secsolution magazine

15

giugno 2021
anno III

Tecnologie e soluzioni per la sicurezza professionale

www.secsolutionmagazine.it

Per fare una smart city ci vuole una smart home

Phygital security: quale protezione contro gli attacchi informatici?

Cybersecurity: le principali minacce per le aziende

Controllo accessi e rilevazione presenze: convivenza quasi perfetta

Tecnoalarm®

Hi-Tech Security Systems

Sistemi antintrusione ad alta tecnologia

RSC® (Remote Sensitivity Control): comunicazione tra l'impianto e il centro di controllo tecnico dell'installatore

HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY

www.tecnoalarm.com

Tecnofire®

Hi-Tech Fire Alarm Systems

Sistemi di rivelazione automatica di incendio

RSC® (Remote Sensitivity Control): programmazione, telegestione e controllo di tutti i parametri di funzionamento

HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY

www.tecnofiredetection.com

www.eea-security.com

MASTER

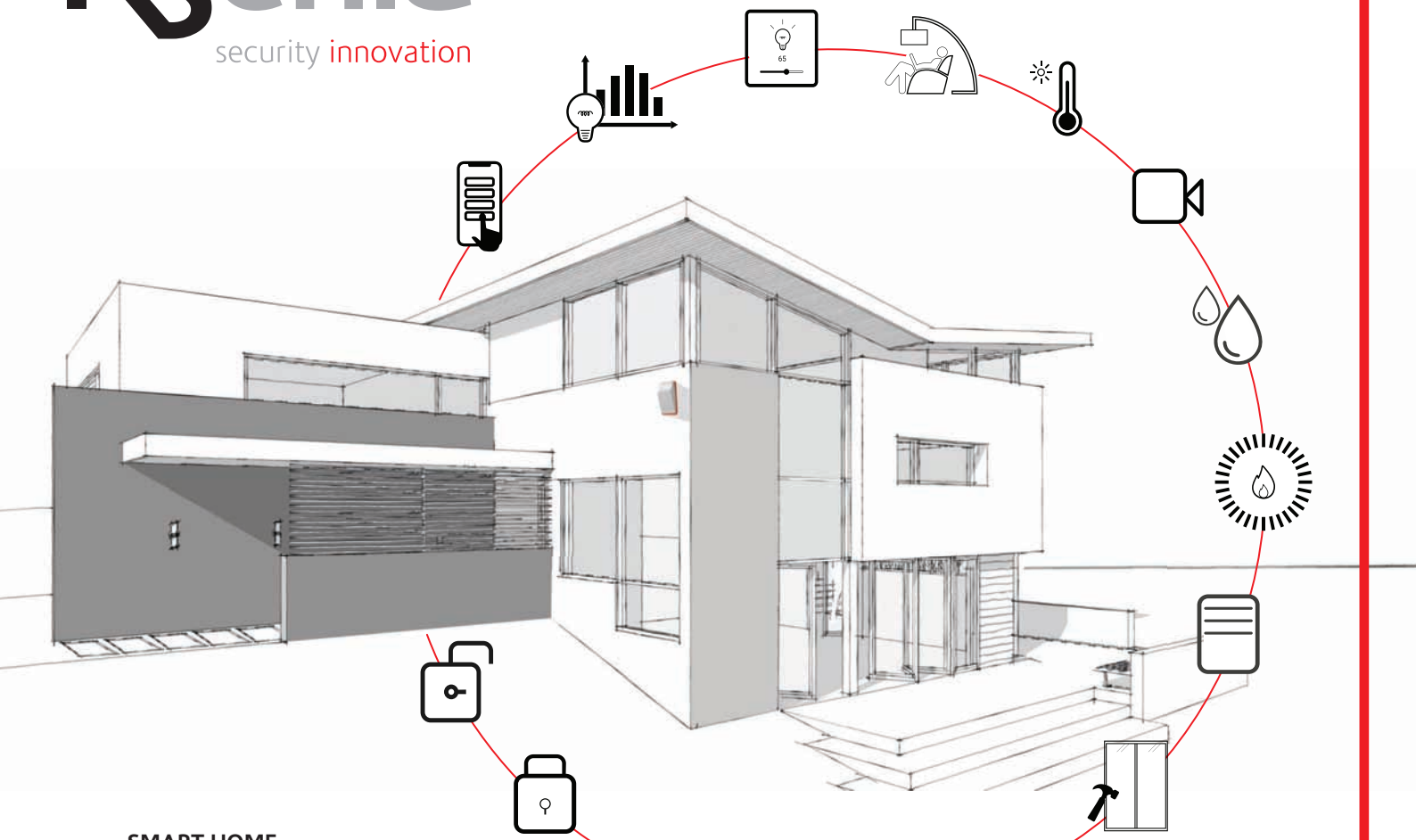
Rilevatore tripla tecnologia da esterno

DETECTION
MADE IN ITALY

Per la protezione di spazi esterni più ampi ed esposti all'intemperie, occorre un rilevatore che ha le caratteristiche ambientali paragonabili con le PROTEZIONI PERIMETRALI IN ESTERNO, ma che risolva l'esigenza di non determinare la rilevazione ad una "barriera a tenda", ma ad un volume più ampio.
Il prodotto in grado di soddisfare tutte queste esigenze con soluzioni tecnologiche all'avanguardia è certamente il MASTER PLUS, rilevatore multifascio, tripla tecnologia (doppio IR e MW), disponibile nelle due versioni 12.8 PLUS e 12.8 PLUS AJ (per istallazioni comprese tra 0,80-1,20mt), e 21.23 PLUS (per istallazioni comprese tra 2,10-2,30mt).

GUARDA IL VIDEO

Ksenia®
security innovation



SMART HOME

Scegliendo la Domotica Ksenia si ha il pieno controllo di tutte le automazioni desiderate: luci, riscaldamento, climatizzazione, irrigazione, tapparelle, apertura e chiusura di porte, cancelli, garage, e tanto altro.

Gestire queste funzioni è estremamente semplice: grazie all'App gratuita lares 4.0 basta un click per eseguire l'azione. L'impianto può essere monitorato giorno e notte anche da remoto, avendo così il totale controllo della propria Casa.

lares 4.0

Smart Home

CERTIFICATA
EAC
EN50131 Grado 3 - Classe II
T031:2017
SSF 1014 Larmklass 3

lares 4.0
lares 4.0
App Store
Google play

www.kseniasecurity.com

QUANDO LA TECNOLOGIA
INCONTRA IL DESIGN

ICON

Sistema innovativo **modulare.**

SICEP®

Sicuri e connessi **Sempre.**

www.sicep.it

secsolution magazine

tecnologia
normative
mercato
eventi

15
giugno 2021
anno III

secsolution.com
/ethosmediagroup
/SecSolution
/SecSolution.it
SECURITY MEDIA ALLIANCE

SOLUTIONS GALLERY

MERCATI VERTICALI

DITE LA VOSTRA

TECNOLOGIA

Cyber security for dummies

Responsabilità for dummies

Installazione for dummies

NORMATIVE

VOCI DAL MERCATO

FOCUS PRODUCT

Editoriale

Houston, abbiamo un problema

Possiamo dircelo tra noi, con garbo, sottovoce, senza darci la zappa sui piedi? Il comparto sicurezza ha un problema e non piccolo. Una discreta fetta del settore non possiede le competenze per definirsi "professionale": troppi non conoscono le norme o non le hanno mai lette, qualcuno nemmeno sa della loro esistenza. Per non parlare della documentazione da rilasciare.
Senza fare dietrologia spicciola sulle responsabilità (è colpa del canale che non si qualifica o del mercato che accetta l'improvvisazione, magari senza manco accorgersene, pur di non spendere una lira?), la domanda è: per quanto ancora si potrà andare avanti così? Il Covid ha messo il nostro comparto sotto i riflettori, mostrando le potenzialità delle tecnologie di sicurezza e calandole nel quotidiano di tutti noi, facendo luce sulle nostre figure chiave e accordando loro una professionalità e una dignità che oggi più che mai siamo chiamati a capitalizzare. Dunque, aspetteremo che la formazione e la certificazione delle competenze diventino obbligatorie (tutto si sta muovendo in quella direzione, quindi è solo questione di tempo, facciamocene una ragione) o sapremo giocare d'anticipo e sfruttare il vantaggio competitivo di cui oggi - non domani, né ieri - godiamo?

La rivista è disponibile in versione PDF da scaricare sul vostro computer o tablet su ***secsolution.com***

Buona lettura! ☺

Tiandy

SOLUTIONE PER PEOPLE COUNTING

Alta precisione + Facilità di installazione + OSD

TC-A52P6 spec: E/4mm

- Immagini a colori a 1080p
- Ingresso/Uscita/Attraversamento/Stazionamento
- Algortimo versatile
- Algortimo adattivo
- Adattabile in contesti differenti con altezza da 2,5 a 4 metri

Tiandy Technologies Co.,Ltd.
Email: sales@tiandy.com Tel: +86-22-58596178
Website: en.tiandy.com Fax: +86-22-58596048

Bella, da rimanere incantati!

Tu non potrai smettere di guardarla, Lei di parlarti!

combivox.it

UNICA PRO WHITE

UNICA PRO BLACK AND WHITE

UNICA PRO DOUBLE BLACK

Unica

SEMPLICE, FUNZIONALE ED ELEGANTE.

UNICA PRO è la nuova tastiera LCD/LED su BUS RS485 compatibile con tutte le centrali Combivox.

Grazie ad un design completamente rinnovato nella **linea ultraslim e nelle finiture di alta qualità**, UNICA PRO si integra perfettamente in ogni tipo di ambiente residenziale e commerciale.

Disponibile in tre varianti di colore **"White, Black and White e Double Black"**, UNICA PRO rimane fedele alla sua tradizione ed è dotata di microfono e altoparlante per l'esclusivo menù vocale Combivox.

Nelle versioni "**Black and White e Double Black"**: a display spento, diventa un oggetto del tipico e apprezzato design italiano, mimetizzandosi con eleganza nell'ambiente in cui è installata. **Una soluzione estetica e tecnologica esclusiva nella categoria delle security keypad**.

Oggi più facile da installare tramite **staffa con circuito ad innesto** per il collegamento al Bus, UNICA PRO dispone di 1 zona di allarme on board e di **lettore di prossimità integrato** per le funzioni di inserimento/disinserimento e l'attivazione di scenari.

MADE IN ITALY

COMBIVOX
ENJOY LIFE, SAFELY.

NESSUNO
PASSA INOSSERVATO

Nuova gamma di NVR e Telecamere Eyemotion con Intelligenza Artificiale: la tua sicurezza ha un alleato in più.

eyemotion

- **Accesso facilitato** senza necessità di installazione di plug-in. Compatibilità con i browser più diffusi (Edge, Chrome, Firefox, Safari e altri)

- **ONVIF Profilo G/T**. Eventi da Motion, Analisi Video e Tamper con telecamere Onvif, Audio bidirezionale.

- **Combinazione allarmi** tra gli eventi AI di Intrusione/Attraversamento Linee/Motion e gli ingressi del videoregistratore.
Utile ad esempio per inviare notifiche PUSH e/o EMAIL di allarme solo ad impianto inserito.

- **Maggiore sicurezza** con il nuovo algoritmo di cifratura **SHA512**

- **Perfetta integrazione** con piattaforma IKLAS

Macro features:

Intelligenza Artificiale
Grazie ai potenti algoritmi di deep learning a bordo camera, è possibile classificare e ricercare rapidamente persone e/o veicoli.

Riconoscimento volti
E' possibile confrontare in real time i volti rilevati con un database interno, generando notifiche di vario tipo.

Recording
Ogni persona e/o veicolo viene registrato ed indicizzato per un successivo utilizzo in playback o ricerca.

Search
E' possibile ricercare volti di persone indicando il grado di somiglianza ad un soggetto presente nel database. Il volto di riferimento può essere caricato nel DB anche tramite App Mobile SuperCam Plus.

Tracking
E' possibile tracciare i passaggi di persone in determinate aree ed indicare il percorso effettuato su una mappa, per una migliore comprensione dell'accaduto.

Allarmi
L'intelligenza artificiale a bordo telecamera rende estremamente semplice la configurazione dell'analitica e riduce al minimo la possibilità di falsi allarmi rendendo tali sistemi un'ottima soluzione per le protezioni perimetrali.

Grafici e Statistiche
La soluzione permette di visualizzare l'andamento temporale del numero di accessi di persone e/o veicoli in entrata e uscita su base giornaliera, settimanale, mensile o su periodo definito dall'amministratore.

Distribuito da

ELECTRONIC'STIME®

Via Madonna Piccola, 32 /R-Q 74015 Martina Franca (TA) Italy | +39 080 4802711 | www.eyemotion.it | www.electronicstime.it | info@electronicstime.it

AlarmHub 4 INPUTS

Trasmettitore a variazione di stato

Cos'è AlarmHub?

È IL TRASMETTITORE RADIO PRONTO ALL'USO!

4 Ingressi

Protezione jammer

Batteria a lunga durata

Senza WIFI o SIM

sigfox

Connettività la unica rete IoT pubblica

Piattaforma proprietaria

Alimentazione

- Tensione nominale: 3,6 Vcc (batteria litio)
- Durata: 5 anni circa (in funzione dell'utilizzo)

Antenna

- Modulo radio: 868MHz
- Potenza: 25mW (+14dBm)
- Connettore: SMA
- Temperatura operativa: -20°C/+60°C
- Temperatura di trasporto e immagazzinamento: +10°C/+30°C (limite batteria)
- Umidità relativa (senza condensa): < 95%
- Grado protezione: IP 40

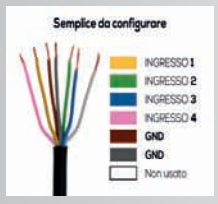
Meccanica

- Peso: 140g senza antenna
- Dimensioni: 33x55x112 mm
- Montaggio: Parete, soffitto e pavimento

Come funziona

01

Installa il dispositivo e collega gli ingressi che vuoi monitorare



02

Compila il modulo sulla nostra piattaforma proprietaria

03

Ricevi notifiche tramite SMS, e-mail e Telegram

Controlla la copertura: dynamicservicetool.com

AlarmHub
Accessori per la protezione e il controllo

Sempre connesso!

www.alarmhub.it info@alarmhub.it 340.0647559

spark
Italian inSight

UN ANNO DI **FORMAZIONE** GRATUITA

In Spark produciamo telecamere, dispositivi e software per la sicurezza.

Selezioniamo le migliori tecnologie per offrire nuove soluzioni.

Insieme a Ethos Academy stiamo organizzando webinar di formazione gratuita per system integrator, distributori e installatori.

Resta aggiornato sui prossimi appuntamenti su www.secsolution.com

«Più impari, in più posti andrai.»
(Dr. Seuss)

in collaborazione con

ETHOSACADEMY

www.spark-security.com

La flessibilità diventa centrale

Axel Srl

www.axelweb.com

Il nostro obiettivo è migliorare gli innumerevoli stili di vita delle persone. Noi progettiamo e produciamo sistemi di sicurezza e domotici che siano semplici da installare e diano protezione, flessibilità, affidabilità all'utente. La versatilità dei nostri prodotti permette una vita quotidiana più agile, sicura, interconnessa: per residenziale, commerciale, industriale.
Con Axel decidi di andare oltre, per la sicurezza, oggi.

AXEL
SICUREZZA E DOMOTICA

PRODOTTO ITALIANO

25 1996 2021

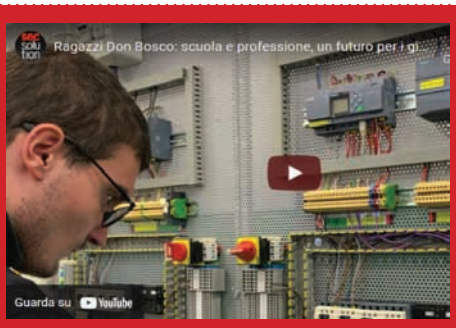
Per un aggiornamento completo e quotidiano sulle novità del comparto sicurezza, visita www.secsolution.com

secsolution news

EDGE ANALYTICS: QUANTO VALE E QUANTO CRESCE IL MERCATO

Lewes (DE, USA) – Basterebbe l'infografica a sintetizzare l'impennata che, secondo le previsioni di Verified Market Research, subirà il mercato dell'Edge Analytics, un mercato che nel 2019, prima del Covid, valeva 4,9 miliardi di dollari. Le stime degli analisti di VMR lo vedono infatti proiettato fino ai 46,91 miliardi di dollari entro il 2027, con un tasso di crescita CAGR del 35,23%, dal 2020 al 2027. Ma in che cosa consiste nella pratica l'Edge Analytics? È la definizione anglosassone per indicare il processo di raccolta, elaborazione e analisi dei dati che si svolge "ai margini" (edge) di una rete, a bordo o in prossimità di un qualunque tipo di sensore (una telecamera IP, per esempio, in un sistema di videosorveglianza o di sicurezza integrato), di uno switch di rete o altro dispositivo connesso. L'analisi avviene in tempo reale, nel punto stesso dove vengono raccolti i dati, e può essere descrittiva o predittiva. Al numero crescente di dispositivi connessi, di pari passo con l'evoluzione dell'Internet of Things (IoT), si deve la grande mole di dati e informazioni che vengono raccolti nei dispositivi periferici della rete in molti settori. Per esempio, nel retail, dove questo approccio alimenta le analisi di vendita e orienta le strategie commerciali, nel manifatturiero, nei trasporti e nel settore energetico.

https://www.secsolution.com/notizia.asp?id=13874&c=1



RAGAZZI DON BOSCO: FUTURI PROFESSIONISTI DELLA SECURITY 4.0

ROMA – A partire dal prossimo anno scolastico, prenderanno posto tra i banchi, anzi, i banconi degli attrezzati laboratori del Centro Ragazzi Don Bosco di Roma, i futuri professionisti della Security 4.0. Il programma ha visto la nascita di tre nuovi moderni laboratori interni, molto sofisticati, nei settori building automation, sicurezza anticrimine, videosorveglianza, controllo accessi, sicurezza antincendio, con un'annessa area esterna tecnologicamente avanzata, per le simulazioni progettuali e funzionali direttamente in campo. Il direttore del centro, Alessandro Chiorri, e il responsabile del corpo docente Gaetano Capozzi, supportati da un esperto certificato del settore security, Giovanni Villarosa, con questo progetto riescono a dare ai ragazzi una formazione non solo scolastica, ma a tutto tondo, sostenuta dallo stesso mondo del lavoro. Il progetto è destinato a proseguire: grazie all'introduzione dei laboratori interattivi, saranno presto attivati corsi di alta specializzazione manageriale per i professionisti certificati della sicurezza urbana e sussidiaria, con uno specifico supporto del CESPIS, un'associazione formata da alti professionisti della sicurezza, di cui Villarosa è membro, e parte del comitato tecnico scientifico.

https://www.secsolution.com/notizia.asp?id=13858&c=1

SICUREZZA

SICUREZZA 2021, FOCUS SULL'ANTINTRUSIONE

MILANO - Un sistema antintrusione ha dietro di sè una filiera articolata ed è dalle competenze e dalle capacità di tale rete che derivano la qualità e l'affidabilità dei sistemi installati. Alcune delle aziende che aderiscono a SICUREZZA 2021, hanno raccontato il valore aggiunto che la capacità innovativa di chi produce e la competenza di chi distribuisce e installa possono garantire all'utente finale. Qualità nella produzione, investimento nell'innovazione, costruzione di una rete di collaborazione con i distributori e formazione continua per gli installatori sono le linee guida comuni che emergono dai loro racconti.

https://www.secsolution.com/notizia.asp?id=13814&c=2

URMET: GRATIS UN THERMAL GATE PER L'HUB VACCINALE API

TORINO - L'hub vaccinale istituito presso la sede di API Torino è entrato a pieno regime: Urmet ha fornito gratuitamente un "Thermal Gate" in grado di effettuare il "Pre-Triage" dei cittadini e dei lavoratori che accedono alla struttura. La struttura, collocata presso la sede di via Pianezza, è dedicata alla vaccinazione del personale dipendente (e familiari) delle piccole e medie imprese associate al sistema Confapi di Torino, Biella e Cuneo, ma anche ai dipendenti delle imprese e delle cooperative di altre associazioni. Questa apparecchiatura consentirà una migliore organizzazione del lavoro di monitoraggio e un controllo più efficace dell'ingresso al Centro Vaccinale, con la rilevazione della temperatura e la verifica dell'utilizzo corretto delle mascherine.

https://www.secsolution.com/notizia.asp?id=13873&c=1

IDENTITÀ FISICA E CONTROLLO ACCESSI: AL RADDOPPIO NEL 2025

Northbrook (USA) – La trasformazione digitale aziendale passa anche attraverso la sicurezza e la gestione delle identità fisiche e logiche di dipendenti, clienti, partner e fornitori. Al "Mercato dell'identità fisica e della gestione degli accessi" è dedicato l'ultimo report di MarketsandMarkets che ne analizza i vari aspetti e le dimensioni su scala globale, con previsioni fino al 2025. Primo dato utile fornito dalla ricerca, le dimensioni del mercato: gli analisti prevedono una crescita a un tasso CAGR del 14,2%, dai 789 milioni di dollari del 2020 ai 1.535 milioni di dollari entro il 2025. Il report riflette sull'evoluzione di questo mercato attraverso una dettagliata analisi per componente, servizio, dimensione dell'organizzazione, mercati verticali e aree geografiche. I driver individuati includono la crescente necessità di interventi di sicurezza "a prova di futuro", l'incremento delle minacce interne e la conformità alle direttive di sicurezza e governative.
In base alle dimensioni dell'organizzazione, sarà il segmento delle grandi imprese a guidare il mercato nei prossimi mesi. Nondimeno, anche tra le piccole e medie imprese si assisterà a un incremento nell'adozione di software e servizi di identità fisica e gestione degli accessi. I fornitori di questi sistemi aiutano le imprese, grandi e piccole, a soddisfare le esigenze di sicurezza delle applicazioni "business-critical", per proteggerle da attacchi informatici sempre più sofisticati.

https://www.secsolution.com/notizia.asp?id=13813&c=1

EURALARM: NUOVO REPORT 2020-2021

ZURIGO (CH) – Benché in genere l'annuale rapporto pubblicato da Euralarm copra il periodo che intercorre tra le Assemblee Generali di due anni consecutivi, per l'edizione 2020-2021 - causa Covid - si è preferito divulgare il Report a maggio, nonostante la prossima assemblea generale sia programmata a novembre. Fin dalla sua fondazione, cinquant'anni fa, Euralarm ha contribuito in modo proattivo ai processi di standardizzazione: ha fornito indicazioni per la digitalizzazione del settore, ha elevato gli standard di formazione e le qualifiche per rispondere alle nuove esigenze della società in materia di sicurezza e protezione, e ha collaborato con gli istituti di ricerca per trasformare le tecnologie emergenti in soluzioni sostenibili, fondate su conoscenza e innovazione. Nel periodo 2020-2021 Euralarm ha registrato una crescita delle adesioni con l'ingresso di Vanderbilt, Verisure, Kiwa e Open Security & Safety Alliance (OSSA). Per consultare il report: https://euralarm.org/E-Books/

https://www.secsolution.com/notizia.asp?id=13786&c=1

NON TUTTA LA BIOMETRIA È UGUALMENTE SICURA

MILANO - Il riconoscimento biometrico si basa sull'analisi e la comparazione dei tratti propri di ciascun individuo come voce, impronta digitale o parametri facciali. Ma, in termini di sicurezza, non tutte le biometrie sono uguali. Le tanto diffuse impronte digitali, per esempio, non sono esenti da rischi. I lettori rivolti al mercato consumer, infatti, in genere immagazzinano solo una parte dell'impronta e la confrontano con un'ulteriore impronta parziale: se l'analizzassero nella sua interezza, non riuscirebbero a garantire la medesima fluidità e velocità. E' di conseguenza piuttosto facile creare delle impronte false. Il riconoscimento facciale, poi, da molti considerato la tecnologia del futuro per gli aeroporti, destinata a pensionare biglietti, carte d'identità e passaporti, apre però questioni importanti in termini di privacy. La Commissione Europea ha recentemente annunciato una stretta nei confronti del riconoscimento facciale - salvo casi eccezionali - quando utilizzato in attività svolte in luoghi accessibili al pubblico. Il riconoscimento vocale, invece, usato per aprire porte o disattivare antifurti e accedere a servizi che richiedono un alto livello di privacy (ad es. in ambito bancario, assicurativo o sanitario), ha un vantaggio fondamentale: nessuna informazione viene memorizzata o conservata sui dispositivi mobili Inoltre, la voce umana è anche molto più complessa da imitare.

https://www.secsolution.com/notizia.asp?id=13829&c=1

FAAC ACQUISISCE COMETA

BOLOGNA - Con l'acquisizione strategica del Gruppo COMETA, la multinazionale bolognese FAAC amplierà l'attuale gamma degli ingressi automatici e arricchirà di competenze specifiche sia la produzione, quanto la progettazione di bussole antirapina, porte di emergenza, porte blindate antieffrazione, portali rototraslanti, revolving doors, elettromagneti e serrature di sicurezza. Il closing dell'operazione è previsto per fine settembre 2021.

https://www.secsolution.com/notizia.asp?id=13883&c=1

evolution

Tecnoalarm®

Grandi tecnologie per impianti wireless

Il nuovo sistema radio bidirezionale
ideale per ogni esigenza di protezione di beni e persone

DESIGN BY
pininfarina

Sicuri e protetti sempre

Tecnoalarm®
HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY

EN 50131
Grado 2

Amazon, Alexa and all related logos are trademarks of Amazon.com, Inc. or its affiliates

works with
amazon alexa

Tecnoalarm arricchisce la gamma dei componenti domotici

EV TERM BWL

Rilevatore di temperatura e di umidità

Dispositivo wireless
per la regolazione climatica multi-ambientale

Grazie alla funzione *cronotermostato*
l'app Evolution consente di impostare
fino a 5 diversi livelli di temperatura
su 8 fasce temporali quotidiane

ISO 9001

MADE IN ITALY

Tecnoalarm®
Via Ciriè, 38 - 10099 - San Mauro T.se Torino (Italy)
tel. +39 011 22 35 410 - fax +39 011 27 35 590
info@tecnoalarm.com - **www.tecnoalarm.com**

Intelligenza artificiale per acquisti in totale sicurezza

La problematica

A seguito delle restrizioni entrate in vigore all'inizio della pandemia utili a contenere i contagi, si è resa necessaria, nel rispetto del distanziamento sociale, una riorganizzazione degli spazi all'interno dei supermercati Conad di Capannoli (PI) che garantisse alla clientela un'esperienza d'acquisto gradevole ed in totale sicurezza. La committenza ha quindi richiesto l'adozione di una tecnologia a basso impatto economico, precisa e fruibile in breve tempo, in grado di monitorare il numero di persone presenti in un determinato reparto, senza rivoluzionare il sistema di videosorveglianza preesistente.

I supermercati Conad di Capannoli (PI) necessitavano di riorganizzare gli spazi per garantire alla clientela un'esperienza d'acquisto in totale sicurezza

La soluzione

A tale scopo si è deciso di installare un modulo AI GANZ modello ZN-AIBOX8, caratterizzato da velocità e prestazioni eccezionali, che ha consentito al sistema di monitoraggio preesistente di effettuare un'analisi professionale e precisa dell'immagine, senza dover sostituire né postazioni di ripresa, né sistema di registrazione. Una volta impostati i criteri e le soglie di allarme desiderati, modificabili e definibili in base alle metrature delle aree, si è ottenuto un controllo puntuale ed in tempo reale del

numero di persone presenti nei vari reparti, garantendo una densità in linea con le norme sul distanziamento sociale. Per ogni telecamera sono state impostate le zone di permanenza necessarie ed abilitate le licenze specifiche.

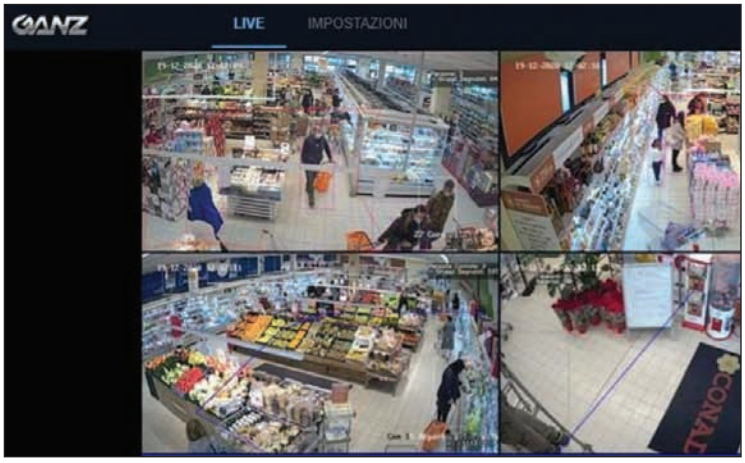
I benefici

La configurazione semplice e la messa in servizio rapida del sistema, senza necessità di calibrazione, hanno consentito al punto vendita Conad di Capannoli (PI), di continuare ad operare garantendo sicurezza e protezione a clienti e dipendenti. L'interfaccia semplice e l'immediatezza di programmazione degli algoritmi AI GANZ hanno portato ad una rapida integrazione ed al raggiungimento degli obiettivi. La soluzione impiegata non ha richiesto stravolgimenti all'impianto di sicurezza, garantendo massima affidabilità e costi di realizzazione contenuti. La committenza cercava infatti una soluzione che consentisse di operare in un ambiente sicuro, anche in assenza di operatori impiegati a disciplinare e verificare le regole anti-assembramento. La richiesta presupponeva che la messa in opera fosse il meno invasiva possibile a livello strutturale, che i costi fossero contenuti e che la realizzazione venisse implementata in tempi brevi. La soluzione fornita dall'installatore Domus Srl è stata ultimata senza stravolgimenti strutturali, in quanto la tecnologia AI GANZ si avvale del sistema di videosorveglianza preesistente. Di conseguenza, anche i costi sono stati contenuti. Questo ha permesso al punto vendita Conad Soc. Coop. Capannoli (PI) di dare una risposta immediata alle nuove esigenze emerse con la pandemia, garantendo al cliente di fare la spesa in sicurezza, sentendosi a proprio agio in un luogo in cui la tutela della salute è un valore primario. Il progetto è stato poi riprodotto anche all'interno dell'altro supermercato della stessa proprietà, ubicato a Casciana Terme Lari (PI).

