

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

Sicurezza

OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID (in attesa di conferma).



INDICE

4 Il cyber crime mette a rischio l'innovazione e gli asset aziendali

- 6 Vecchie e nuove minacce mettono a rischio aziende e governi
- 8 Il GDPR è alle porte, ultimi avvisi
- 10 L'80% delle aziende italiane non è pronto per il GDPR
- 12 Più sicurezza per i manager automatizzando la protezione degli account
- 14 L'automazione riduce i rischi aziendali
- 16 Come garantire la sicurezza dei Container
- 18 Endpoint al sicuro con l'intelligenza artificiale e il blocco comportamentale
- 20 Un perimetro digitale per proteggere l'impresa
- 22 Come mettere al sicuro le infrastrutture e i sistemi industriali
- 24 Sicurezza e GDPR: i tre punti cardine
- 26 Applicazioni al sicuro con i Cloud Service
- 28 Con Blockchain dati e transazioni al sicuro da cyber attacchi
- 30 L'analisi predittiva in ambiente cloud rende sicuri dati e applicazioni
- 32 Per un'Industry 4.0 sicura servono soluzioni specializzate
- 34 Business Always-On e dati critici al sicuro su Microsoft Azure

36 La protezione fisica serve quanto quella logica

- 41 Con SiMPNiC la sicurezza dell'ambiente business e home diventa smart
- 42 Data Protection e videosorveglianza per una maggiore sicurezza
- 44 Salvaguardare la privacy a dispetto del visual hacking
- 46 Proteggere l'ambiente per proteggere il business e le persone

Direttore responsabile: Gaetano Di Blasio
In redazione: Giuseppe Saccardi,
Gaetano Di Blasio, Paola Saccardi,
Edmondo Espa
Grafica: Aimone Bolliger
Immagini da: Dreamstime.com
Redazione:
via Marco Aurelio, 8 - 20127 Milano
Tel 0236580441 - fax 0236580444
www.reportec.it
redazione@reportec.it

Direction Reportec • anno XV - numero 102

Stampa:
Media Print Srl, via Brenta 7,
37057, S.Giovanni Lupatoto (VR)

Editore: Reportec Srl, via Marco Aurelio 8,
20127 Milano

*Il Sole 24 Ore non ha partecipato alla
realizzazione di questo periodico e non
ha responsabilità per il suo contenuto*

Presidente del C.d.A.: Giuseppe Saccardi
Iscrizione al tribunale di Milano
n° 212 del 31 marzo 2003
Diffusione (cartaceo ed elettronico)
50.000 copie
Tutti i diritti sono riservati;
Tutti i marchi sono registrati e di proprietà
delle relative società.

di
Gaetano
Di Blasio

Il cyber crime mette a rischio l'innovazione e gli asset aziendali

Prevista una crescita degli attacchi mirati alle imprese con vere e proprie estorsioni. La Digital Transformation richiede una sicurezza logica e fisica a 360 gradi

Il momento storico favorisce lo sviluppo di nuovi modelli di business e spinge le imprese a investire in innovazione, in parte anche grazie al piano Calenda.

È la crescita delle tecnologie "personal", che hanno portato strumenti sempre più sofisticati in mano a ogni individuo, il seme che sta germogliando la cosiddetta Digital Transformation. Le imprese stanno velocemente comprendendo quanto, per esempio grazie al cloud ma non solo, si possano ridurre i costi della tecnologia, come rendere più efficienti i processi, migliorare la relazione con i clienti, espandere le proprie attività attraverso nuovi servizi.

Tutto ciò è però messo a rischio dal costante aumento delle minacce alla sicurezza.

Gli asset aziendali digitali sono critici, perché la ricchezza dell'attuale sistema economico risiede principalmente nella proprietà intellettuale. La centralità della tecnologia, inoltre, rende impossibile per un'impresa operare senza il supporto dei sistemi informatici o senza una connessione Internet.

Ma anche lo sviluppo delle tecnologie industriali, come la robotica, e il crescente utilizzo di software nei sistemi fisici, come le automobili, pongono ulteriori rischi: è facile immaginare i danni, anche alla persona, che un grande braccio meccanico possa causare in una fabbrica se manovrato da un hacker che sia riuscito a prenderne il controllo. Ancor più facile pensare ad auto che non rispondono ai comandi dei conducenti, come già hanno rappresentato gli autori di *Fast&Furious 8*.

Questo numero di *Direction* esplora lo stato dell'arte della sicurezza logica e fisica, che sono due lati della stessa medaglia e sempre più diventeranno un singolo ambito.

Vecchie e nuove minacce mettono a rischio aziende e governi

Le analisi di Trend Micro sulla cyber security nel 2018 preannunciano il dilagare degli attacchi informatici, con nuove forme di ricatto e la crescita di "servizi" per campagne di propaganda

Il 2018 appena iniziato vedrà crescere ancora la pressione del cybercrime, con vecchie e nuove minacce, oltre quelle "reingegnerizzate". Gli oltre duemila ricercatori di Trend Micro hanno stilato le previsioni sulla sicurezza, che vede sempre più strumenti automatici sofisticati utilizzare tecnologie all'avanguardia, come il machine learning e la blockchain, per eludere i controlli e sfruttare ogni vulnerabilità.

Queste ultime sono i "buchi" del software che andrebbero "rattoppati" con le operazioni dette di patch management, sulle quali punta il dito Gastone Nencini, country manager di Trend Micro Italia: «Molti attacchi, che sono stati devastanti nel 2017, hanno sfruttato vulnerabilità conosciute e le loro conseguenze si sarebbero potute evitare se i sistemi fossero stati aggiornati preventivamente. Per questo patch management e formazione dei dipendenti devono diventare una priorità». Per questo ma non solo, aggiunge il manager, spiegando: «Abilità e risorse sono i due elementi che costituiscono l'arsenale di un aggressore che, tuttavia, non è in grado di violare la sicurezza o addirittura eseguire attacchi sofisticati senza aver prima individuato i punti deboli di un sistema. Attacchi malware massivi, furti tramite email, dispositivi compromessi e servizi interrotti richiedono tutti una vulnerabilità nella rete, sotto forma di tecnologia o persona, per poter essere attivati. Il GDPR (General Data Protection Regulation) sarà certamente un'occasione per spingere le imprese a investire nella sicurezza, ma per assurdo, teme Nencini, rappresenta un'opportunità per i cyber criminali, che potrebbero fissare il costo del riscatto, nel caso dei ransomware, basandosi sulle sanzioni previste dal regolamento europeo cui bisogna essere conformi dal 25 maggio prossimo.

Gli importi dei riscatti saranno sempre più ingenti, perché cresceranno gli attacchi di questo tipo mirati ad alcune imprese e preceduti da una fase di analisi e raccolta dati per "tarare" le richieste.

La superficie di attacco, inoltre, cresce, rimarca ancora il manager italiano, perché



Gastone Nencini, country manager di Trend Micro Italia

alle tecnologie informatiche si sommano le tecnologie operative, cioè quelle tipiche di ciascun settore, finora ritenute sicure in quanto isolate nelle fabbriche o in varie strutture, ma oggi sempre più connesse e quindi a rischio. In generale una connettività sempre maggiore porterà nuove opportunità ai cybercriminali per penetrare nelle reti aziendali.

Ci sono già stati attacchi di Denial of Service (cioè servizi Internet bloccati) che hanno sfruttato infrastrutture preposte ad altro, come le videocamere per la sorveglianza usate per trasmettere dati in massa, saturando la rete e causando danni da centinaia di milioni di dollari alle imprese dell'e-commerce.

9 miliardi di dollari sfumati per le "Business Email Compromise"

Attenzione particolare, Nencini la dedica agli attacchi BEC (Business Email Compromise), che purtroppo hanno ottenuto molti successi. Si tratta delle false email, confezionate con cura e spesso precedute da un'accurata fase di raccolta dati per colpire al momento giusto. Tipico è il caso della falsa email spedita dal Ceo al Cfo con una richiesta di effettuare un bonifico urgente. Qui la sicurezza è una questione di processi e di cultura aziendale.

Esistono anche attacchi Business Process Compromise, che cercano di sfruttare appunto i processi, in genere del reparto finanziario, modificandoli, possibilmente tramite le vulnerabilità della supply chain (la catena di fornitura). Sono stati devastanti per Target nel 2014,

ma richiedono una pianificazione a lungo termine e maggiore lavoro e in Trend Micro ritengono meno probabile che questi attacchi emergeranno nel 2018, mentre valutano che le perdite globali generate dalle truffe Business Email Compromise supereranno i 9 miliardi di dollari, dopo aver raggiunto nel 2017 i 5 miliardi.

La cyber propaganda e le fake news

In Italia si vota il 4 marzo, ma nel 2018 ci sono elezioni in diverse nazioni, compresi gli Stati Uniti: un'opportunità di mercato per i "servizi" di cyber propaganda, le cui campagne saranno perfezionate utilizzando tecniche già sperimentate con successo in precedenza. In effetti, sembra che nel dark blue siano disponibili pacchetti di cyber propaganda as a service.

Il triangolo delle fake news consiste in motivazioni su cui si basa la propaganda, i social network che servono come piattaforma per il messaggio e gli strumenti e servizi che sono impiegati per spedire il messaggio stesso.

«Nel 2018 - spiega Nencini - ci aspettiamo che la cyberpropaganda si veicoli attraverso tecniche familiari, come quelle utilizzate nel passato per diffondere lo spam tramite e-mail e il Web».

Il manager aggiunge: «Kit software fai da te, per esempio, possono eseguire spam automatizzato sui social media. Anche l'ottimizzazione del motore di ricerca Black Hat è stato adattato per l'ottimizzazione dei social media, con una base utenti di centinaia di migliaia, in grado di

fornire traffico e numeri a diverse piattaforme. Dalle e-mail spear phishing inviate ai ministeri degli Esteri all'uso plateale di documenti per screditare le autorità, al contenuto dubbio che può diffondersi liberamente e scatenare opinioni violente o addirittura proteste reali».

