ανιχνευτής PIR εσωτερικού χώρου με ενσωματωμένη κάμερα

Με τους ανιχνευτές MotionCam της Ajax ο κάθε χρήστης θα γνωρίζει ανά πάσα στιγμή την κατάσταση στον χώρο του πριν ο κάθε εισβολέας καταλάβει τι έχει συμβεί! Η μονάδα που συνδυάζει ανίχνευση κίνησης και λήψη βίντεο, με το που ανιχνεύσει κίνηση, θα λαμβάνει μια σειρά από διαδοχικές φωτογραφίες όπου θα αποστέλλονται στον χρήστη προκειμένου να αξιολογήσει την κατάσταση!

Το MotionCam χρησιμοποιεί ταυτόχρονα δύο εξειδικευμένα πρωτόκολλα. Το Jeweller για την αποστολή άμεσων συναγερμών και το Wings για γρήγορη παράδοση εικόνων. Το πρώτο στιγμιότυπο του συμβάντος, θα ληφθεί εντός 9 δευτερολέπτων από την ανίχνευση κίνησης!

Η κάμερα ενεργοποιείται μόνο όταν ανιχνευθεί κίνηση, ενώ τα δεδομένα που καταγράφονται κωδικοποιούνται τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση, παρέχοντάς σας τη μέγιστη ασφάλεια.

Η εγκατάσταση του MotionCam μπορεί να γίνει σε απόσταση έως και 1700 μέτρων από το Hub2 (σε ανοιχτό χώρο) αποκτώντας οπτικό έλεγχο ακόμα και των πιο κρίσιμων περιοχών. Ο νέος ανιχνευτής διακρίνεται για την υψηλή λειτουργική απόδοση με έως και 4 χρόνια διάρκεια ζωής της μπαταρίας!



Electrosystems | www.electrosystems.gr | τηλ.: 210 9640258

Avon Beam Barrers

Ασύρματες μπάρες υψηλής αξιοπιστίας



Η Avon Experts αποτελεί εδώ και 8 χρόνια μια κορυφαία εταιρία στο τομέα των συστημάτων περιμετρικής προστασίας, στην γκάμα της οποίας συναντάμε μεταξύ άλλων νέες ασύρματες και αδιάβροχες μπάρες συναγερμού. Οι Avon Beam Barrers, είναι εξοπλισμένες με ευφυή τεχνολογία ανάλυσης Fuzzy Logic, επιτυγχάνοντας ασφαλή ανίχνευση των πραγματικών αιτιών που μπορεί να διακόψουν την επικοινωνία μεταξύ πομπού και δέκτη ή τυχόν περιβαλλοντικές αλλαγές που προκαλούνται από τον δέκτη υπερύθρων, οι οποίες δεν είναι φυσιολογικές. Η σύγχρονη αυτή τεχνολογία επιτυγχάνει ακριβή και ταχεία λειτουργία του συναγερμού με ταυτόχρονη εξάλειψη ψευδών συναγερμών. Η μέγιστη απόσταση ανίχνευσης είναι μέχρι 10 μέτρα και η ρυθμιζόμενη ισχύς γίνεται σε 2 επίπεδα με το χρόνο απόκρισης διακοπής της δέσμης να είναι μικρότερος από 40ms. Απαιτούν τροφοδοσία από μπαταρίες λιθίου 3,6V με

εκτιμώμενο χρόνο λειτουργίας 2,5 με 3 χρόνια. Διαθέτουν ειδικό σχεδιασμό στο κέλυφος τους για προστασία από απευθείας έκθεση στο φως και βαθμό στεγανότητας IP65 για προστασία από υγρασία, σκόνη και βροχή. Στη σειρά συναντάμε μοντέλα με δυο δέσμες και ύψος 48 εκατοστά και με 4 δέσμες και ύψος 65 εκατοστά.