GANZ
www.ganzsecurity.eu

Occorreva una tecnologia a basso impatto economico per monitorare le persone presenti in un determinato reparto, senza rinunciare alla videosorveglianza preesistente

Il modulo AI GANZ modello ZN-AIBOX8 consente al sistema di monitoraggio preesistente di effettuare un'analisi precisa dell'immagine, senza sostituire postazioni di ripresa o registrazione



La configurazione semplice e la messa in servizio rapida del sistema, senza necessità di calibrazione, hanno consentito al punto vendita di continuare ad operare garantendo sicurezza

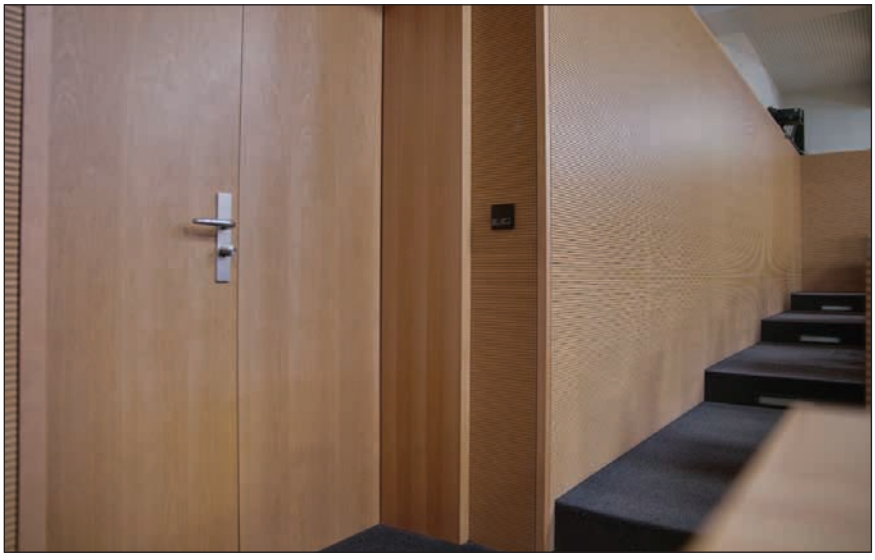
Controllo accessi wireless per una realtà educational del Lazio

La problematica

Anche nei complessi scolastici aumenta la necessità di implementare il livello di sicurezza delle strutture ed in particolare di aumentare la dotazione tecnologica presente sulle porte.

L'obiettivo dei dirigenti scolastici è duplice: risolvere un problema gestionale, ovvero snellire il sempre proliferante parco chiavi circolante, ed implementare il livello di security e di safety.

Si parla di security con riferimento ad un maggiore controllo degli asset scolastici su aule, laboratori, mense, auditorium, biblioteche, impianti sportivi, uffici e appartamenti per studenti. Si parla di safety ponendosi l'obiettivo di disporre di una tracciabilità in merito agli spostamenti di tutti gli operatori scolastici che permetta così di ricostruire gli spostamenti all'interno degli edifici in caso di emergenza.



La tecnologia di controllo accessi wireless SimonVoss evita costi elevati di installazione, il problema delle doppie credenziali e garantisce funzionalità ed usabilità immediate

La soluzione

Un'importante realtà della regione Lazio[1] aveva iniziato un'opera di ammodernamento che prevedeva l'installazione di lettori a parete collegati ad elettroserrature montate sulle porte per l'apertura con badge in possesso di ogni singolo utente. Questo tipo di scelta ha però presto evidenziato i suoi limiti: 1) elevati costi di installazione,

[1] In ossequio alla privacy, non menzioniamo in chiaro la committenza. Per informazioni sul caso di specie contattare SimonsVoss

specialmente su edifici oggetto di restauro (lunghi tempi di montaggio per stendere i cavi laddove prima non erano previsti e per la predisposizione delle porte); 2) il permanere di doppie credenziali di apertura (a causa dell'elevato costo di implementazione si poteva intervenire solo per zone limitate, costringendo gli utenti all'uso sia del badge sia della chiave meccanica, di fatto appesantendo la situazione invece di semplificarla); 3) software di gestione non immediati (ovvero con funzionalità ed usabilità molto limitate che portavano nella pratica ad assegnare per comodità ad ogni badge tutte le porte, di fatto mancando l'obiettivo stesso del sistema). La risposta a questa tipica situazione di stallo è stata l'adozione della tecnologia di controllo accessi wireless SimonVoss.

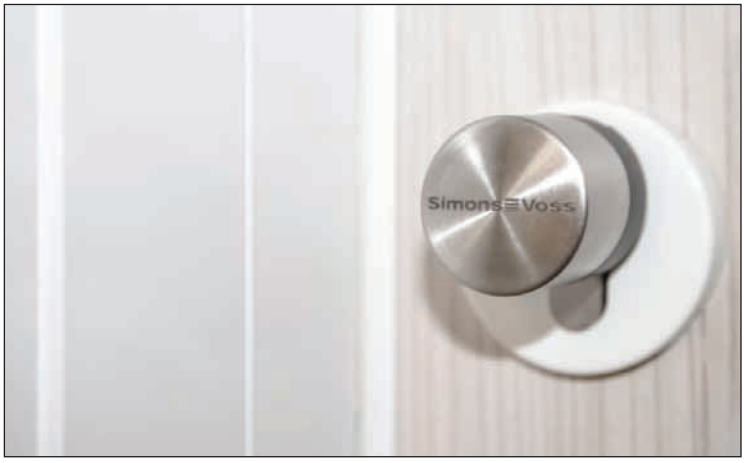
I benefici

I sistemi di chiusura senza fili di nuova generazione hanno consentito di raddrizzare immediatamente la bilancia costi/benefici ed estendere le applicazioni è diventato subito più facile. Cilindri e maniglie digitali wireless si adattano a qualsiasi tipo di porta esistente provvista di serratura a profilo europeo e danno modo di modificare, aggiungere o bloccare gli utenti in rapidità, definendo i diritti di accesso in maniera personalizzata e di registrare gli accessi eseguiti.
Non è necessario alcun cablaggio, sono alimentati da batterie che possono durare diversi anni, anche quando sono molte le attivazioni realizzate ogni giorno. Un solo badge consente l'apertura di centinaia di porte, i diritti nelle singole aree vengono assegnati in base ad esigenze e bisogni specifici. La scalabilità del sistema rende tutto ancora più semplice: questi dispositivi possono essere installati gradualmente, in base alle esigenze e al budget a disposizione al momento, consentendo il riutilizzo immediato dei dispositivi da un varco ad un altro qualora non dovessero essere più necessari in una determinata area.

SIMONSVOSS
www.simons-voss.com/it

Cilindri e maniglie digitali wireless: per modificare, aggiungere o bloccare gli utenti definendo i diritti di accesso in maniera personalizzata registrando gli accessi

Non serve cablaggio: sono alimentati da batterie che possono durare diversi anni, anche quando sono molte le attivazioni realizzate ogni giorno



Sistema scalabile in base alle esigenze e al budget, con riutilizzo immediato dei dispositivi da un varco ad un altro qualora in un'area non fossero più necessari

ETHOS MEDIA GROUP
MILANO (ITALY)
ETHOS@ETHOSMEDIA.IT
WWW.ETHOSMEDIA.IT

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

INNOVAZIONE
NELLA
COMUNICAZIONE

RIVISTA

secsolution magazine

WWW.SECSOLUTIONMAGAZINE.IT

ONLINE

secsolution
security online magazine

WWW.SECSOLUTION.COM

EVENTI

secsolution forum
The digital event for the security industry

WWW.SECSOLUTIONFORUM.IT

APP

CheckAPP
VIDEOSORVEGLIANZA

APP.SECSOLUTION.COM

GLOBAL MULTIMEDIA CHANNEL

Ilaria Garaffoni

Smart city, safe city, city Covid-free

Tra le tavole rotonde che hanno caratterizzato il format di secsolutionforum2021, si annovera anche quella dedicata ad uno dei cavalli di battaglia di Ethos Media Group: "Videosorveglianza urbana integrata - Smart & Safe City e impatto privacy". Perché rinnovare oggi questo appuntamento indirizzato agli operatori delle Forze di Polizia Nazionali e Locali, ai Responsabili degli uffici tecnici comunali, ai DPO (Data Protection Officer - Responsabile Protezione Dati) e ai professionisti della sicurezza? Perché il tema della sicurezza urbana dopo il Covid ha assunto una connotazione diversa, che abbraccia anche in maniera massiva la protezione sanitaria.

Del resto la definizione di sicurezza "urbana", di per sé dinamica, ha sempre più a che fare con la percezione di sicurezza nel contesto urbano, quindi la città sicura, la città smart, oggi deve di necessità essere anche una città Covid-free. Ma – questa è la buona notizia - la raccolta di dati dai vari sensori (telecamere ma non solo) disseminati sul territorio e l'intelligenza artificiale permettono già oggi di simulare scenari e di ipotizzare dove potranno svilupparsi, ad esempio, nuovi focolai di Covid.

Esperienze estere

In Corea del Sud si utilizza uno Smart City Data Hub per tracciare le persone infette e far rispettare il distanziamento sociale: chiaro, alle nostre latitudini ci sarebbero grossi sollevamenti di scudi in materia di diritti fondamentali della persona, ma l'esperienza coreana potrebbe essere una base di ragionamento per utilizzare su larga scala dei big data. E ancora: le città potrebbero valutare l'efficacia delle misure di distanziamento sociale messe in campo conteggiando (con i sensori pedonali) di quanto sono diminuiti il traffico pedonale e il traffico veicolare (con i sistemi di lettura targhe) rispetto agli scorsi anni nello stesso periodo e mettendo a punto degli algoritmi in grado di misurare la distanza sociale, capaci anche di sanzionare le possibili violazioni. L'hanno fatto a Newcastle l'anno scorso, non è fantascienza.

"Videosorveglianza urbana integrata: Smart & Safe city e impatto privacy" (secsolutionforum 2021)

Sensori e wi-fi pubblico

L'uso della sensoristica in campo e del wi-fi pubblico permettono infatti già oggi di monitorare la mobilità in tempo reale e di potenziare gli strumenti di emergenza e allarme di cui le città sono dotate. Mappando le città in base al loro grado di "rischio Covid-19", si potrebbero mettere in campo dei correttivi rapidi ed efficaci, partendo dall'assicurazione dei servizi prioritari: gestione rifiuti,, sanificazione delle strade, distribuzione mirata delle forze di sicurezza, immediata convocazione di task force per agevolare le categorie a rischio nell'approvvigionamento di cibo, farmaci ecc.

PA: il convitato di pietra

Da lì si potrebbe partire con lo step successivo: un modello di partenariato pubblico-privato che metta a fattor comune tutti i dati rilevanti per minimizzare l'impatto del Covid-19 nella vita sociale e nelle attività economiche. Ma – c'è sempre un ma – per potenziare gli strumenti che già oggi permettono di innescare un allarme precoce, il grande assente, il solito convitato di pietra, è la pubblica amministrazione, che stenta a svecchiarsi.

Oggi la crisi si chiama Covid, ma domani si potrebbe chiamare terrorismo, cybercrime o altro. E alla prossima dovremo essere preparati

Eppure bisogna pensarci oggi perchè oggi la crisi si chiama Covid, ma domani si potrebbe chiamare terrorismo, cybercrime o altro. Di certo questa non sarà né la prima né l'ultima crisi: solo che alla prossima dovremo essere più preparati.

Come? Ce ne hanno parlato **Alessandro Bove** - Ingegnere, ricercatore di tecnica e pianificazione urbanistica; **Giulio Iucci** - Presidente di ANIE Sicurezza; **Marco Soffientini** - Avvocato, esperto di Privacy e Diritto delle nuove Tecnologie, docente Ethos Academy e **Fabio Boiani** - South Europe Regional Manager di Tattile.

Alessandro Bove
Ingegnere, ricercatore di tecnica e pianificazione urbanistica

Progettare la sicurezza urbana

La progettazione della sicurezza necessita di partire dal basso perché la città è il layer fondamentale attorno al quale tutto si posa. La strutturazione della città crea un insieme di interazioni sulle quali deve incardinarsi il modello organizzativo della sicurezza. Occorre quindi valutare la PERICOLOSITÀ, ossia la probabilità che un evento criminoso a carattere spaziale si verifichi in un'area con una certa intensità e in un determinato intervallo temporale. Occorre cioè valutare il rischio per individuare gli elementi che favoriscono gli eventi criminosi, tenendo presente che il pericolo della città moderne non è esterno bensì interno (rispetto alle città fortezze medievali o alle citta rinascimentali, ad esempio) perchè è generato dalla stessa città: grandi migrazioni, necessità di integrazione tra i vari ceti, trasporto pubblico, attrattori forti nelle città con masse concentrate (terreno fertile per una certa criminalità, come nel caso dell'attentato terroristico ai mercati di Natale tedeschi) ed elementi di degrado. Occorre poi valutare la VULNERABILITÀ, ossia l'attitudine dello spazio urbano (intesa in termini di assetto fisico e funzionale) a scoraggiare o favorire il verificarsi di un determinato reato a carattere spaziale. La vulnerabilità dello spazio urbano dipende dai criteri costruttivi (che sono quasi sempre pensati in funzione del traffico, del commercio, delle esigenze di residenzialità con la sicurezza urbana spesso in secondo piano), ma anche dai caratteri del tessuto urbano, dagli elementi di marginalita/esclusione (pensiamo alle banlieue di Parigi o alle Vele di Scampia) e dalle aree di degrado (parchi o parcheggi possono diventare luoghi pericolosi se non sono progettati in maniera intelligente o presidiati in maniera continua). I centri commerciali, ad esempio, sono grandi attrattori quando sono attivi, ma il parcheggio quando il centro è chiuso diventa terra di nessuno. Ultimo elemento è l'esposizione (elementi,siti, persone esposti al rischio derivante dal verificarsi o meno di un determinato evento criminoso in una data area): la popolazione residente (es. comunità isolate – gated community) e la presenza di attrattori. Oggi l'analisi del rischio urbano si può attuare attraverso dei modelli matematici, che ci permettono anche di comprendere la strutturazione del rischio e la sua variabilità in presenza di tecnologie, di diversi orari e momenti e quartieri, con una mappa del rischio dinamica e che permette di fare valutazioni preventive che consentono di investire e potenziare alcune aree per contenere il rischio.

"Progettare la sicurezza: integrazione tra tecnologie e progetto urbano": intervento integrale di Alessandro Bove a secsolutionforum 2021

Giulio Iucci
Presidente di ANIE Sicurezza

Tecnologie e gestione della sicurezza nell'emergenza Covid-19

Le tecnologie attuali sono state "abilitanti" per la pandemia, perché hanno facilitato tutti i processi di sicurezza nell'emergenza Covid19. Ma, in qualche modo, sono anche state "abilitate". Questa crisi, come tutte le crisi, ha una funzione "maieutica" sui processi e sulle specificità di ogni settore economico e non. Le tecnologie utilizzate durante questa crisi pandemica - in realtà in gran parte esistenti anche prima dell'emergenza - sono state sdoganate nel loro utilizzo, strumentale e necessario per l'emergenza in corso, anche e soprattutto nei contesti di Sicurezza Urbana. Sia le tecnologie, sia le procedure. Che sono diventate un "concetto" base per far ripartire il motore dell'economia e che hanno di fatto attivato un volano virtuoso sull'utilizzo delle tecnologie. Tali tecnologie, esistenti anche prima del diffondersi della pandemia, sono state valorizzate nel loro utilizzo, necessario per l'emergenza in corso, in tutte le declinazioni della sicurezza. Temi quali professionalità, certificazioni, qualità, oggi possono essere vissute dal mercato come garanzie di sicurezza, in un approccio win-win. Sono stati sdoganati concetti del nostro comparto: rischio, crisi, emergenza, procedure, prevenzione, processi che appartengono oggi ad un linguaggio comune. E le figure chiave del nostro comparto sono diventate professioni di riferimento. Il fatto che però ormai si debba ragionare in maniera sistemica, organica, senza compartimenti stagni tra aree tecnologiche che ormai rappresentano "definizioni" (sicurezza fisica e logica, security e safety, protezione degli asset e personale), deve indurre chi progetta la sicurezza urbana a porsi almeno 10 domande: 1) i singoli sistemi sono realizzati seguendo un'architettura ed una visione strategica globale? 2) abbiamo la mappatura (numerica, geografica e funzionale) ed il controllo di tutti i sensori in campo? 3) che tipo di collegamento hanno i singoli sistemi e dove arrivano i segnali generati dai sensori? 4) i singoli sistemi si "parlano" tra loro e sono predisposti per parlare tutti con la stessa centrale? 5) chi legge la mole di dati che verrebbe generata da tutti questi sensori? 6) come vengono interpretati informazioni ed allarmi diversi e con quali azioni correlate si attivano le procedure di intervento? 7) come deve essere strutturata una Centrale Operativa per supportare tale attività? 8) quanti devono essere gli operatori in Centrale Operativa, con quali coperture e competenze? 9) le procedure di ricezione allarme, presa in carico ed intervento, sono uniformate e coerenti le une con le altre (Safety, Security, Automation)? 10) quali sono i costi diretti, indiretti di tale operazione?

"Tecnologie e gestione della sicurezza nell'emergenza Covid-19": intervento integrale di Giulio Iucci a secsolutionforum 2021

Marco Soffientini
Avvocato, esperto di privacy e Diritto delle Nuove Tecnologie, docente Ethos Academy

Intelligenza Artificiale e Safe City: le linee guida sul riconoscimento facciale

A metà Febbraio 2021 il Consiglio d'Europa ha rilasciato tramite il Comitato della Convenzione 108 le linee "di indirizzo" per i governi, i legislatori, i fornitori e le imprese interessati dalla tecnologia del riconoscimento facciale. Le linee guida forniscono una serie di misure tecniche e organizzative indirizzate a governi, ricercatori, produttori, fornitori di servizi e in generale a tutti i titolari del trattamento che utilizzano tecnologie di riconoscimento facciale affinché venga gestito il c.d. rischio inerente il trattamento e cioè gli impatti negativi sui diritti, sulle libertà fondamentali e sulla dignità degli interessati. Per il segretario generale del Consiglio d'Europa, Marija Pej inovi Buri , il riconoscimento facciale può essere "comodo", aiutando le persone a superare gli ostacoli nel quotidiano. Tuttavia può anche porsi come una minaccia ai diritti umani "essenziali", tra cui la privacy, la parità di trattamento e la non discriminazione, autorizzando le autorità statali e altri terzi "determinati o meno" a monitorare e controllare aspetti importanti della vita dei cittadini europei, spesso senza la loro piena conoscenza né consenso. Per la Buri tali abusi possono essere fermati con delle linee guida che dovranno garantire la protezione della dignità personale, dei diritti umani e delle libertà fondamentali, compresa la sicurezza dei dati personali. Le linee guida del Consiglio d'Europa chiedono che le legislazioni degli Stati vietino di ricavare dati biometrici dalle fotografie trovate su internet quando non ci sono finalità legittime ed il trattamento è necessario e proporzionato per questi scopi (es. Forze dell'Ordine o scopi medici). Il Consiglio d'Europa ha anche affermato che l'uso del riconoscimento facciale in ambienti "affollati" deve essere strettamente necessario per garantire la sicurezza pubblica. Per il Consiglio d'Europa le aziende private non dovrebbero essere autorizzate a utilizzare questa tecnologia negli spazi pubblici per scopi di marketing o di sicurezza privata.

"Intelligenza Artificiale e Safe City: le linee guida sul riconoscimento facciale": intervento integrale di Marco Soffientini a secsolutionforum 2021

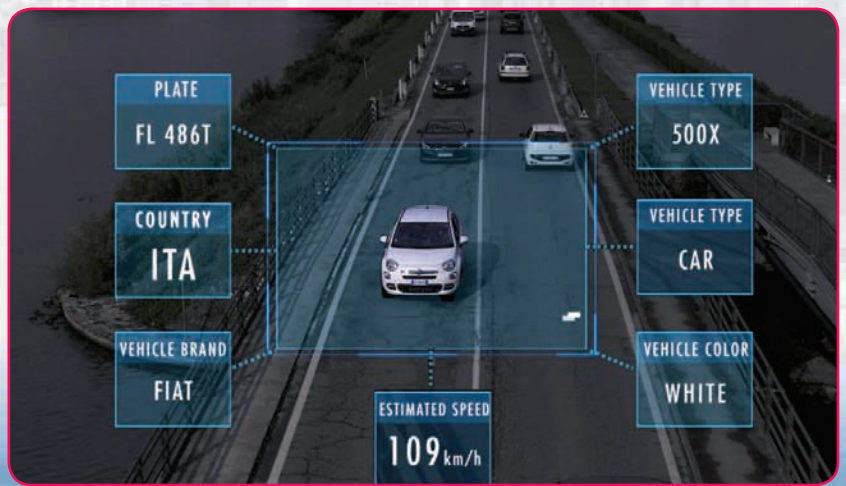
Fabio Boiani
South Europe Regional Manager Tattile

Un occhio instancabile per le moderne Smart City

Tattile contribuisce ad incrementare e migliorare la sicurezza e la qualità della vita nelle moderne smart city non solo con la solo lettura delle targhe ma anche tramite un dettagliato riconoscimento del veicolo (marca, modello, classe e colore). Un sistema intelligente di raccolta dati che trova impiego in svariate applicazioni, dalla lotta e prevenzione del crimine alla riduzione dell'inquinamento urbano.

"Un occhio instancabile per le moderne Smart City": intervento integrale di Fabio Boiani a secsolutionforum 2021

Le citttà del futuro: problemi vs opportunità



ELKRON - LE SFIDE

#1974 2021

Ci sono storie che hanno il sapore della sfida. Ci sono sfide che coniugano crescita e successo. Quella di ELKRON è una storia cominciata 45 anni fa.
Scoprila dalla voce dei protagonisti.

VAI SU **SFIDE.ELKRON.IT**

ENRICO PORCELLANA
Responsabile Business Unit Elkron

PAOLO ATTANASIO
Direttore Generale Elkron

ELKRON - LE SFIDE ti porta alla scoperta del mondo Elkron. Dal racconto del brand alle strategie di prodotto. Da un nuovo ecosistema di comunicazione ai piani per il futuro. Sfida dopo sfida, segui la storia e entra nella nuova dimensione Elkron. Conoscerai il partner con cui condividere i tuoi progetti di sicurezza. **Accetti la sfida?**

ELKRON
The key to security

www.sfide.elkron.it | elkron.it

Giovanni Villarosa (*)

Per fare una smart city ci vuole una smart home

"L'argomento Smart City riflette la crescita demografica dei centri urbani: una rilevazione statistica delle Nazioni Unite datata 1950 ci ricorda che solo il 30% della popolazione mondiale viveva nelle città, mentre nuove proiezioni ci dicono che entro il 2050 si arriverà al 70%. Altro dato interessante: si passerà dalle attuali 31 megalopoli del pianeta, alle 43 del prossimo 2030. Un quadro che mette in risalto quanto la trasformazione digitale delle città sia una tematica importante e non più rinviabile, considerazione che occupa un ruolo predominante nella società, tanto nell'opinione pubblica quanto nel dibattito politico. Basti pensare alla politica degli stanziamenti sul tema che Unione europea ha messo in atto, stanziando oltre 450 miliardi di euro per finanziare progetti legati allo sviluppo delle smart cities. Ora spetterà dunque ai singoli Enti locali individuare programmi di sviluppo e strategie di business che possano stimolare l'accesso a tali fondi di investimento. Ma cos'è realmente una smart city?

(*) Esperto di Sicurezza Fisica per Infrastrutture, CSO e DPO, Vice Presidente di SECURTEC

> **Una città intelligente è più sicura, partecipata, inclusiva e green grazie a tecnologie capaci di abbattere le distanze tra PA e cittadino**

> **Una città smart permette agli enti locali una gestione sempre più efficace e funzionale, a vantaggio della crescita del cittadino smart, cardine centrale della digital society**

Possiamo definirla fondamentalmente come una infrastruttura composta da più sistemi, più o meno complessi, dove i processi nevralgici e vitali vengono rivisti, ridefiniti, con lo scopo primario di migliorare la vivibilità degli spazi da parte dei cittadini, secondo presupposti di benessere e di ottimizzazione dei servizi pubblici, producendo quella innovazione digitale che avrà concrete ricadute sul territorio, ma soprattutto, ne sarà il reale volàno dello sviluppo sociale ed economico. Una città può essere infatti *intelligente* solo quando determinati assi primari della sua governance, come la sua amministrazione, l'economia, i trasporti, la mobilità, l'energia, l'ambiente, la cittadinanza, risultino un insieme di elementi integralmente smart.

Smart e critica

Su questo punto, ricordo ancora le parole del Dr Joseph Bruno, Commissioner Office of Emergency Management di New York city, ascoltate durante un convegno sul tema presso la camera dei deputati nel marzo 2014: illustrando il suo progetto di NY smart city, Bruno poneva la "Grande Mela" come city a livello di un'infrastruttura critica (IC), per via della sua complessità sistemica e fortemente smart. Commentando il suo progetto, applicato peraltro in uno scenario urbano articolato e dal contesto multiforme come NY, sottolineava più volte come il giusto approccio da seguire fosse proprio quello di considerare un city system come quel complesso infrastrutturale fortemente eterogeneo, per l'appunto critico, evidenziando tra le altre cose, un altro particolare aspetto: la necessità di mettere in campo una partnership tra pubblico e privato, tramite una sostanziale azione sinergica vantaggiosa al raggiungimento delle finalità progettuali.

Cambiamenti radicali

Dunque, parlando di Città Intelligenti, parliamo di cambiamenti radicali che le città dovranno fronteggiare per trasformare il loro "stato dell'arte" nello "state of the art" che contraddistingue le compiute smart city, ovvero: il più alto livello di sviluppo tecnologico con la massima integrazione sistemica possibile, ed energeticamente autosufficiente. Smart grid, smart homes, smart buildings, smart mobility, smart security, industrial automation, tutto dovrà essere più efficiente e confortevole, user friendly, accessibile a tutti: una società digitale, oltre a migliorare la vita quotidiana con una serie di utili automazioni, deve ridurre i consumi

energetici e l'impatto ambientale. Ma non si realizzerà mai una funzionale smart city senza una concreta smart home...

Si parte dalla smart home

Ed è proprio iniziando dalle abitazioni private che si realizzerà un vero ecosistema digitale urbano, grazie alle tecnologie dell'Internet of Things (IoT) e dell'Artificial Intelligence (AI); dunque, solo con la concreta interconnessione degli edifici si potranno realizzare quei progetti di trasformazione dei nostri spazi urbanizzati in veri ambienti intelligenti, perché solo a queste condizioni tutti i dati raccolti nelle singole abitazioni, interagenti tra loro grazie alle tecnologie IoT, porteranno i benefici attesi su larga scala, con l'obiettivo successivo di ottimizzare una singola smart home in una funzionale smart community.

1,3 mld di dispositivi connessi

Studi di settore ci raccontano come nel medio termine avremo circa 1,3 miliardi di dispositivi connessi all'interno delle aree urbanizzate: TVCC, sensori di misura dell'inquinamento, IoT indossabili, illuminazione smart ecosostenibile, sistemi di gestione del traffico e per l'automazione dei parcheggi, trasporti e mobilità intelligente. Tutto ciò farà si che gli spazi urbani diventeranno ambienti sempre più integrati dalla digitalizzazione, altamente fruibili, con risvolti positivi sulla qualità della vita. Ebbene, tutte queste complesse interazioni intelligenti significano, fondamentalmente, la creazione di infrastrutture digitali, come le reti wireless, connessioni ultra veloci 5G, lo sviluppo di complesse strutture pubbliche interagenti, dove tutti i devices connessi si scambieranno on time le informazioni, generando una considerevole quantità di Big Data che supporteranno, in tempo reale, servizi pubblici (mobilità, scuola, sanità, turismo, servizi pubblici, fiscalità, etc) più evoluti, permettendo agli enti locali una gestione sempre più efficace e funzionale, a tutto vantaggio della crescita del cittadino smart, il cardine centrale della digital society.

Security (e safety) first

Ma nessuna comunità può essere intelligente, se non garantisce ai suoi abitanti il diritto alla sicurezza; ecco perché una città attenta ai bisogni e alla tranquillità dei suoi cittadini deve essere protetta da un efficace sistema di sicurezza integrata, inserito però in una strategica pianificazione urbanistica. Ma c'è un'altra peculiarità da tenere nella giusta considerazione, quella giocata dal ruolo della sicurezza safety-emergency, argomento che assume una funzione di assoluta importanza nel predisporre efficaci piani di emergenza comunali, resi operativi da una efficiente organizzazione di protezione civile. Insomma, una metropoli intelligente è certamente più sicura, con un tasso minore di criminalità, perché più partecipata e inclusiva: questo grazie alla tecnologia, capace di abbattere le distanze che fino ad oggi dividevano la pubblica amministrazione dalla cittadinanza.

sec solution **sec solution forum**
The digital event for the security industry

SOLUZIONI E APPLICAZIONI

Entra e assisti alle innovative soluzioni e applicazioni presentate all'edizione 2021

AXIS COMMUNICATIONS

COMMSCOPE RUCKUS

ermes

1 everbridge

Ksenia security innovation

2 everbridge

MARSS enjoy a Smart life!

ORCA CONNECTING THE WORLD

Tattile Custom Vision Solutions

TKH GROUP TKH SECURITY

Continuate a seguirci nel sito dell'evento, dove stiamo progressivamente raccogliendo gli streaming di tutti gli interventi di aggiornamento tecnologico, normativo e di scenario, rivolti a chi realizza e gestisce impianti di videosorveglianza, controllo accessi, antintrusione, antincendio e integrati.