Azioni per la sicurezza

Dato lo scenario, gli esperti di Trend Micro suggeriscono di adottare soluzioni di cyber security per una protezione multilivello, in modo da ridurre al minimo i rischi di compromettere ogni ambito aziendale. Occorre, per questo, una visibilità su tutti i livelli, con strumenti che possano fornire rilevamento real time e protezione contro vulnerabilità e attacchi.

«Qualsiasi potenziale intrusione e compromissione degli asset verrà evitata grazie a una strategia di protezione dinamica che utilizza tecniche transgenerazionali adeguate alle varie minacce», afferma Nencini, che conclude: «È fondamentale seguire pratiche di comportamento adeguato alla sicurezza, come modificare le password predefinite, utilizzandone di complesse e uniche per i dispositivi smart, specialmente per i router; implementare la crittografia in modo da prevenire il monitoraggio e l'utilizzo dei dati non autorizzati; applicare puntualmente le patch, aggiornare il firmware alla sua versione più recente; evitare il social engineering prestando attenzione alle email ricevute e ai siti visitati in quanto potrebbero essere usati per spam, phishing, malware e attacchi mirati».





Il GDPR è alle porte, ultimi avvisi

di
Giuseppe
Saccardi

Sta scadendo il tempo concesso alle aziende per mettersi in regola, ma i motivi dei ritardi sono in parte giustificati dalla complessità e dai costi per farlo

Fatte le debite proporzioni quando si affronta il tema del GDPR alle porte (GDPR, General Data Protection Regulation) viene in mente la frase preoccupata di Tito Livio “Dum Romae consulitur, Saguntum expugnatur” (mentre a Roma si discute, Sagunto viene espugnata). E i dati, mutatis mutandis e proiettati a oggi in relazione alle normative europee riguardo la riservatezza e la protezione dei dati sensibili, e le azioni da intraprendere per mettersi in regola, sembrano dare ragione al preoccupato Livio.

Gli obiettivi del GDPR (cui dal 25 maggio di quest'anno è necessario essere conformi) sono semplici ma di non semplice attuazione. Riguardano la tutela e la uniformazione del trattamento dei dati personali all'interno dell'Unione Europea e sostituiscono la precedente Direttiva Comunitaria. Gli estensori del regolamento hanno anche voluto introdurre nuove disposizioni atte a snellire l'utilizzo e i flussi di dati personali tra gli stati membri dell'Unione e tra questi e i paesi extra-UE. In sintesi l'obiettivo del GDPR è assicurare che coloro che gestiscono dati personali procedano nella raccolta, conservazione e trasferimento in modo corretto e responsabile. Peraltro, il regolamento ha anche l'obiettivo di ridurre le lungaggini burocratiche e così facendo dare la massima priorità ai diritti delle persone e alla sicurezza dei dati.

Il GDPR: una necessità giustificata dai fatti

Va osservato che qualcosa in proposito alla sicurezza e alla riservatezza dei dati andava fatto. Secondo dati contenuti nel rapporto Clusit 2017, l'Associazione Italiana per la Sicurezza Informatica, il 2016, e non è che quello da poco chiuso sia stato poi meglio, è risultato l'anno nero per la sicurezza informatica in tutto il mondo e tra le nazioni più colpite c'è stata anche l'Italia, che è risultata tra le prime dieci per quanto riguarda gli attacchi più gravi registrati e il numero di utenti colpiti. Nutriti per la realtà italiana sono stati li attacchi ransomware, una tipologia di malware che cripta i file presenti sull'hard disk e poi chiede il pagamento di un riscatto all'utente per rimetterli in libertà.

La motivazione è semplice: le aziende nazionali sono risultate impreparate e dotate di limitate difese da questo tipo di cyber attacco e spesso hanno quindi

dovuto obbligo di abbozzare e porre mano al borsellino per poter avere di nuovo accesso a file importanti. La cosa preoccupante è che si è trattato di eventi che hanno coinvolto non solo privati o piccole aziende, ma anche enti pubblici e ospedalieri.

Il GDPR, che stringe le maglie della sicurezza, è quindi per molti aspetti un benvenuto perché mette di fronte a responsabilità e obblighi ben precisi.

suoi avversari, nelle vesti di cyber hacker, ne avevano evidentemente uno migliore.

In altri settori altrettanto strategici e in particolare nel Manufacturing e nei Servizi la percentuale delle aziende che hanno iniziato di recente ad affrontare il problema è, anche se non di molto, superiore e pari rispettivamente al 53% e al 60%.

Stante i dati riportati da IDC qualche raggio di sole riesce però a fil-

Il perché del ritardo

Viene spontaneo chiedersi a cosa sia dovuto. In proposito IDC ritiene che dipenda dalla percezione che hanno le aziende di come alcuni requisiti della nuova normativa siano vere e proprie sfide tecnologiche e organizzative. In particolare per la realtà italiana, oltre la metà delle aziende considera molto impegnativi i requisiti tecnici, per esempio l'obbligo di segnalare quando si riscontrano perdite di dati entro tre giorni, il dover implementare soluzioni di crittografia o atte a rendere anonimi i dati nonché il dover definire casi d'uso specifici nella gestione del consenso.

Ma ci sono altri aspetti che riguardano l'organizzazione che risultano molto critici e sollevano perplessità da parte delle aziende e dei loro manager. Quelli che sono ritenuti costituire la sfida maggiore, con una percentuale oltre il 60%, sono inerenti la classificazione dei dati, la sensibilizzazione dei dipendenti ai cambiamenti nelle policy di sicurezza e il dover eliminare i dati irrilevanti.

Il motivo delle preoccupazioni è sostanzialmente di tipo economico. Quelli da introdurre in azienda per ottemperare al GDPR sono cambiamenti importanti che comportano anche dei costi significativi da affrontare. Implicano il dover creare nuovi processi documentali e intervenire e cambiare le modalità di comunicazione interna e di formazione, a cui si aggiunge quanto dovrà essere fatto in tema di Identity and Access Management, per la mappatura dei dati e l'aggiornamento dei processi di back-up. ✱



La situazione delle aziende

A confermare però la sensazione di sostanziale ritardo nell'attuazione di quanto richiesto dal GDPR sono i dati riportati da IDC che indicano in un esiguo 3% la percentuale delle aziende con oltre 10 dipendenti che afferma di essere compliant, e in poco oltre il 40% quelle che hanno iniziato ad analizzare la cosa. Solo poco più del 50% ha affermato di avere un piano per la conformità. Rimane da capire cosa vuol dire avere un piano e quanto sia effettivamente efficace, perché, viene da dire, anche Napoleone la mattina di Waterloo un piano l'aveva. Ma i

trarre dalle nubi ancora abbastanza grigie. I settori strategici come il Finance e la PA si evidenziano sono quelli ove si ha un maggior tasso di compliance, rispettivamente con una percentuale del 10% e dell'8%, e anche con roadmap già definite per l'adeguamento con una rispettiva percentuale del 76% e dell'85%.

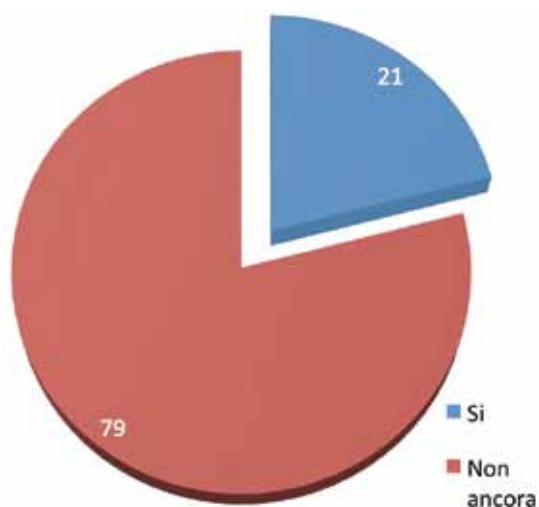
Il quadro generale di sostanziale ritardo, in alcuni settori e fasce di aziende anche molto forte, si conferma anche tra le aziende oltre i 250 dipendenti. Aspetto consolante, non solo italiane ma anche europee.

L'80% delle aziende italiane non è pronto per il GDPR

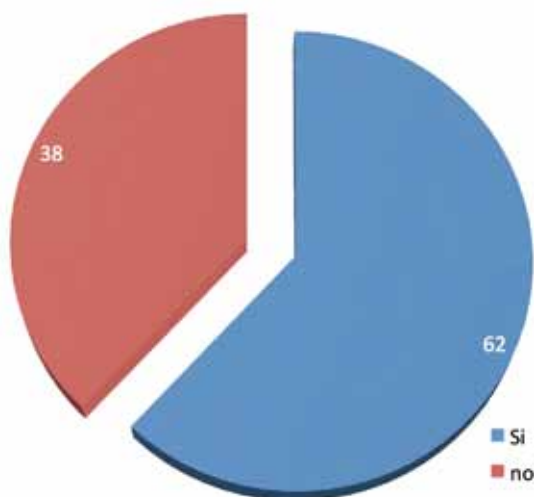
Un'inchiesta della nostra redazione ha sondato il tema della conformità al regolamento europeo e quello della spesa per la struttura dedicata alla sicurezza informatica

La General Data Protection Regulation è stata varata dall'Unione Europea nell'aprile del 2016 ed è entrata in vigore il 25 maggio dello stesso anno, fissando al 25 maggio del 2018 la data in cui avrà efficacia. In altre parole sono stati concessi due anni di tempo per mettersi in regola con la normativa. Sono rimasti poco più di quattro mesi, ma le imprese italiane non sono ancora pronte, almeno stando a una nostra inchiesta, realizzata sulla base di alcune interviste dirette e, soprattutto, un sondaggio cui hanno partecipato oltre 200 addetti ai lavori.

La tua azienda è già compliant con il GDPR?



Ritieni che il GDPR aumenterà la protezione delle imprese?



Sondaggio che non ha alcun presupposto statistico, non trattandosi di un campione significativo, né in termini numerici né quale rappresentanza dell'universo di specialisti ICT, security manager e business manager (le tre tipologie di intervistati contattati). Peraltro, i risultati ottenuti, costituiscono una base di riflessione che ci permette d'integrare le opinioni espresse da numerosi esperti, sia in seno a società di ricerca qualificate, sia presso vendor del settore ICT, specializzati in sicurezza.