Keeper Group | www.keeper.gr | τηλ.: 210 2025705

Ajax 12 V PSU

Μονάδα τροφοδοσίας για σύνδεση, το Hub/ Hub2/ Hub plus και το Rex σε πηγές χαμηλής τάσης



Η Ajax παρουσίασε τη νέα μονάδα τροφοδοσίας 12 V PSU που μπορεί να χρησιμοποιηθεί για την εγκατάσταση ενός Ajax hub σε τροχόσπιτα, σκάφη, φωτοβολτα-

ϊκά πάρκα και άλλους χώρους που δεν υπάρχει δυνατότητα τροφοδοσίας 220V ή δεν υπάρχει σταθερή παροχή. Η μονάδα τροφοδοσίας είναι συμβατή με το Hub/Hub Plus και το Rex, ενώ διατίθεται διαφορετική πλακέτα για το Hub 2. Το τροφοδοτικό επιτρέπει τη σύνδεση των παραπάνω συστημάτων σε δίκτυο χαμηλής τάσης ή σε μπαταρία. Η μονάδα 12V PSU τοποθετείται στο σώμα της συσκευής και αντικαθιστά την προεγκατεστημένη μονάδα τροφοδοσίας 110/230V. Σχετικά με τα τεχνικά του χαρακτηριστικά έχουμε τάση εισόδου: 8-20V DC - τάση εξόδου: 4.65 V $\pm$ 3% - ρεύμα εισόδου: <1 A - ρεύμα εξόδου: 1,5 A.

Electrosystems

www.electrosystems.gr | τηλ.: 210 9640258

RISCO Touch

Νέο πληκτρολόγιο Αφής 8" σε συνδυασμό με cloud λειτουργίες

Το νέο πληκτρολόγιο της RISCO διαθέτει έξυπνες λειτουργίες συνδυάζοντας υψηλή χρηστικότητα και CLOUD λειτουργίες. Διαθέτει υψηλής ανάλυσης οθόνη 8" με πολύ εύκολο Menu ίδιο με

την εφαρμογή iRisco. Μπορείτε να δείτε τις κάμερες ζωντανά, να ελέγξετε τον συναγερμό σας, να λάβετε ειδοποιήσεις, οπλισμός, αφοπλισμός, να λάβετε εικόνα σε ζωντανό χρόνο και να ελέγξετε το έξυπνο σπίτι σας. Όλα αυτά σε ένα πληκτρολόγιο της RISCO. Δημιουργήστε τα σενάρια σας συνδυάζοντας τα με άλλες λειτουργίες. Υποστηρίζει επικοινωνία: Wi-Fi & RS485 και ανάλυση: 1280*800.



G.I Security S.A

www.gisecurity.gr | τηλ.: 210 6040601



ADESCO

Λεωφόρος Αμαρουσίου 27
141 23
Τηλ.: 210 2912915
e-mail: info@adesco.gr
website: www.adesco.gr



ELECTROSYSTEMS

Λεωφόρος Βουλιαγμένης 262
173 43 Αγ. Δημήτριος
Τηλ.: 210 9640258
Fax: 210 9640258
e-mail: sales@electrosystems.gr
website: www.electrosystems.gr



GRANDE

Λ. Πρωτοπαπαδάκη 83, 111 47 Γαλάτσι
Τηλ. & Fax: 210 2222210 & 210 2135886
e-mail: info@grande.gr
website: www.grande.gr



AKATOS

Σκρά 26 & Θεσσαλονίκης
143 42 Ν. Φιλαδέλφεια
Τηλ.: 210 8074453
Fax: 210 8074425
e-mail: info@akatos.net
website: www.akatos.net



ESA SECURITY SOLUTIONS

Ηνιόχου 26, 152 38 Χαλάνδρι
Τηλ.: 214 1001400
Fax: 214 1001499
e-mail: info@esasecurity.gr
website: www.esasecurity.gr



HELLAS DIGITAL MONITORING SERVICES

Ι. Μεταξά 14, 190 02 Παιανία
Τηλ.: 210 6028120
Fax: 210 6646196
e-mail: info@hellasdms.com
website: www.hellasdms.com



ARTION

Λεωφόρος Αθηνών 189
124 61 Χαϊδάρη
Τηλ.: 210 5712000
Fax: 211 800 2861
e-mail: info@artion-sec.gr
website: www.artion-sec.gr



EUROPA SECURITY

Μακεδονίας 43
241 00 Καλαμάτα
Τηλ.: 27210 24500
e-mail: info@europa.gr
website: www.europa.gr



HIKVISION EUROPE

Dirk Storklaan 3
2132 PX Hoofddorp, The Netherlands
Tel: +31 23 5542770
Fax: +31 23 5631112
general email: sales.eu@hikvision.com
technical support: support.eu@hikvision.com



ATLAS SECURITY

Λεωφόρος Βουλιαγμένης 85
166 74 Γλυφάδα
Τηλ.: 210 9600556
e-mail: info@atlasecurity.gr
website: www.atlasecurity.gr



FORCE

Στ. Σαράφη 15, 122 41 Αιγάλεω
Τηλ.: 210 5757227
Fax: 210 5787342
e-mail: athens@force.gr
website: www.force.gr



ICTS HELLAS

Λ. Βουλιαγμένης 107
166 74 Γλυφάδα
Τηλ.: 210 9616363
Fax: 210 9615238
e-mail: info@icts.gr
website: www.icts.gr



BOOS S.A.