VISITA IL SITO!

www.secsolutionforum.it #secsolutionforum

Stadio: come prevenire un attentato esplosivo

Pierdavide Scambi (*)

Le analisi di scenario e la conseguente valutazione dei rischi, riferiti ad un impianto sportivo di elevata capacità ricettiva, richiedono particolare accuratezza in virtù di problematiche specifiche. Se consideriamo uno stadio, non dobbiamo infatti dimenticare quanto la struttura di questo tipo durante il proprio arco temporale di fruizione, possa essere utilizzata per attività diverse: eventi di carattere sportivo, concerti musicali, riunioni politiche, assembramenti di natura sociale o religiosa. Analizzeremo in questa sede il rischio specifico dato dall'utilizzo dei materiali esplodenti.

La variabilità operativa, infatti, è data dalla tipologia di esplosivo utilizzato, dalla modalità di confezionamento dell'ordigno, dal mezzo impiegato per trasportarlo all'interno e conseguentemente dalle tecnologie di detection, che devono essere attuate per ridurre le minacce attraverso una fase di prevenzione efficace. In questa occasione ci proponiamo di circoscrivere lo scenario a quello rappresentato da un evento sportivo, tra due squadre del nostro Paese, limitandoci alle analisi e gestione delle problematiche specifiche all'interno del perimetro dell'impianto.

(*) Studio Scambi Vicenza **www.studioscambi.com**

Partita di campionato

Nel fatto specifico di una partita di campionato è da escludere l'impiego criminale di esplosivi di matrice terroristica, eventualità quest'ultima che permette ragionevolmente di non considerare il caso di esplosivi detonanti di derivazione sia civile che militare. La ricerca sarà dunque per materiali di natura incendiaria e pirotecnica, costituita rispettivamente da liquidi infiammabili e polvere deflagranti di varia origine.

Liquidi e polveri

Entrambe le tipologie di materiali, infatti, sono caratterizzate dalla necessità comune di dover essere contenuti in recipienti o in un involucro: i liquidi infiammabili, in virtù del loro stato fisico, tendono a disperdersi nell'ambiente in assenza di un recipiente; parimenti le polveri deflagranti necessitano di essere chiuse all'interno di un involucro qualora si vogliano sfruttare appieno le loro caratteristiche. La finalità dell'involucro appunto è quella di costringere i gas prodotti durante la combustione della polvere al raggiungimento della pressione di rottura, disperdendo nell'ambiente circostante schegge e frammenti di varie forme e dimensioni.

Le analisi di scenario e la conseguente valutazione dei rischi, riferiti ad un impianto sportivo di elevata capacità ricettiva, richiedono particolare accuratezza in virtù di problematiche specifiche

Radiogeni e metal detector

Le proiezioni, propagandosi a velocità elevatissime, possono causare il ferimento, la morte di persone, generare danni a finestre e vetrate, aumentando il danno esponenzialmente. La necessità comune di dover essere contenuti in involucri e recipienti genera però un grosso limite per i materiali di natura incendiaria e pirotecnica, in quanto rende possibile la rilevazione mediante l'utilizzo di tecnologie radiogene e, se stipati in recipienti metallici, attraverso la metal detection. Infatti, utilizzando tali tecnologie, è molto più semplice rilevare un contenitore piuttosto che i materiali deflagranti ivi racchiusi. Quindi ci sono due opzioni per rilevare un ordigno deflagrante: trovare il contenitore deputato al contenimento del materiale esplodente o individuare il materiale stesso.

Controllo accessi e rilevazione

La detection, all'ingresso di un impianto sportivo, si attua con l'accesso attraverso varchi simili a quelli in ambito aeroportuale. Il passaggio obbligato di tutte le persone e dei loro oggetti, attraverso uno o più varchi presidiati e allestiti con tecnologie fisse, deve tener conto di:

- il breve periodo di tempo entro il quale totalità delle persone deve transitare attraverso i varchi di controllo;
- gli obiettivi da perseguire in via prioritaria durante la detection;
- l'efficacia della detection stessa.

Le tecnologie

Le procedure e le tecnologie di detection di eventuali materiali esplodenti, applicabili durante un evento sportivo, sono principalmente:

- la metal detection in primis per individuare oggetti contundenti o armi, e, nel caso di esplodenti nascosti, i contenitori entro i quali essi sono racchiusi, nonché i corpi contundenti quali chiodi, viti, bulloni, lamette che vengono incluse nell'ordigno per aumentare gli effetti indotti dall'esplosione;
- il controllo visivo e la perquisizione personale, atti a scovare bombe carta, fumogeni, petardi, oggetti pirotecnici in generale, ove le tecnologie a raggi X non siano possibili per motivi di sicurezza umana o per privacy;
- le tecnologie radiogene x-ray, abbinate alla metal detector all'interno dello stesso varco, per individuare per forma caratteristica materiali esplodenti per colorazione; questi materiali riconducono a determinate cromaticità per le caratteristiche chimiche e la densità delle sostanze che le compongono;
- l'impiego di cani addestrati a riconoscere sostanze di varia natura tra cui gli esplosivi.

Le unità cinofile sono una grande risorsa, le cui attività devono però essere pianificate con grande attenzione e gestite con estrema intelligenza. Queste strategie, se opportunamente attuate, risultano estremamente efficaci per il modello di evento rappresentato e sicuramente possono essere integrate, qualora richiesto, alla scansione di codici QR code green pass Covid-19.

Le interviste

Fiera SICUREZZA... a tutta sicurezza

Intervista a

Paolo Pizzocaro
Exhibition Director
di SICUREZZA 2021

In questa rubrica dedicata alla sicurezza negli eventi a grande accoglienza di natura sportiva, musicale e fieristica, non potevamo non occuparci in maniera più dettagliata della manifestazione di riferimento per il comparto sicurezza: la biennale SICUREZZA, di scena il 22-24 Novembre 2021. Mentre le ultime disposizioni danno il via libera alle fiere, nel rispetto delle linee-guida per la ripresa delle attività economiche e sociali emanate dalla Conferenza delle Regioni, il mercato della sicurezza si sta infatti muovendo e cominciano a fioccare le conferme degli espositori. Ma come sarà la nostra biennale di riferimento, in un mondo in cui restano obbligatorie le mascherine, consigliati i percorsi differenziati in entrata e uscita e raccomandati i pagamenti elettronici? Ne abbiamo parlato con l'Exhibition Director.

Sgombriamo subito il campo dagli interrogativi più ricorrenti: che tipo di organizzazione avete impostato (a quanto è dato sapere ad oggi, ovviamente) per gestire la sicurezza nei giorni di fiera? Saranno previste restrizioni agli accessi o contingentamenti?

Grazie alla collaborazione con un team di esperti e in sinergia con i principali players del settore, Fiera Milano da un anno si è dotata di un "Protocollo per il contenimento della diffusione del nuovo coronavirus" che consente la permanenza in fiera in piena sicurezza e che ormai è parte integrante delle modalità di visita di ogni appuntamento che si svolga nei nostri quartieri. Eventuali ulteriori dettagli potremo naturalmente definirli più avanti, in linea con l'evoluzione della situazione e seguendo le linee guida nazionali che ci saranno in quel momento, ma le procedure di massima sono estremamente chiare e sono già state testate con successo nelle fiere che si sono tenute tra luglio e settembre dello scorso anno. Non dimentichiamo, poi, che la campagna vaccinale sta procedendo a pieno ritmo e a novembre, quando ci vedremo per SICUREZZA, la percentuale di vaccinati con la seconda dose sarà sicuramente altissima. Per la sicurezza di espositori e visitatori prevediamo una intensificazione delle attività di pulizia, il controllo della temperatura all'ingresso e l'uso della mascherina, ma saranno soprattutto i servizi digitali a fornire un valido aiuto in termini di sicurezza e semplificazione delle procedure. In particolare, sarà ulteriormente incentivata la preregistrazione online, eliminando assembramenti alle casse e passaggio di biglietti cartacei. Grande supporto verrà poi dal digital signage, la nuova infrastruttura tecnologica che, con 80 ledwall ad alta risoluzione presenti in tutto il quartiere, consente un'informazione immediata, indicando, per esempio, quali ingressi usare o quali padiglioni in un determinato momento sono troppo affollati. Una heatmap permette infatti la geolocalizzazione, monitorando flussi e percorsi e garantendo il distanziamento. Infine, attraverso la nuova App di quartiere si potrà usufruire di nuovi servizi digitali, come la prenotazione online dei parcheggi o l'acquisto del pasto.

E veniamo ai contenuti: quale sarà il tema portante e come intendete svilupparlo, lato esposizione ma anche lato lavori congressuali?

SUCUREZZA 2021 sarà focalizzata sui temi e i trend che in questo particolare momento storico stanno trainando l'innovazione tecnologica del comparto: convergenza, digitalizzazione e certificazione della professione. La convergenza ormai da tempo ha cambiato l'approccio alla security, che oggi diventa parte integrante di sistemi più complessi e richiede, da parte di progettisti e installatori, un approccio olistico e sempre più competente. Conoscere la singola tecnologia non basta più: è necessario studiare ogni soluzione come fosse un abito su misura costruito intorno alle esigenze del cliente e al contesto applicativo in cui si inserisce. La crescente digitalizzazione è la seconda sfida da affrontare, e non solo per chi produce. Perché oggi chi progetta o installa deve necessariamente avere nuove competenze in Cyber Security, a tutela dei dati che l'impianto gestisce e raccoglie, ma anche delle proprie responsabilità. Infine, centrale sarà la valorizzazione di competenze e conoscenze, dunque della professionalità. Il settore guarda

da tempo al valore delle certificazioni come punto di riferimento per costruire un'offerta di mercato affidabile e diverse realtà associative si stanno interrogando sulla opportunità di un passaggio dalla certificazione volontaria a quella cogente. I primi due temi che ho citato saranno naturalmente centrali nella proposta espositiva e tecnologica, mentre tutti e tre troveranno spazio nella proposta formativa. Proprio in queste settimane stiamo cominciando a confrontarci con i nostri partner per definire il palinsesto, che ancora una volta sarà ricco e costruito intorno alle reali esigenze di aggiornamento di tutti gli operatori del settore.

Sono stati anni pesanti, soprattutto per il settore fieristico: che reazioni sta avendo il mercato della sicurezza alla vostra proposta fieristica e che affluenza ci si può attendere, allo stato dell'arte?

Devo dire che, nonostante la complessa situazione che ci circonda, stiamo registrando risposte positive. La rete di partner che da anni ormai si è stretta intorno a SICUREZZA, riconoscendola come punto di riferimento per il settore, sta continuando a lavorare in stretta collaborazione con noi per costruire un progetto rispondente alle esigenze di questo particolare momento storico. Siamo dunque certi che chi visiterà la manifestazione troverà un'offerta estremamente ricca di spunti e opportunità di aggiornamento. Parlando di espositori, grazie alle conferme di brand leader di diversi settori, la proposta tecnologica si conferma già oggi molto rappresentativa di tutte le anime del mercato. Come la scorsa edizione, abbiamo optato per un layout organico, con padiglioni contigui e una connotazione merceologica degli spazi: nei padiglioni 5 e 7, in aree ben connotate, si concentreranno videosorveglianza, antincendio, antintrusione e cyber security, mentre il padiglione 10 sarà dedicato a sicurezza passiva, controllo accessi e a Smart Building Expo, con la sua proposta focalizzata sulla integrazione tecnologica, che integra e amplia l'offerta di SICUREZZA, inserendosi negli stessi spazi espositivi senza soluzione di continuità. Altra novità di questa edizione sarà l'ulteriore contemporaneità con MADE expo, che consentirà di offrire un'offerta a 360° su tutte le soluzioni e le tecnologie rivolte al mondo del building. Una sinergia positiva soprattutto per i visitatori che, in un solo contesto, potranno scoprire e approfondire le sfide che sistemi, impianti, prodotti, soluzioni e normative dovranno affrontare nella fase di ripresa. Non dimentichiamo che tante delle tecnologie in mostra rappresentano strumenti di innovazione in chiave di digitalizzazione ed efficienza energetica, due dei pilastri su cui si fonda il PNRR, cui necessariamente i produttori saranno chiamati a guardare nei prossimi mesi.

ARITECH

Una soluzione di sicurezza intelligente e integrata per un mondo connesso

Le soluzioni di sicurezza Advisor Advanced di Aritech coprono tutti gli aspetti della sicurezza per la tua abitazione, ufficio, negozio o edificio, permettendoti di concentrarti sulla tua attività. Crea il sistema attorno alle esigenze dei tuoi clienti in modalità standalone o come parte di un sistema integrato con controllo accessi, video e protezione antincendio.

Un sistema di controllo accessi, ad esempio, si integra perfettamente con il rilevamento delle intrusioni, offrendo una soluzione estremamente efficiente in termini di funzionalità e di costi.

ultraSync Empowered

UltraSync è una soluzione conforme con i più elevati requisiti di cybersecurity che ti consente di controllare e gestire il tuo sistema di sicurezza integrato da qualsiasi dispositivo, in tempo reale ed in completa sicurezza.

Ottieni maggiori informazioni su Advisor Advanced e sulla soluzione UltraSync

www.aritech.it

Carrier

Aritech is a Carrier company.

Luca Cardone (*)

5G ed Edge computing per la Pubblica Sicurezza

Il 5G è la tecnologia in grado di abilitare, con prestazioni superiori ai precedenti standard, le comunicazioni tra rete e dispositivi, potendo contare sulla capillarità e la diffusione dei dispositivi di ricezione e collegamento. Le peculiarità del 5G e le sue potenzialità rivestiranno un ruolo di fondamentale importanza nella vita quotidiana dei cittadini e per le aziende e per gli Enti pubblici: grazie a questo standard sarà possibile, infatti, sviluppare soluzioni innovative di utilizzo della rete favorendo lo sviluppo digitale del Paese. La Commissione Europea dell'Action Plan 5G ha evidenziato che "i servizi pubblici possono essere un early adopter e un promotore di soluzioni basate sulla connettività 5G, incoraggiando l'emergere di servizi innovativi, contribuendo a una massa critica di investimenti e affrontando questioni importanti per la società". È prevedibile, tenendo conto dell'impatto che il 5G avrà sui cittadini, che lo Stato farà da committente per la richiesta di servizi per la tutela degli spazi pubblici e del tessuto urbano. Insomma, per la sicurezza.

(*) Marketing Manager di Retelit **www.retelit.it/**

Attualmente le reti di telecomunicazioni sono basate per lo più su tecnologie wireless mobili terresti a banda stretta come TETRA (Terrestrial Trunked Radio): si tratta di reti con capacità di dati limitate nate per supportare comunicazioni mission-critical da dispositivo a dispositivo. La richiesta di accesso ad applicazioni e contenuti in tempo reale, l'utilizzo di sistemi di Intelligenza Artificiale e Big Data e, in aggiunta, l'estrazione di dati da sistemi di rilevamento di persone e oggetti con l'utilizzo della Realtà Aumentata, consentono di individuare degli ambiti particolarmente di interesse in tema di 5G e Pubblica Sicurezza. Per esempio: per il supporto alle forze dell'ordine in termini di Search & Rescue, videosorveglianza, riconoscimento facciale, gestione di infrastrutture e trasporti, monitoraggio e tracciamento di dispositivi IoT, sistemi di sicurezza avanzata per prevedere attacchi informatici; per la gestione di emergenze e catastrofi con sofisticati sistemi di allerta, monitoraggio, predizione e simulazione. In questo scenario ben si inserisce il 5G, in grado di offrire "nativamente" caratteristiche che vanno a completare e integrare sostanzialmente le esigenze delle reti mission critical.

Nuove prestazioni

Grazie al multi-access edge computing, la capacità di processare dati più vicini all'utente, saranno abilitate in maniera più sicura e con una latenza più bassa le applicazioni in ambito smart city e smart mobility e con il network slicing, fiore all'occhiello della tecnologia 5G, sarà possibile "ritagliare" le reti virtuali per esigenze di Pubblica Sicurezza prioritizzandone il traffico. Diffondendosi, il 5G permetterà l'integrazione di ulteriori tecnologie. Su tutte il Blockchain. Negli ecosistemi 5G e IoT, infatti, per poter controllare e coordinare i flussi operativi si imporrà l'uso di questa tecnologia di cui saranno sfruttate tutte le potenzialità. Nelle situazioni emergenziali, per esempio, c'è l'esigenza per molteplici enti autorizzati ad accedere, anche in mobilità, alle infrastrutture IoT per controllare le segnalazioni pubbliche. Le tecnologie Blockchain/DLT possono autenticare gli accessi provenienti da autorità competenti (forze di Polizia e Carabinieri, Protezione Civile, ecc.) ai servizi di controllo remoto e monitoraggio di dispositivi.

Il ruolo dell'AI

Un ruolo particolare lo rivestirà l'intelligenza artificiale, che presenta grandi capacità di supporto ai servizi per la sicurezza pubblica, soprattutto per l'analisi e l'apprendimento dei dati di geolocalizzazione forniti dai sensori, offrendo previsioni accurate che elevano la sicurezza e il benessere dei cittadini riducendo i costi. L'AI offre un apporto indispensabile nel monitoraggio dello stato di salute di costruzioni, ponti e palazzi, nella prevenzione e gestione dei disastri, nelle attività di sorveglianza di persone e territori.

Il 5G rivestirà un ruolo fondamentale per l'evoluzione della società, permettendo agli Enti pubblici di offrire servizi innovativi, in particolare in materia di sicurezza

5G

"Reti, edge computing e 5G: l'impatto sulla sicurezza fisica e la videosorveglianza": intervento integrale di Luca Cardone a secsolutionforum 2021

La formazione non si ferma!

Abbiamo affiancato alla formazione in aula, una valida proposta formativa a distanza.

Resta a casa, noi veniamo da te!

L'offerta formativa a distanza è stata validata dal TÜV Italia e riconosciuta anche idonea per il mantenimento della certificazione secondo lo schema CEI - TÜV Italia.

Il team dei nostri docenti ha modulato le varie proposte, affinchè siano fruibili a distanza con gli stessi standard di apprendimento. Molti dei corsi prevedono anche un test finale per la verifica dell'apprendimento.

Rimani aggiornato su tutti i corsi su www.ethosacademy.it

ETHOS ACADEMY
FORMAZIONE

Tel. +39 051 0475136
academy@ethosacademy.it
www.ethosacademy.it

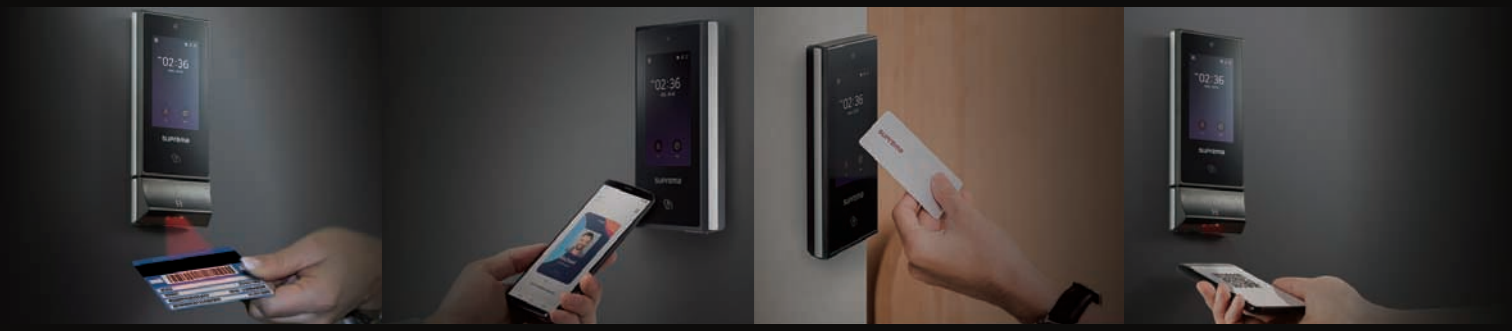
CORSI RICONOSCIUTI DA
TÜV SÜD
Examination Institute

suprema

X-Station 2

Versatile Intelligent Terminal

Suprema X-Station 2 è un terminale che supporta Carte Mobile, carte RFID e codici QR dalle prestazioni eccezionali.
La Soluzione **ECOPASS** è il sistema di controllo accessi in grado di identificare tramite il codice fiscale
letto dal barcode della tessera sanitaria, ideale per aree ecologiche o altre aree pubbliche.
Il dispositivo è completamente gestibile tramite il software **BioStar 2**, con di interfaccia Web, anche da remoto.



ETER Srl
BIOMETRIC TECHNOLOGIES

ETER Biometric Technologies Srl
Via Mattei 21 - Casinalbo di Formigine (MO) - Italy
Tel. +39 **059 7874 620** - Fax +39 059 7874 622
info@eter.it - **www.eter.it**

La Redazione

Phygital security: quale protezione contro gli attacchi informatici?

Non più solo physical e certamente molto digital: la security come la conoscevamo una volta è da tempo diventata "Phygital", con tutto ciò che il digitale porta con sé - a partire dal rischio di hacking. Sono diverse le strategie messe in campo dai produttori del comparto sicurezza per contenere la minaccia di attacchi cyber ai dispositivi posti in commercio, ma è evidente che per mitigare un rischio per sua natura dinamico, variabile e in continuo aggiornamento occorre un "patto di filiera" tra produttori, integratori ed utilizzatori finali che permetta di immaginare una catena di responsabilità trasparenti e condivise. Le stesse certificazioni non possono assicurare che un prodotto sia cyber security-proof, perché nell'eterna lotta tra guardie e ladri è destino che vinca il ladro (che di mestiere fa solo quello e ci pensa 24/365). Magari sarebbe utile che un ente indipendente fungesse da riferimento per l'intero comparto per definire ciò che può essere considerato "accettabilmente sicuro". Senza dubbio è essenziale (e non così scontato) mantenere aggiornati gli apparati, magari in una logica di automazione come è prassi per PC, tablet e smartphone. Su questi ed altri temi abbiamo interrogato il mercato, concentrandoci su quattro domande-chiave.

Dite la vostra

le domande

1. Quali misure ponete in essere "by design" per garantire la sicurezza cyber dei vostri prodotti?

2. Quali misure procedurali/formative ponete in essere per istruire il canale (e tramite il canale, la stessa utenza finale) alla sicurezza cyber dei vostri prodotti?

3. Se lasciato alla sola iniziativa dell'utente finale, non solo il cambio della password di default, ma anche l'aggiornamento dei firmware può non essere operato in maniera diligente, e quindi esporre i dispositivi a rischi di violazioni. Sarebbe utile prevedere degli aggiornamenti a cadenze "obbligate" (modello PC o smartphone)?

4. Ogni produttore vanta le proprie certificazioni: per armonizzare le valutazioni ed elevare la sicurezza cyber (dunque la credibilità) dell'intero comparto, sarebbe utile definire un ente di certificazione unitario cui l'intera industry mondiale possa fare riferimento?

Dite la vostra

Andrea Monteleone

National Sales Manager - Axis Communications

1 L'Azienda ha già da tempo introdotto tutta una serie di metodologie e prassi per mitigare quanto più possibile i rischi correlati alla cyber security, non solo nelle modalità con cui firmware e software sono sviluppati e testati per rispondere ai più alti standard di qualità e sicurezza, ma anche nella gestione e protezione della supply-chain in tutte le sue fasi: dall'approvvigionamento dei componenti alla delivery del prodotto.

2 Storicamente Axis ha sempre investito molto sulla educazione e formazione di Partner e Clienti finali. A tal proposito, il nostro impegno per contribuire a rendere sempre più consapevole il mercato non è destinato a diminuire, anzi. L'impegno è, principalmente, orientato a supportare tutti gli stakeholder nella fase di progettazione e implementazione dei sistemi di sicurezza, oltre che nella gestione di eventuali incidenti nel modo più proattivo e trasparente possibile.

3 Il tema è molto dibattuto e non esiste una risposta univoca e risolutiva. Più che imporre un aggiornamento obbligatorio o cadenzato – pratica che in certi ambienti potrebbe addirittura risultare controproducente o addirittura impossibile da applicare – sarei più propenso a proporre strategie condivise per mantenere sempre al massimo livello ammissibile il livello di sicurezza di un qualsiasi sistema ICT.

4 Lo spunto di riflessione è già stato recepito dalla Comunità Europea e, in certi settori, si va proprio in questa direzione. Il tema è quello di stabilire i criteri di verifica, che sono ancora lontani dall'essere ben definiti.

Il tema vero è: come stabilire i criteri di verifica della sicurezza informatica? Chi lo deve fare? Da chi deve essere accreditato?

Per leggere le interviste integrali ai player di mercato sul tema cyber security

Dieci vostre

Giampiero Miceli
Direttore Commerciale - Bettini

1 La sicurezza informatica dei dispositivi si basa sia su caratteristiche dei prodotti stessi (cifratura dei dati, profilazione accessi, mancanza di password di default, possibilità di disabilitare servizi non utilizzati), sia su procedure di controllo atte a garantire che l'intero pacchetto FW sia sempre allineato con le soluzioni delle vulnerabilità più recentemente individuate e risolte. Penetration test interni sono eseguiti frequentemente, in un processo consolidato che si completa con il rilascio di un aggiornamento e la sua pubblicazione sui nostri canali.

2 Con la pandemia Covid abbiamo adottato un nuovo modo di diffondere la cultura aziendale, abituandoci ad interagire attraverso strumenti digitali (webinar e meeting online). Formazione e informazione online per noi sono oggi validi canali comunicativi. Questi incontri trattano temi che spaziano dagli aspetti normativi a quelli tecnici, formativi e commerciali e si rivolgono a tutti coloro che appartengono al mercato della sicurezza: installatori, progettisti e vigilanze fino agli utenti finali.

3 Firmware e software degli apparati GAMS sono sviluppati in Italia e, da sempre, rilasciamo aggiornamenti periodici. Questo metodo consente ai clienti di essere informati sulle novità e di trasferirle agli utenti finali, affinché apprezzino l'attenzione che poniamo all'aggiornamento normativo e tecnico dei nostri dispositivi.

4 Crediamo che sia necessario avere regole e procedure certe. Il fai da te, pur essendo encomiabile, spesso nasce dall'impegno del singolo e non da processi normati a beneficio del mercato.

Stefano Riboli
Marketing Manager Security - Bosch Security Systems

1 Implementiamo diverse misure di sicurezza by design nelle telecamere IP, tra le quali: a) il firmware crittografato contiene il signing; b) il firewall integrato (in caso di errori di inserimento password, la modalità "autoriparante" fa continuare i soggetti autorizzati); c) il chip Trusted Platform Module (TPM) all'interno della telecamera protegge le chiavi e i dati più segreti; d) porte e servizi non necessari sono disabilitati; d) l'installatore può abilitare un sigillo alla configurazione che, in caso di modifiche alle impostazioni della telecamera, la stessa può notificare.

2 La piattaforma Bosch Security Academy prevede, per la data security, diversi corsi online e in aula con relatore ed esame finale. Durante i corsi, per mezzo del tool di configurazione, è possibile verificare il livello di vulnerabilità della telecamera IP.

3 L'aggiornamento di FW e SW sono solo una delle misure da mettere in atto e dovrebbero essere previsti durante la manutenzione. Un altro tema è la valutazione da parte del produttore del rilascio degli aggiornamenti a seguito della fine di produzione del prodotto. Per Bosch si parla di 5 anni di manutenzione del FW, considerata come una garanzia firmware estesa delle telecamere IP. Per queste attività, in base al rischio, bisognerebbe periodicamente valutare le vulnerabilità e fare test di penetrazione.

4 Un ente certificatore potrebbe essere un'ulteriore garanzia per la clientela, ma è fondamentale che il produttore testi i prodotti facendo riferimento a tutti gli standard di mercato. Nei datasheet dei prodotti, Bosch dichiara le normative di riferimento utilizzate e mette a disposizione un team di esperti PSIRT (Bosch Product Security Incident Response Team) come punto di contatto centrale per ricercatori esterni per la sicurezza, partner e clienti per segnalare informazioni sulla sicurezza relative ai prodotti. La divulgazione responsabile delle vulnerabilità consente di correggerle, informare i clienti sulle correzioni e migliorare continuamente la sicurezza dei prodotti.

Walter Pizzen
Electronic Division Director – CBC Europe

1 Da anni GANZ ha rimosso e bloccato i servizi P2P in tutte le telecamere che vengono sviluppate con firmware chiusi e stabili, testati ed approvati nei nostri uffici europei. I nostri videoregistratori vengono forniti con funzioni P2P e DDNS disabilitati.

2 La password deve essere impostata al primo avvio ed i servizi di sicurezza sono tutti abilitati di default. Sono i clienti a dover scegliere che grado di sicurezza adottare, in base alla sensibilità dell'impianto, disabilitando le protezioni e non viceversa. Capiamo la comodità di assicurarsi prodotti plug&play ma, da tempo, abbiamo scelto di non servire quel mercato che preferisce effettuare configurazioni rapide, a scapito della sicurezza dei dati.

3 Spinti da un servizio della televisione di stato, oggi non si parla d'altro che di cybersecurity. Siamo sicuri che vogliamo rendere i nostri prodotti vulnerabili esponendoli, ad esempio, ad aggiornamenti automatici, soltanto per seguire la corrente del momento? Per noi la sicurezza dei dati deve essere la priorità e gli impianti devono essere manutenuti da operatori professionali. Vendiamo sicurezza e non smartphone! Viviamo in un paese in cui si chiudono i recinti dopo che il bestiame è scappato e, per tamponare, vorremmo inserire burocrazia invece che risolvere i problemi.

4 Ritengo che il nostro settore abbia già gli strumenti per affrontare questo tipo di problematica, ma la scelta sia stata quella di "voltarsi dall'altra parte". Non credo che possa servire aggiungere un nuovo organismo, mentre far rispettare le regole già esistenti sì! Potrebbe essere una bella novità…

Daniele Sisinio
Director - Dallmeier Italia

1 Il "Made in Germany" ci impone un livello molto alto di sicurezza sia nello sviluppo sia nella produzione dei prodotti per garantire, in ogni fase del processo (sviluppo, programmazione, produzione, penetration test esterni, ecc.), che vengano prese in considerazione le più elevate esigenze degli standard internazionali (ad es. EU GDPR) e dei clienti. Disponiamo di uno dei più grandi portafogli di precauzioni: dalla crittografia end-to-end secondo gli standard più elevati alle tecniche di security gateway, ai sistemi anti-hacking e alle corrispondenti tecnologie di autenticazione (IEEE 802.1X).