Un dato che emerge è che il 79% delle imprese non è ancora pronto per il GDPR. Sappiamo bene che in Italia siamo abituati a ridurci all'ultimo momento, ma non sempre poi ci riescono le ciambelle col buco, come può testimoniare l'attuale sindaco di Milano, Giuseppe Sala, chiamato all'ultimo momento per far partire l'Expo 2015 e ora accusato di aver usato qualche scorciatoia. Meno male che è stato un successo, perché Gian Piero Ventura, ex commissario tecnico della nazionale di calcio, non può nemmeno consolarsi dell'esito finale. Ad andarci di mezzo è stato anche il suo "capo" Carlo Tavecchio, costretto alle dimissioni dalla presidenza della Federazione Italiana Giuoco Calcio.

Rischi che corrono anche dirigenti delle imprese che non saranno conformi al GDPR in tempo.

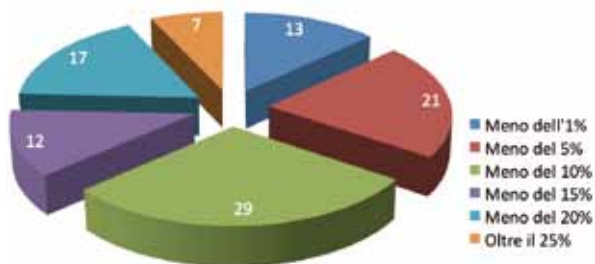
Purtroppo in molti hanno ritenuto il 25 maggio prossimo, come la data in cui cominciare a realizzare il piano per la sicurezza e adeguarsi alle nuove norme. Di fatto, invece, è il giorno in cui potrebbero arrivare le prime ispezioni.

Molti degli esperti con cui abbiamo parlato (taluni presenti nelle prossime pagine) sono convinti che la corsa alla compliance partirà veramente solo dopo che floccheranno le prime multe.

Un aspetto importante è la possibilità di "scaricare" parte della responsabilità a una società esterna. Un vantaggio per chi già utilizza servizi di terze parti per la sicurezza, cioè il 38% dei rispondenti.

Un dato positivo, invece è il punteggio maggiore ottenuto dalla sicurezza nella scelta di un cloud provider, mentre il costo è l'ultima delle preoccupazioni. ❁

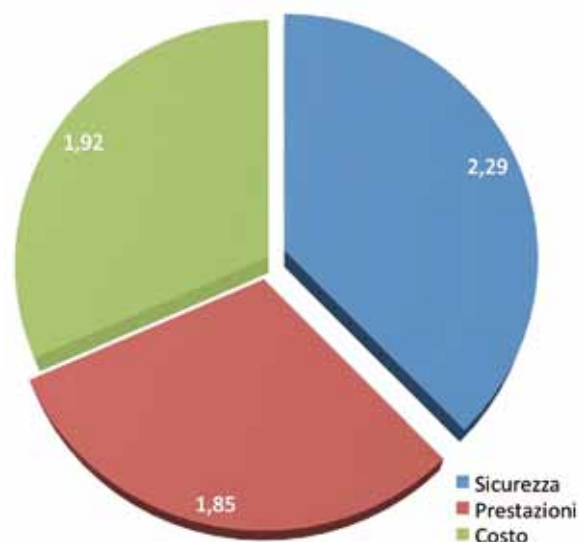
Quale percentuale del budget ICT dedichi alla cyber security?



La gestione della cyber security nella tua azienda è tutta interna o in parte in outsourcing?



Nella scelta del cloud provider in quale ordine hai considerato la sicurezza, le prestazioni e il costo (mettiti in ordine da 1 a 3 dove 1 è quello considerato il più importante).



Più sicurezza per i manager automatizzando la protezione degli account

Proteggere le credenziali è un punto chiave per la sicurezza degli utenti privilegiati, sia on-premise sia nel cloud. A garantirla ci ha pensato CyberArk

Per garantire la sicurezza degli account privilegiati CyberArk, società specializzata nella protezione ad alto livello di utenti business critici per le aziende, ha inglobato nel suo portfolio numerosi sviluppi che accelerano l'adozione di soluzioni di sicurezza che si posizionano tra quelle più avanzate disponibili sul mercato. Le funzionalità hanno l'obiettivo di rendere più semplici le modalità necessarie per rafforzare la sicurezza, migliorare l'automazione dei processi di security e ridurre il rischio complessivo in cui possono incorrere gli utenti privilegiati.

Nel loro insieme, evidenzia CyberArk, fanno di CyberArk Privileged Account Security Solution V10 (CyberArk V10) una piattaforma di sicurezza che può scalare in funzionalità al fine di proteggere da exploit critici gli account privilegiati ovunque si trovino, sia quando utilizzano infrastrutture ICT on-premise che quando accedono ad applicazioni e dati tramite cloud o attraverso workflow DevOps.

Accelerazione dei processi di sicurezza

Un punto chiave di CyberArk v10 è quello di accelerare fortemente il deployment di una soluzione di sicurezza e semplificare i processi di protezione degli account privilegiati. L'obiettivo è perseguito tramite:

- **User experience snella:** gli aggiornamenti apportati con la V10 hanno perseguito l'obiettivo di ridurre di un ordine di grandezza il tempo che deve essere dedicato per garantire la protezione dei privileged account e allo stesso tempo ridurre di un fattore 5 l'impegno dedicato dagli auditor IT nell'analisi delle registrazioni delle sessioni. La user interface semplifica anche i workflow, visualizza i rischi,



monitorizza le attività privilegiate ed è compliant con quanto prescritto da policy e Audit.

• **Strategia Customer-Driven basata su API:** Si basa su API funzionalmente estese che permettono di accelerare l'integrazione della soluzione CyberArk Privileged Account Security all'interno dell'architettura di sicurezza esistente, delle Operation e degli strumenti DevOps. Ad esempio, nuove REST API danno la possibilità all'IT di ridurre di sino al 90% il tempo necessario



per inserire nel sistema di sicurezza gli account, un aspetto critico in aziende di ampie dimensioni che devono distribuire la sicurezza a migliaia di utenti contemporaneamente.

Machine learning per una protezione ubiqua delle credenziali

La crescente mobilità di personale e manager che costituiscono account privilegiati e l'utilizzo di reti mobili e cloud pone il problema di come proteggere le credenziali in contesti

ad alto rischio, sia per le carenze nei criteri di security che possono essere native delle reti o del cloud pubblico, sia dell'ambiente pubblico in cui l'account privilegiato fisicamente si muove. Credenziali non adeguatamente protette costituiscono un target molto attraente per gli attaccanti esterni o per malintenzionati interni all'azienda stessa. Si tratta di rischi che sono amplificati per quelle aziende che hanno fatto del cloud la loro strategia di digital transformation e hanno allo stesso tempo accelerato l'adozione di DevOps.

Indipendentemente dalle dimensioni dell'azienda, le nuove funzionalità presenti nella versione V10 di CyberArk Privileged Account Security Solution sono volte a permettere di:

• **Prevenire l'attacco ad account privilegiati sugli Endpoint:** Gli end-point costituiscono uno dei punti maggiormente critici per la sicurezza, soprattutto per la crescente mobilità degli utenti privilegiati. Per eliminare il rischio connesso alla perdita di dati o credenziali, CyberArk ha sviluppato CyberArk Endpoint Privilege Manager, una soluzione che ha il compito di bloccare e contenere attacchi dannosi proteggendo l'end-point da exploit che mirano alle credenziali privilegiate. In pratica, tramite le funzionalità contenute in CyberArk Application Risk Analysis Service si ha la possibilità, mediante funzioni di machine learning e analitiche basate su cloud, di aiutare a bloccare gli attaccanti e impedire, rilevando le applicazioni potenzialmente dannose e in grado di accedere a

dati e informazioni sensibili, che questi possano posizionarsi in un end-point.

• **Accelerare la sicurezza nel cloud:** V10 estende il supporto per Amazon Web Services (AWS), automatizza il caricamento delle credenziali tramite l'integrazione con CloudWatch e Auto Scaling. In pratica, viene ridotto significativamente il rischio di credenziali non gestite in ambienti di elastic computing e il team dedicato alla sicurezza ha la possibilità di ridurre sensibilmente il tempo che vi deve dedicare in modo da potersi meglio focalizzare sulla mitigazione dei potenziali rischi. CyberArk garantisce anche la sicurezza delle credenziali attraverso piattaforme cloud pubbliche quali AWS, Microsoft Azure e Google Cloud Platform (GCP) ed ha validato la sua capacità di attivare la sicurezza per account privilegiati su AWS in un massimo di 15 minuti.

Per quanto riguarda il cloud e le funzionalità di CyberArk Privileged Account Security Solution v10 relativamente alla Google Cloud Platform (GCP), la tipica configurazione GCP comprende l'esecuzione delle vault primarie e di disaster recovery, nonché il monitoraggio della sessione in modo da rendere sicuro il workload che gira in un ambiente nativo GCP.

L'organizzazione aziendale può, in alternativa, estendere la propria installazione di CyberArk (ad esempio che gira su piattaforma on-premise, AWS o Azure) in modo che possa aiutare nel rendere sicuro anche l'accesso alla console GCP e a renderne sicuri i relativi workload. *

L'automazione riduce i rischi aziendali

di
Gaetano
Di Blasio

Il management investe ancora poco in sicurezza, ma le reti "Intent-Based" di Fortinet si proteggono da sole

Secundo una recente ricerca commissionata da Fortinet, specialista della network security, quasi la metà dei decision maker appartenenti al dipartimento IT in aziende di tutto il mondo, con oltre 250 dipendenti, ritiene ancora che il management non veda nella cyber security una priorità assoluta, né un'area d'interesse, nonostante continuino a verificarsi attacchi informatici di alto profilo.