Λεωφόρος Μεσσογείων 262
155 62 Χολαργός
Τηλ.: 210 6549590
e-mail: info@boos.gr
website: www.boos.gr



G.I. SECURITY S.A.

16ο χλμ. Λεωφ. Λαυρίου, 190 02 Παιανία
Τηλ.: 210 6040601
Fax: 210 6658710
e-mail: sales@gisecurity.gr
website: www.gisecurity.gr



ILKA

Τεμπών 14, 153 42 Αγ. Παρασκευή
Τηλ.: 210 6071510
Fax: 210 6071599
e-mail: sales@ilka.gr
website: www.ilka.gr



CPI AE

Ραφαηλίδου 1 & Αγρινίου
177 78 Ταύρος
Τηλ.: 210 4805800
Fax: 210 4805801
e-mail: info@cpi.gr
website: www.cpi.gr



GQ TECH SA

17ο χλμ. Λ. Λαυρίου, 190 02 Παιανία
Τηλ.: 210 6640025
Fax: 210 6640027
e-mail: sales@gqtechgr.com
website: www.gqtechgr.com



INTERTECH SA

Αφροδίτης 24
167 77 Ελληνικό
Τηλ.: 210 9692300
e-mail: info@intertech.gr
website: www.intertech.gr



KEEPER GROUP

Ανθυπολοχαγού Ρεγκούκου 3
111 45 Αθήνα
Τηλ.: 210 2025705
Fax: 210 2018634
e-mail: info@keeper.gr
website: www.keeper.gr



PERIMETRICA

Νίκ. Καζαντζάκη 4
135 61 Άγιοι Ανάργυροι
Τηλ.: 210 8547225
Fax: 210 8547226
e-mail: contact@perimetrica.com
website: www.perimetrica.com



SIGNAL ELECTRONICS SECURITY

Παναγή Τσαλδάρη 25 & Υδρας
176 76 Καλλιθέα
Τηλ.: 210 9576351
Fax: 210 9533464
email: info@signalsecurity.gr
website: www.signalsecurity.gr



NOVO TECHNOLOGIES

Τρωάδος 15
142 33 Νέα Ιωνία
Τηλ.: 210 2723127
Fax: 210 2723128
e-mail: info@novo.gr
website: www.novo.gr



PERSONAL SECURITY

Μεσογείων 99, 151 26 Μαρούσι
Τηλ.: 210 8068675
Fax: 210 6122531
e-mail: info@personalsecurity.gr
website: www.personalsecurity.gr



SPARTAN SECURITY

Δ. Σέχου 17 & Αντιμαχίδου
117 43 Αθήνα
Τηλ.: 210 9232437
Fax: 210 9245747



NSC HELLAS

Στ. Καζαντζίδη 47
555 35 Πυλαία Θεσσαλονίκης
Τηλ.: 2311 821295
Fax: 2311 821296
e-mail: info@nsc-hellas.gr
website: www.nsc-hellas.gr



PGM SYSTEMS

Λευκωσίας 68
121 33 Περιστέρι
Τηλ.: 210 5777800
Fax: 210 5718080
e-mail: info@pgm.gr
website: www.pgm.gr



TECHFORALL

Μ. Αννίνου 10
546 46 Θεσ/νίκη
Τηλ.: 2310 428083
Fax: 2310 428795
e-mail: sales@techforall.gr
website: www.techforall.gr



OLYMPIA ELECTRONICS

72 χλμ. Π.Ε.Ο. Θεσσαλονίκης Κατερίνης
60 300, Τ.Θ. 06 Αιγίνο Πιερίας
Τηλ.: 23530 51200
Fax: 3530 51486
e-mail: info@olympia-electronics.gr
website: www.olympia-electronics.gr



PLANET SECURITY

Μενελάου 32
141 22 Ηράκλειο
Τηλ.: 210 2841680
Fax: 210 2841872
e-mail: info@planet-security.gr
website: www.planet-security.gr



VECTOR SECURITY

Αγίου Σάββα 2, 104 47 Αθήνα
Τηλ.: 210 4925473
Fax: 210 4256763
e-mail: info@vectorsecurity.gr
website: www.vectorsecurity.gr



PARADOX HELLAS

Κορίνθου 3, 144 51 Μεταμόρφωση
Τηλ.: 210 2855000
Fax: 210 2855020
e-mail: paradox-hellas@paradox.gr
website: www.paradox.gr



SDC SECURITY DISTRIBUTION CENTER

87 B&C Aglantzias Avenue Aglantzia
2112 Nicosia, Cyprus
Tel.: +357 22 252040
e-mail: tech@sdccom.cy
website: www.sdccom.cy



Ε.Ο.Α.