2 Sempre più spesso la documentazione di "Security and Privacy by Design" è tra le prime richieste dei clienti. Noi offriamo una documentazione completa, guide alle migliori pratiche e linee guida di implementazione che vanno ben oltre le semplici funzionalità e forniscono un punto di vista olistico prima dell'implementazione.

3 Abbiamo già implementato queste linee guida. Quando gli utenti avviano una telecamera Dallmeier, sono costretti a creare la password e ID nel rispetto di rigorose sintassi di sicurezza. All'interno della nostra piattaforma software HEMISPHERE®, l'amministratore può impostare politiche di password individuali come la modifica forzata della password dopo un certo intervallo di tempo, rispettivamente, consentiamo la completa integrazione AD.

4 Alcune certificazioni vanno già in questo senso, come LGC Forensic, ma potrebbe essere utile disporre di ulteriori istituzioni di certificazione indipendenti dal fornitore. Soprattutto per prevenire abusi, come vediamo con presunte "certificazioni GDPR", che non sono in alcun modo certificati ufficiali, dal momento che le condizioni quadro per le certificazioni GDRP non sono state nemmeno ratificate.

Dite la vostra

Alberto Patella

Key Account Geovision - Gvision Italia

1 I nostri prodotti non sono concepiti con Chipset di derivazione Huawei / Hisilicon. Di conseguenza non vengono instaurate delle connessioni in uscita verso terze parti per la condivisione di dati sensibili. Oltre a ciò su tutti i nostri progetti è possibile applicare la garanzia di certificazione VA/PT nella quale viene evidenziata la totale assenza di falle informatiche.

2 Attraverso i nostri canali Social vengono argomentate tutta una serie di attività utili per i progettisti ma anche l'utenza finale.

3 E' una soluzione che abbiamo da più tempo caldeggiato, ma la disomogeneità dei prodotti e la sicurezza di molte reti IP, a volte rendono vani questi sforzi.

4 La CyberSecurity è una branca in continuo sviluppo e carente ancora di tante figure professionali estremamente necessarie. Noi come GVision e Geovision ci siamo appoggiati agli specialisti che allo stato attuale riteniamo possano essere la massima espressione di sicurezza, ma auspichiamo un'armonizzazione con un ente unico a cui far riferimento.

Potrebbe essere utile disporre di ulteriori enti di certificazione indipendenti dal fornitore

Dite la vostra

Francesco Panarelli

Key Accounts & Business Development Director - Hikvision Italy

1 I prodotti Hikvision soddisfano i più alti standard di sicurezza riconosciuti a livello internazionale da diverse certificazioni (FIPS 140-2, CC con garanzia EAL2+, ISO 27001, ISO 9001:2008, ISO 28000, CMMI Livello 5). Hikvision aderisce ad CVE, è Numbering Authority ed offre diversi strumenti di sicurezza: crittografia, strumenti di trasporto sicuri sulla rete (es. HTTPS), certificati e credenziali di accesso, codici univoci di sicurezza per ogni singolo device, programmabili solo dall'utente/utilizzatore. Anche se non impostate adeguatamente, le telecamere Hikvision non inviano immagini a server remoti e Hikvision Italy non offre soluzioni "Cloud storage" che prevederebbero l'invio di flussi ad uno storage condiviso e raggiungibile tramite una connessione ad un Cloud proprietario.

2 Hikvision Italy ha pronto un programma di formazione da "interiorizzare" e calare sulla realtà italiana, in particolare gli installatori.

3 Per mitigare un rischio dinamico come la sicurezza informatica, occorre che gli apparati vengano mantenuti aggiornati. La protezione dagli attacchi cyber può essere implementata solo grazie alla cooperazione fra Vendor, System Integrator ed End-User. Sarebbe auspicabile che, partendo dal responsabile della protezione dei dati e cioè l'End-User, diventasse prassi richiedere al manutentore di includere fra i servizi offerti anche l'aggiornamento degli apparati, in modo sistematico e rigoroso. Anche l'automazione degli aggiornamenti è un tema interessante, ma, proprio per una concezione di sicurezza dei sistemi, occorre ricordare che soprattutto in applicazioni tradizionali non sono concessi accessi verso internet per i componenti. Isolando gli apparati si ha una protezione maggiore, ma si impediscono aggiornamenti "push" (tipici dei device personali sempre connessi).

4 Ad oggi nessuno può certificare un prodotto come "cyber-sicuro", in quanto l'assenza di vulnerabilità oggi, non esclude la presenza di una vulnerabilità domani. Sarebbe però auspicabile la nascita di un ente che si occupasse almeno della definizione di un percorso di sviluppo e produzione capace di rispettare determinati parametri, che definisse i processi e gli step obbligati per poter considerare un prodotto sufficientemente sicuro da necessitare il "solo" mantenimento dei livelli di sicurezza raggiungibili con il rilascio regolare di FW.

Dieci vostre

Massimo Grassi

Security Sales Engineer - Panasonic Business

1 Il firmware di tutti i prodotti Panasonic iPRO è controllato in fabbrica e non è alterabile, criptabile né modificabile. Ogni accesso alle telecamere o al firmware stesso è bloccato o protetto, non vi sono back-door o porte di rete aperte se non quelle essenziali al funzionamento dei dispositivi. All'utente è quindi lasciata la sola possibilità di aprire porte aggiuntive in base ai servizi che vuole gestire, in piena sicurezza.

2 Tramite il Panasonic Partner Portal è possibile diventare Partner Certificato Panasonic e accedere a training di vario livello dedicate anche alla cybersecurity. Supportiamo i partner passo dopo passo, dando loro gli strumenti per realizzare un impianto di sicurezza totalmente configurato e cyber-proof.

3 I firmware Panasonic, in quanto criptati e sottoposti a continuo controllo, consentono di ridurre notevolmente i rischi di violazioni. L'i-PRO Configuration Tool (iCT) permette alle aziende di tenere costantemente aggiornato il sistema di videosorveglianza e di verificare automaticamente la disponibilità di nuovi aggiornamenti del firmware e di sistema.

4 Auspichiamo la definizione di una norma condivisa, che si affianchi alla regolamentazione degli enti di certificazione esistenti. Panasonic 5 anni fa ha siglato un accordo con la Certification Authority Symantec (poi acquisita da DigiCert) per certificare i prodotti; più recentemente ci siamo affidati all'Autorità di certificazione GlobalSign per il rilascio di certificati di encryption e di sicurezza che li rendono conformi a standard internazionali come l'americana FIPS per l'utilizzo anche in ambiti difesa, banche e PA negli USA. Al momento non esiste una norma equivalente in Europa, ma speriamo venga introdotta.

Massimiliano Marchionni

Camera Manager – Spark Security

1 In Spark lavoriamo costantemente sul firmware delle telecamere che produciamo anche per innalzare il livello di sicurezza. Per esempio, chiediamo obbligatoriamente di definire nome utente e password al primo avvio e prevediamo il blocco automatico del dispositivo in caso di troppi login falliti. Anche la Digest Authentication di default è utile nel trasferimento delle credenziali, così come la possibilità di accedere ai video solo tramite autenticazione.

2 Per Spark questo è un argomento di importanza cruciale e infatti ci facciamo spesso promotori di attività di formazione rivolte anche ai distributori e agli installatori. Inoltre, vogliamo realizzare un servizio di diagnostica che consenta a chi utilizza i nostri prodotti di verificare lo stato dei dispositivi e mantenerli costantemente aggiornati, garantendo così maggior sicurezza e performance a tutto l'impianto.

3 Sicuramente può essere utilissimo inviare periodicamente degli avvisi sull'eventuale obsolescenza della password e del firmware per mettere in guardia l'operatore sui potenziali rischi dell'impianto. Ancora una volta l'aspetto che fa la differenza è la conoscenza. Ovviamente è fondamentale investire a monte di tutto anche sulla sicurezza della rete e dei server ad essa connessi.

4 Per rendere più sicuri i nostri prodotti, in Spark prendiamo spunto dalle principali direttive europee e statunitensi in materia. Allo stesso tempo, riteniamo che sia ormai necessaria la nascita di un apposito ente certificatore, come già avviene per le certificazioni elettromagnetiche, che fornisca direttive uniche a cui tutti i produttori possano fare riferimento per elevare la cybersecurity delle loro soluzioni.

Dite la vostra

La difficoltà maggiore sarà la scelta di un Ente Certificatore che sia completamente autonomo e fuori delle dinamiche di mercato

Ermal Xhaferi

Technical Support Manager - Syac-TB

1 I prodotti SYAC-TB sono stati sviluppati interamente su sistema operativo Linux, customizzato e configurato con i soli moduli necessari al funzionamento del dispositivo. Inoltre sono stati attivati solo i servizi essenziali legati alla comunicazione del Digieye (il core tecnologico della soluzione) che non sono legati ad un server SSH o telnet. In più tutta la comunicazione viene realizzata su un protocollo proprietario sviluppato internamente. Questo ha come risultato che nessun Daemon o client di comunicazione, come aggiornamenti automatici, mascherati o meno, possa essere attivato verso un server nascosto.

2 Per noi di SYAC-TB è fondamentale creare una rete di partner qualificati per i nostri prodotti, quindi la formazione dei nostri installatori e distributori è fondamentale per garantire un corretto funzionamento e utilizzo dei nostri sistemi di protezione in termini di cyber security. Abbiamo attivato quindi una Academy attraverso la quale formiamo tutti gli operatori e partner che dovranno utilizzare i nostri prodotti di Security.

3 L'aggiornamento delle nostre macchine avviene solo tramite accesso locale di un'utenza supervisore o connessione con i nostri software di centralizzazione, sempre con diritti di supervisore. I nostri sistemi non prevedono aggiornamenti automatici e/o da Cloud, che potrebbero rendere insicuro ed instabile il sistema di protezione.

4 Sarebbe interessante stabilire degli standard di sicurezza omogenei per l'intera industria in modo che anche gli utenti riescano ad avere tutte le informazioni necessarie per una scelta più consapevole del proprio sistema. Sicuramente la difficoltà più importante sarà la scelta di un Ente Certificatore che sia completamente autonomo e fuori delle dinamiche di mercato.

XD-2

Rilevatore multifunzione filare

XD-2 opera in 4 modalità differenti: contatto magnetico, rilevatore d'urto, rilevatore d'urto con contatto magnetico a doppio canale e rilevatore di allagamento (con sonda esterna FPX-1).

Per maggiori informazioni visita:
www.satel-italia.it

Gianluca Mauriello (*)

Pnrr: spenderlo bene puntando su cybersecurity e privacy

"Da una parte abbiamo i soldi del Next Generation EU e una serie di priorità per spenderli, indicate sia dall'Europa che dal Ministro per l'innovazione tecnologica e la transizione digitale, Vittorio Colao. Dall'altra nel 2020 gli attacchi di dominio pubblico verso realtà con base in Europa (aziende, istituzioni pubbliche, strutture sanitari, etc.) sono cresciuti dall'11% al 17% rispetto al 2019, secondo il Rapporto Clusit 2021[1]. Come spendere in modo intelligente questa pioggia di quattrini?

[1] **https://clusit.it/rapporto-clusit/**

(*) Regional Sales Manager Italia, Genetec Inc. **www.genetec.com**

Duecentodieci sono i miliardi di euro delle risorse del programma Next Generation EU, integrate dai fondi stanziati con la programmazione di bilancio 2021-2026. Per cogliere questa occasione, l'Italia ha ideato il Piano nazionale di ripresa e resilienza (Pnrr) che prevede un insieme di azioni e interventi per superare l'impatto economico e sociale della pandemia.

Sicurezza: un tema sociale

Fra le priorità strategiche per il nostro paese, concordate a livello europeo, si annoverano la digitalizzazione e l'innovazione. Ma nell'attesa di questa svolta tecnologica a lungo termine, grandi aziende, PMI e Pubblica Amministrazione devono far fronte a problemi molto concreti e attuali. **La sicurezza non è più un tema individuale, ma un tema sociale, che ci impone di intraprendere un percorso culturale di formazione per non sprecare gli investimenti** allocati dall'Unione Europea. Se un singolo è vittima di un attacco informatico o di un data breach, a pagarne i danni sarà potenzialmente tutta la collettività. Per i professionisti della sicurezza fisica è arrivato il momento di collaborare con le controparti nei dipartimenti IT, con l'obiettivo di comprendere i veri limiti dei perimetri di sicurezza e sviluppare processi e governance solidi in grado di mitigare i rischi di attacchi informatici.

Se un singolo è vittima di un attacco informatico o di un data breach, potrebbe doverne pagare i danni l'intera collettività

Dati sempre più allarmanti

A livello globale sono stati 1.871 gli attacchi gravi di dominio pubblico rilevati nel corso del 2020. I settori maggiormente colpiti sono stati i cosiddetti "Multiple Targets" (20% del totale, attacchi realizzati in parallelo verso obiettivi molteplici), Settore Governativo, Militare, Forze dell'Ordine e Intelligence (14% degli attacchi a livello globale), Sanità (12%), Ricerca/Istruzione (11%), Servizi Online (10%). Banking & Finance (8%), Produttori di tecnologie hardware e software (5%) e Infrastrutture Critiche (4%) hanno visto addirittura un aumento di tali attacchi.

Qualcuno sta già reagendo

Nel gennaio 2021, Genetec ha svolto un sondaggio rivolto ai professionisti della sicurezza fisica che operano in Europa, Medio Oriente e Africa (EMEA). Dopo un esame delle risposte ricevute, 1550 risposte sono state incluse nel campione analizzato e i cui risultati sono stati pubblicati sul Report "Sicurezza fisica nell'area EMEA nel 2021". Da questo studio emerge che **il 67% degli intervistati intende dare priorità al miglioramento della propria strategia di sicurezza informatica nel 2021.** Nonostante una più elevata pressione fiscale, la maggior parte degli intervistati ritiene inoltre che la trasformazione digitale della sicurezza e delle operazioni sia fondamentale.

Pnrr

Cyber hygiene

Ecco alcune buone pratiche per diminuire le possibilità di cadere vittima di un attacco informatico. La Cyber hygiene prevede di garantire un livello di cybersecurity alto in tutta la supply chain, gestire i flussi di comunicazione in modo attento, puntare sulla formazione dell'utente e dotarsi di una assicurazione cyber.

La necessità di potenziare tutta la filiera della sicurezza informatica deve spingere le organizzazioni ad investire maggiori risorse per limitare le vulnerabilità. Attraverso la gestione del rischio della supply chain è possibile contare su una rete di partner e vendor affidabili con cui lavorare a stretto contatto per avere un quadro chiaro delle politiche di protezione dati e privacy.

Formazione dell'utente

Un attacco informatico può avere conseguenze negative sul lungo periodo in termini di perdita di dati o danni economici. Ecco perché è fondamentale formare i dipendenti, fin dall'assunzione, spiegando loro l'importanza di strategie quali una scelta di una password forte. Tutti possiamo sbagliare, ma con la giusta mentalità e formazione, possiamo ridurre notevolmente il rischio di cadere in trappole tese da hacker che ci traggono in inganno con campagne di "social engineering" per ottenere dati personali e privati. Questi messaggi sospetti o insoliti devono essere individuati con prontezza.

I professionisti della sicurezza fisica devono collaborare con le controparti nei dipartimenti IT per sviluppare solidi processi e governance robuste

Cyber liability insurance

Ormai molte compagnie di assicurazioni offrono polizze e pacchetti per coprire i rischi legati alla criminalità informatica. Investire nella soluzione giusta è quindi una parte essenziale della strategia di cybersecurity. Proprio in virtù delle numerose possibilità, sarà essenziale leggere con attenzione tutte le clausole per scegliere la copertura più adeguata e comprendere con chiarezza il processo di richiesta indennizzo, per evitare confusione e stress in un momento in cui sarete già messi a dura prova dall'attacco informatico.

BETTINI
VIDEO & SECURITY TECHNOLOGY

GAMS
Digital Video Solution

WEBINAR
ISCRIZIONE GRATUITA

Academy

NUOVI APPUNTAMENTI

dalle 10.30
alle 11.30

GIUGNO | LUGLIO 2021

Dal 15 Giugno ripartono i webinar Bettini!

15 Giugno
"GAMS" - La Videosorveglianza avanzata tutta Italiana

17 Giugno
Telecamere speciali "GAMS" - Lettura Targhe LPR e Visione 180 gradi

22 Giugno
La Cyber Security per la Videosorveglianza - Rischi e Precauzioni

24 Giugno
"AVIGILON" - Intelligenza Artificiale al servizio della Sicurezza

29 Giugno
"LINKIT" - Soluzioni Radio per le Smart Cities

1 Luglio
"AVIGILON" - Unificazione Controllo Accessi e Video

6 Luglio
"SFERA" - Telecamere IP Gams - Privacy Accuracy

13 Luglio
"TECNOSENS" - Lettura Targhe professionale pronta da usare

15 Luglio
"AVIGILON" - Body Worn Camera - Sicurezza per chi si occupa di Sicurezza

Al termine di ogni webinar, verrà rilasciato un **attestato di partecipazione Bettini**.

Per supporto o informazioni
eventi@bettinivideo.com | 02 89651000
Vi aspettiamo, non mancate!

Dettagli e registrazione su
bettinivideo.com

Alvise Biffi (*)

Nuova rubrica

CYBER SECURITY "FOR DUMMIES": LE PRINCIPALI MINACCE PER LE AZIENDE

Dopo il successo delle nostre rubriche "for dummies" dedicate ai temi dell'installazione e delle normative di settore, inauguriamo un nuovo filone contenutistico su un aspetto di grande attualità e dal quale nessun professionista può ormai prescindere: la cyber security dei sistemi di sicurezza. Grazie all'apporto di Alvise Biffi (Imprenditore, business angel, coordinatore Steering Committee Cyber Security di Assolombarda), affronteremo con la massima semplicità i principali rischi e le principali misure che possono essere messe in campo, non solo per elevare la sicurezza dei sistemi ma anche per mettersi al riparo da possibili profili di responsabilità. Partiamo con una disamina dei pregiudizi più comuni (e pericolosi) per affrontare rischi e soluzioni.

(*) Imprenditore, business angel, coordinatore Steering Committee Cyber Security di Assolombarda

Le imprese oggi affrontano i temi della Digital Transformation, della Manifattura 4.0 (o industry 4.0), dell'IoT (Internet of Things) ormai già evoluto nell'IoE (Internet of Everythings), connettendo non solo i propri sistemi informativi ma anche i propri prodotti e le stesse linee di produzione con "componenti intelligenti", di fatto ibridi di Hardware e Software, in ecosistemi applicativi web esposti al mondo. Finalmente anche il tema che per lungo tempo è rimasto fuori dal tavolo del Board e relegato alla scrivania dell'IT manager (rigorosamente fuori dal Board nella maggior parte delle imprese italiane) è approdato all'attenzione del Top Management: la Cybersecurity.

Eppure...

La sicurezza informatica (come la chiamavamo prima che fosse trendy chiamarla cybersecurity) non è però ancora un "Must to Have". Nella logica imprenditoriale italiana non è ancora integrata all'R&D di prodotto: prima va portato sul mercato con la maggior quantità di innovazione possibile e poi, quando raggiunge il successo, si inizia a pensare anche agli aspetti relativi alla security...anzi, ad essere sinceri, salvo rarissime eccezioni il tema diventa realmente rilevante al primo "security breach", quando piove la prima tegola.

Nonostante i rischi, la cybersecurity non è ancora un "Must to Have"

Perché accade questo?

False convinzioni

Le (false) convinzioni fortemente radicate nei più si possono riassumere in queste tre risposte - reali - di moltissimi imprenditori (ma anche manager) sul tema:

1. **mai avuto nessun problema;**
2. **non siamo un target interessante;**
3. **non abbiamo nulla di valore nelle nostre informazioni.**

"Mai avuto problemi"

Negli ultimi mesi la prima risposta, che per molti anni è stato l'alibi più diffuso, ha iniziato a vacillare vistosamente perché, anche tra le PMI, sfortunatamente, sono pochi a non essersi ancora scottati. Una impresa su 4 ha infatti dichiarato di aver subito un incidente informatico negli ultimi 12 mesi (rapporto Clusit 2021).

"Non ho nulla di valore"

Per chi si riconosce nella terza risposta concordo che non ha senso parlare di Cybersecurity, piuttosto si dovrebbe capire come rimanere sul mercato senza valore nel proprio knowhow...

Il resto del mondo

Per tutti gli altri descrivo di seguito le due principali cyberminacce per le aziende oggi, in modo da avere consapevolezza del rischio, volutamente lasciato sottotraccia da chi ne ha fatto un business di svariati miliardi, per prendere con contezza le proprie decisioni. Tanto per dare un numero: secondo una dichiarazione del MISE, il "danno stimato" da cybercrime per le imprese italiane nel 2020 sia di ben 7 miliardi di euro.

Man in the Middle (MITM)

Un attacco Man-in-the-Middle (MITM) è piuttosto semplice e non si limita al mondo online o agli home computer. Attraverso questi attacchi il criminale si inserisce tra due entità che stanno cercando di comunicare tra loro, *avvelena* la comunicazione e intercetta i messaggi inviati. Il criminale solitamente sfrutta punti di debolezza che gli permettono il controllo della mail e si finge alternativamente una delle parti per *avvelenare* i messaggi: si inserisce tra il target (la vittima) e la fonte (il server o il router) che la prima sta cercando di contattare. Se il criminale riesce, ad esempio, a violare il sistema di posta, allora né la vittima, né la fonte che il criminale sta impersonificando avranno modo di rendersene conto. Esempi di diverse aziende visti sui principali quotidiani possono essere riassunti cosi: il direttore finanziario della BigCorp riceve un messaggio del nuovo CEO, salito al vertice della

società da poco meno di un mese ma già nel board da tempo. L'oggetto della mail è un ordine tutto sommato di routine all'interno di realtà con flussi di cassa nell'ordine delle centinaia di milioni di dollari: il CEO chiede di effettuare un pagamento da 3 milioni di dollari per un nuovo fornitore cinese…. naturalmente il CEO non ha mai fatto la richiesta e sono stati rubati 3 milioni di dollari!

La digitalizzazione è una grande opportunità, ma va affrontata considerando anche le minacce

Ransomware

Il ransomware è un tipo di malware (virus-software evoluto e automatizzato con fini frodatori) che blocca l'accesso ai dati presenti nel proprio dispositivo (solitamente PC, ma può attaccare anche smartphone\tablet) sino a quando non si paga un riscatto che va a finire nelle tasche del criminale di turno.I modi più diffusi per "infettarsi" con un malware sono aprire email di phishing (ad esempio con mail di presunto aggiornamento del sistema operativo etc.), installando programmi infetti, visitando siti web infetti, ma più frequentemente semplicemente non aggiornando con le patch di sicurezza i programmi regolarmente installati sul PC. Naturalmente il malware si può diffondere in tutta la rete aziendale crittografando il contenuto delle cartelle condivise dove l'utente infettato ha l'accesso e tutto questo può portare alla totale paralisi dell'azienda. Il 30% degli incidenti informatici è riconducibile ad estorsione da malware.

Nella manifattura 4.0

Se chi ha un normale processo di backup può cavarsela con un semplice sforzo organizzativo di ripristino in caso di ransomware, più complicata è la exit strategy in caso di attacchi ransomware alla linea di produzione, che vede la stessa logica estortiva applicata al blocco dei macchinari/prodotti.

Scenario 1: la linea di produzione è bloccata dietro richiesta di riscatto

Scenario 2 (molto peggiore): le macchine/prodotti installate presso i clienti vengono bloccate dietro richiesta di riscatto

Conclusioni

La digitalizzazione è una grande opportunità ed è inevitabile per rimanere sul mercato, ma va affrontata a 360° considerando anche le minacce, perché dietro il Cybercrime non ci sono solo "hacker" e "ragazzini", ma anche grandi organizzazioni criminali internazionali. Il punto non è più se saremo attaccati o meno, ma quando. Morale: amici imprenditori, arrivate preparati!

Security Summit: record di partecipazione per la seconda edizione virtuale

SARAJEVO (BIH) – I rischi legati agli assembramenti hanno creato lo spazio per una nuova generazione di eventi anche nel comparto della sicurezza. Eventi come il **Security Summit 2021,** che dal 4 al 6 maggio scorso, ha raggiunto oltre 3000 professionisti, in quasi 100 paesi. Basandosi sul successo della **precedente esperienza**, la seconda edizione virtuale del Security Summit, di cui SecSolution è stato media partner, è riuscita ad aprire nuovi orizzonti: quasi 1.200 persone si sono registrate per la prima volta, per un totale di 3.282 partecipanti, che si sono riuniti sulla piattaforma b2match, tecnicamente potenziata rispetto all'anno scorso. Il fatto di avere accolto ospiti da 96 paesi proietta il Security Summit in una dimensione ancora più internazionale. Rispetto all'edizione in presenza 2019, che si è svolta in Macedonia del Nord, il numero di paesi di provenienza degli ospiti è letteralmente triplicato. Con l'evidenza dei dati, è possibile affermare che il Security Summit ha oltrepassato i confini della regione adriatica ed è diventato uno degli eventi più significativi dell'Europa centrale, sud-orientale e orientale. Complessivamente, l'edizione 2021 è stata supportata da 71 sponsor ed espositori. **Cathesis Europe, Huawei, MOBOTIX** sono apparsi come sponsor platino, mentre **Dahua Technology, Eagle Eye, Hikvision Digital Technology, Secura, Seagate Technology, SoftGuard Technologies, Špica, 360 Vision Technology, Vanderbilt e ComNet** hanno svolto il ruolo di golden sponsor.

Il programma 2021 si è articolato in 14 conferenze principali, la presentazione di 11 progetti di successo e 21 seminari aziendali. Tra gli speaker, ricordiamo **Leo Levit**, nuovo presidente di **ONVIF**, intervenuto in tema di **interoperabilità** tra sistemi e dispositivi di diversi produttori; **Jakub Kozak**, Sales Manager Eastern/Central Europe di **Genetec**, che ha offerto una panoramica sul comparto della sicurezza, citando i dati di una recente ricerca di mercato; **Radoslaw Kedzia**, Vice Presidente di **Huawei** per l'Europa centrale, orientale e il Nord Europa, con una conferenza sulla rivoluzione innescata dalla **tecnologia 5G**.

Adria Security Summit torna in presenza il 13-14 ottobre 2021 a Belgrado presso l'Hotel Holiday Inn.

https://vsecuritysummit.com

Nuova rubrica

Roberta Rapicavoli (*)

QUALI MISURE PER LA SICUREZZA DEI SISTEMI DI VIDEOSORVEGLIANZA?

Quando si decide di utilizzare un sistema di videosorveglianza che consente di rilevare e/o registrare immagini di persone fisiche (e dunque di trattare dati personali), occorre prestare attenzione al profilo della sicurezza fin dalla fase di pianificazione e, dunque, fin dalla fase di scelta del sistema, di sua progettazione, installazione e configurazione.

Le immagini di un sistema di videosorveglianza, infatti, al pari di qualsiasi dato personale, devono essere protette con specifiche misure di sicurezza, da individuare e adottare in modo da assicurare un'adeguata protezione dei dati in tutte le fasi di trattamento (dall'acquisizione delle immagini attraverso le telecamere, alla loro trasmissione ai mezzi di visualizzazione e/o dispositivi di registrazione fino alla loro elaborazione e cancellazione definitiva).

Quali misure di sicurezza adottare?

Secondo la vigente normativa, non esiste un elenco di misure di sicurezza obbligatorie, ma spetta al titolare e al responsabile del trattamento valutare concretamente quali misure - tecniche e organizzative – adottare, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

(*) Avvocato esperto in Information Technology e privacy e Docente Ethos Academy **www.ethosacademy.it**

Linee guida 3/2019

La maggior parte delle misure da impiegare, specialmente quando si utilizzano apparecchiature e software digitali, non sono diverse da quelle impiegate per altri sistemi informatici per cui, come indicato nelle Linee guida 3/2019 sulla videosorveglianza del Comitato europeo per la protezione dei dati, è utile considerare, nella definizione delle misure, gli standard internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi multimediali e la sicurezza dei sistemi informatici in generale. Secondo le indicazioni contenute nelle richiamate Linee guida, al fine di garantire la sicurezza del sistema e dei dati, dovrebbero essere attivate misure di protezione fisica dell'intera infrastruttura (comprese telecamere, cablaggio e alimentazione) contro manomissioni fisiche e furti, misure di protezione della trasmissione delle riprese con canali di comunicazione sicuri contro l'intercettazione e la cifratura dei dati, soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici, nonché misure che consentono di rilevare guasti di componenti, software e interconnessioni e di ripristinare la disponibilità e l'accesso ai dati in caso di problemi fisici o tecnici.

Individuare chi può accedere ai sistemi e ai dati rileva sia per i profili tecnici che per quelli di tipo organizzativo

Controllo degli accessi

Nelle Linee guida vengono poi indicate le misure di controllo (fisico e logico) degli accessi al sistema e ai dati, che includono la protezione contro l'accesso non autorizzato a tutti i locali in cui viene effettuato il trattamento (come la control room o la sala tecnica in cui è collocato il DVR), il corretto posizionamento dei monitor (in modo tale che solo gli operatori autorizzati possano visualizzarli), l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate, la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso, l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente (tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica), la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati).

Accesso ai dati

In ordine agli accessi al sistema e ai dati, può inoltre essere utile richiamare quanto indicato già nel provvedimento del Garante privacy in materia di videosorveglianza del 2010, in base al quale, in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini e, laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza. Si precisa poi che la definizione di coloro che possono accedere ai sistemi e ai dati rileva, evidentemente, non solo per i profili tecnici, ma anche per quelli – altrettanto importanti - di tipo organizzativo. Coloro che sono coinvolti nel trattamento, quali persone autorizzate o responsabili del trattamento, infatti, devono ricevere le specifiche istruzioni da osservare nello svolgimento delle attività e conoscere le procedure relative alla gestione del sistema di videosorveglianza (quali, ad esempio, le procedure per le richieste di accesso alle immagini e per le modalità di gestione di eventuali data breach), che rientrano tra le misure organizzative, la cui adozione, come detto, rileva al pari delle misure tecniche.