Le minacce, peraltro, continuano ad aumentare d'intensità, forse anche a causa di questo atteggiamento, infatti Filippo Monticelli, regional director Italy in Fortinet, riporta: «Il nostro Global Threat Landscape Report mette in evidenza come una scarsa attenzione alle pratiche di sicurezza informatica e l'utilizzo di applicazioni rischiose consentano ad attacchi distruttivi worm-like di sfruttare gli exploit a velocità record. I criminali impiegano meno tempo a sviluppare nuove modalità d'intrusione, concentrandosi invece sull'uso di strumenti automatici e intent-based per insinuarsi con un maggiore impatto sulla continuità del business».

Il manager italiano, aggiunge, però: «Negli anni abbiamo visto come la cyber security sia diventata un investimento fondamentale per le aziende, dove un numero crescente di manager di alto profilo la considerano parte integrante della propria strategia IT».

Oggi siamo quindi in una fase per certi versi transitoria, con il 44% dei decision maker IT italiani, il quale ritiene che la sicurezza informatica non rappresenti ancora una priorità assoluta per il consiglio di amministrazione. Ma ciò non sembra avere un impatto sui budget, dato che il 53% delle aziende dichiara di aver investito addirittura oltre il 10% del proprio budget IT in sicurezza, in aumento dallo scorso anno per il 72% degli intervistati.

Inoltre i manager, per il 79%, sono convinti che la cyber security diverrà una priorità assoluta. Una tendenza guidata, secondo i rispondenti italiani, da tre fattori chiave:

- Aumento di security breach e attacchi informatici a livello globale, che ha influenzato il 48% delle aziende, soprattutto dopo attacchi globali come WannaCry.
- Maggiore pressione dai regolamenti, soprattutto per il rischio delle pesanti sanzioni previste dal GDPR.
- Migrazione verso il cloud nell'ambito del proprio percorso di trasformazione digitale, che spinge a investire in sicurezza il 77% delle imprese, con 83% degli intervistati che indica in come priorità assoluta la cloud security nei prossimi 12 mesi.



*Filippo Monticelli,
regional director Italy di
Fortinet*

La sicurezza automatica con il Security Fabric

Fortinet ha investito da tempo nello sviluppo di sistemi in grado di correlare tutti i dati raccolti dagli strumenti presenti sulla rete aziendale, affinché questi possano intervenire automaticamente quando rilevano attività che potenzialmente nascondono una minaccia. Oggi il Fortinet Security Fabric è un elemento chiave di una strategia di Intent-Based Network Security caratterizzata da funzionalità avanzate di automazione quali self-provisioning, self-operating e self-correcting.

Le reti "Intent-Based" sono nate nell'intento, appunto, di svolgere al meglio i servizi che s'intendono realizzare, in pratica per supportare la digital transformation e aumentare l'agilità della rete, incrementando al contempo affidabilità e

disponibilità.

La crescente complessità delle reti, da un lato, la carenza delle competenze (progettazione, implementazione e operatività) dall'altro e la necessità di gestire processi sempre più in tempo reale, praticamente obbligano a un'automazione sempre più spinta.

A complemento delle tecnologie di rete specifiche, la vision di Fortinet è di fornire alle reti Intent-Based una sicurezza che permetterà al Security Fabric di tradurre automaticamente le necessità di business in azioni per la sicurezza di rete sincronizzate senza intervento umano. A detta dei responsabili di Fortinet, ciò consentirà di progettare architetture di sicurezza avanzate, ma più semplici da gestire riducendo gli oneri operativi, fino a fornire infrastrutture tecnologiche

in gran parte autosufficienti, capaci di mantenere una posizione di sicurezza ottimale su tutta la superficie di attacco.

L'automazione del Security Fabric è anche la chiave per un futuro sicuro per l'IoT, affermano sempre in Fortinet, evidenziando l'onerosità di analisi in un tale contesto, impossibile da gestire senza automazione. Il Security Fabric è anche la risposta alle preoccupazioni, espresse in recente studio di ESG Research da un 62% di professionisti della cybersecurity, circa la difficoltà a ottenere lo stesso livello di visibilità sui workload che si trovano nel cloud, rispetto a quelli nel reti fisiche. Così come fornisce una soluzione al 56% dello stesso campione che non ha livelli appropriati per l'automazione e orchestrazione necessari per il cloud. ❁

Il Global Threat Landscape Report di Fortinet

La ricerca, effettuata dagli esperti del FortiGuard Labs di Fortinet su base trimestrale, evidenzia come una scarsa attenzione alle pratiche di sicurezza informatica e l'utilizzo di applicazioni rischiose facilitano lo sviluppo di nuove modalità d'intrusione. Di seguito alcuni elementi di riflessione.

Attacchi disastrosi, come WannaCry e NotPetya, resi noti dalle cronache e appartenenti alla categoria dei worm-like, non sarebbero stati neanche realizzati se le imprese avessero una buona gestione della sicurezza, mantenendo aggiornati i sistemi e applicando le patch, spiegano gli esperti dei FortiGuard Labs.

A parte le modalità di diffusione, il ransomware che approfitta delle vulnerabilità è comunque in crescita: il 90% delle organizzazioni ha registrato exploit su vulnerabilità vecchie di tre o più anni. Anche dopo dieci o più anni dalla scoperta di una falla, il 60% delle imprese registra ancora attacchi correlati.

Le minacce automatizzate non si riposano mai: quasi il 44% di tutti i tentativi di attacco si sono verificati il sabato o la domenica. Il volume medio giornaliero nei fine settimana è stato il doppio dei giorni feriali.

I cybercriminali sono pronti a sfruttare debolezze o opportunità legate a nuove tecnologie o servizi. In particolare, l'uso di software di estrazione non aziendale e la vulnerabilità dei dispositivi IoT su reti iperconnesse rappresentano un rischio potenziale se non gestiti correttamente.

La crittografia del traffico Web, in forte crescita, anche se è un bene per la privacy e la sicurezza su Internet, crea problemi a molti strumenti di difesa, che hanno scarsa visibilità su comunicazioni crittografate.

Le applicazioni non sicure, come il peer-to-peer, creano vettori di rischio: le aziende che le consentono registrano botnet e malware sette volte più numerosi rispetto a quelle che non le consentono.

Analogamente, le aziende che consentono applicazioni proxy denunciano una presenza di botnet e malware quasi nove volte superiore rispetto a quelle che non le consentono.

Quasi un'organizzazione su cinque ha registrato un malware destinato ai dispositivi mobili, mentre quelli IoT sono una sfida perché non hanno il livello di controllo, visibilità e protezione dei sistemi tradizionali.

Come garantire la sicurezza dei Container

di
Giuseppe
Saccardi

Un Container può agire come punto di diffusione per attacchi cibernetici.
Come evitare questo rischio

I container rappresentano la componente di una architettura per i dati che permette di rendere le applicazioni più portatili tra ambienti di sviluppo, test e produzione. In sostanza, aiutano a semplificare gli sviluppi del software e a risparmiare tempo, e di conseguenza costi di sviluppo.

Proprio per la loro portabilità e il fatto che contengano in un unico contenitore tutto quanto relativo a uno specifico progetto o attività di business, ne risulta un aumento dei rischi connessi alla sicurezza. “Smarrire” o aprire la strada a un cyber criminale a un intero container non è come perderne una limitata parte. In proposito un recente studio Forrester ha rivelato che il 53% dei decision-maker IT ha identificato la sicurezza come principale freno all'adozione dei container. Le aziende che intendono adottarli dovrebbero quindi guardare attentamente al modo in cui garantirne la sicurezza, focalizzandosi su provenienza, contenuto, isolamento e fiducia.

Certificare e ispezionare il Container

La prudenza si impone. Oltre il 30% delle immagini ufficiali su Docker Hub, contengono vulnerabilità importanti secondo uno studio di BanyanOps. La certificazione con firme digitali, per esempio, aggiunge un livello di sicurezza confermando chi ha creato il container e a quale scopo.

Per aumentare la sicurezza società leader di mercato stanno lavorando per stabilire standard e practice per la certificazione dei container in modo da garantire che:

- Tutti i componenti provengono da fonti fidate.
- I container host non siano stati manomessi e siano aggiornati.
- L'immagine container non presenti vulnerabilità note nei component della piattaforma e nei suoi livelli.
- I container siano compatibili e operino in ambienti ospitanti certificati.

Verificare da dove viene un container è quindi importante, ma analizzare quello che c'è dentro l'immagine del container lo è ancora di più.



Come la deep packet inspection studia i pacchetti che viaggiano in rete alla ricerca di contenuti malevoli, così la Deep Container Inspection (DCI) guarda il contenuto. Avere visibilità sul codice all'interno del container è fondamentale per mantenere la sicurezza durante e dopo lo sviluppo.



Isolare per mettere al sicuro il business

Una volta che le applicazioni container-based sono composte da container sicuri, bisogna assicurarsi che non vengano compromessi da altre immagini container sullo stesso host. La realtà è che i container non contengono veramente delle applicazioni, è più corretto dire che i container pacchettizzano il codice di un'applicazione con le sue dipendenze.

Se si pensa ai container come a oggetti con delle pareti, si deve essere consapevoli che sono estremamente sottili. I contenuti malevoli in un container possono passare a un

altro o al sistema operativo host. Ogni singolo processo che gira all'interno di un container parla direttamente con l'host kernel e per tutti i container su quell'host. Il kernel può in sostanza fungere da single point of failure. Una vulnerabilità all'interno del kernel Linux potrebbe permettere a coloro che accedono a un container di impossessarsi dell'host OS e di tutti gli altri container sull'host.

Per questo è fondamentale affidarsi a un host OS che venga mantenuto da kernel engineer e che sia aggiornato frequentemente con i più recenti fix di sicurezza. I container basati su host deboli ereditano il modello di sicurezza compromesso di quell'host. Il kernel deve includere funzionalità che offrono livelli di isolamento e separazione appropriati come SELinux, Seccomp, Namespaces, e altri.

La variabile tempo gioca contro

Un'altra variabile che va considerata è quella temporale. Se nell'istante t zero l'applicazione container-based viene messa in produzione, cosa succede il giorno uno? Il giorno due? Nuove vulnerabilità vengono identificate quotidianamente e l'immagine container è sicura come il codice e le dipendenze che contiene. Ma di vulnerabilità ne è sufficiente una per compromettere il container e, potenzialmente, l'intero stack infrastrutturale.