Παραδείσου 29 και Ζαγοράς
15125 Παράδεισος Αμαρουσίου
Τηλ.: 210 6851086
e-mail: eoa.sec@gmail.com



PARTNERNET

Σαρανταπόρου 9
155 61 Χολαργός
Τηλ.: 210 2116501
e-mail: sales@partnernet.gr
website: www.partnernet.gr



SIGMA SECURITY - Χ. ΦΕΙΔΑΣ

Εθν. Μακαρίου 5, 173 43 Αγ. Δημήτριος
Τηλ.: 210 9716046
Fax: 210 9754864
e-mail: sales@sigmasec.gr
website: www.sigmasec.gr



Σ.Α.Ε.Ε.Σ.Α.Ε.

Αγ. Δημητρίου Όπλων 82
11145 Αθήνα
Τηλ.: 211 1825516
e-mail: info@saeesae.gr
website: www.saeesae.gr

Axis Brands
Geovision Mobotics Hikvision
Vivotek Crow DSC
Ksenia

> Εγκατάσταση συστημάτων ασφαλείας (συμβατικά, IP)
> Ολοκληρωμένες λύσεις επίβλεψης χώρων με αναλογικές ή IP κάμερες
> Συστήματα πυρανίχνευσης
> Συστήματα ελέγχου πρόσβασης - Access control systems

GWORKS
integrated solutions

Παρθενώνος 1-3 & Τοτσίου 122, Ν. Ερυθραία • Τ.: 211 8006565, 6974 792875 • info@gworks.gr

ΑΘΗΝΑ

Στράτος Πατσέλης
Σύμβουλος Ασφαλείας

Μαιάνδρου 48-50
Αθήνα 14341

Κιν. +30 6932 479 727
Τηλ.: +30 210 7780060

• Εκτίμηση Τρωτότητας
• Διαχείριση Κινδύνου

www.patselis.gr | info@patselis.gr | stratos.patselis@gmail.com

Λέων Λεοντίδης

Main Net

Μελέτες – Εγκαταστάσεις
Συστημάτων Ασφαλείας
Κλειστών Κυκλωμάτων Τηλεόρασης
Έξυπνο Σπίτι

Email: info@mainet.gr

Ηρακλείτου 1, Τ.Κ. 16341 Ηλιούπολη
Τηλ/Fax: 210 9739243. Κιν: 6944 363093 www.mainet.gr

ΑΘΗΝΑ

ΚΑΛΑΜΑΤΑ

SECURE SYSTEMS.GR
Γιαννακόπουλος Νικήτας

✓ Συναγερμοί ✓ Κάμερες
✓ Ελεγχόμενη Πρόσβαση ✓ Πυρανίχνευση
✓ Μηχανή Καπνού ✓ Θυροτηλεόραση
✓ Εφαρμογές Δικτύων ✓ Αυτοματισμοί
✓ Αυτόνομα Φωτοβολταϊκά

Σταδίου 80, Καλαμάτα | Τηλ.: 6974 367 811 – 27210 24564
e-mail: info@securesystems.gr | e-shop: www.securesystems.gr

B-SAFE
ΤΑ ΠΑΝΤΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΑΣ

ΣΥΝΑΓΕΡΜΟΙ | ΠΕΡΙΜΕΤΡΙΚΗ ΦΥΛΑΞΗ |
ΘΥΡΟΤΗΛΕΦΩΝΑ – ΘΥΡΟΤΗΛΕΟΡΑΣΕΙΣ | ΕΛΕΓΧΟΣ
ΠΡΟΣΒΑΣΗΣ | ΠΥΡΑΝΙΧΝΕΥΣΗ | ΧΡΗΜΑΤΟΚΙΒΩΤΙΑ |
ΚΑΜΕΡΕΣ ΑΣΦΑΛΕΙΑΣ | ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ |
ΜΠΑΡΕΣ | ΚΑΓΚΕΛΑ ΑΣΦΑΛΕΙΑΣ | ΛΟΥΚΕΤΑ | ΚΛΕΙΔΑΡΙΕΣ