Ruolo degli installatori

L'individuazione delle misure adeguate a garantire la protezione dei dati spetta al cliente e a coloro di cui lo stesso si avvale per la scelta e implementazione delle misure o per lo svolgimento di attività che incidono sui profili legati alla sicurezza dei dati trattati. Tra tali soggetti rientrano sicuramente gli installatori di sistemi di videosorveglianza, sia nel caso in cui siano chiamati ad effettuare le sole operazioni di installazione, sia nel caso in cui siano coinvolti nella scelta del sistema da installare e/o nelle attività di verifica e aggiornamento delle misure di sicurezza.
Le diverse attività comportano, evidentemente, diversi compiti e responsabilità circa le misure di sicurezza, ma si tratta di tema rispetto al quale gli installatori rivestono comunque un ruolo di rilievo.

Scarica le Linee guida 3/2019 sulla videosorveglianza del Comitato europeo per la protezione dei dati

Nuova rubrica

Giovanni Villarosa (*)

PROTEGGERE UN SUPERMERCATO: L'INCOGNITA DEL "FRESCO"

"Nei numeri scorsi abbiamo visto come proteggere attività commerciali esposte, come quelle rappresentate dai tabaccai; in questo numero affronteremo il tema della sicurezza nei supermercati, un perimetro commerciale ancora più critico, vulnerabile ai furti, alle rapine, al taccheggio, al danneggiamento e agli atti vandalici dimostrativi.

Nel settore della distribuzione alimentare, le differenze inventariali rappresentano un valore negativo superiore al 2% del fatturato annuale, percentuale derivante dalla sommatoria data dalle frodi, i furti e il taccheggio; fenomeno quest'ultimo che rimane per il settore della GDO la principale causa degli ammanchi di magazzino. Per arginare tali criticità le organizzazioni di settore investono mediamente, in tecnologie di sicurezza, lo 0,6% del loro fatturato globale. La valutazione e la misura del rischio *(risk severity, risk frequency)* è estremamente importante quando parliamo di ambienti commerciali vulnerabili, ampi e difficilmente controllabili il più delle volte, considerando la notevole dimensione dei locali, spesso collocati in aree di sviluppo industriale extraurbane lontane dai centri abitati.

(*) Laureato in Scienze dell'Intelligence e della Sicurezza, esperto di Sicurezza Fisica per Infrastrutture, CSO e DPO, Vice Presidente di SECURTEC

Gli obblighi della EN 50131

E' bene ricordare allora come tali analisi rappresentano un vincolo normativo contenuto all'interno della EN 50131, un obbligo che tutti i professionisti (installatori, progettisti) del settore security condividono con la committenza. Uno studio che si baserà sulla raccolta di specifiche informazioni, utili nello stilare un elenco delle caratteristiche fisiche degli edifici, l'uso e il periodo temporale di funzionamento del sito, i potenziali conflitti degli spazi in uso, la tipologia dei reati commessi, tanto per citarne alcuni. Inoltre, in un secondo tempo, andrà redatto l'elenco dei sistemi/impianti da proteggere, indispensabili alla sopravvivenza della struttura commerciale stessa, come le cabine elettriche, i sistemi di alimentazione di *backup*, di spegnimento incendi, le reti informatiche di comunicazione, gli impianti del freddo. Successivamente, si passerà all'elencazione delle protezioni verso i sistemi di sicurezza passiva, come le casse (protezione del flusso di contante), i mezzi forti per la sicurezza del denaro, il controllo delle uscite di emergenza e di tutte le altre aperture secondarie verso il perimetro fisico esterno. Nell'analisi poi, andrà valutata la presenza di recinzioni, barriere, grate di sicurezza, cancelli, etc, verificando attentamente anche le sistemazioni degli arredi esterni a supporto dell'attività commerciale, che non incidano negativamente con il campo visivo della videosorveglianza.

Le camere termiche rilevano gli alimenti freschi/congelati occultati sotto gli indumenti dei ladri

L'importanza della luce

Altro aspetto molto importante sarà la valutazione delle caratteristiche illuminotecniche esterne, l'efficienza funzionale degli impianti con la compatibilità notturna delle ottiche dei sistemi video (CEI EN 62676), specialmente per le riprese a colori e ad alta definizione.
Rammentiamo sempre che un buon sistema di illuminamento riduce di molto la possibilità di attività criminali; infatti, secondo la normativa di settore, un coefficiente di 0,7 di difformità (tra zone chiaro/scure) ci permette di riconoscere facilmente un volto a una distanza di oltre 10 m, a tutto vantaggio dei sistemi di video controllo.

Il fresco

In ultimo, vorrei richiamare l'attenzione su un particolare argomento: il cibo fresco! Rappresenta oggi la maggior vulnerabilità nel settore e presenta il maggiore impatto sulle perdite inventariali; da esperimenti in campo è emerso che un investimento tecnologico, mediante l'uso di etichette antitaccheggio sui cd freschi, è decisamente alto, talvolta superiore al valore merceologico stesso, incidendo, peraltro, sulla qualità e sulla freschezza di determinati prodotti. In questo specifico caso la videosorveglianza può far poco, come detto i sistemi Rfid ancor meno, l'antintrusione neanche a parlarne! Ora, la mancata capacità di mettere in sicurezza talune merci, tracciandole opportunamente, pone una decisa attenzione su queste aree vendita all'interno dell'organizzazione, mettendo il professionista davanti ad un grosso interrogativo: come garantire la sicurezza di questi prodotti, data la complessità architettonica delle superfici espositive e le delicate proprietà organolettiche? E allora, quale soluzione proporre alla committenza? Ebbene, è senz'altro da valutare l'aiuto che arriva in questi casi dalla tecnologia "termica", giacché è notorio un fatto: i taccheggiatori indossano sempre abiti decisamente comodi, in modo tale da poter nascondere i prodotti in maniera trasparente! Ebbene, solo le camere termiche possono rilevare tutto ciò che è occultato sotto gli indumenti, poiché i sensori IR hanno la capacità di identificare, discriminandoli, gli alimenti freschi/congelati posti in contrasto termico con la superficie corporea del malvivente.

Sinergie con il RSPP

In ultimo, ricordiamoci che in questo specifico settore il professionista della security dovrà sempre rapportarsi con il responsabile della safety aziendale (RSPP), per potere pianificare le giuste soluzioni di sicurezza integrata, adeguate ai precisi obblighi dettati dal TU 81/08 sulla salute e la sicurezza sui luoghi di lavoro, che si intrecciano con il DM 37/08, decreto che norma la sicurezza degli impianti elettronici.

Secondo la ricerca "Retail security in Europe. Going beyond shrinkage", realizzata da Crime &Tech e Checkpoint Systems, in Europa si spende in sicurezza poco più del 2% del fatturato annuale del settore retail: oltre 49 miliardi di euro (somma tra le differenze inventariali pari a 1,45% e spese relative alla sicurezza pari allo 0,61%).

Marco Soffientini (*)

La proposta di Regolamento sull'AI della Commissione Europea

Ad Aprile 2021 la Commissione Europea ha rilasciato la proposta di Regolamento del Parlamento Europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale.

(*) Esperto di Privacy e Diritto delle Nuove Tecnologie e docente Ethos Academy

Il 2021 si conferma l'anno delle novità in tema di intelligenza artificiale in quanto, a distanza di pochi mesi dalle Linee Guida del Comitato per la protezione dei dati della Convenzione 108 in tema di riconoscimento facciale, la Commissione predispone un regolamento in tema di intelligenza artificiale (IA) destinato ad avere valore di legge in tutti gli Stati membri dell'Unione. Le ragioni che hanno spinto la Commissione a questa decisione sono chiarite nella relazione di accompagnamento, dove si legge che: *L'utilizzo dell'IA con le sue caratteristiche specifiche (ad esempio opacità, complessità, dipendenza dai dati, comportamento autonomo) può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("la Carta"). La presente proposta mira ad assicurare un livello elevato di protezione di tali diritti fondamentali e ad affrontare varie fonti di rischio attraverso un approccio basato sul rischio chiaramente definito.*

Perché un Regolamento

La scelta di un regolamento come atto giuridico, si legge nella relazione alla proposta di regolamento, è giustificata dalla *necessità di un'applicazione uniforme delle nuove regole, come la definizione di IA, il divieto di talune pratiche dannose consentite dall'IA e la classificazione di taluni sistemi di IA. L'applicabilità diretta di un regolamento, conformemente all'articolo 288 TFUE, ridurrà la frammentazione giuridica e faciliterà lo sviluppo di un mercato unico per sistemi di IA leciti, sicuri e affidabili. Tale obiettivo sarà conseguito in particolare introducendo una serie armonizzata di requisiti di base per quanto concerne i sistemi di IA classificati come ad alto rischio e di obblighi riguardanti fornitori e utenti di tali sistemi, migliorando la tutela dei diritti fondamentali e garantendo certezza del diritto tanto per gli operatori quanto per i consumatori.*

Approfondisci la proposta di Regolamento sull'AI della Commissione Europea

La base giuridica della proposta

La base giuridica della proposta è costituita dall'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno. Con questa proposta di regolamento vengono definiti dei requisiti obbligatori comuni applicabili alla progettazione e allo sviluppo di alcuni sistemi di IA prima della loro immissione sul mercato, che saranno resi ulteriormente operativi attraverso norme tecniche armonizzate.

Il contenuto della proposta

La proposta di Regolamento definisce regole armonizzate per lo sviluppo, l'immissione sul mercato e l'utilizzo di sistemi di IA nell'Unione seguendo un approccio proporzionato basato sul rischio, differenziando tra gli usi dell'IA che creano:

1) un rischio inaccettabile;

2) un rischio alto;

3) un rischio basso o minimo.

Rischio inaccettabile

Nella prima categoria, contenuta nel titolo II, rientrano tutti i sistemi di IA il cui uso è considerato inaccettabile in quanto contrario ai valori dell'Unione, ad esempio perché viola i diritti fondamentali. Tra gli usi vietati (rischio inaccettabile) rientrano:

a) le pratiche che presentano un elevato potenziale in termini di manipolazione delle persone attraverso tecniche subliminali, senza che tali persone ne siano consapevoli;

b) l'uso di sistemi di IA che sfruttano le vulnerabilità di specifiche categorie di interessati, quali i minori o le persone con disabilità, al fine di distorcerne materialmente il comportamento in maniera tale da provocare, a loro o ad un'altra persona, un danno psicologico o fisico;

c) l'uso di sistemi di attribuzione di punteggi sociali (c.d. di social scoring come ad esempio quelli utilizzati in Cina) da parte delle autorità pubbliche;

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" (come i sistemi di riconoscimento facciale) in spazi accessibili al pubblico a fini di attività di contrasto, fatta salva l'applicazione di talune limitate eccezioni.

Rischio alto

Nella categoria "ad alto rischio", relativa ad utilizzi dell'IA che pongono rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone, rientrano:

a) L'uso di sistemi di IA utilizzati come componenti di sicurezza di prodotti sottoposti a controlli di conformità come ad esempio i componenti di presidi medici o dei giocattoli.

b) L'uso di specifici sistemi IA elencati in un allegato del regolamento, come ad esempio i sistemi finalizzati a valutare la solvibilità delle persone.

Rischio basso o minimo

Nella categoria "a basso rischio o minimo" rientrano infine tutti quei sistemi sottoposti ad obblighi minimi di trasparenza, come ad esempio i sistemi di IA che manipolano contenuti (c.d. deep fake) o i software che consentono di parlare con le persone (c.d. chatbot).

Come verranno applicate le regole

Si legge nella relazione di accompagnamento che: *Le regole proposte saranno applicate tramite un sistema di governance a livello di Stati membri, sulla base di strutture già esistenti, e un meccanismo di cooperazione a livello dell'Unione con l'istituzione di un comitato europeo per l'intelligenza artificiale. Vengono inoltre proposte misure aggiuntive per sostenere l'innovazione, in particolare attraverso spazi di sperimentazione normativa per l'IA, e altre misure per ridurre gli oneri normativi e sostenere le piccole e medie imprese ("PMI") e le start-up.*

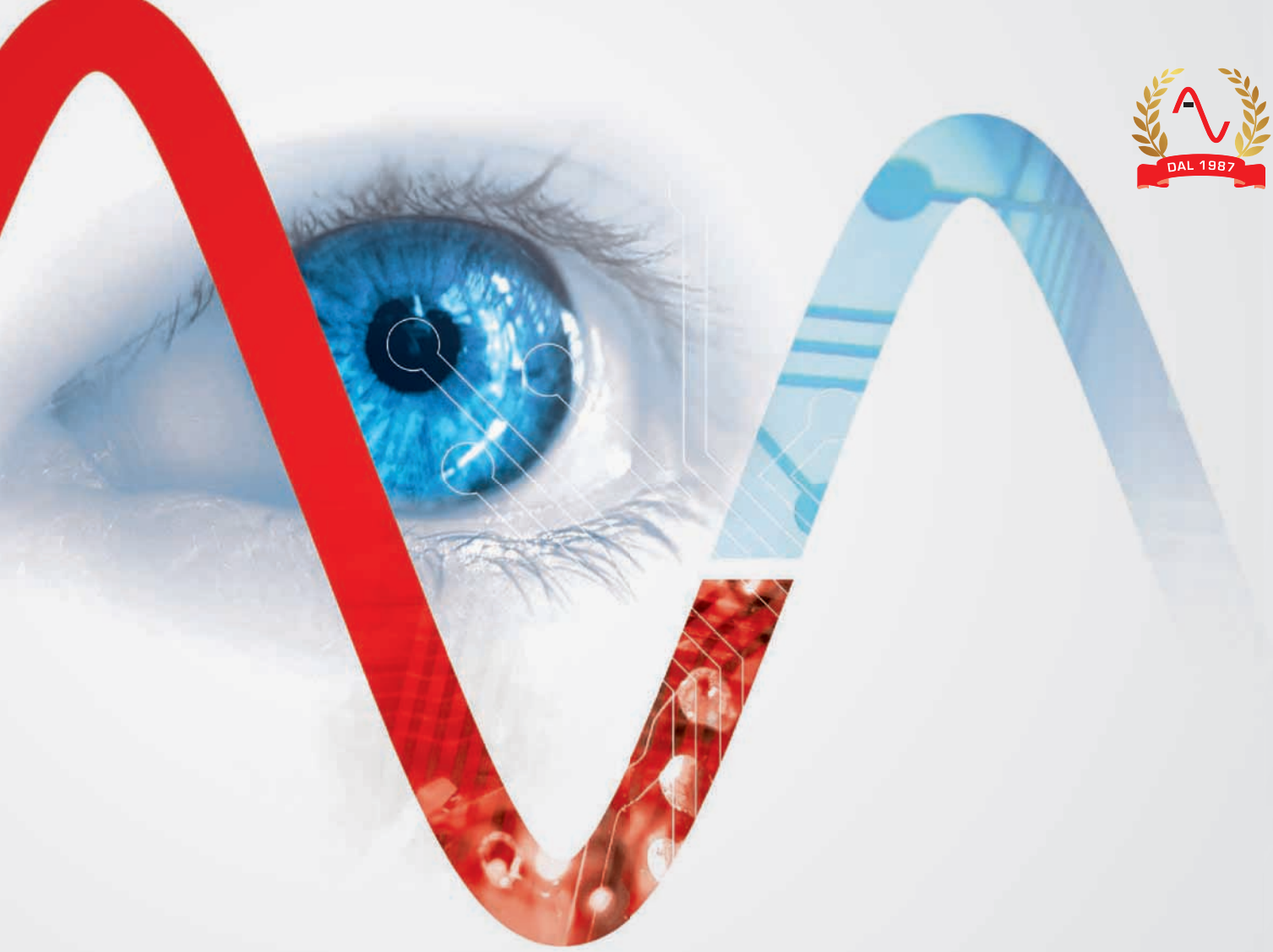
Le sanzioni

L'articolo 71 della proposta di Regolamento prevede tre diversi scaglioni di sanzioni:

1) [Art. 71 par. 3] Le seguenti violazioni sono soggette a sanzioni amministrative pecuniarie fino a 30 000 000 di EUR o, se l'autore del reato è una società, fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
   a) inosservanza del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5 (Pratiche di intelligenza artificiale vietate);
   b) non conformità del sistema di IA ai requisiti di cui all'articolo 10 (Governance dei dati).

2) [Art. 71 par. 4] La non conformità del sistema di IA ai requisiti o agli obblighi previsti dal presente regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 di euro, se l'autore del reato è una società, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

3) [Art. 71 par. 5]La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro, se l'autore del reato è una società, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.



DAL 1987

PROFESSIONISTI DELLA SICUREZZA

La sicurezza è un bene prezioso per la vita e il lavoro delle persone e delle aziende, da salvaguardare e garantire in ogni ambito: residenziale, commerciale, industriale e bancario.
Dai piccoli centri urbani alle grandi città su tutto il territorio italiano, Alessio Elettrosicurezza progetta, sviluppa e fornisce assistenza su sistemi d'alta tecnologia all'insegna della massima sicurezza.

Scopri di più.
www.alessioelettrosicurezza.it

Alessio Elettrosicurezza s.r.l.
www.alessioelettrosicurezza.it

Via Dell'Economia 3 | 31033
Castelfranco Veneto (TV)

Tel. 0423 493602

in

ALESSIO ELETTROSICUREZZA
SICUREZZA E CONTROLLI

La Redazione

Controllo accessi e rilevazione presenze: convivenza (*quasi*) perfetta

Controllo accessi e gestione presenze, oltre a vivere sotto lo stesso tetto, hanno molte cose in comune. A iniziare dagli utenti da controllare e dalla tecnica con la quale riconoscerli (badge, transponder ecc.). Il primo ha come missione la sicurezza fisica, il secondo quella di dare un aiuto concreto nella gestione delle risorse umane. Oggi i due sistemi operano per lo più ognuno per conto proprio, a volte condividono la base dei dati, raramente sono integrati in un'unica soluzione. Come per l'antintrusione e l'antincendio, la via dell'integrazione è irta d'ostacoli ma almeno in questo caso la coppia parla (quasi) la stessa lingua.

La gestione informatizzata delle presenze al lavoro rappresenta uno dei tasselli essenziali nel management delle risorse umane. Si tratta, in particolare, di una delle applicazioni di software gestionale più complesse e sofisticate in assoluto per via delle numerose regole legate alla disciplina del lavoro e soprattutto per la varietà dei regolamenti aziendali in gioco. Un sistema elettronico di gestione presenze consente, in sintesi, di acquisire gli orari di entrata e uscita dei lavoratori (timbrature), rendere disponibile (in tempo reale o in differita) la lista dei presenti e assenti (e ritardatari), "quadrare" le ore lavorate, mettere in evidenza le "anomalie" rispetto a quanto atteso, gestire le assenze e le eccedenze (ferie, permessi, malattie, straordinari ecc.). E ancora: calcolare le ore totali secondo determinate regole e suddividerle per classi di retribuzione, trasferire i dati mensili alla procedura paghe per l'elaborazione dei salari e degli stipendi, offrire un'ampia scelta di report storici e statistici.

L'evoluzione dei sistemi

- Un sistema soltanto, accessi o presenze
- Due sistemi indipendenti, accessi e presenze, che condividono (o meno) la stessa tecnica ID (badge, transponder ecc.)
- Sistema di gestione presenze con integrate funzioni (basilari) di controllo accessi
- Sistema di controllo accessi con integrata funzione di raccolta timbrature
- Due sistemi che, oltre alla tecnica ID, condividono risorse comuni (database, profili orari ecc.), si condizionano a vicenda e concorrono alla formazione della lista eventi
- Sistema integrato per la gestione delle risorse umane, comprendente oltre alle presenze e agli accessi, altre prestazioni: curricula, formazione, DPI, automezzi aziendali, sorveglianza sanitaria ecc.

Il sistema elettronico di controllo accessi e quello adibito alla gestione delle presenze al lavoro, nella maggior parte delle fabbriche e aziende di servizi, operano in modo indipendente uno dall'altro. Eppure non sarebbero poche le risorse che potrebbero condividere.

I punti di contatto

Un sistema elettronico di controllo accessi, oltre a convivere sotto lo stesso tetto, ha molte cose in comune con la gestione delle presenze. A iniziare dagli utenti coinvolti. I controlli da effettuare in automatico, infatti, se si escludono gli ospiti e i visitatori, riguardano gli stessi lavoratori: da un lato ai fini della sicurezza fisica, dall'altro sotto il profilo contabile e gestionale. Così come è quasi sempre in comune ai due impianti la credenziale di riconoscimento (badge, transponder ecc.): negli accessi per permettere di eseguire, una volta riconosciuto l'utente, le verifiche logiche, spaziali e temporali prima di autorizzare o negare il transito (chi, dove, quando); nelle presenze per acquisire l'orario di inizio e fine lavoro con l'eventuale causale di timbratura (permesso, missione ecc.). A volte anche l'hardware specializzato è condiviso da entrambi i sistemi: un'unità di controllo accessi installata su un tornello, ad esempio, può registrare le timbrature così come un terminale di rilevazione presenze può nel contempo aprire la porta.

I principali punti di contatto

- La tecnica d'identificazione (badge, transponder ecc.)
- L'hardware specializzato (in grado sia di controllare gli accessi che registrare gli orari di entrata/uscita)
- Il database anagrafico (gli utenti sottoposti al controllo degli accessi sono in larga parte gli stessi soggetti alla rilevazione delle presenze)
- Gli orari di lavoro e altri profili (specie nelle turnazioni può essere utile controllare gli accessi in base all'orario di lavoro praticato dai lavoratori)
- La creazione in comune della lista dei presenti/assenti in tempo reale ai fini della sicurezza
- Il condizionamento in situazioni particolari (come quello di subordinare la timbratura a una o più verifiche svolte dal controllo accessi e viceversa)

Gemelli diversi

Il fatto che i due sistemi abbiano molti aspetti in comune (database anagrafico, credenziale di accesso ecc.) potrebbe indurre a ritenere che la soluzione integrata sia quella ottimale ovvero che sarebbe meglio disporre di un unico sistema capace di assolvere entrambi i compiti. Non è così. Intanto vi sono enti e imprese che non gestiscono le presenze al lavoro (o lo fanno in modo manuale tradizionale) mentre, al contrario, hanno stringenti esigenze di sicurezza nel controllo degli accessi. Così come vi sono aziende in cui la gestione delle presenze è prioritaria e non sanno cosa farsene del controllo accessi. In altri contesti, infine – per ragioni storiche, divisione di compiti ecc. – i due sistemi devono essere indipendenti, di pari importanza o con uno dei due che prevale di gran lunga sull'altro.

La parte del leone

Se di integrazione si deve parlare, allora è il sistema di gestione presenze che deve fare la parte del leone, ossia incorporare gli accessi. Per un verso questa soluzione ha il vantaggio di avere un unico database condiviso e di regolare gli ingressi in accordo con i profili orari dei lavoratori (specie nelle imprese con turnazioni), per l'altro verso limita di molto le potenzialità offerte da un controllo accessi indipendente ed evoluto in quanto gran parte di queste funzioni appaiono quasi marziane agli occhi di chi si occupa di salari e stipendi tutto il giorno. Sul fronte opposto, un sistema elettronico di controllo accessi ha ben poco da offrire alla gestione delle presenze, se non raccogliere le timbrature su determinati varchi e trasferirle altrove. Una soluzione intermedia, con i pro e i contro (che non mancano mai), è l'adozione di due sistemi separati che condividano, oltre alla tecnica d'identificazione, un unico database anagrafico (generalmente quello delle presenze), si condizionino a vicenda ove è necessario, concorrano alla formazione della lista dei presenti in tempo reale.

Il sistema che verrà

La soluzione ottimale è di là da venire. Qualche tentativo, in verità, c'è già ma è molto carente sul fronte degli accessi. La tecnologia informatica sta lentamente evolvendo, anche in ambito PMI, verso l'offerta di soluzioni capaci di gestire le risorse umane a 360 gradi considerando, oltre alle presenze, anche curricula, piani formativi, DPI e altre dotazioni, gli automezzi aziendali, la sorveglianza sanitaria ecc. Nell'integrare gli accessi è necessario tener conto delle molteplici funzionalità offerte dagli attuali sistemi più evoluti, e non limitarsi, come avviene oggi, al classico clic da dare alla serratura per aprire la porta.

L'integrazione tra controllo accessi e rilevazione presenze, oggi inesistente o realizzata in forma embrionale, è destinata a compiere un notevole balzo in avanti con l'avvento sul mercato dei sistemi informatici per la gestione delle risorse umane a 360 gradi.

ECONOMIA

Cancella il Debito: come liberarsi dalla morsa dei debiti

Le rate vi schiacciano? Non riuscite più a seguire i mutui e i finanziamenti che avete in corso? Non vi preoccupate: il modo per uscirne e riappropriarsi della propria vita c'è.
Ve lo spiegano **Carmina Gallucci ed Elisabetta Ribatti**, che già da tempo hanno fondato **un'Associazione che si chiama CID, "Cancella il Debito"**.

ECONOMIA

Locazioni commerciali al tempo del Covid

Per il nostro tessuto economico, l'attuale stato di emergenza sanitaria è purtroppo destinato a protrarsi ancora e rappresenta un evento tanto singolare quanto traumatico. In questo scenario, una spina nel fianco delle imprese decisamente gravosa è rappresentata dalle locazioni commerciali. Ecco come trovare le possibili soluzioni correttive.

RICERCHE DI SETTORE

Italian Security Leaders, TOP 25: Il mercato italiano della sicurezza sotto la lente

L'indagine Italian Security Leaders, Top 25, **condotta dall'analista Plimsoll in collaborazione con Ethos Media Group** su 362 società operanti sul territorio nazionale, tratteggia un **comparto della sicurezza** che è cresciuto dell'8%, raggiungendo i 2,03 miliardi di euro.

NORMATIVA

Statuto dei Lavoratori e Videosorveglianza
L'installazione di telecamere nella disciplina dello Statuto dei Lavoratori

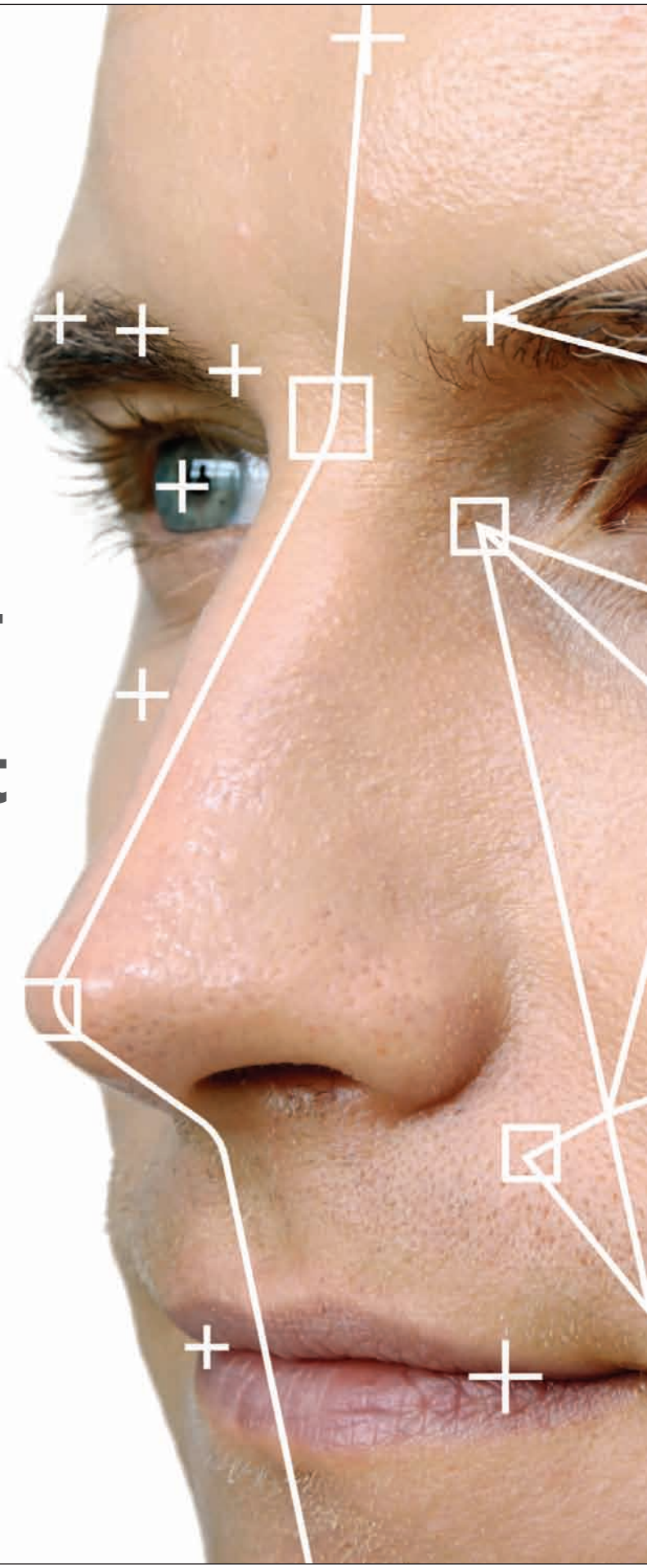
La miniguida rappresenta uno strumento operativo in mano a titolari del trattamento e consulenti, data protection officer e installatori, sulle modalità di presentazione all'Ispettorato del Lavoro delle istanze ai sensi dell'articolo 4 L. n. 300/1970 alla luce della Circolare I.N.L. n.5/2018.

media.secsolution
security & safety media store

e-mail: media@ethosmedia.it www.media.secsolution.com

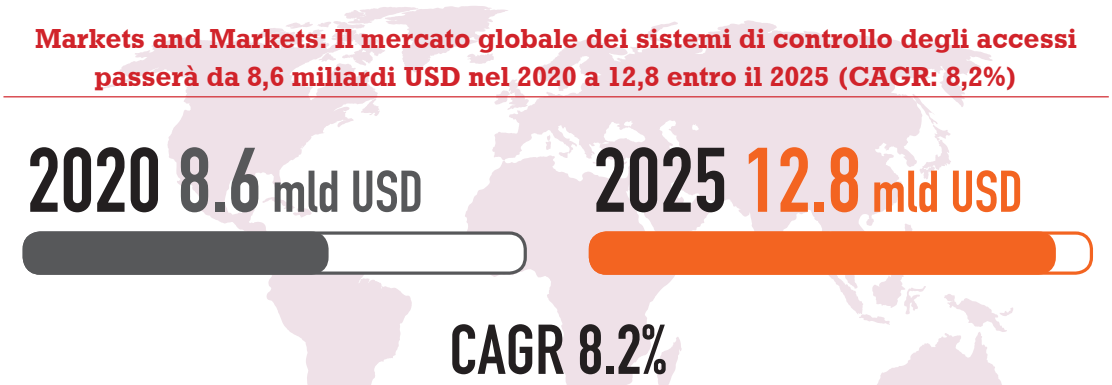
Annalisa Coviello

Controllo accessi: integrazioni ed evoluzioni in uno scenario post pandemico



Fino a poco tempo fa, il controllo accessi, nella percezione comune, era una prerogativa delle banche, di alcuni uffici "sensibili", magari anche delle ville dei vip più famosi. La pandemia invece ci ha abituato a essere sempre "controllati", anche quando entriamo in un negozio, in un supermercato, in uno studio medico, dove, come minimo, ci viene misurata la temperatura, che è comunque un mezzo per evitare o permettere l'accesso alle persone. Ora, che ci stiamo tutti preparando a un graduale ritorno alla normalità, i sistemi di controllo accessi giocano un ruolo preponderante nel mantenere un ambiente, che sia di lavoro o di svago, il più sicuro possibile e proprio il post-pandemia aprirà nuovi scenari e opportunità per tecnologie e modi di vita che, volenti o nolenti, ormai si sono consolidati dappertutto.