Quello che ne deriva è che anche i container e i loro host devono

essere gestiti durante l'intero ciclo di vita. Le aziende necessitano quindi di tooling policy-driven che automatizzi la gestione di versioni e upgrade, identità e accessi, sicurezza e prestazioni.

Come fare per mitigare il rischio

Anche se velocità e agilità rappresentano driver fondamentali per l'adozione dei container in azienda, non devono essere integrati a spese della sicurezza. Ecco perché una Deep Container Inspection di classe enterprise, associata a certificazioni, policy e fiducia è parte integrante dello sviluppo, deployment e gestione dei container. In sostanza, suggerisco gli operatori del settore, per trarre il massimo vantaggio dai container pur garantendo la sicurezza di questi ultimi e dei loro contenuti, l'azienda deve trovare modi più efficaci per determinarne:

- **Provenienza.** Prima di spostare un container in rete, accertarsi di sapere cosa contiene e dove ha avuto origine, nonché analizzare la tecnologia di validazione e le certificazioni relative alle fonti.
- **Isolamento.** Considerare l'isolamento del percorso di esecuzione del container e, in ambienti multi-tenant, valutare l'associazione di container con la virtualizzazione per disporre uno strato di sicurezza aggiuntivo.

Come evidenziato, non si deve poi trascurare di ispezionare regolarmente i contenuti dei container per ridurre eventuali rischi alla sicurezza per identificare ed eliminare le vulnerabilità. *

Endpoint al sicuro con l'intelligenza artificiale e il blocco comportamentale

Le funzionalità di Protection Service for Business di F-Secure migliorano le capacità di blocco comportamentale per Windows e Mac e difendono dalle nuove minacce

F-Secure, società che sviluppa soluzioni per la cyber security, ha annunciato il potenziamento della sua suite per la sicurezza degli endpoint, Protection Service for Business, una soluzione di sicurezza basata su cloud. La nuova versione è stata sviluppata per migliorare la propria tecnologia di protezione degli endpoint aggiungendovi capacità di blocco comportamentale per Windows e Mac in modo da proteggere contro le minacce usate dagli attaccanti.

Protection Service for Business, ha evidenziato l'azienda, comprende la tecnologia XFENCE, che la società ha annunciato lo scorso aprile, e ora ne ha integrato le capacità in Computer Protection for Macs.

F-Secure XFENCE evita che processi e applicazioni abbiano accesso ai file, ai dati, e anche a microfoni, tastiere, e webcam senza il permesso dell'utente.

Fondamentalmente agisce come un firewall per file evitando, per esempio, che il ransomware crittografi file sui dispositivi infettati. La nuova release include numerosi aggiornamenti, tra cui:

- Un motore di rilevazione su base comportamentale per Windows, DeepGuard di F-Secure che include un uso estensivo dell'intelligenza artificiale per prendere decisioni su file e processi malevoli senza chiedere nulla agli utenti.
- Un firewall aggiornato con una maggior compatibilità con applicazioni e appliance di terze parti, nonché un set di regole per contrastare le minacce come ad esempio quelle ransomware auto-propaganti e a movimento laterale.
- Una gestione dei profili che facilita la schedulazione delle scansioni, il profile grouping, il product filtering.
- Una funzionalità di Device Control che impedisce l'uso di hardware non autorizzato come chiavette USB, hard disk esterni e webcam.



*Mikko Hypponen, Chief
Research Officer di
F-Secure*

Un portfolio per la security riconosciuto da Gartner

L'offerta attuale di protezione per gli endpoint cloud-based Protection Service for Business si affianca a Business Suite, una soluzione per la sicurezza on-premise anch'essa erogante capacità di protezione basate sul comportamento.

Entrambe le soluzioni, tramite numerosi miglioramenti funzionali apportati nell'ultimo anno, permettono di affrontare i punti deboli delle organizzazioni in fatto di cyber security e assicurano la protezione dalle minacce più recenti.

A Protection Service for Business, per esempio, è stato aggiunto DataGuard, una funzione che fornisce un livello ulteriore di protezione contro minacce come il ransomware; una nuova funzione di protezione delle password che rende semplice usare password forti e univoche per le organizzazioni; e un'architettura software migliorata che permette a F-Secure di sviluppare e implementare rapidamente aggiornamenti o nuove funzionalità.

A questo si aggiunge nel portfolio F-Secure anche una soluzione di rilevazione e risposta (detection and response) chiamata Rapid Detection Service.

L'approccio alla cyber security adottato da F-Secure e centrato sull'analisi comportamentale e sull'intelligenza artificiale è stato riconosciuto da Gartner, che l'ha posizionata come Visionaria nel report Magic Quadrant 2018 per le Piattaforme di Protezione Endpoint.

Protezione degli end-point e IoT

La sicurezza degli end-point vede F-Secure impegnata anche nel segmento in forte evoluzione dell'IoT.

L'Internet of Things (IoT) così come la si conosce, osserva F-Secure, apre forti opportunità per quanto concerne la digital transformation e l'evoluzione verso una smart economy ma, di fatto, rappresenta una minaccia considerevole per i consumatori a causa di regolamenti inadeguati sulla sicurezza e sulla privacy.

Questo è quanto evidenziano e su cui mettono in guardia gli esperti intervistati nella realizzazione del report "Internet of Things: Pinning down the IoT" sponsorizzato da F-Secure.

Milioni di dispositivi end-point e connessi in rete o via cloud, evidenzia F-Secure, sono già stati compromessi per essere usati come parte della botnet Mirai. E non sono pochi i produttori che immettono prodotti velocemente sul mercato senza prendere in considerazione i requisiti e le impostazioni minime di sicurezza. Anche se milioni di nuovi dispositivi si connettono online ogni giorno, gli utenti non sono poi ancora generalmente consapevoli che i loro nuovi apparati "intelligenti" andranno online.

«Col tempo quasi tutti i dispositivi domestici saranno online e non

sembreranno dispositivi intelligenti all'utente finale. Sembreranno dispositivi stupidi, ma saranno in realtà intelligenti pur non offrendo alcuna funzionalità al consumatore finale, perché il vero motivo per cui andranno online sarà per riferire e riportare dati al produttore che li ha costruiti», mette in guardia nel report Mikko Hypponen, Chief Research Officer di F-Secure evidenziano la necessità di proteggere e controllare adeguatamente gli end point, di qualsiasi tipo si tratti.

La prova dell'assunto di Hypponen è semplice: già oggi è difficile trovare un modello di un qualsiasi dispositivo, per esempio un televisore, che non supporti la connessione a Internet.

La realtà, evidenzia F-Secure, è che in breve tempo miliardi di dispositivi saran-

no potenziali punti di attacco alla sicurezza e le aziende sembrano ignorare il problema, e sino a che gli utenti non inizieranno a chiedere che questi dispositivi siano anche sicuri i produttori difficilmente considereranno la sicurezza come una priorità.

F-Secure è attivamente impegnata nel garantire la sicurezza degli end-point, ma la loro parte devono farla anche i governi, che devono preoccuparsi della qualità della tecnologia che viene messa nelle mani e nelle case degli utenti, si osserva nel report. *



Un perimetro digitale per proteggere l'impresa

di
Gaetano
Di Blasio

La ricetta per proteggere il business e la reputazione delle aziende nell'era del cloud ibrido

Nuove e sempre più sofisticate minacce, un perimetro aziendale che per effetto della trasformazione digitale assume confini meno definiti e quindi più difficili da proteggere, una graduale migrazione dei workload dalla rete locale al cloud, regolamenti comunitari (come il GDPR) che richiedono l'adozione di misure di sicurezza ben oltre l'ambito prettamente tecnologico: sono questi solo alcuni dei principali problemi delle aziende italiane, a cavallo tra l'esigenza di crescere nel competitivo scenario internazionale e il rischio costante di vedere messa a repentaglio la propria immagine e la sicurezza dei dati critici per il proprio business e per quello dei clienti. Per contrastare queste e altre minacce in costante evoluzione senza rinunciare ai benefici della trasformazione digitale, le imprese devono adottare nuovi paradigmi di cybersecurity basati su sistemi, architetture e modelli che tengano in considerazione l'evoluzione del mondo IT. In base a una recente survey, l'83% dei CIO, CISO e IT Executive ritiene che la complessità delle infrastrutture IT tradizionali non rappresenti soltanto un problema per il business, ma introduca anche un considerevole rischio di sicurezza.

«Sebbene tuttora in atto, la Digital Trasformation ha già modificato in maniera significativa i connotati delle imprese. Ciò che un tempo era un'eccezione, ovvero la presenza di lavoratori mobili, l'utilizzo di device personali per l'accesso a dati aziendali, la fruizione di servizi cloud e così via, è diventato ormai una regola e la Security non può che adeguarsi al nuovo scenario» evidenzia David Cenciotti, Sales Engineer e Security Evangelist di Citrix.

Con l'avvento del cloud, dello smart working e l'imminente proliferazione dei device IoT (Internet of Things) è dunque necessario cambiare approccio: occorre definire un nuovo perimetro digitale di sicurezza e gestire il cyber risk in un ambiente ibrido, in cui l'utente accede in mobilità, da qualsiasi rete e con qualsiasi device ad applicazioni e dati che possono essere situati ovunque, all'interno di un datacenter o nella "nuvola". «In tale scenario, il posto di lavoro non è più un luogo ben preciso, ma una configurazione che assume caratteristiche differenti a seconda del "contesto". Facciamo un esempio molto semplice: si consideri un utente che deve accedere a un'applicazione aziendale. Se l'utente si collega da un hotspot pubblico all'interno di un aeroporto, ovvero da un ambiente non presidiato dove il rischio di sicurezza è più elevato, dovrà superare uno o più step di autenticazione supplementari e avrà l'accesso limitato a un sottoinsieme di applicazioni



David Cenciotti, Sales Engineer e Security Evangelist di Citrix Systems

rispetto al dipendente che accede dalla sede aziendale e che lo potrà fare autenticandosi una sola volta. Parliamo quindi di "Secure Digital Workspace", ovvero di uno spazio di lavoro virtuale, che segue l'utente e adatta le misure di sicurezza al contesto di accesso. È un modo per garantire la sicurezza rendendo la security "sostenibile", cioè senza inficiare la fruibilità dell'applicazione».