Γεωργίου Παπανδρέου 51, Θεσσαλονίκη, 546 46
Τ. +30 2310 953 253 F. +30 2313 018 728
www.b-safe.gr | info@b-safe.gr

ΘΕΣΣΑΛΟΝΙΚΗ

ΘΕΣΣΑΛΟΝΙΚΗ

ΚΡΗΤΗ

TECHFORALL™
συστήματα ασφαλείας • κλειστά κυκλώματα tv • δίκτυα

Μ. Αννίνου 10, 546 46 Θεσ/νίκη • techforall.gr
2310 428 083 • 6944 655 660

ΗΛΕΚΤΡΟΝΙΚΗ ΠΡΟΣΤΑΣΙΑ

SECURITYCENTER ((ALARM)) 24

Φραγκιαδάκης Κωνσταντίνος
Συστήματα & Υπηρεσίες Ασφάλειας

Καζαντζάκη 14, Ηράκλειο Κρήτης. Τηλ.: 28910 22262 - Κιν. 694 6216 581

Τα Περιοδικά **Security Manager & IT Security Professional** είναι στο Facebook

facebook.com/SecManagerGr
facebook.com/ITSecProGr

... ΚΑΝΤΕ like και ενημερωθείτε άμεσα για όλες τις εξελίξεις στο χώρο της ασφάλειας



P▲R▲DOX HELLAS A.E.
Συστήματα Ασφαλείας & Πυρανίχνευσης



30 χρόνια δίπλα στον εγκαταστάτη!

▲ Με εκπαιδεύσεις σε νέες τεχνολογίες & νέα προϊόντα!

▲ Με την πλέον άρτια τεχνική υποστήριξη!

▲ Με σεβασμό & διαφάνεια στον εγκαταστάτη!

...και με περισσότερα από 2.000 προϊόντα άμεσα διαθέσιμα!



Συστήματα
Ασφαλείας



Πυρανίχνευση



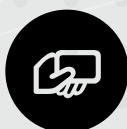
Φωτιστικά
Ασφαλείας



CCTV



Θυροπλεόραση



Access Control



Παραγωγή
Ομίχλης



Εργαλεία
Αναλώσιμα

www.paradox.gr

Κεντρικά: Κορίνθου 3, Μεταμόρφωση 14451 • Τηλ.: 210 28 55 000 • Fax: 210 28 55 020

Εργοστάσιο: 69ο χλμ. Ε.Ο. Αθηνών Λαμίας, Βρύσες Ριτσώνας, Αυλίδα

NXG-8 **NEW 2021** ΗΡΘΕ ΔΥΝΑΜΙΚΑ



- ✓ 8 έως 48 ζώνες
- ✓ 8 περιοχές
- ✓ 100 χρήστες
- ✓ 4 προγραμματιζόμενοι έξοδοι
 - ✓ Ενσωματωμένη IP
 - ✓ Ενσωματωμένο Z-Wave
 - ✓ Web browser
 - ✓ 4G/Wi-Fi plug-on
- ✓ Προαιρετικός δέκτης 433MHz RF
 - ✓ xGen & NX bus επικοινωνίας
- ✓ UltraSync συμβατό
- ✓ EN Grade 2

**ΣΤΗΝ
GQ TECH
ΕΠΙΣΗΜΟ
&
ΑΠΟΚΛΕΙΣΤΙΚΟ
ΑΝΤΙΠΡΟΣΩΠΟ**

TECH SUPPORT
210-664-0025

Η GQ TECH παρέχει
τεχνική υποστήριξη

- Δευτέρα - Παρασκευή
9:00π.μ.-9:00μ.μ.
- Σάββατο
9:00π.μ.-6:00μ.μ.

Δηλώστε συμμετοχή για την παρουσίαση
των νέων προϊόντων της σειράς



xGen
CONNECT



xGen

Η παρουσίαση θα γίνει μέσω ZOOM από τους τεχνικούς
μας οι οποίοι έχουν **εκπαιδευτεί** και **πιστοποιηθεί**
από τον κατασκευαστή (Carrier) για τη νέα σειρά
της NetworX (NX): XGenConnect & xGen.

Δηλώστε συμμετοχή