Markets and Markets: Il mercato globale dei sistemi di controllo degli accessi passerà da 8,6 miliardi USD nel 2020 a 12,8 entro il 2025 (CAGR: 8,2%)



Fonte: Access Control Market with COVID-19 Impact by Offering (Card-based Readers, Biometric Readers, Electronic Locks, Controllers, Software, Services), ACaaS (Hosted, Managed, Hybrid), Vertical, and Region - Global Forecast to 2025

È per questo motivo che il mercato del controllo accessi non ha mai conosciuto, nemmeno nei periodi più "bui", un trend al ribasso, anzi, tutt'altro. Una ricerca di Markets and Markets prevede che le dimensioni del mercato globale dei sistemi di controllo degli accessi cresceranno da 8,6 miliardi di dollari nel 2020 a 12,8 miliardi di dollari entro il 2025, con un CAGR dell'8,2%.

Ma quali saranno le soluzioni più rispondenti a quelle esigenze che, ormai, sono diventate davvero di tutti? In epoca di "smart building", un ruolo fondamentale lo giocano le tecnologie di intelligenza artificiale e di apprendimento automatico, che consentiranno non solo di regolare il flusso delle persone all'interno di un edificio, ma anche di attuare quelle strategie di "distanziamento sociale" che sono strettamente legate al contenimento del Covid-19, così come di tutte le altre malattie trasmissibili che dovessero presentarsi, auspichiamo di no, in futuro.

Un VMS (visitor management system) adeguato è la base di un percorso efficace di controllo accessi

Sistema gestionale

Alla base di tutto, dicono gli esperti, ci deve essere un sistema gestionale adeguato. E' stato chiamato VMS, acronimo di "visitor management system", e consente a qualsiasi tipo di azienda di garantire la sicurezza di dipendenti e visitatori, eseguendo su chi entra un processo di screening che controlla, ad esempio, la temperatura, la presenza della mascherina, ma anche il trovarsi, fisicamente, in un determinato luogo, proibendo l'accesso allo stesso se i numeri non sono adeguati, per evitare assembramenti e mantenere così il distanziamento. Inoltre, ormai molte aziende richiedono la preregistrazione dei visitatori, in modo da poter autorizzare chi sarà, in un determinato orario, in un determinato luogo. Anche il mondo del lavoro, come ben sappiamo, è stato stravolto dalla pandemia e si sono create delle situazioni diverse rispetto a prima, con orari flessibili, dipendenti in ufficio e altri in smartworking. Se non c'è una "cabina di regia", rappresentata appunto da VMS, dietro a tutto questo, è difficile non solo distanziare, ma anche, al di là del problema sanitario, tenere traccia delle presenze, dei turni e via dicendo.

HVAC e risparmio

Inoltre, con il fatto che numerosi dipendenti lavorano ormai in smartworking, solo le analisi degli spazi rese possibili dai sistemi gestionali consentono di valutare, in tempo reale, quali parti di un edificio sono realmente occupate oppure no, in modo da attuare le opportune strategie di risparmio in termini di luce, HVAC e quant'altro. E, proprio a proposito di questi ultimi sistemi, il controllo sulle reali presenze e il livello di occupancy di un edificio consentono di attuare le necessarie misure anche per ciò che riguarda l'ormai indispensabile, sempre a fini sanitari, filtrazione dell'aria. Il sistema di controllo dell'accesso fisico dovrà quindi integrarsi sempre di più non solo con i sistemi di sicurezza tradizionali come videosorveglianza e intrusione, ma con il BMS e, appunto, il VMS.

Il controllo accessi si integra con videosorveglianza e intrusione, ma anche con BMS e VMS

Evoluzione post pandemica

Vediamo ora come, sul campo, stanno evolvendo le tecnologie di controllo accessi. La pandemia ha rapidamente accelerato, in primo luogo, i sistemi con credenziali mobili. Ormai, queste stanno sostituendo un po' dappertutto le credenziali fisiche tradizionali. E' intuitivo che proprio la diffusione del virus ha provocato questo timore nel toccare le cose, siano esse porte, maniglie o tastierini, e favorito i lettori abilitati NFC o Bluetooth. In questo modo, per entrare è sufficiente toccare il proprio smartphone…Fra l'altro, tramite le tecnologie di autenticazione a più fattori (ad esempio, PIN e altre combinazioni) è possibile raggiungere dei livelli di sicurezza che fino a non molto tempo fa erano impensabili.

La nuova biometria

Nuove frontiere, e un mercato di sicuro promettente, si sono aperte per tutto ciò che riguarda il settore della biometria: i lettori integrati con le telecamere termiche per il rilevamento delle temperature e della presenza dei dispositivi di protezione individuale, che, per giunta, sono di default contactless, appartengono ormai al nostro quotidiano e, se riescono a "parlare" con il sistema di gestione, possono bloccare l'accesso a una persona che non soddisfa i requisiti di sicurezza anche senza necessità dell'intervento umano. Le soluzioni che invece prevedono i codici QR sono particolarmente utili negli edifici che hanno numerosi visitatori su base regolare e devono gestire l'accesso ad aree con diversi livelli di restrizioni. Gli strumenti di contact tracing che sono conformi alle linee guida sanitarie e la sistemazione dello spazio di lavoro o dei negozi o supermercati che mantengono il social distancing garantiscono che chiunque sia sicuro e protetto - il che, virus o meno, non è poco.

Privacy Officer e Consulente della Privacy nel settore Videosorveglianza

CORSO SPECIALISTICO • IIª edizione

4 sessioni pomeridiane

14 • 21 • 28 ottobre 2021
4 novembre 2021

Per informazioni e registrazioni

http://bit.ly/2MlQ6bg

Formazione a distanza • Webinar

L'attestato rilasciato sarà valido ai fini dell'aggiornamento formativo richiesto dallo schema TÜV Italia per "Privacy Officer e Consulente della Privacy" per n. 16 crediti.

L'attestato rilasciato sarà valido ai fini dell'aggiornamento formativo richiesto dallo schema per gli Esperti di impianti di Allarme Intrusione e Rapina n. 16 crediti

CORSO RICONOSCIUTO

TÜV SÜD Examination Institute

Media Partner

secsolution magazine
www.secsolutionmagazine.it

secsolution security online magazine
www.secsolution.com

Consulenza scientifica e patrocinio:

FEDERPRIVACY

Ethos Academy srl - Via Venini, 37 - 20127 Milano (Italy) - Tel. +39 051 0475136 - Fax +39 039 3305841
academy@ethosacademy.it - www.ethosacademy.it

Dal prezzo al costo totale di proprietà: acquistare videosorveglianza oggi

Wanda Nijholt (*)

Scegliere il sistema di videosorveglianza più economico non è particolarmente strategico. Sono infatti molteplici i fattori da considerare: qualità costruttiva e affidabilità dei dispositivi, facilità di installazione e manutenzione, serio approccio alla sicurezza informatica, flessibilità a prova di futuro. Solo se tutti questi elementi strategici saranno pienamente soddisfatti, l'acquisto di una soluzione di videosorveglianza potrà aggiungere reale valore al business dell'utente finale.

(*) European Manager Marketing, Security Solutions di Panasonic Business Europe
https://business.panasonic.it/

Nella scelta delle telecamere i primi criteri da valutare sono l'affidabilità e il tasso MTBF (Mean Time Between Failure), che sono elementi di particolare interesse per le telecamere da esterni (spesso installate in luoghi critici e remoti, che quindi richiedono uno sforzo di organizzazione e coordinamento delle risorse e attente previsioni sulle tempistiche di installazione e manutenzione). Ma invero qualunque telecamera può essere bersaglio di vandalismo, oltre che soggetta ai fattori climatici ed ambientali. Design robusto e resistenza alle intemperie e alla polvere sono quindi fattori strategici da valutare, per garantire sicurezza in tutti i contesti[1].

E l'installazione?

In tutte le fasi successive alla produzione, il fattore tempo è cruciale per assicurare il migliore TCO. Le fasi di disimballaggio, configurazione e posizionamento dei dispositivi possono infatti richiedere tempi anche molto lunghi, e il tempo – si sa – è denaro. I produttori più accorti prevedono quindi un packaging che rende il processo di configurazione semplice ed efficiente, con un'apertura a finestra che permette di collegare semplicemente un cavo per configurare le telecamere senza doverle disimballare prima che vengano spedite al punto di installazione. Esistono poi soluzioni per configurare più telecamere IP contemporaneamente (evitando al contempo possibili errori di configurazione manuale)[2].

[1] Panasonic esegue test d'impatto sui modelli antivandalo per assicurarsi che gli urti esterni siano assorbiti fino a standard superiori a IK10. Specifici test garantiscono la resistenza a condizioni climatiche estreme e alle vibrazioni (in modo che la messa a fuoco sia sempre mantenuta). Ispezioni ai raggi X individuano eventuali difetti hardware in fabbrica e ulteriori test garantiscono la perfetta tenuta dell'imballaggio.

[2] L'imballaggio Easy Kitting (con un'apertura a finestra che permette di configurare le telecamere senza disimballarle) e lo strumento i-PRO di Panasonic (che facilita la configurazione delle telecamere di rete, dei disk recorder e degli encoder, consentendo l'accessibilità in batch dei dispositivi al momento della configurazione iniziale o dell'aggiornamento firmware), fanno risparmiare preziose ore lavoro.

E la manutenzione?

I costi di manutenzione possono superare di gran lunga il prezzo di acquisto iniziale: ecco perché occorre scegliere un hardware che minimizzi le necessità di interventi nel tempo. Anche solo mantenere l'obiettivo della telecamera pulito e libero da sporcizia e polvere può essere un vero time-killer. Esistono specifiche funzionalità per ridurre al minimo questi inconvenienti[3]. Un rivestimento idrofilo offre alle telecamere una migliore visibilità anche sotto la pioggia, o di notte (se abbinato alla visione a infrarossi), e previene l'accumulo di sporcizia. Risultato: meno manutenzione e un forte risparmio sui costi, senza compromessi nella qualità delle immagini. Un'altra causa di guasti può essere la condensa dell'atmosfera che si accumula all'interno della telecamera e oscura le lenti. In genere si usano cristalli di umidità o pacchetti di gel per assorbire le gocce d'acqua, ma anche questi si saturano col tempo. Per superare il problema sono stati progettati appositi deumidificatori[4].

E la cyber security?

Il pericolo di attacchi informatici e la protezione dei dati personali secondo il dettame del GDPR sono altri elementi cruciali. Un sistema all'avanguardia deve quindi assicurare che la minaccia di attacchi e perdite di dati sia davvero ridotta al minimo. Rimuovere tutte le password di default dai prodotti di sicurezza è un primo accorgimento (affatto scontato, visto che le password più utilizzate a livello globale continuano ad essere 12345 o admin)[5].

Fattori da considerare per aggiungere vero valore al sistema di monitoraggio:

E il futuro?

Poter personalizzare le telecamere rispetto alle diverse esigenze che possono insorgere nel tempo è un altro fattore chiave: il COVID-19 ci ha fatto toccare con mano il valore aggiunto dei sistemi di sicurezza in grado di risolvere le nuove problematiche pandemiche senza impattare eccessivamente sui costi. L'intelligenza artificiale è un altro elemento chiave, che sposta il focus da un uso della videosorveglianza di tipo reattivo (che utilizza le immagini come prova al verificarsi di criticità), ad un approccio all'AI e alle telecamere di tipo proattivo, volto alla prevenzione (ad esempio attraverso il monitoraggio di eventuali violazioni del rispetto di linee guida aziendali per la salute e la sicurezza dei lavoratori, piuttosto che la segnalazione di modelli di comportamenti sospetti prima che gli incidenti si verifichino)[6]. Le opportunità di applicazione di questo approccio alla tecnologia sono potenzialmente infinite: dai trasporti alla sorveglianza della città, passando per la logistica, l'agricoltura, la sanità, il manufacturing, il retail, con impatto anche sul consumo di risorse energetiche.

[3] Panasonic applica sulla cupola esterna delle telecamere un rivestimento idrofilo con effetto auto-purificante che crea uno strato protettivo invisibile contro polvere e sporcizia.

[4] Panasonic li monta direttamente in fabbrica su tutte le telecamere per esterni. Il dispositivo mantiene il livello di umidità all'interno al minimo e previene la condensa sul coperchio e sull'obiettivo senza riscaldatori o ventilatori.

[5] Il firmware delle telecamere e dei recorder i-PRO è criptato in modo sicuro. Secure Communications è una piattaforma che protegge contro ogni manomissione video, alterazione, spoofing e snooping.

[6] La nuova serie X i-PRO integra capacità AI ed esegue tre diverse applicazioni allo stesso tempo.

Antonio Strazzullo (*)

Piano Transizione 4.0: stop agli F24 e recupero degli investimenti

19 Miliardi nel Recovery Fund sono pronti per essere utilizzati dalle imprese italiane, oltre al Piano Nazionale Transizione 4.0 che prevede 24 miliardi di euro in 2 anni, con l'obiettivo di stimolare gli investimenti privati e di dare certezze alle imprese con misure strutturali che avranno effetto fino a giugno 2023. Il Piano offre una boccata d'ossigeno a quanti in questo momento lamentano problemi di liquidità, dovuti alla congiuntura economica. Facendo richiesta dei crediti d'imposta l'imprenditore potrà recuperare gli investimenti fatti dal 2016, in alcuni casi fino al 95% dell'importo speso.

(*) Commercialista e fondatore di ZeroF24, network di oltre 217 professionisti esperti in agevolazioni per le imprese e crediti fiscali **www.zerof24.it**

I crediti d'imposta possono salvare le aziende che da oltre un anno non fatturano e, nonostante questo, devono pagare gli F24

Per tutti i crediti d'imposta sui beni strumentali materiali la fruizione è ridotta da 5 a 3 anni, inoltre è ammessa la compensazione immediata (dall'anno in corso) e, infine, per gli investimenti in beni strumentali "ex super" e in beni immateriali (non 4.0) effettuati nel 2021, il credito d'imposta è fruibile in un anno, se i ricavi o i compensi dell'azienda sono inferiori a 5 milioni di euro.

secsolutionforum
The digital event for the security industry

"Le 7 risposte sul Piano Transizione 4.0 che ti faranno recuperare liquidità": intervento integrale di Antonio Strazzullo a secsolutionforum 2021

Per scaricare il video integrale

Crediti d'imposta Industria 4.0

Le piccole, medie e grandi imprese italiane possono beneficiare di questi 43 miliardi di euro sotto forma di Crediti d'imposta Industria 4.0, Ricerca & Sviluppo, Innovazione, Design e Green, di Credito Formazione 4.0. Rispetto ad analoghe misure precedenti, questo provvedimento in vigore dal novembre 2020, oltre a ridurre i tempi, vede maggiorati sia i tetti sia le aliquote degli investimenti che ogni azienda può trasformare in liquidità immediata. Inoltre possono richiedere il Bonus Pubblicità dedicato alle aziende che investono in attività di comunicazione pubblicitaria; ed il Crediti d'imposta Mezzogiorno che permettono agli imprenditori del sud di recuperare fino al 45% degli investimenti in impianti, macchinari e attrezzature. Per i crediti d'imposta è la grandezza dell'azienda a determinare l'ammontare del recupero.

Alessandro Mario Malnati (*)

Che succede dal 1 Luglio 2021? Il punto sui licenziamenti

Il c.d. Decreto Sostegni bis (D.L. 73/2021, Gazzetta ufficiale 123 del 25 maggio 2021) non rinnova ulteriormente il blocco dei licenziamenti sino ad ora previsto per l'emergenza epidemiologica da Covid 19, stabilendo, peraltro, un regime articolato e differenziato in base al quale le aziende potranno tornare alla disciplina ordinaria dei licenziamenti secondo scadenze differenziate. Ferma restando la generale disciplina dei licenziamenti per giustificato motivo soggettivo (in sostanza i licenziamenti che sono motivati da responsabilità del dipendente per sua condotta illecita), sempre rimasta in vigore anche durante il "blocco emergenziale", per quanto riguarda invece i licenziamenti individuali o collettivi per giustificato motivo oggettivo (attinente all'attività dell'impresa) le aziende potranno nuovamente licenziare i lavoratori a far data dal 01 luglio 2021 in quanto il divieto di licenziamento per motivi economici e/o organizzativi rimane fermo solo sino al 30 giugno.

(*) Contitolare Studio Legale GMV di Varese
http://gmvstudiolegale.it/index.html

Tuttavia il divieto di licenziamento continua ad applicarsi, fino alla data del 31 ottobre 2021, per i datori di lavoro che sospendono o riducono l'attività lavorativa per via del Covid chiedendo contemporaneamente l'ammissione agli istituti di sostegno al reddito quali l'assegno ordinario Fis (Fondo d'integrazione salariale), la cassa integrazione in deroga o la cassa integrazione per operai agricoli: in sostanza, a fronte della concessione a strumenti di sostegno al reddito dei lavoratori, lo Stato richiede che in cambio le aziende ammesse garantiscano la stabilità dei posti di lavoro per un ulteriore lasso di tempo.

Una terza fattispecie

Viene altresì introdotta un terza fattispecie rispetto alla quale il blocco dei licenziamenti si protrae sino al 31 dicembre 2021: si tratta delle imprese che dal 1° luglio 2021 non potranno più utilizzare gli ammortizzatori sociali straordinari per Covid; per tali imprese, difatti, è stata prevista la possibilità, in via straordinaria, di accede gratuitamente alla cassa integrazione ordinaria o straordinaria con esonero, fino al 31 dicembre 2021 appunto, dal pagamento dei contributi addizionali (9%-12%-15% della retribuzione che sarebbe spettata al lavoratore per le ore non prestate, a seconda della durata di utilizzo).

Il "Sostegni bis" non rinnova il blocco dei licenziamenti, ma stabilisce un regime articolato e differenziato per tornare alla disciplina ordinaria secondo scadenze e modalità diverse

Altre ipotesi

Rimangono peraltro fermi i casi nei quali era possibile procedere al licenziamento per giustificato motivo oggettivo anche prima del luglio 2021: sono le ipotesi di azienda che cessa un appalto nel quale subentra un'altra realtà; dell'ipotesi di cessazione definitiva dell'attività dell'impresa o dalla cessazione dell'attività senza continuazione, anche parziale, salvo che si configuri la cessione di un complesso di beni o attività che possano concretizzare un trasferimento d'azienda o di un suo ramo; del caso di fallimento dell'impresa, quando non sia previsto l'esercizio provvisorio della stessa ovvero ne sia disposta la cessazione. Se l'esercizio provvisorio è disposto per uno specifico ramo dell'azienda, sono esclusi dal divieto i licenziamenti riguardanti i settori non compresi nello stesso.

Casi specifici

Il licenziamento è altresì precluso nell'ipotesi in cui sussista un apposito accordo collettivo aziendale (art. 14 D.L. 104/2020, art. 1 co. 311 L. 178/2020), stipulato dalle organizzazioni sindacali più rappresentative a livello nazionale, che preveda un incentivo alla risoluzione del rapporto di lavoro e limitatamente ai lavoratori che aderiscono a tale accordo. Non si tratta in realtà di una deroga in senso tecnico essendo sì contemplata dalla legge, ma essendo invero effetto dell'adesione su base volontaria (quindi a fonte contrattuale) ad un accordo che, appunto, prevedendo tempi e modi della risoluzione consensuale del rapporto di lavoro, non consente ovviamente poi di interrompere lo stesso se non nei tempi e modi stabiliti: in tal caso, al fine di incentivare la sottoscrizione di tali accordi, in deroga alla disciplina generale viene previsto che il lavoratore cessato possa accedere alla Naspi (c.d. disoccupazione).

Giuseppe Ligotti (*)

Innovare il lavoro, partendo dalla retribuzione

"Si sente sempre parlare di innovazione: "bisogna adeguarsi all'innovazione, sfruttare l'innovazione, accettare l'innovazione" (spesso supinamente, come qualcosa che deriva da un mondo che non possiamo controllare). Abbiamo reparti specifici che studiano, affinano tecniche e processi affinché i prodotti siano sempre più performanti.

Ma siamo certi di interpretare bene il termine innovazione? Siamo sicuri di applicarlo correttamente a tutte le aree dell'azienda?

(*) Consulente in gestione HR Profittevole, Presidente di Federlavoro Varese
https://giuseppeligotti.it/

Molto spesso il termine innovazione viene limitato al suo approccio di processo, ovvero alle implementazioni del prodotto che lo rendono del tutto nuovo o significativamente migliorato. Il termine INNOVAZIONE però ha un significato ben più ampio. Il vocabolario Treccani fornisce questa definizione:

> *"**1a.** L'atto, l'opera di innovare, cioè di introdurre nuovi sistemi, nuovi ordinamenti, nuovi metodi di produzione.*
>
> ***1b.** In senso concreto, ogni novità, mutamento, trasformazione che modifichi radicalmente o provochi comunque un efficace svecchiamento in un ordinamento politico o sociale, in un metodo di produzione, in una tecnica, ecc.: un'innovazione felice, ricca di conseguenze e di risultati; le innovazioni sinora introdotte si sono dimostrate insufficienti; proporre, progettare, tentare innovazioni; i. tecnologica; i. organizzativa (in un'azienda); incentivare le i. dei processi produttivi; anche in particolari meccanismi o prodotti dell'industria: nell'ultimo modello sono state apportate interessanti innovazioni. (...)*

Innovare il lavoro

Il punto 1b accosta al concetto di innovazione una connotazione concreta, definendola come quel processo che, attraverso azioni di novità, produca una trasformazione che modifichi radicalmente o provochi un efficace svecchiamento. Con queste premesse, voi che dell'innovazione fate un fiore all'occhiello delle vostre imprese: pensate mai in modo innovativo anche al lavoro, ed in particolare alla retribuzione?

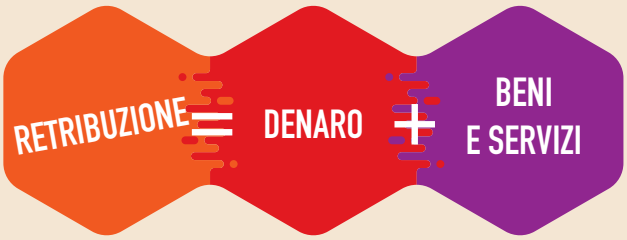
Non solo denaro

L'assioma è che il lavoro debba essere retribuito. Occorre però comprendere che la retribuzione non necessariamente deve essere erogata in denaro. Retribuire vuol dire ricompensare. Potremmo entrare nel merito dell'entità della ricompensa ma sarebbe un altro tipo di analisi: oggi voglio portare la vostra attenzione sulla forma, sul metodo del compenso. L'evoluzione ci ha portato dall'economia di scambio basata sul baratto all'economia monetaria: un processo che ha cambiato radicalmente i rapporti commerciali. Tuttavia oggi viviamo un'era economica nella quale la moneta sembra aver raggiunto un suo limite. Le economie hanno raggiunto livelli tali per i quali sarebbe necessario incentivare i consumi, ma per farlo bisognerebbe aumentare i redditi, ma aumentare i redditi comporterebbe aumentare i costi e aumentare i costi vorrebbe dire togliere risorse alla produzione, rendendo insostenibile il costo del lavoro.

Altri spunti per l'innovazione d'impresa nell'intervento di Giuseppe Ligotti a secsolutionforum 2021 "Formazione finanziata e fondo nuove competenze"

Un cane che si morde la coda?

Iniziamo intanto con il ripensare alla ricompensa e alle modalità di erogarla. Per aumentare il potere di acquisto dei dipendenti pensiamo ad un sistema integrato di retribuzione. La retribuzione oggi deve essere composta da un paniere di beni diversi. L'assioma deve essere:



Dobbiamo essere capaci di INNOVARE il mercato del lavoro. Dobbiamo superare un sistema che ha avuto il suo massimo sviluppo dopo la seconda guerra mondiale, quando, giustamente, il salario (inteso come compenso in denaro) era l'unica forma di retribuzione. Oggi le condizioni economiche sono differenti, i lavoratori hanno bisogno di più reddito, ma contemporaneamentehanno necessità di tenere sotto controllo l'ISEE, hanno necessità di ottenere Assegni Familiari ed incentivi economici - tutte questioni che si scontrano con il bisogno primario di avere un maggior reddito. Ma come fare? Le aziende hanno la necessità di ridurre il costo del lavoro ma contemporaneamente vorrebbero andare incontro ai dipendenti offrendo maggior reddito, ma come fare? Ancora una volta la risposta sta nella nostra capacità di INNOVARE. In questo scenario il concetto di RETRIBUZIONE INTEGRATA trova la giusta collocazione. Perché innovare a volte vuol dire anche gestire i processi evolutivi.

I lavoratori chiedono più reddito,
ma devono tenere sotto controllo l'ISEE,
Assegni Familiari e incentivi.

Le aziende devono ridurre il costo del lavoro
ma vorrebbero andare incontro ai dipendenti.

Come?

Con una retribuzione integrata

focus product

Rilevatore di movimento wireless a tenda bidirezionale

DualCurtain Outdoor di Ajax controlla il perimetro senza creare ostacoli alle persone che si trovano già all'interno. Due sistemi ottici indipendenti con settori di campo visivo ristretti e impostazioni flessibili consentono di regolare in modo accurato 30 metri di campo di rilevazione, escludendo possibili fonti di falsi allarmi. Il software ELSA, unico nel suo genere, risponde agli intrusi, escludendo le cause che possono far scattare l'allarme, come interferenze naturali e animali domestici.

Funzionalità

Sui lati del rilevatore vi sono due sistemi ottici con settore di campo visivo ristretto, ciascuno dotato di due sensori PIR. Grazie alla compensazione termica, il rilevamento è sempre accurato. I segnali del sensore sono analizzati dal nuovo algoritmo digitale ELSA firmato Ajax. Il rilevatore attiva l'allarme solo se due sensori dello stesso sistema ottico rilevano simultaneamente il movimento di persone.

La tecnologia che espande l'area protetta (unica tra i rilevatori di movimento a tenda da esterno) risolve il problema dell'angolo cieco

Distintività

DualCurtain Outdoor è dotato di una tecnologia che espande l'area protetta: una caratteristica unica tra i rilevatori di movimento a tenda da esterno. Quando il rilevamento dell'area vicina è attivato, il sensore PIR superiore del rilevatore riceve un ulteriore settore stretto di visione, diretto con un angolo di 40 gradi verso il basso rispetto a quello principale. Questa funzionalità permette ad entrambi i sensori di rilevare il movimento quando una persona attraversa il perimetro protetto vicino al corpo del dispositivo, risolvendo il problema dell'angolo cieco, che è tipico di tali rilevatori. Il rilevamento dell'area vicina è progettato per proteggere le finestre e gli altri passaggi a cui gli animali non hanno accesso. La prossimità delle zone di rilevamento riduce significativamente l'efficienza dell'immunità agli animali domestici.

Due sistemi ottici indipendenti consentono di regolare in modo accurato 30 m di campo di rilevazione, escludendo falsi allarmi

Caratteristiche

Il raggio di rilevamento dei due sistemi ottici è regolabile in modo indipendente. Questo consente di impostare con precisione il perimetro protetto da DualCurtain Outdoor ed evitare i falsi allarmi. Per evitare che il campo visivo del rilevatore sia ostruito da una colonna o da una grondaia che scende lungo la facciata, i sistemi ottici possono essere orientati verticalmente. All'interno dell'app è possibile regolare la sensibilità o disattivare uno dei sistemi ottici.

DualCurtain Outdoor non può essere oscurato o disabilitato in modo impercettibile anche se il sistema di sicurezza è disinserito. I sistemi ottici del rilevatore sono rinforzati con sensori con antimascheramento avanzato che rispondono agli ostacoli, alla copertura e alla verniciatura delle lenti. Il meccanismo anti-manomissione non permetterà di rimuovere il dispositivo dal supporto senza farsi notare. E persino nel caso in cui il rilevatore venga distrutto sul momento, l'hub impiega meno di un minuto a rilevare la perdita di comunicazione e ad informare del problema la centrale di monitoraggio e gli utenti.

Grazie al basso consumo di energia, DualCurtain Outdoor funziona per anni con le batterie pre-installate. La stazione di monitoraggio e gli utenti saranno avvertiti anticipatamente in caso di interventi di manutenzione necessari sul dispositivo.

Infine, il procedimento di connessione e configurazione di DualCurtain Outdoor fa risparmiare tempo all'installatore: per aggiungere un rilevatore al sistema, basta infatti scansionare il codice QR con l'app Ajax e assegnargli un nome e una stanza. È possibile configurare il dispositivo in tempo reale mentre si effettua il test delle zone di rilevamento e della comunicazione. Se necessario, il rilevatore può essere disabilitato o i parametri di sistema possono essere riconfigurati da remoto, senza interventi in loco.

Il software ELSA, unico nel suo genere, risponde agli intrusi, escludendo le cause che possono far scattare l'allarme, come interferenze naturali e animali domestici.