In questo modo, un "perimetro digitale sicuro" consente di applicare un approccio centralizzato basato sull'identità, ma anche di cambiare molto rapidamente e dinamicamente le policy aziendali.

Si possono scegliere impostazioni diverse per chi si collega al cloud, dall'ufficio o da un'altra postazione ritenuta sicura e per chi invece si connette da un hot spot pubblico in un aeroporto o da un albergo.

Location, dispositivo usato (e caratteristiche specifiche dello stesso), applicazione richiesta e comportamento dell'utente sono tutti elementi utilizzabili per variare le condizioni di accesso e uso delle applicazioni e dei servizi aziendali. Sono dati, infatti, che permettono di definire una "postura" di sicurezza attorno alla quale applicare le regole aziendali.

Ma non solo. Uno degli aspetti più importanti del nuovo paradigma di sicurezza Citrix è rappresentato dall'utilizzo di strumenti di analisi predittiva che consentono la rilevazione degli attacchi e l'adozione di contromisure in maniera automatizzata. Per contrastare in maniera efficace le minacce più evolute è infatti necessario acquisire quella

che gli esperti Citrix definiscono "Information Superiority", ovvero una superiorità informativa basata sulla conoscenza di quanto accade all'interno e all'esterno del Secure Digital Perimeter e tradurla, grazie a logiche di Machine Learning, in capacità di scoperta di attacchi che si nascondono nel "rumore di fondo" della normale operatività o che si sviluppano in intervalli temporali molto ampi.

Gli elementi Secure Digital Perimeter

Il Secure Digital Perimeter è un modello che semplifica l'erogazione di applicazioni su qualsiasi device, garantendo una security a 360 gradi, attiva, reattiva e predittiva attraverso strumenti di analytics che permettono di estendere il controllo anche nel cloud.

I mattoni di questo modello, ci spiega Cenciotti, sono:

- **La Virtualizzazione delle sessioni**, ovvero l'esecuzione centralizzata delle applicazioni, indifferentemente da luogo, rete e dispositivo, grazie a un app store dal quale viene lanciata l'applicazione.
- **L'Application Delivery Controller**, vero front-end

dell'applicazione virtualizzata, che implementa le policy di autenticazione, security e ottimizzazione e che pubblica l'app store, disaccoppiando l'utente dalla risorsa acceduta

- **L'SD-WAN** è la tecnologia usata per ottimizzare le prestazioni per gli utenti remoti, potendo realizzare anche un'infrastruttura hybrid cloud, interfacciandosi con i provider.
- **Il Mobile Store** che controlla le applicazioni installate sui sistemi mobile in uno scenario BYOD (Bring Your Own Device)
- **L'Analytics Service**, cioè la componente essenziale per la gestione dell'architettura, basata su algoritmi di machine learning e Big Data analysis, per fornire la massima visibilità agli IT manager sull'intero ambiente con tracciamento delle irregolarità nel comportamento degli utenti.

• **Management Plane**, ovvero lo strato di management, per effettuare le configurazioni di tutta l'architettura.

E la cosa interessante è che ognuno di questi componenti è disponibile sia on-premise (ovvero localmente) che direttamente sul Cloud di Citrix.



Come mettere al sicuro le infrastrutture e i sistemi industriali

Dalle smart grid ai trasporti, dai servizi pubblici all'IoT niente è più al sicuro. Proteggerli e garantirne la disponibilità è il compito che si è assunto Selta

Il diffondersi della trasformazione digitale, l'evoluzione verso l'Industry 4.0 e la realizzazione di infrastrutture e servizi pubblici a forte automazione, sta ponendo all'attenzione di manager e autorità pubbliche il problema di come proteggere adeguatamente infrastrutture, fabbriche e servizi, che per loro natura devono essere sempre operativi e a prova di attacchi cibernetici.

Se realizzare soluzioni di protezione per l'end user, il suo pc, lo smartphone o il tablet, è relativamente semplice e le soluzioni sul mercato non mancano, ben diverso si presenta il problema quando si tratta di garantire la sicurezza di impianti e servizi pubblici primari perché, evidenzia Selta, azienda italiana specializzata nello sviluppo di soluzioni per infrastrutture critiche, questo richiede una forte esperienza impiantistica nel settore e nei relativi standard, dallo SCADA all'IoT, nonché dei dispositivi connessi.

«Selta è nata 45 anni fa nel settore dell'automazione energetica, poi si è espansa alle Tlc tradizionali. Tutto quello che è il mondo dell'IoT e dell'automazione è quindi un mondo che percorre da decenni. Da molti anni si occupa di data security, prima ancor che si chiamasse così e quindi per noi unire le nostre varie anime è stato piuttosto semplice. Ora Selta è proiettata nel mercato della creazione di prodotti e la fornitura di servizi per le infrastrutture critiche nazionali, che non vuol dire solo crearle ma anche metterle in sicurezza, che sono due cose indivisibili. Sono soluzioni innovative e soprattutto progettate in Italia nei nostri due centri di R&D perché, anche se farlo nel nostro paese è complicato e costoso, riteniamo che per quanto riguarda le infrastrutture critiche che realizziamo in Italia e all'estero la progettazione fatta e certificata in Italia, sia intrinsecamente più sicura», ha evidenziato Gianluca Attura, AD di Selta.



Gianluca Attura,
Amministratore Delegato
di Selta

Infrastrutture critiche, SCADA e IoT al sicuro con la tecnologia italiana

I settori di interesse e in cui Selta opera sono tipicamente quelli infrastrutturali. Le soluzioni che sviluppa trovano applicazione nella sicurezza ed efficienza di impianti critici per l'economia nazionale e il

anche la business continuity e il disaster recovery.

«Per quanto concerne l'offerta di Selta, a partire dai sistemi di automazione energetica, sviluppiamo soluzioni che mettono in sicurezza le infrastrutture critiche, consentono l'applicazione di protocolli di sicurezza internazionali, sistemi di

telecomunicazioni cifrati, eccetera. amo però molto enti e preoccupa-

Le soluzioni Selta mettono SCADA al sicuro



benessere dei cittadini. Tra queste: embedded cyber security per settori quali i trasporti e i servizi di telecomunicazioni; l'accesso sicuro a reti ultrabroadband di service provider; la sicurezza di soluzioni UCC/IoT in ambienti cloud e on-premise pubblici e privati; la sicurezza di ambienti governativi e della difesa. Uno dei settori su cui si sono concentrati gli sviluppi della società è quello dell'IoT e delle soluzioni SCADA, alla base dell'Industry 4.0. La interconnessione in rete di apparati e impianti industriali e la diffusione di dispositivi IoT, se migliora produzione e time to market, apre però la strada ad attacchi potenzialmente disastrosi. Basandosi sull'esperienza acquisita negli anni nel settore industriale, Selta ha sviluppato soluzioni e servizi specifici per la protezione ad alto livello di ambienti SCADA, in modo da garantirne non solo la protezione ma

ti per l'estensione del mondo dell'IoT, perché si è sviluppato in maniera disorganica e insicura. Basti pensare che esistono nove famiglie di protocolli principali, più una infinità di sotto protocolli; uno scenario che apre enormi falle nella sicurezza. Così come siamo preoccupati per i sistemi SCADA e siccome SCADA è alla base di grandi infrastrutture critiche, il compito che ci siamo assunti è di operare al fine di creare attorno al mondo SCADA una bolla di sicurezza che permetta di filtrare eventuali attacchi. In un mondo dove la tecnologia ha preso il sopravvento dobbiamo fare il possibile affinché la sua diffusione sia messa sotto controllo», ha osservato Attura.

La cyber security inizia dall'uomo

L'approccio alla Cyber Security si articola, nella strategia di Selta, in due direzioni complementari: lo

sviluppo di soluzioni e la fornitura di servizi di sicurezza.

Il portfolio di prodotti comprende soluzioni per la protezione dell'ambiente di lavoro, la gestione di dati classificati o non classificati, sistemi anti intercettazione (protezione da intercettazioni realizzate tramite emissioni elettromagnetiche del computer). Ampio è parimenti il portfolio dei servizi. Comprende servizi di consulenza professionale nella progettazione di reti sicure, l'analisi delle vulnerabilità, assessment, cybersecurity e crittografia, la gestione a più livelli di dati classificati, soluzioni di disaster recovery.

Per chi desidera esternalizzare del tutto la complessità della Cyber Security Selta fornisce soluzioni per l'erogazione di servizi di gestione dal centro. Ma in definitiva, mette in guardia Attura, il problema è nell'essere umano.

«Il problema della Cyber Security è principalmente un problema umano, non di infrastrutture tecnologiche. Gli attacchi avvengono perché all'interno delle aziende ci sono uomini. Quindi si deve partire da una grande campagna di informazione e sensibilizzazione, oltre che dalla definizione di architetture segmentabili in modo che l'attacco possa essere individuato prima che si diffonda; resta fondamentale comunque partire dalla strategia e dalla formazione delle persone, dopo e solo dopo intervengono le macchine e l'infrastruttura tecnologica. Selta, con la sua esperienza e la sua offerta, può supportare efficacemente le aziende in tutto questo», conclude Attura.



Sicurezza e GDPR: i tre punti cardine

di
Paola
Saccardi

Controllo dell'IT su misura, IT che si coniuga con il risk management, e trasferimento del rischio a un'assicurazione fanno parte dell'approccio GDPR-ready di G DATA alla sicurezza

La sicurezza IT è un argomento che non si dovrebbe sottovalutare in nessuna circostanza, tuttavia ad essa non sempre viene tributata la dovuta attenzione, specie nelle piccole aziende che non dispongono di personale interno specializzato. L'entrata in vigore del GDPR obbliga però a confrontarsi con molteplici proposte non di rado poco chiare. In questo frangente, l'offerta "GDPR-ready" di G DATA, diretta in Italia dal suo country manager Giulio Vada, proprio ai fini della chiarezza contempla strumenti con cui si è proposta di consentire alle PMI di avventurarsi nel percorso verso la compliance con tranquillità, esternalizzare la gestione della sicurezza della propria infrastruttura e trasferire il rischio economico residuo a terzi.

Controllo e tutela dell'IT su misura e a consumo

Le recenti sfide informatiche hanno reso improcrastinabile un radicale cambiamento di paradigma per le politiche di sicurezza IT. La sicurezza, intesa come best practice e tutela integrata degli asset aziendali, va considerata quale parte integrante del risk management e quindi deve permeare i processi produttivi di qualsiasi organizzazione. Ciò non solo per adeguarsi al GDPR, ma soprattutto per proteggersi efficacemente contro le perdite economiche conseguenti a un incidente informatico, contro l'impatto economico delle sanzioni previste e l'impatto reputazionale in presenza di un furto di dati.

Quello della sicurezza è però un impegno a largo spettro. Una risposta olistica che la vede come un processo e non un mero prodotto è stata ideata da G DATA con lo sviluppo di soluzioni che consentono di implementare una buona strategia di sicurezza, con la garanzia di avvalersi di strumenti conformi ai dettami del nuovo regolamento e in grado di proteggere in modo proattivo l'infrastruttura IT dalle eventuali minacce.

La sicurezza IT si coniuga con il risk management

Ai fini operativi, tramite la suite G DATA Total Control Business la società ha voluto mettere a disposizione delle aziende una soluzione che fosse affidabile contro



Giulio Vada, Country
Manager di G DATA Italia

minacce esterne e interne e restituire all'IT manager la supervisione costante della propria infrastruttura. Per farlo, la suite monitora la rete verificando lo stato operativo dei sistemi e notifica in tempo reale eventuali disservizi o comportamenti anomali delle macchine. A questo abbina una piattaforma di patch management che semplifica la manutenzione di periferiche e client e velocizza la chiusura di vulnerabilità come quelle sfruttate

che desiderano esternalizzare i servizi di sicurezza IT affidandoli a professionisti, di abbattere gli investimenti e diluire i costi operativi in canoni mensili.

A ciò aggiunge la possibilità di attivare o disattivare tempestivamente licenze in base alle esigenze, con un controllo trasparente dei costi e delle installazioni attraverso una piattaforma professionale per la gestione remota quotidiana del parco installato.

a partire dal secondo trimestre 2018. Con l'introduzione del GDPR, osserva G DATA, è necessario adottare le migliori armi di difesa presenti sul mercato per mettere in sicurezza la rete aziendale e i dati trattati, ma questo non senza un'attenta analisi preliminare dell'infrastruttura.

Trasferire il rischio residuo a un'assicurazione cyber

Con l'introduzione del GDPR le aziende devono preoccuparsi più che in precedenza del rischio di furto di dati sensibili e della vulnerabilità dell'infrastruttura di operatori a cui hanno commissionato servizi che richiedono la condivisione dei propri dati riservati. Ai rischi legati alla propria sicurezza concorre anche l'intrinseca debolezza dei processi legati al trattamento dei dati rispetto alle esigenze normative.

Dalla collaborazione tra G DATA, Reale Mutua e il broker Margas, è così derivata la soluzione Insurtech, denominata Privacy & Cyber Risk, che integra le tecnologie di sicurezza G DATA con una polizza assicurativa per la Responsabilità Civile dedicata alle PMI, in modo che queste possano intraprendere più tranquillamente il percorso verso la compliance normativa.

La polizza non sostituisce una corretta Data Governance, avvisa G DATA, ma sostiene finanziariamente i fruitori delle proprie soluzioni in caso di leakage, trasmissione di ransomware e pubblicazione di informazioni lesive della reputazione e della privacy di terzi, come conseguenza di un incidente informatico. ❁



da WannaCry e Petya.

La soluzione fa inoltre leva sulla nuova tecnologia anti-ransomware integrata in tutte le suite per la sicurezza del suo portfolio e consente di gestire policy e filtri centralmente, anche per i dispositivi mobili, che vengono gestiti come qualsiasi altro client di rete. In pratica, evidenzia G DATA, implementare la suite permette di ancorare saldamente la sicurezza IT al risk management.

Per le aziende che hanno l'esigenza di ottimizzare Capex e Opex, le soluzioni sono fruibili anche in modalità MES (G DATA Managed Endpoint Security), una formula a consumo che si fa carico delle esigenze di flessibilità delle aziende

Conoscere le vulnerabilità dell'infrastruttura a priori

Implementare qualsiasi misura protettiva senza aver condotto un'analisi delle vulnerabilità dell'infrastruttura equivale ad affidarsi al caso, una condizione già intrinsecamente rischiosa. Dato che il mero malfunzionamento di un sistema critico ha ripercussioni economiche che, in base a gravità ed estensione, potrebbero minare l'esistenza dell'azienda, è quanto meno opportuno identificare tutti i fattori di rischio presenti nella rete. Per aiutare le aziende a valutare le vulnerabilità delle infrastrutture, G DATA ha sviluppato il servizio G DATA Advanced Analytics, che sarà disponibile progressivamente

Applicazioni al sicuro con i Cloud Service

Radware ha sviluppato servizi in cloud per garantire la protezione di reti, dati e applicazioni mediante l'analisi comportamentale e la gestione automatica delle policy

Approntare soluzioni in grado di bloccare attacchi sempre più sofisticati è un compito complesso. Richiede una profonda esperienza nel settore e una pari conoscenza delle dinamiche aziendali e delle specifiche esigenze, in primis quelle normative.

Un approccio pragmatico al problema è stato adottato da Radware, società pubblica worldwide con oltre 1000 dipendenti, che per individuare le specifiche necessità ha realizzato un rapporto centrato sulle applicazioni globali e sulla sicurezza delle reti in modo da individuare le dinamiche derivabili da attacchi e casi reali di clienti e identificare cosa serve ai manager preposti della sicurezza. Il rapporto ha evidenziato punti specifici che sono stati alla base delle risposte date da Radware alle esigenze emerse tramite i suoi canali commerciali, tra i quali Arrow, uno dei maggiori attori italiani nella distribuzione di soluzioni di sicurezza. In particolare:

- Lo scenario di chi attacca, cosa attacca e perché attacca.
- Il potenziale impatto sulle aziende in termini di costi associati ai vari cyber-attacchi.
- Le esperienze di organizzazioni dei vari settori.
- Le minacce emergenti e come proteggerci.

I paragrafi seguenti esaminano come Radware ha risposto alle esigenze espresse dai responsabili della sicurezza tramite servizi fruibili in cloud, che permettono di esternalizzare la complessità insita nell'assicurare una protezione aggiornata, dinamica e aderente alle normative.

Al sicuro con l'analisi comportamentale

La sfida che si pone quando si migrano applicazioni su cloud, evidenzia Nicola Cavallina, Channel Manager per Italia di Radware, è quella del controllo, della governance e della visibilità. Per contrastare attacchi DDoS che possono bloccare le applicazioni, Radware ha sviluppato il servizio Cloud DDoS Protection Service, basato su un robusto motore di analisi comportamentale. Il servizio protegge da attacchi DDoS sia la rete aziendale



Nicola Cavallina, Channel Manager Italia, Grecia, Cipro e Malta di Radware

sia le applicazioni, crea firme dinamiche in tempo reale per proteggere contro attacchi zero-day e dispone di una protezione SSL DDoS adattabile a specifiche esigenze. La soluzione è completata da una dashboard che dà una profonda visibilità sia sulla rete interna sia nel cloud.

Come gli altri sviluppati da Radware, ha evidenziato Cavallina, permette di esternalizzare il compito della sicurezza e di disporre di una protezione sempre aggiornata e garantita da SLA.

Cloud WAF Service per la protezione in Web

Un secondo aspetto critico, osserva Cavallina, è la complessità nello sviluppo di applicazioni web e la vulnerabilità a cui sono soggette. Per contrastare le minacce Radware ha sviluppato il servizio Cloud WAF, basato su un modello di machine learning che fornisce un'esauritiva protezione contro le vulnerabilità evidenziate da OWASP, la comunità aperta che abilita le organizzazioni a sviluppare applicazioni sicure. Il servizio mappa in real-time le applicazioni, individua i cambiamenti e attiva dinamicamente le policy che ottimizzano la sicurezza. Tra i compiti del servizio vi sono policy di sicurezza che individuano ed eliminano i falsi positivi, realizzano una protezione DDoS built-in, integrano la protezione da attacchi Bot net e aiutano



Roberto Branz, Division Director Security e IoT, Arrow ECS Italia

Cloud Malware Protection Service rivela, blocca e riporta gli attacchi zero-day

nel proteggere i dati in aderenza al GDPR.

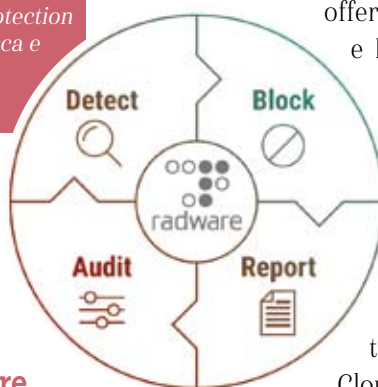
Numerose le certificazioni, che includono PCI e HIPAA e standard di sicurezza in cloud quali le ISO 27001, ISO 27017, ISO 27018 e ISO 27032.

Per verificare le difese analizza il comportamento posturale relativo ai malware e alle policy di sicurezza, valuta la resilienza delle infrastrutture verso comportamenti non corretti nella comunicazione verso l'esterno e compara lo stato di protezione dei gateway verso internet in riferimento a benchmark globali.

Partnership al servizio delle aziende

«Radware è per Arrow una componente fondamentale della nostra offerta in tema Sicurezza, Cloud e IoT - ha dichiarato Roberto Branz, Division Director Security e IoT Arrow ECS Italia -. Con Radware i partner di Arrow hanno a disposizione gli strumenti ideali per proteggere il business a valore dei loro clienti. La protezione garantita dai servizi Cloud permette quella continuità di business necessaria alle aziende innovative che cavalcano progetti IoT, cloud computing e intelligenza artificiale».