AJAX SYSTEMS

ofilat.n@ajax.systems

http://ajax.systems/it/

focus product

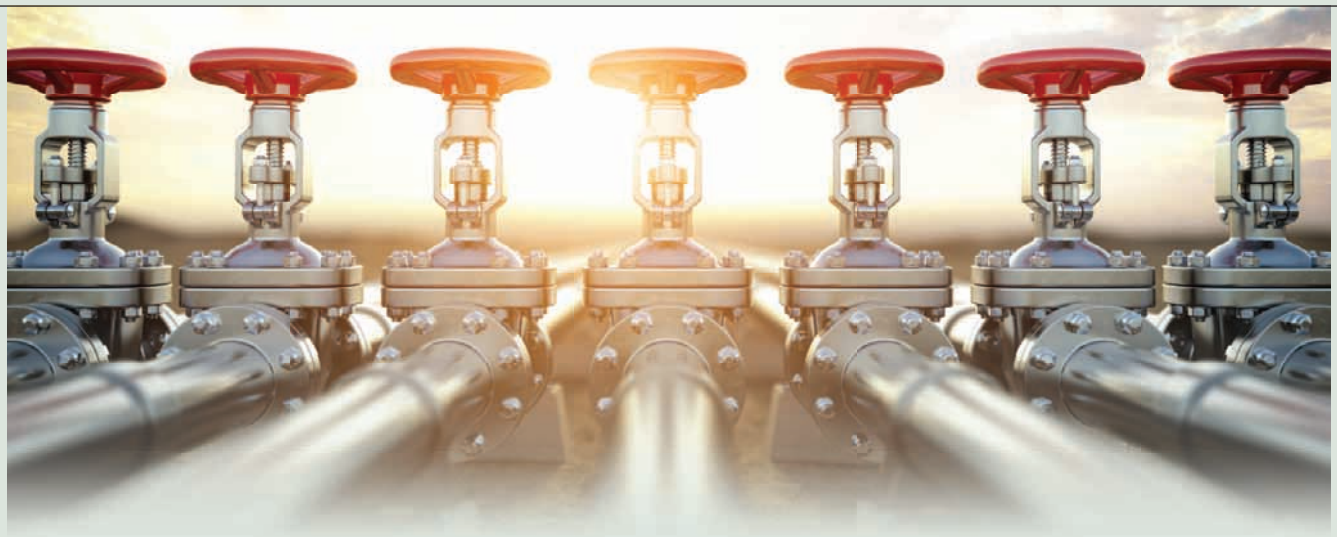
Rivelazione gas ad aspirazione ad alta sensibilità

Notifier presenta XCL Sensepoint, la rivoluzionaria gamma di rivelatori di gas affiancata alla rivelazione ad aspirazione VESDA-E. La gamma comprende rivelatori per molteplici gas tossici (monossido di carbonio, anidride carbonica, ammoniaca, idrogeno, deficienza di ossigeno, etc.) ed infiammabili, potendo così rispondere a qualsiasi esigenza del cliente.

Caratteristiche

I rivelatori di gas XCL Sensepoint sono posti direttamente sulla tubazione di aspirazione ed analizzano l'aria in transito per l'eventuale presenza di gas. Questo permette l'installazione dei sensori in posizioni remote, lontane dagli ambienti protetti e dalle eventuali atmosfere pericolose, potendo così operare le attività di commissioning e manutenzione in tutta sicurezza, oltre che a ridurre drasticamente le tempistiche ne-

XCL Sensepoint è la gamma di rivelatori di gas firmata Notifier affiancata alla rivelazione ad aspirazione VESDA-E



La gamma XCL comprende rivelatori per vari gas tossici (monossido di carbonio, anidride carbonica, ammoniaca, idrogeno, deficienza di ossigeno, etc.) ed infiammabili

cessarie per queste attività. Un singolo rivelatore XCL Sensepoint può far capo a più fori di campionamento presenti sulla tubazione del rivelatore di fumo ad aspirazione e questi fori possono essere posti anche a decine di metri di distanza dal sensore XCL. Questo permette, ad esempio, di monitorare più apparecchiature, flange, etc. Senza bisogno di impiegare localmente molteplici sensori come nelle soluzioni tradizionali puntiformi, difficili poi da manutenere se installati in spazi di difficile accesso. Lungo la stessa tubazione è poi possibile prevedere più rivelatori XCL Sensepoint, così da monitorare l'aria di una singola tubazione per più tipologie di gas differenti.

Applicazioni

Notifier XCL è disponibile in due versioni, XCL Sensepoint Large Bore per l'impiego con la tubazione di aspirazione tradizionale da 25mm facente capo ad un rivelatore Notifier VESDA-E, oppure XCL Sensepoint Micro Bore, da collegare sulle microtubazioni indirizzate del rivelatore Notifier VESDA-E VEA. Quest'ultimo permette di monitorare fino a 40 punti di aspirazione fumo e gas, singolarmente identificati e distanti cadauno fino a 100mt dall'unità di aspirazione. L'impiego con un rivelatore VESDA-E permette quindi non solo di offrire un'innovativa soluzione nel panorama della rivelazione gas, ma anche di sfruttare la rivelazione di fumo ad aspirazione ad altissima sensibilità VESDA, presente sul mercato mondiale da più di 30 anni.

Funzionalità

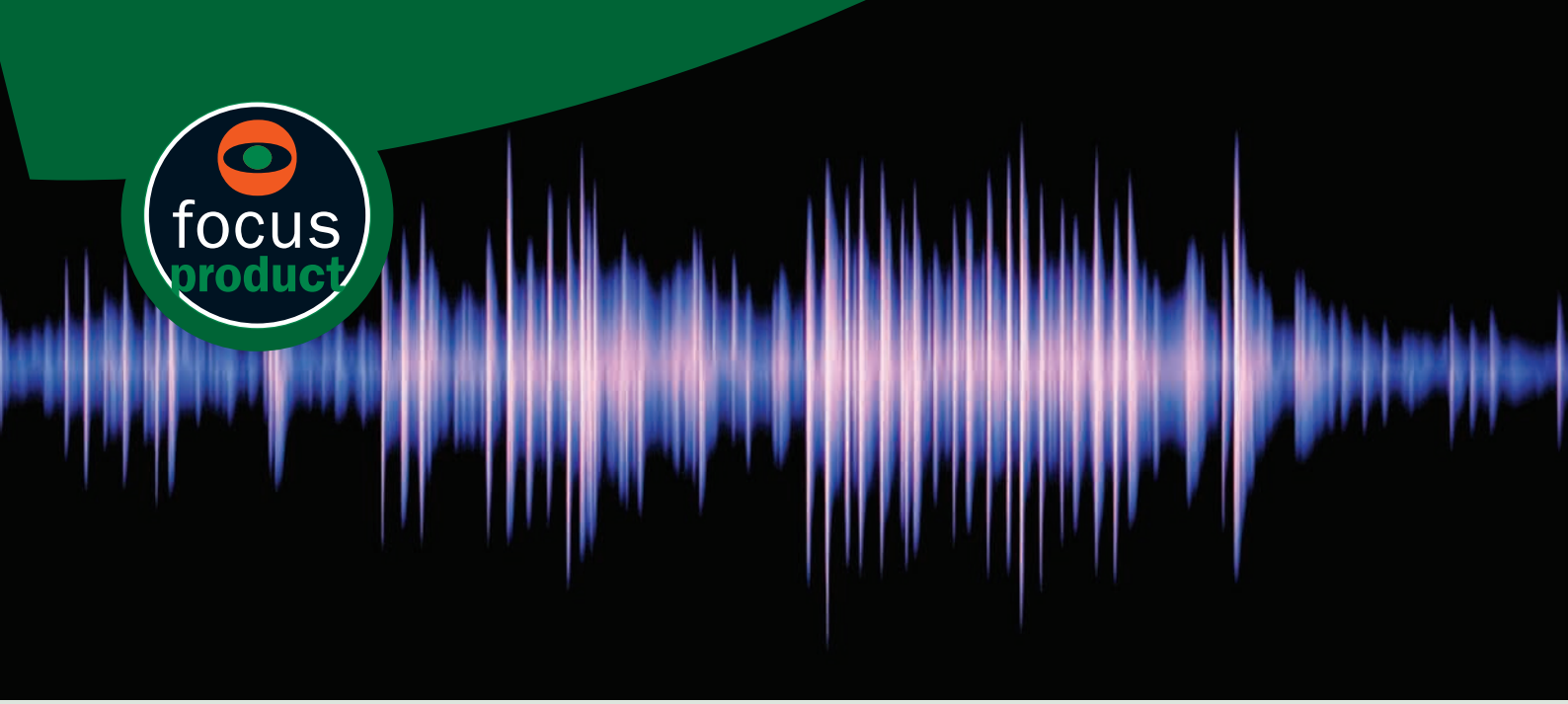
La configurazione e manutenzione del rivelatore XCL Sensepoint è poi facilitata dalla comoda interfaccia bluetooth integrata, così che tutte le attività di commissioning siano a portata di smartphone per l'operatore. Grazie ad un QR code presente su ogni sensore è possibile collegarsi con l'app ed effettuare le attività di calibrazione e verifica. Frontalmente il sensore XCL dispone di un led di stato per la segnalazione di funzionamento normale, guasto, allarme e comunicazione bluetooth.
I sensori XCL sono disponibili nelle versioni con uscite relé, 4-20mA e Modbus RTU.

I rivelatori di gas XCL Sensepoint sono posti direttamente sulla tubazione di aspirazione ed analizzano l'aria in transito per l'eventuale presenza di gas.

Notifier Italia

info@notifier.it

www.notifier.it



focus product

Sirena radio evoluta con acustica differenziata

Axel propone la sirena radio Flix, moderna ed evoluta, con antischiuma, antishock e antiperforazione, oltre a tamper antiapertura e antistrappo, con comunicazione intelligente e dinamica con la centrale, che riceve comandi multipli, segnala stati e anomalie, con acustica differenziata in base alle diverse funzionalità programmate. Il box a verniciatura speciale è garantito contro scolorimento e sfaldamento per 10 anni.

Caratteristiche

Flix appartiene alla linea di prodotti wireless Axeta® della SerieSW, e si programma quindi direttamente dal software Oberon X senza necessità di mettere mano nella sirena. In altre parole: si fissa la sirena al muro, si chiude e si programma direttamente dalla centrale. La sirena Flix è nata nel laboratorio di R&D Axel, utilizzando le prerogative funzionali e di alta sicurezza del brevetto radio Axeta® di Axel ed è il risultato della coprogettazione con Venitem, azienda leader in Europa nella produzione di sounders di alta qualità e dall'estetica inconfondibile.

Flix si può installare anche a centinaia di metri dalla centrale, ha batterie durature, è sicura e si monitora in centrale e localmente con segnalazioni ottiche e acustiche programmabili

Flix è parte della linea wireless Axeta® della SerieSW e si programma dal software Oberon X: si fissa la sirena al muro, si chiude e si programma direttamente dalla centrale

Distintività

L'ampia portata radio del sistema Axeta® consente l'installazione di Flix a centinaia di metri dalla centrale, la sicurezza e l'alta resilienza allo jamming del protocollo radio DSSS, la durata di diversi anni delle batterie, il monitoraggio delle parti vitali della sirena in centrale e localmente con segnalazioni ottiche e acustiche programmabili sono solo alcuni dei punti distintivi di Flix.

Funzionalità

Fino a 4 sirene wireless Flix possono essere installate nel medesimo impianto con scelta tra 8 suoni, differenziati per ogni sirena; il livello di suono da 1% al 100% e la durata per le segnalazioni, che possono essere di diversi tipi e avere programmazioni differenziate. Analogamente si gestisce il lampeggiatore a colori variabili e programmabili.

Per le segnalazioni funzionali il suono dell'altoparlante può avere un livello differente dall'allarme, in modo da essere udibile ma non fastidioso, e così dicasi delle funzioni lampeggiatore. Se si desidera, può essere attivata la segnalazione ottica di stato impianto (acceso/spento), temporanea o permanente, in base alla propria filosofia e alle richieste dell'utente.

Ogni tipo di funzionamento richiesto può essere tranquillamente gestito grazie all'ampia programmabilità e al numero di funzioni di Flix. Il lampeggiatore a 6 LED ad alta potenza RGB e la suddivisione dei colori permettono, ad esempio, la segnalazione accensione totale ON rossa, parziale INT gialla, parziale PAR blu e spegnimento verde.

Così come la differenziazione di colore in caso di allarme furto, e quella di altro tipo, come incendio, presenza gas nell'ambiente interno o altro. Le segnalazioni tecniche riportate in centrale sono il basso livello batteria individuale, il guasto tromba, il tamper, l'antischiuma, l'antishock e l'antiperforazione.

Si possono installare fino a 4 sirene wireless Flix nello stesso impianto con scelta tra 8 diversi suoni, un livello di suono da 1% al 100% e tipo/durata delle segnalazioni e del lampeggiatore

Con il software OberonX è possibile programmare tutte queste variabili, e da qui vengono trasferite alla sirena Flix in modalità wireless, per una comodità di installazione, setup e manutenzione per l'installatore evoluto e l'utente esigente.

AXEL

commerciale@axelweb.com

www.axelweb.com

focus product

Piattaforma per la supervisione di aree critiche

Le infrastrutture per le telecomunicazioni, per la produzione di energia e per la distribuzione di acqua, energia e gas rappresentano un asset strategico, di cui è essenziale garantire il funzionamento e la sopravvivenza in caso di attacchi od eventi naturali. La supervisione di queste reti estremamente complesse, tipicamente non presidiate e distribuite su un territorio vasto, rappresenta da sempre una sfida complicata. La necessità è quella di controllare diverse grandezze fisiche, come la temperatura, l'umidità, l'allagamento, oltre a gestire le politiche di accesso, monitorare le intrusioni e la presenza di fumo o incendi. Tutte queste variabili oggi possono essere gestite da un unico apparato, sviluppato appositamente per questa necessità. Non più diverse centraline interfacciate tra loro, ma un unico dispositivo compatto, che gestisce tutte le tecnologie. Un'unica interfaccia operatore che rappresenta in modo intuitivo lo stato del sito remoto.

Caratteristiche

Due controllori appositamente sviluppati per due tipologie di applicazione; un controllore (ApolloN) pensato per la supervisione di siti non presidiati dotati di

Con un solo apparato si controllano temperatura, umidità, allagamento, accessi, intrusioni, fumo, incendi

Tutta la sensoristica è gestita dal controllore che permette di monitorare e gestire da remoto anche le politiche di accesso ai siti, sfruttando le più moderne tecnologie Keyless

energia elettrica e connettività di rete; un controllore (Juno) sviluppato per tutti i siti che non dispongono di alimentazione elettrica e connettività di rete. Tutta la sensoristica viene gestita dal controllore che permette di monitorare e gestire da remoto anche le politiche di accesso ai siti, sfruttando le più moderne tecnologie Keyless. I controllori comunicano verso la centrale di controllo attraverso la rete Internet o IoT.

Funzionalità

Nella centrale di controllo tutti i siti sono costantemente monitorati in tempo reale, permettendo di gestire prontamente ogni situazione anomala. L'operatore con un semplice click può abilitare un manutentore ad entrare nella cabina remota o ad aprire un armadietto stradale. Lo smartphone del manutentore sarà abilitato a sbloccare la serratura. Nessuna tessera o chiave da gestire, non più il problema di poterle perdere o rompere. Il tutto con la serenità che tutte le informazioni sono protette e sicure, utilizzando le più recenti tecnologie per la crittografia e la protezione dei dati.

Applicazioni

Questa soluzione è dedicata in particolare alla supervisione di infrastrutture critiche, quali:

- Telecomunicazioni: stazioni (PoPs) e armadietti di strada
- Acqua: chiusure, stazioni di pompaggio e pozzi d'acqua
- Energia: stazioni di trasformazione, stazioni di commutazione, stazioni di alimentazione, centrali elettriche e centrali eoliche
- Infrastrutture: armadietti stradali, torri radar, stazioni di misurazione e armadi per sistemi di controllo del traffico e di monitoraggio ambientale
- Trasporti: aeroporti, siti portuali e aree industriali

ApolloN: controllore pensato per supervisionare siti non presidiati dotati di energia elettrica e connettività di rete

Juno: connettore per tutti i siti che non dispongono di alimentazione elettrica e connettività di rete

TKH Security

info.it@tkhsecurity.com

https://tkhsecurity.it/

focus product

Rivelatore per la protezione di varchi e accessi

Smart, wireless e completa: Tecnoalarm implementa la già ricca gamma di componenti della linea Evolution con il nuovo sensore per interni EV REDWAVE BWL.

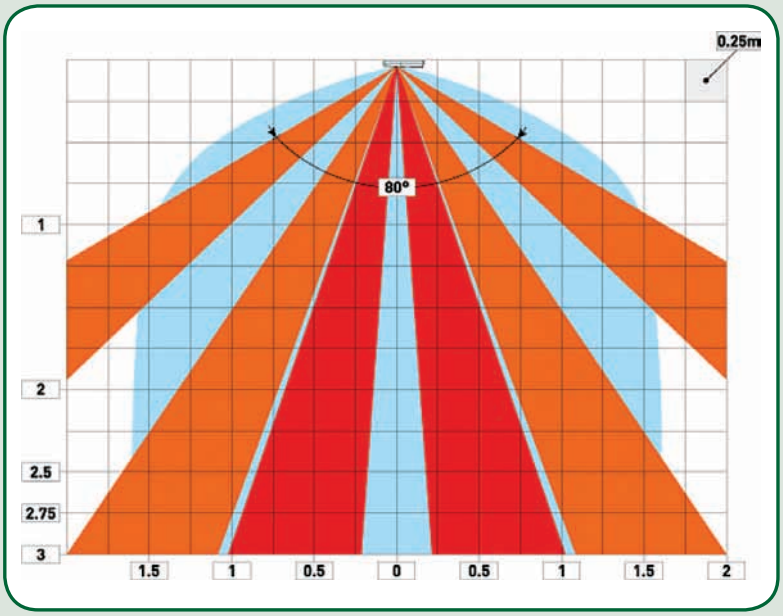
Caratteristiche

Il rivelatore wireless bidirezionale protegge varchi, porte e finestre grazie alle sue due unità di rilevazione indipendenti. La prima unità di rilevazione - doppia tecnologia per una protezione volumetrica ad infrarosso passivo più microonda - dispone di sei zone sensibili su un piano di rilevazione con angoli di apertura 80° sul piano orizzontale, 18° sul piano verticale, ha una portata massima di tre metri e presenta un contatore di impulsi programmabile. La logica di rivelazione è AND gestita da un algoritmo di elaborazione con segnale dinamico e compensazione automatica della temperatura. La seconda unità di rilevazione invece è perimetrale con contatto reed interno e/o ingresso per dispositivo esterno, come un contatto, contatto a fune o inerziale.

Tecnoalarm implementa l'ampia gamma di componenti della linea Evolution con il nuovo sensore per interni EV REDWAVE BWL

Applicazioni

La programmazione del sensore, procedura guidata sul software Centro Tecnoalarm, consente di impostare la sezione a microonda per la protezione di una finestra o di una porta, adattando così la tipologia di protezione necessaria, fino ad un'altezza massima di tre metri. È possibile regolare quattro diversi livelli di sensibilità della microonda per i due tipi di installazione.
Per la sezione infrarosso, è possibile scegliere il numero di impulsi e, se diverso da uno, impostare il tempo di validità, espresso in secondi.



Si può impostare la sezione a microonda per la protezione di una finestra o di una porta, adattando la tipologia di protezione, fino ad un'altezza massima di tre metri

Funzionalità

Remote Sensitivity Control® - L'esclusiva tecnologia Tecnoalarm consente di programmare, telegestire e controllare tutti i parametri di funzionamento di ogni singola apparecchiatura del sistema.

Tecnoalarm Connect Service - Attraverso il servizio telematico TCS, tutti i componenti della gamma Evolution sono costantemente supervisionati e connessi. L'eccellente dotazione di vettori di telecomunicazione permette inoltre di sfruttare, in modo semplice e veloce, le molteplici funzioni di controllo e gestione. In particolare, nuove funzionalità sono state dedicate all'utente per la gestione del sistema direttamente dal proprio smartphone attraverso la nuova app, scaricabile gratuitamente dal proprio app store.

Design Pininfarina - Tecnoalarm si distingue da sempre per le linee moderne ed eleganti dei propri prodotti. La felice e ormai consolidata collaborazione con una delle firme più prestigiose del design internazionale – Pininfarina – è una caratteristica distintiva della serie Evolution. EV REDWAVE BWL è disponibile nella versione bianca o marrone.

Con Tecnoalarm Connect Service tutti i componenti Evolution sono costantemente supervisionati e connessi.

TECNOALARM

info@tecnoalarm.com

www.tecnoalarm.com/it-it/

focus product

Monitorare consumi e carichi = risparmiare 'energia'

Per gestire in modo semplice e veloce la potenza impegnata nel proprio impianto elettrico monofase, evitando l'intervento della protezione del contatore, il classico "salto di corrente" a causa dell'accensione contemporanea di carichi con potenza totale eccessiva, sempre più persone stanno installando nelle loro case *'energia'*. Infatti *energia* rappresenta la soluzione ideale per rispondere a molteplici esigenze: monitoraggio dei consumi, gestione dei carichi, controllo dell'impianto elettrico e risparmio energetico. La vera innovazione risiede nell'integrazione ad un sistema di Smart Home come *lares 4.0*.

Avere un'App in grado di integrarsi con il sistema di domotica permette di analizzare e visionare i dati da un'unica piattaforma con estrema comodità

Caratteristiche

'energia' è stato progettato da Ksenia Security per il monitoraggio giornaliero, settimanale e mensile dei propri consumi. Ogni modulo dispone di due linee di alimentazione distinte sulle quali misura l'assorbimento, ciascuna linea può supportare carichi fino a 6kW. La comunicazione con la centrale *lares 4.0* di Ksenia avviene tramite BUS e rappresenta il completamento ideale in ambito di automazione domestica. Ma non solo. Questo modulo, infatti, consente la gestione dei carichi programmando specifiche soglie, oltre le quali si ha un distacco in successione degli elettrodomestici in funzione.

L'App gratuita lares 4.0 presenta una sezione in cui è possibile visionare i report dei consumi, in base al periodo di tempo che si intende esaminare

Distintività

Ogni modulo possiede 4 uscite relè utilizzabili sia per pilotare dei relè esterni per la disconnessione dei carichi, sia come uscite generiche della centrale. Infatti, è possibile impostare due soglie. La prima è la soglia di assorbimento massimo della potenza, oltre la quale viene inviata una notifica push sull'App *lares 4.0*, avvisando dell'eccessivo consumo. La seconda soglia riguarda la disconnessione: se non si interviene, infatti, *'energia'* provvede a distaccare i carichi in base alla sequenza prescelta dall'utente (ad esempio si può decidere di far staccare prima l'asciugatrice anziché il forno). Grazie ad *'energia'* si ha finalmente accesso ai consumi di casa in tempo reale, con la possibilità di capire se stiamo consumando e quindi spendendo troppo. Controllare i consumi è semplicissimo tramite l'App gratuita *lares 4.0*: è stata creata un'apposita sezione in cui è possibile visionare i report, in base al periodo di tempo che si intende analizzare.

Funzionalità

Poter accedere allo storico dei consumi consente di individuare eventuali sprechi, determinando così gli interventi da attuare per evitare le inefficienze, e concorre al raggiungimento di efficienza energetica. Infatti, *'energia'* è una periferica BUS utilizzabile nell'ambito della gestione dei carichi elettrici, comprese le fonti rinnovabili, il controllo e il bilancio dei consumi. L'analisi inizia con la raccolta dei dati forniti dal modulo stesso, successivamente strutturati e memorizzati secondo una logica applicativa che li elabora e che, infine, vengono rappresentati attraverso grafici a barre che ne mostrano l'andamento temporale, con una visione d'insieme di tutti gli elettrodomestici coinvolti.

Innovazione ed eco-sostenibilità sin dalla sede a Ripatransone (AP): il rispetto dell'ambiente è nel DNA di Ksenia Security

Controllare i consumi evita gli sprechi e concorre al raggiungimento dell'obiettivo di efficienza energetica

KSENIA Security

info@kseniasecurity.com

www.kseniasecurity.com/it

focus product

Integrazione e comunicazione in una centrale unica

I sistemi di allarme antintrusione stanno attraversando una trasformazione profonda, in conseguenza dell'evoluzione di internet e della diffusione degli smartphone che identificano il desiderio di connessione totale e immediata, unito alla necessità di semplificare le operazioni di configurazione con soluzioni rapide e intuitive. La risposta tutta italiana a queste esigenze arriva da GESCO con la nuova centrale SECURBOX IT1, espressione di due concetti fondamentali: integrazione e comunicazione.

Caratteristiche

La centrale è costituita da una scheda completamente integrata e alloggiata in un contenitore compatto dal design ricercato, illuminato da una barra LED RGB ad effetto pulsante. Dispone della connessione WiFi, del modulo LTE (4G/3G/2G) e della radio bidirezionale nella banda degli 868 MHz oltre alla sirena per interni, a ingressi ed uscite e ad un bus seriale per collegare tastiere, lettori RFID, sirene, espansioni. Grazie all'app gratuita e al server cloud proprietario Gesco Ubiway®, la centrale è disponibile sempre e comunque. Le segnalazioni di stato e allarme vengono inoltrate tramite notifiche push, messaggi vocali personalizzati grazie alla tecnologia text-to-speech, sms, email preconfigurata e protocollo IP SIA-DC09. L'avvio dell'impianto è riservato all'installatore registrato, che procede alla configurazione tramite app sfruttando il servizio cloud o, in assenza di connessione, agendo direttamente con la centrale in modalità access point.

Il design moderno è ideale per ogni ambiente

Funzionalità

La centrale SECURBOX IT1 gestisce 16 ingressi cablati, di cui 8 a bordo scheda, e 32 sensori radio con distinzione delle singole protezioni. Le uscite disponibili sono 4 di cui 2 a relè, espandibili a 12 con moduli dedicati alle attivazioni domotiche sia su bus seriale che via radio. Otto utenti possono agire sui tre stati di servizio definibili liberamente e accedere alla memoria eventi a 1000 posizioni.

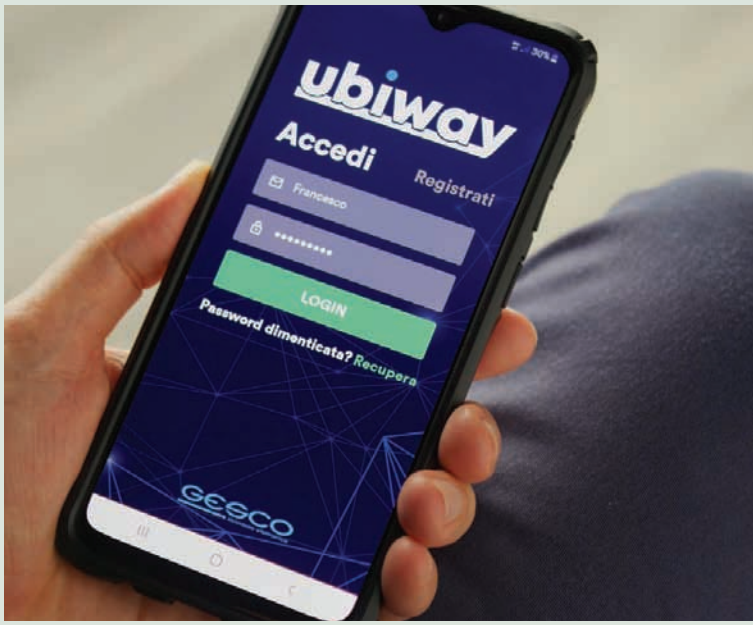
L'app Gesco Ubiway® consente inoltre di guardare i video delle telecamere di sicurezza in tempo reale. Grazie all'integrazione profonda con Dahua, Imou e Uniview, l'abbinamento è immediato e non richiede configurazioni dei dispositivi di rete. È supportato anche il protocollo RTSP, standard adottato dalla maggior parte delle telecamere e DVR presenti sul mercato.

Distintività

La centrale SECURBOX IT1 rappresenta lo stato dell'arte dei sistemi di sicurezza antintrusione residenziali: tecnologicamente avanzata, professionale, solida, affidabile ma anche facile da programmare e gestire, bella da vedere e completamente realizzata in Italia, frutto dell'esperienza Gesco maturata dal 1975. La progettazione accurata ha permesso di realizzare un prodotto affidabile, competitivo, che richiede cablaggi limitati e con diagnostica completa e bassi assorbimenti di corrente. La vasta gamma di accessori permette di realizzare impianti strutturati, in modo da soddisfare qualsiasi esigenza di sicurezza.

Applicazioni

Le caratteristiche tecniche e il design moderno trovano perfetta applicazione in ambito residenziale, dove estetica e semplicità di utilizzo vanno di pari passo all'efficacia del sistema, ma anche in ambito commerciale dove l'attenzione è posta sulla praticità e la completezza delle informazioni.



L'app Gesco Ubiway® è gratuita e disponibile per Android e iOS

Connessione WiFi, modulo LTE (4G/3G/2G) e radio bidirezionale 868 MHz, sirena per interni, ingressi ed uscite e un bus seriale per collegare tastiere, lettori RFID, sirene, espansioni

GESCO

info@gesco.it

www.gesco.it

focus product

Sistema d'allarme radio con videoverifica

Axiom PRO è il nuovo sistema di allarme radio con videoverifica che integra nativamente la tecnologia video Hikvision ed è parte di un sistema convergente che condivide risorse ed interagisce con gli altri dispositivi tramite APP semplici ed intuitive, pensate per l'installatore e l'utente finale. Le caratteristiche della centrale, combinate con l'ampia gamma di componenti e accessori, rendono Axiom PRO ideale per scenari residenziali e commerciali.

Axiom PRO integra nativamente la tecnologia video Hikvision ed è parte di un sistema convergente che condivide risorse ed interagisce con gli altri dispositivi tramite APP semplici ed intuitive

Distintività

Il nuovo sistema radio intelligente professionale Hikvision si contraddistingue per:

- radiofrequenza TRI-X & CAM-X (doppia frequenza Tri-X e Cam-X e tecnologia Frequency Hopping multi canale garantiscono immunità alle interferenze, comunicazione fino a 2.000m di distanza e fino a 6 anni di autonomia per i dispositivi)
- intruder verification (fornisce un videoclip registrato di 7 secondi pre e post evento per una videoverifica in sub-stream, direttamente da Axiom PRO, oppure in Cloud)
- programmazione semplice e intuitiva (i dispositivi possono essere installati con l'APP Hik-ProConnect tramite QR Code)
- comunicazione multipla (Lan, wi-fi, GPRS e 3G/4G integrate nativamente nella centrale offrono una varietà di tecnologie per la comunicazione senza eguali).

La doppia frequenza Tri-X e Cam-X e la tecnologia Frequency Hopping multi canale garantiscono immunità alle interferenze, comunicazione a lunga distanza e lunga autonomia dei dispositivi

Funzionalità

Axiom PRO comprende un'ampia gamma di dispositivi e accessori ed è dotato di tecnologie di rilevazione all'avanguardia, quali: IFT (adatta i rivelatori alle condizioni esterne regolandone automaticamente la sensibilità in base al rumore ambientale); Break Glass (un microfono omnidirezionale di alta qualità rileva, senza falsi allarmi, la flessione o la rottura di vetri su spessori fino a 6.4mm); Videoverifica con PIRCAM (GIF animata di 20 fotografie per una verifica immediata dell'allarme. Integra fotocamera con risoluzione fino a 640x480 e LED infrarossi per le scene a scarsa illuminazione).

Caratteristiche

Axiom PRO è per tutti: il lettore Mifare semplifica infatti l'accesso, mentre la guida vocale fornisce un feedback immediato. I dispositivi di emergenza consentono di attivare l'evento ed effettuare chiamate vocali, sms e notifiche push su APP agli utenti.

La configurazione del sistema è intuitiva ed immediata. I dispositivi possono essere installati con l'APP Hik-ProConnect grazie alla scansione tramite QR Code, ottimizzando le attività manuali e i tempi di installazione

Il lettore Mifare semplifica l'accesso mentre la guida vocale fornisce un feedback immediato

Applicazioni

Hik-ProConnect, piattaforma cloud ideata per gli installatori, consente ad Axiom PRO di convergere con i device Hikvision di Videosorveglianza, Intercom e Controllo Accessi, lavorando come un unico sistema e condividendo le risorse. Hik-Connect è invece l'applicazione ideata per gli utenti finali che, da un unico dispositivo, permette di gestire tutti i prodotti Hikvision. Verifica lo stato del sistema, inserisce/disinserisce e riceve notifiche d'allarme, verifica lo stato del singolo dispositivo (temperatura, livello del segnale, stato della batteria) e, attraverso la verifica, può confermare il singolo evento di allarme. I Monitor Supervisori, con un'interfaccia semplice e intuitiva, consentono di gestire tutti i dispositivi Hikvision da un unico sistema: non solo security con allarme, videocitofonia e TVCC, ma anche automation grazie all'integrazione con APP di terze parti.

HIKVISION

info.it@hikvision.com

www.hikvision.com/it

focus product

Sistema antintrusione wireless e di design

Secur Hub è il sistema antintrusione wireless connesso al Cloud di Comelit che include sia la connettività Wi-Fi sia LAN. Pensato per un'installazione rapida ed aggiornabile via Cloud, il sistema non necessita di apertura porte sul router nemmeno per quanto riguarda la App, sia per la gestione del sistema sia per la visualizzazione delle telecamere connesse. Grazie al wizard di installazione a bordo, inoltre, l'impianto si può configurare in pochi minuti anche senza l'utilizzo del PC.

Caratteristiche

La comunicazione tra la centrale e tutti i dispositivi wireless connessi avviene per mezzo di un protocollo radio criptato sviluppato nei centri R&D Comelit, cui si aggiungono funzioni come l'anti-jamming (che rileva possibili disturbi intenzionali sulle frequenze utilizzate dal sistema) ed una portata radio che soddisfa e supera le esigenze di tutte le applicazioni.

Secur Hub è il sistema antintrusione wireless connesso al Cloud di Comelit, che include sia la connettività Wi-Fi sia LAN

Grazie alla bi-direzionalità dei messaggi tra centrale e sensori, questi ultimi possono essere programmati totalmente dalla centrale o dal software dedicato Hub Manager, anche da remoto, con grande risparmio di tempo e senza la necessità di dover accedere all'interno degli stessi. Tecnologie di ultima generazione consentono inoltre di prolungare la vita delle batterie fino ad 8 anni per alcuni dei sensori più utilizzati.

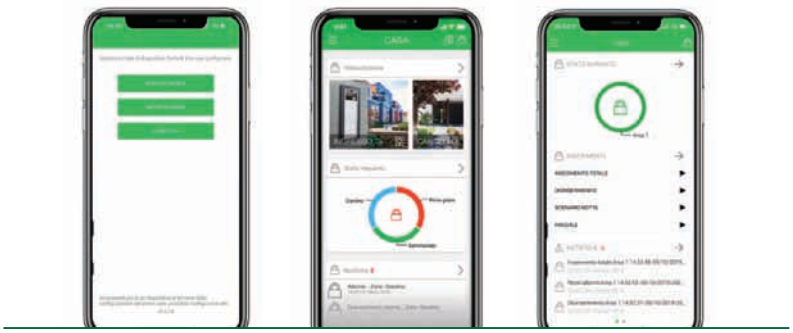
Distintività

Installazione semplice, affidabilità ed ergonomia sono i valori che Secur HUB mette al servizio della sicurezza delle persone e degli ambienti. Valori che si aggiungono ai numerosi servizi messi a disposizione da Comelit per accompagnare l'installatore passo dopo passo dalla formazione, online o in presenza, alla scelta dei prodotti fino alla messa in servizio dell'impianto. Non solo, i professionisti possono rivolgersi anche all'assistenza tecnica telefonica o capillare su tutto il territorio per consulenze progettuali, supporto diretto in cantiere e qualsiasi altra esigenza.

Applicazioni

E per facilitare ulteriormente la gestione dell'impianto, attraverso Comelit App, che consente la gestione unificata di tutti i sistemi Comelit, è possibile monitorare la centrale Secur Hub anche lontano da casa, controllando lo stato del sistema d'allarme, dei suoi sensori o visualizzando lo storico degli eventi registrati dalla centrale, con la certezza di essere sempre tempestivamente avvisati in caso di necessità. È possibile anche collegare fino a 16 telecamere IP con risoluzione HD e quattro di queste possono registrare direttamente sulla centrale in modo da inviare, insieme alle notifiche di allarme, anche dei brevi video che consentono di visionare direttamente l'accaduto. La centrale permette inoltre l'installazione di moduli 2G, 3G e 4G. Integrazione, flessibilità d'installazione, semplicità di utilizzo e un design studiato nei minimi dettagli, riconosciuto anche da una Menzione d'Onore del Compasso d'Oro, rendono Secur HUB un sistema facilmente inseribile anche in un contesto residenziale a vista, dove l'attenzione ai dettagli è più importante, rendendo il sistema un complemento d'arredo oltre che un dispositivo di sicurezza.

Integrazione, flessibilità, semplicità di utilizzo e un design con Menzione d'Onore del Compasso d'Oro, rendono Secur HUB un complemento d'arredo oltre che un dispositivo di sicurezza



Comelit App consente di monitorare Secur Hub anche lontano da casa, controllare lo stato del sistema d'allarme, dei suoi sensori e visualizzare lo storico degli eventi registrati

Comelit Group

info@comelit.it

www.comelitgroup.com/it-it/

TRASMETTITORE UNIVERSALE PER SENSORI LOW POWER

AX-CN09sw, trasmettitore universale, permette l'implementazione nei sistemi Axel di sensori low power alimentati a 3V.
AX-CN09sw e sensore sono alimentati da unico pacco batterie scelto dall'installatore. Come tutti i dispositivi Serie Axeta®SW, la sezione wireless è programmabile remotamente dalle centrali Axò e con programmazione classica con la Base Station Axeta®.
Oltre alle prerogative professionali Axeta®, gestisce 3 segnalazioni distinte alla centrale: allarme, tamper e mascheramento, occupando una sola zona in centrale. La funzionalità è analoga a una zona filare a triplo bilanciamento.
Negli impianti con dotazione Axeta®, amplia la scelta di qualsiasi rilevatore da esterno si giudichi importante per la protezione desiderata. Ha portata 1000mt a/l su 1000 e sono ammesse diverse frequenze in banda.

AXEL
www.axelweb.com

SISTEMA DI ALLARME RADIO CON VIDEOVERIFICA

Axiom PRO è il nuovo sistema di allarme radio con videoverifica che integra nativamente la tecnologia video Hikvision ed è parte di un sistema convergente che condivide risorse ed interagisce con gli altri dispositivi tramite APP semplici ed intuitive, pensate per l'installatore e l'utente finale. Le caratteristiche della centrale, combinate con l'ampia gamma di componenti e accessori, rendono Axiom PRO ideale per scenari residenziali e commerciali. Axiom PRO è dotato di tecnologie di rilevazione all'avanguardia, quali: IFT (adatta i rivelatori alle condizioni esterne regolandone automaticamente la sensibilità in base al rumore ambientale); Break Glass (un microfono omnidirezionale di alta qualità rileva, senza falsi allarmi, la flessione o la rottura di vetri su spessori fino a 6.4mm); Videoverifica con PIRCAM (GIF animata di 20 fotografie per una verifica immediata dell'allarme).

HIKVISION
www.hikvision.com/it

RILEVATORE PER CENTRO FINESTRE

Il rilevatore CENTRUM CX è pensato per installazioni centro finestra e per la protezione dei varchi.
Tra gli elementi che lo caratterizzano spiccano l'antimascheramento di infrarosso a led attivi che rileva qualsiasi tentativo di mascheramento nelle immediate vicinanze del rilevatore.
La funzione tapparella permette, in presenza di finestre con tapparelle, di aver la migliore efficacia di rilevazione.
I due parzializzatori per la lente di Fresnell rendono il rilevatore PET immune.
Fra le altre caratteristiche: interfacciabilità con gli accessori STAFFA 90°, disponibile in diversi colori, grado di protezione IP54.

EEA
www.eea-security.com

SISTEMA DI SICUREZZA COMPLETO, MODULARE E SEMPLICE

La lunga esperienza nella security fa di EBS ALARM SYSTEMS un importante tassello della vasta gamma di centrali di elaborazione e sensoristica filare & wireless. Disponibili contatti magnetici con ingressi ausiliari, rivelatori di rottura vetri, sensori di movimento pet-immune e microcamera a colori integrata, sonde antiallagamento, rivelatori di fumo e gas e accessori di comunicazione.
La nuova centrale di allarme EBS - AVA PRO è la combinazione vincente tra sistema antifurto professionale e smart-home, garantendo sicurezza e comfort, oltre alla facilità di messa in servizio, usando smartphone e APP dedicata (oppure tramite QR-code) con una gestione intuitiva da tastiera +tag di prossimità (oppure tramite APP gratuita e notifiche PUSH), tutte doti e funzioni molto apprezzate sia dagli installatori che dagli utenti finali. Pertanto l'architettura modulare di EBS - AVA PRO risponde a modernità, comfort, funzionalità, design moderno.

ELECTRONIC'S TIME
www.electronicstime.it

DISPOSITIVI PER EFFICIENZA ENERGETICA ED ECOBONUS

Con Ksenia Security è possibile beneficiare dell'Ecobonus fino al 31 dicembre 2021, con una detrazione fiscale dal 65 al 110%.
Infatti, la combinazione di una centrale lares 4.0 con i moduli 'domus' ed 'energia' rientra nella definizione di dispositivi multimediali installabili per lavori di efficientamento energetico. Nello specifico, il modulo multifunzione 'domus' incarna al tempo stesso ben 4 sensori: un sensore di movimento, di temperatura, di umidità relativa e un sensore di intensità luminosa. Un prodotto, quindi, che determina un significativo risparmio energetico.
Naturalmente, per poter accedere all'Ecobonus, è necessario rivolgersi a figure professionali competenti che possano analizzare, caso per caso, la fattibilità delle detrazioni fiscali.

KSENIA SECURITY
www.kseniasecurity.com/it/

TELECAMERE PER PUNTI CIECHI E PERIMETRALE

Le telecamere WV-S8531N e WV-X8571N multisensor si aggiungono alla serie i-PRO Extreme, offrendo immagini dotate di qualità e risoluzione elevate – FHD e 4K – nelle installazioni più complesse.
Il primo modello dispone di quattro ottiche varifocali 2,5x (2.9-7.3mm) motorizzate nello zoom per semplificarne il puntamento ed è dotato di alimentazione PoE+ (22 Watt); il modello WV-X8571 monta ottiche grandangolari fisse 4.6mm e alimentazione PoE+ (20Watt) o 12VDc (1,2A/15Watt). Grazie alla funzionalità "Continuous view assistance", consentono l'ottimizzazione automatica del campo visivo in base alla disposizione e al campo di ripresa, utilizzando lo zoom motorizzato, e sono la soluzione ideale per applicazioni in punti ciechi e perimetrali, incroci stradali, stazioni e contesti di videosorveglianza urbana o dove sia necessario riprendere soggetti e veicoli in rapido movimento.

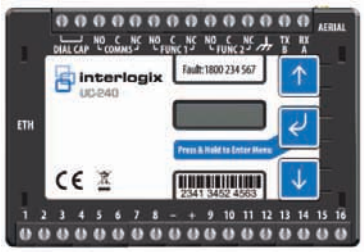
PANASONIC BUSINESS
https://business.panasonic.it/

PIATTAFORMA E APP PER IL BENESSERE AZIENDALE

Zucchetti ha deciso di entrare nella compagine societaria di Beaconforce, che ha sviluppato una soluzione che, con una solida base scientifica, coniuga intelligenza emotiva e intelligenza artificiale per elaborare lo "stato di salute" delle persone e delle organizzazioni e fornisce punti di attenzione e suggerimenti di azioni correttive per creare ambienti di lavoro stimolanti e motivanti e per migliorare, quindi, i livelli di performance e produttività.
Le risorse apportate da Zucchetti svilupperanno ulteriormente le capacità predittive della piattaforma che hanno consentito di ridurre il turnover indesiderato, gestire tempestivamente le criticità, avere un quadro chiaro della motivazione delle persone anche in contesti di lavoro remoto, individuare gli investimenti più efficaci per migliorare la motivazione delle persone e, di conseguenza, la loro produttività.

ZUCCHETTI
www.zucchetti.it

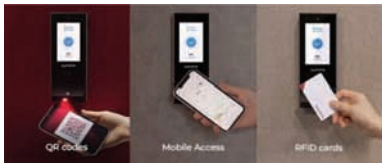
COMUNICATORI UNIVERSALI



I comunicatori UltraSync aggiungono funzionalità moderne a qualsiasi sistema di sicurezza e antincendio che, a causa della progressiva dismissione delle linee PSTN, ha perso le proprie caratteristiche di comunicazione.
Il comunicatore mette a disposizione ingressi/uscite, un simulatore di linea, per catturare il contactID e trasformarlo in notifiche push ed e-mail, e una porta seriale per la telegestione delle centrali testate. Il tutto tramite il cloud UltraSync™, sicuro e affidabile, e l'APP UltraSync+.
Il comunicatore UltraSync è disponibile in due modelli entrambi con SIM UltraSync a bordo: UC140 (4G/2G) e UC240 (IP - 4G/2G).
I comunicatori UltraSync consentono di affrontare le esigenze dei diversi clienti con un prodotto certificato sia per centrali antincendio che antintrusione.

ARITECH
www.aritech.it

SISTEMI DI CONTROLLO ACCESSI E PRESENZE



Il nuovo lettore di controllo accessi XStation 2 identifica il codice fiscale leggendolo dal bar code della tessera sanitaria. Il sistema, chiamato Ecopass, supporta anche la lettura di QR Code, badge 125Khz e Mifare\DESFire 13,56Mhz, NFC, BLE.
Ecopass è ideale per controllare l'accesso ad aree ecologiche o altre aree pubbliche comunali nelle quali possono entrare solo i cittadini abilitati e per le quali serve monitorare il numero e la frequenza degli accessi stessi.
I terminali possono essere distribuiti sul territorio e gestiti da un software centralizzato tramite connessione del terminale attraverso rete ADSL o UMTS/4G/LTE (utilizzando un router aggiuntivo). Il software è pubblicabile in cloud e raggiungibile da qualunque luogo con interfaccia web.
Grazie al software TimeWalker è possibile implementare eventuali funzionalità per gestire dati abbinati all'accesso.

ETER BIOMETRIC TECHNOLOGIES
www.eter.it

CENTRALE CON CONNETTIVITÀ WI-FI PER DOMOTICA

La nuova centrale Prime 500L, pensata per impianti di medie e grandi dimensioni, incrementa le sue prestazioni domotiche grazie a otto nuovi dispositivi.
Il modulo PrimeWiFi consente di applicare la connettività WiFi. Il modulo Flex/5R su bus offre ben 5 relè (230v). Il modulo domotico Flex2R/2T consente di automatizzare l'azionamento delle tapparelle.
Inim Home, l'APP per l'utente finale, è stata ridisegnata per offrire un'esperienza d'uso straordinariamente semplice. Nexus/4G, il modulo integrato su BUS, consente di connettere le centrali al web e al cloud. PrimeLAN è il modulo opzionale avanzato di connettività IP. nBy/K, il lettore di prossimità da incasso su bus, ha aggancio universale keystone.
Smarty/W, sirena wireless da interno, opera in modo bidirezionale, garantendo una segnalazione d'allarme attendibile e sempre verificabile.

INIM
www.inim.biz

CENTRALE DI SICUREZZA SUPERIBRIDA CON VIDEOVERIFICA

ProSYS™ Plus è la centrale di sicurezza super ibrida di RISCO Group con video verifica visiva radio per installazioni sempre più flessibili e performanti e tastiera touch screen RisControl. Ideale per ogni tipo di installazione da 8 fino a 512 zone, si adatta a strutture residenziali e commerciali offrendo elevati livelli di sicurezza grazie alla conformità agli standard EN Grado 2 e Grado 3.
Oltre alla video verifica abilitata da VUpoint con telecamere IP, offre anche verifica visiva dell'allarme in tempo reale, grazie a sensori radio da interno – eyeWAVE™ – e da esterno – Beyond DT – implementati sulla centrale grazie alla nuova espansione radio dotata di canale video: al momento del verificarsi di un evento, immagini in alta definizione e a colori o brevi clip video sono trasmessi direttamente sullo smartphone dell'utente o alla vigilanza, con la notifica push.

RISCO GROUP
www.riscogroup.it

RILEVATORE FILARE MULTIFUNZIONE

XD-2 è un dispositivo filare multifunzione che soddisfa i requisiti della normativa EN 50131 per il Grado 2.
Utilizzabile con qualsiasi tipologia di centrale, può operare in 4 diverse modalità facilmente selezionabili attraverso dip-switch: contatto magnetico, rilevatore d'urto, rilevatore d'urto e contatto magnetico a doppio canale e rilevatore di allagamento grazie alla sonda esterna FPX-1. La taratura può essere realizzata tramite trimmer e verificata mediante l'attivazione del led integrato.
Viene fornito con due diversi magneti per l'installazione ad incasso o in superficie. Il contenitore dalle dimensioni ridotte, con la stessa estetica della versione wireless AXD-200, e le tre colorazioni disponibili – bianco, antracite e marrone – permettono ad XD-2 di adattarsi ad ogni ambiente.

SATEL ITALIA
www.satel-italia.it

SISTEMA DI ALLARME CON CENTRALE BIDIREZIONALE

Dogma è un nuovo concetto di pensare il sistema di allarme, un HUB capace di monitorare tutti i dispositivi wireless registrati e garantire un elevato standard di sicurezza per la protezione totale di qualsiasi ambiente civile e residenziale.
Queste le caratteristiche: centrale wireless bidirezionale BiTech a 28 zone (+ 4 REP), 4 Aree; 8 attuatori radio per funzioni di smart building; alimentatore interno; batteria tampone ricaricabile (12 ore); connettività tramite Lan (WiFi opzionale) e GSM/GPRS (Sms testo, e-mail); protocollo SIA-IP; sistema anti-jamming integrato; video-verifica attivabile con tecnologia VTech; gestione tramite APP MY-SICEP e Cloud (notifiche push); integrazione avanzata con Centrali di Vigilanza SICEP; programmazione locale e da remoto; ingombri ridotti.

SICEP
www.sicep.it

MANIGLIA DIGITALE CON STRUTTURA MODULARE

SmartHandle AX è la nuova generazione di maniglie digitali SimonsVoss. Grazie alla struttura modulare e all'ampia gamma di varianti, SimonsVoss introduce con la SmartHandle AX un nuovo livello di intelligenza, comfort e sicurezza.
Oltre ad essere un piacere per gli occhi, il design flessibile consente la massima libertà di allestimento. SmartHandle AX è configurabile in sistemi offline, di rete virtuale e full online grazie alla possibilità di installare la scheda di rete anche in un secondo momento. Una nuova soluzione intelligente per porte interne con fissaggio sui fori del quadro maniglia della serratura (DIN 18251) consente all'occorrenza il bypass meccanico ed è utilizzabile in combinazione con la maggior parte dei maniglioni antipanico esistenti.

SIMONSVOSS TECHNOLOGIES
www.simons-voss.com/it

APP CON NOTIFICHE PUSH IN TEMPO REALE

Oltre alla chiamata telefonica, gli sms, le e-mail, i sistemi Evolution comunicano gli eventi di funzionamento tramite notifiche push sui dispositivi mobili.
L'APP consente di interagire da remoto, per gestire in modo semplice e intuitivo l'attività delle zone, i programmi e i telecomandi, l'interazione con sistemi domotici e la richiesta di scatto fotografico per la visualizzazione degli ambienti protetti. La notifica degli eventi di allarme dei sistemi con rivelatori EV CAM BWL è corredata della sequenza di scatti fotografici registrati a fronte di un allarme (video verification). L'APP ha nuove funzioni di filtro che semplificano la consultazione dell'archivio eventi. Inoltre, l'introduzione di comandi rapidi, configurabili dall'utente, consente di velocizzare la gestione dei programmi e/o l'attuazione dei telecomandi. L'APP è disponibile sui diversi APP store.

TECNOALARM
www.tecnoalarm.com

TELECAMERA FULL HD DA ESTERNO PROTETTO

TEL600EXT è una telecamera Full HD da esterno protetto, integrata nel sistema radio Egon. Con risoluzione HD 1080P, obiettivo ultra grandangolare e LED IR, consente di vedere immagini nitide, in qualsiasi momento della giornata, anche nelle ore notturne. Dispone di microfono e altoparlante incorporati con audio bidirezionale e cancellazione dell'eco.
Queste caratteristiche permettono di monitorare l'esterno della propria abitazione tramite il browser web o applicazione EGON per smartphone, con l'invio di clip e foto in caso di allarme.
Clip video e immagini possono essere archiviati localmente su scheda SD o sul cloud EGON, nel totale rispetto della privacy dell'utente.
TEL600EXT può inoltre integrarsi ai dispositivi di home automation presenti nell'impianto.

ELKRON
www.elkron.it

SISTEMI DI SICUREZZA PER SMART HOME

Hinnovation by Nital presenta i prodotti Swann per la smart home.
L'offerta è ampia e versatile: vi fanno parte sistemi avanzati come i Network Video Recorder (NVR) e Digital Video Recorder (DVR) associabili a telecamere 4K con visione notturna a colori, ma anche videocamere IP ideali per qualsiasi contesto di smart home.
Nell'offerta sono presenti telecamere per interni, esterni e dotate di tecnologia Pan & Tilt con Wi-Fi, audio bidirezionale, rilevamento degli oggetti, zoom automatico e integrazione con gli assistenti virtuali Alexa e Google Assistant.
Caratteristica essenziale è il concetto di ecosistema: tutti i prodotti Swann possono dialogare con altri dispositivi della Smart Home (per esempio, via IFTTT) ed essere integrati e controllati con una sola APP, Swann Security, così da rendere la gestione della sicurezza semplice e veloce.

HINNOVATION BY NITAL
www.hinnovation.it

NVR INTEGRATI CON VIDEO 4K HD

La Series 30 di NVR integrati (eNVR), gli NVR più economici e completi, offre una risoluzione video 4K HD (UHD).
Gli eNVR Series 30 di Honeywell sono progettati per essere utilizzati come parte di sistemi video conformi al John S. McCain National Defense Authorization Act 2019 (NDAA), Sezione 889. Sono inoltre conformi allo standard PCI-DSS e includono un livello di cybersecurity avanzato con un chipset FIPS integrato.
Gli utenti beneficeranno anche dello streaming crittografato tra le telecamere delle Series 30 / 60 e la Series 30 NVR, fino all'Honeywell Video Management Viewer (HVMV) e alle applicazioni mobile.
Inoltre, la Series 30 eNVR offre agli utenti la possibilità di scegliere tra NVR da 8 o 16 canali, con diverse configurazioni di storage e fino a 20TB di memoria interna.

HONEYWELL BUILDING TECHNOLOGIES
www.security.honeywell.com/it/

LA APP PER GLI INSTALLATORI DI IMPIANTI DI VIDEOSORVEGLIANZA

CheckAPP VIDEOSORVEGLIANZA

RAPPORTO DI INSTALLAZIONE

Realizzate rapporti di verifica da inviare direttamente via mail al cliente

CARTELLO AREA VIDEOSORVEGLIATA

Inviate al cliente il cartello Area Videosorvegliata correttamente compilato

ANAGRAFICA IMPIANTI

Tenete sotto controllo lo status privacy degli impianti di videosorveglianza dei vostri clienti

MULTI UTENZA

Utilizzabile da più operatori e dispositivi contemporaneamente

QUESTIONARIO SEMPLIFICATO

Rispondete ad un semplice questionario per verificare lo status privacy di ogni impianto

LIBERATORIA

Ottenete dal cliente la liberatoria e acquisite la firma direttamente sullo smartphone

CheckAPP Videosorveglianza è una web application per dispositivi "mobile" (Tablet e Smartphone) dedicata al mondo della Privacy e della Sicurezza.

CheckAPP Videosorveglianza è stata ideata per gli installatori di impianti di videosorveglianza: con questo strumento l'installatore può verificare che ogni impianto installato sia conforme alle disposizioni della normativa Privacy.

CheckAPP Videosorveglianza non richiede l'installazione di una App nel proprio dispositivo: infatti, si può utilizzare direttamente dal browser web. In questo modo lo strumento sarà sempre aggiornato alle disposizioni normative più recenti senza costringere l'installatore a ricordarsi di aggiornare la App.

Per informazioni:
app@ethosmedia.it

Approfondisci e trova il Rivenditore più vicino su app.secsolution.com

secsolution magazine

Tecnologie e soluzioni per la sicurezza professionale

www.secsolutionmagazine.it | www.secsolution.com | www.ethosmedia.it

ISSN 2612-2944

ANNO III – Numero 15
Giugno 2021

Direttore responsabile
Andrea Sandrolini

Coordinamento editoriale
Ilaria Garaffoni
redazione@ethosmedia.it

Direzione Commerciale
Roberto Motta
motta@ethosmedia.it

Ufficio Traffico
Carolina Pattuelli
pattuelli@ethosmedia.it
tel. +39 051 0475136

Ufficio estero
international@ethosmedia.it

Pubblicità
Ethos Media Group srl
pubblicita@ethosmedia.it

Sede Legale amministrazione
Via Venini, 37
20127 Milano

Direzione e redazione
Ethos Media Group s.r.l.
Via Venini, 37
20127 Milano (IT)
tel. +39 051 0475136
Fax +39 039 3305841
www.ethosmedia.it

Registrazione
Tribunale di Bologna al n° 8423
in data 29/06/2016

Iscrizione al Roc
Ethos Media Group s.r.l.
è iscritta al ROC
(Registro Operatori
di Comunicazione)
al n. 19315 del 2 marzo 2010

Periodicità
Bimestrale

Privacy (banche dati)
Le finalità del trattamento dei dati dei destinatari del Periodico consiste nell'assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. Tali dati sono trattati nel rispetto del D.Lgs. 196/2003. Responsabile del trattamento dei dati raccolti in banche dati ad uso redazionale è il direttore responsabile a cui gli interessati potranno rivolgersi per esercitare i diritti previsti dall'art. 7 del D. Lgs. 196/2003.

Grafica / impaginazione
www.agvstudio.com
Pioppe di Salvaro (Bo)

Stampa
MIG - Moderna Industrie Grafiche s.r.l. - Bologna

inserzionisti

secsolution®
security online magazine

WEBSITE

il **security magazine online** per un **aggiornamento** giornalistico quotidiano, interattivo e ricco di spunti e contenuti

secsolution.com

La piattaforma più autorevole nella sicurezza

www.secsolution.com è il portale d'informazione b2b di riferimento per i professionisti della security in Italia. **www.secsolution.com** è un portale dalla navigazione intuitiva studiato per essere massimamente usabile, che contiene un motore di ricerca interno selezionabile per tecnologia, brand e parole chiave. L'ampia gamma di sezioni tematiche copre tutti gli ambiti di interesse per gli operatori: da quelli strettamente tecnologici a quelli normativi, da quelli economico-fiscali alla formazione professionale, fino alle curiosità.

Presente su diversi canali multimediali

L'update quotidiano seguibile anche su Twitter e Facebook, e le seguitissime newsletter, inviate ad un target altamente profilato, chiudono il cerchio dell'aggiornamento settoriale.

www.secsolution.com

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

Ethos Media Group s.r.l.
Via Venini, 37
20127 Milano (Italy)
Fax +39 039 3305841
ethos@ethosmedia.it
www.ethosmedia.it

Satel ITALIA 10th Anniversary

Sistema di controllo accessi ACCO NET

ACCO NET è un sistema di controllo accessi scalabile ad architettura distribuita.

La funzionalità completa, i metodi di gestione intuitivi, la costruzione flessibile e lo sviluppo della struttura del sistema consentono ad ACCO NET di soddisfare le esigenze di grandi e medie imprese, anche con molte divisioni come: reti commerciali, banche e altre istituzioni.

Per maggiori informazioni visita:
www.satel-italia.it