Proprio in ambito IoT, Arrow ha avviato il programma "Sensor to Sunset" in EMEA, un'iniziativa per sviluppare l'ecosistema IoT e facilitare il percorso dei partner di canale nel loro mercato. E' una strategia che ha fatto di Arrow un distributore globale in grado di offrire soluzioni IoT affidabili e sicure, per soddisfare ogni aspetto tecnologico. Con il programma IoT, basato su un'ampia gamma di soluzioni e servizi professionali gestiti, in cui si inserisce anche il portfolio Radware, fornisce al canale anche nuove opportunità di vendita. ✱



Cloud Malware Protection Service

Un ulteriore punto critico per le aziende è costituito dai malware zero-day, circa il 50% degli attacchi malware, e che non sono identificabili dai sistemi basati sulla firma sino a che non è disponibile. Il servizio, che protegge oltre 2 milioni di utenti, complementa le soluzioni dei clienti e difende da malware zero-day analizzando i log file anonimizzati delle comunicazioni su Internet. I dati sono analizzati da oltre 70 algoritmi concorrenti di machine learning, analisi comportamentale e tecniche di sandboxing che isolano in fase di test i potenziali malware e reti di bot Command&Control.

Con Blockchain dati e transazioni al sicuro da cyber attacchi

La tecnologia blockchain al centro dell'interesse del settore privato e pubblico perché apre la strada a transazioni sicure e a una cooperazione trusted

Il verificarsi di attacchi alla cyber security sempre più massicci sta accentuando l'attenzione posta da enti pubblici e privati su blockchain, una metodologia che permette di rendere del tutto sicuri e inalterabili (o in ogni caso rilevarne velocemente l'eventuale alterazione) i dati e le transazioni sensibili. Blockchain è una tecnologia da tempo conosciuta ma sino a poco tempo fa se non negletta perlomeno relegata tra entità specializzate, generalmente del settore del finance, che sulla inalterabilità delle transazioni digitali basano il proprio business e la forza del brand. Il che motiva la riottosità che mostrano nel farlo sapere in caso di tentativi di attacco riusciti.

Il concetto che sta alla base della tecnologia blockchain è semplice e si rifà in un certo qual modo al detto secondo il quale si possono ingannare tanti per poco tempo, pochi a lungo, ma non tanti a lungo.

La soluzione è un poco come l'uovo di Colombo anche se questo richiede che sia disponibile un'ampiezza di supporti di archiviazione e di connettività adeguati generalmente non alla portata della singola impresa. Era proprio il loro ammontare

complessivo, costo e l'inadeguatezza delle reti del passato che aveva e in parte ha sino a ora impedito di applicare su larga scala il concetto e la tecnologia blockchain.

Divide et impera

Nella sua essenza la tecnologia blockchain consiste nella replicazione su un numero elevato di archivi storage dei dati sensibili organizzati in blocchi. Il replicare i dati su più archivi distribuiti su più nodi di rete (intesi come data center) rende estremamente difficile un attacco contemporaneo che ne



modifichi una parte senza che gli altri nodi della rete finiscano con l'accorgersene in un tempo che è questione di pochi minuti.

In pratica, un'architettura blockchain definisce, è spiegato in un interessante documento delle banche popolari italiane icbpi (ora Nexi), un deposito di dati distribuito costituito da una lista di record in continua crescita resistente a modifiche e revisioni, anche da parte degli operatori dei nodi su cui risiede il deposito di dati. Una copia totale o parziale del blockchain è memorizzata su tutti i nodi. I record contenuti sono di due tipi: le transazioni, che sono i dati veri e propri, e i blocchi, che sono la registrazione di quanto e in quale ordine le transazioni sono state inserite in modo indelebile nel database. Le transazioni sono create dai partecipanti alla rete nelle loro operazioni (per esempio, trasferimento di valuta a un altro utente), mentre i blocchi sono generati da partecipanti speciali che utilizzano software e a volte hardware specializzato per creare i blocchi.

Le transazioni, una volta create, sono distribuite sui diversi nodi e la validità di una transazione viene verificata dal consenso dei nodi della rete sulla base di una serie di parametri, che variano secondo l'implementazione specifica dell'architettura. Una volta verificata come valida, la transazione viene inserita nel primo blocco libero disponibile. Per evitare che ci sia una duplicazione, l'architettura prevede un sistema di time stamping, a sua volta decentralizzato, ossia che non richiede un server centralizzato.

Sicurezza e cifratura

Le transazioni viaggiano in rete e sono registrate nel blockchain in forma cifrata e validate dalla firma digitale di chi ha originato la transazione. Ne consegue che l'identità di chi ha generato una transazione è pubblica ma non lo è la natura della transazione. L'inalterabilità è assicurata da una codifica hash a 256 bit, che consiste nella mappatura del contenuto di lunghezza variabile del blocco in una sequenza fissa di 256 bit che viene copiata nel blocco successivo.

In questo modo, il tentativo di modificare un blocco rende invalidi tutti i blocchi successivi, e quella versione della blockchain viene eliminata automaticamente dalla rete. Dal momento che l'integrità della blockchain viene costantemente controllata da tutti i nodi, è molto difficile che una blockchain manipolata possa sopravvivere su qualche nodo per più di una decina di minuti, che è il tempo medio di validazione di una transazione. Ne deriva che con un'architettura blockchain è possibile registrare in modo indelebile, non modificabile, sicuro e distribuito qualunque tipo di dato digitale.

I settori interessati

Svariati i settori interessati o potenzialmente interessati a utilizzare la tecnologia blockchain, propria o fornita da operatori specializzati come servizio. Tra questi:

- **Pubblica Amministrazione.** È possibile conservare e gestire i registri pubblici digitali in modo sicuro e decentralizzato. È inoltre possibile gestire le identità

digitali senza rischi per la privacy e amministrare in modo efficiente e sicuro sistemi di riscossione delle imposte o di assegnazione e tracciatura di fondi. La rete consente infine di analizzare e incrociare grandi moli di dati nel pieno rispetto della riservatezza dei cittadini, con importanti ricadute positive per la governance pubblica.

- **Settore Bancario e Finanziario.** In questi contesti, dove la blockchain è già una realtà ampiamente esplorata, è possibile anche ricorrere a una rete privata che garantisce sicurezza e affidabilità maggiori, a partire da gestione e conservazione dei dati. Protocolli algoritmici possono offrire benefici anche per il data sharing perché permettono la condivisione dei dati anche tra operatori che non si conoscono, rendendo possibile lo sviluppo di nuovi modelli di business fondati sulla collaborazione.

- **Settore Sanitario.** È possibile raccogliere e conservare dati clinici e gestire la verifica dell'identità dei pazienti in totale sicurezza. I dati possono inoltre essere utilizzati a supporto di attività di ricerca medica, per diagnosticare patologie o, in alcuni casi, persino per prevederne l'insorgenza. Il tutto nel pieno rispetto della privacy dei pazienti.

- **Settore Industriale.** In questo ambito è possibile lo scambio di dati tra aziende, anche concorrenti, stimolando l'innovazione e creando nuove opportunità di business. *

L'analisi predittiva in ambiente cloud rende sicuri dati e applicazioni

L'analisi comportamentale predittiva di Forcepoint permette ad aziende private e pubbliche di ridurre i tempi di intervento per la sicurezza e di concentrarsi sugli utenti a più alto rischio

Il diffondersi del concetto di Smart IT e l'impatto che su di esso ha la sicurezza, ha come corollario negativo l'intensificarsi dell'intelligenza degli attacchi cibernetici. Il problema è che, evidenzia Gartner, il tempo medio per rilevare una violazione è di oltre tre mesi, cosa che lascia al malware il tempo di infiltrarsi. Un modo per ridurre questo intervallo consiste nello sfruttare dati ed analitiche. La società di ricerca prevede in proposito che entro il 2018 l'80% delle piattaforme di protezione degli endpoint includerà il monitoraggio delle attività e le capacità forensi e stima che almeno un quarto delle violazioni verrà evidenziato attraverso l'analisi comportamentale.

La criticità del cloud e degli ambienti ibridi

Il problema dei tempi intercorrenti tra il rilevamento di un nuovo tipo di attacco e il momento in cui le patch sono disponibili risulta enfatizzato quando da un ambiente privato si passa ad uno su cloud pubblico o ibrido.

La combinazione di ambienti IT con una forte presenza di dispositivi mobili che si collegano alle applicazioni tramite cloud ibrido apre la strada a problematiche connesse all'aggiornamento delle infrastrutture di terzi interposte tra il dispositivo e i data center dove risiedono dati e applicazioni.

Non che i service provider non apportino rapidamente le necessarie correzioni ma la realtà è che non pochi di essi hanno sviluppato le loro infrastrutture quando gli attacchi di cyber hacker non erano sofisticati come ora, con la capacità di far leva su attacchi distribuiti, complessi e strutturati, attacchi che richiedono per essere rilevati da analisi approfondite non solo del traffico, ma anche di come questo si scosta per il singolo cliente da quello che è l'usuale comportamento delle applicazioni business fruite.

In sostanza, può avvenire che per mettersi al passo con la sofisticatezza degli attacchi si renda necessario apportare modifiche alla infrastruttura, che data la



Luca Mairani, Sales
Engineer di Forcepoint

scala di intervento richiesta ad un provider possono ritardare l'entrata in funzione delle contromisure. Per rimuovere questo potenziale vulnus, Forcepoint, bypassando e compensando le eventuali carenze del provider, ha spiegato Luca Mairani, Senior Sales Engineer di Forcepoint in Italia, ha puntato sull'analisi comportamentale estesa a livello di end-point.

La società, che sviluppa software di sicurezza operante a livello mondiale e con un solido background nella cyber security e nel cloud, ha con questo obiettivo di recente aggiunto al proprio peraltro già ampio portfolio di soluzioni per la sicurezza in cloud, funzionalità che abilitano ulteriori controlli comportamentali previsionali che semplificano la protezione dei dipendenti, dei dati critici e della proprietà intellettuale.

Sicurezza più Smart con l'analisi comportamentale

La vision strategica è consistita nel rendere disponibili funzionalità basate sull'analisi del comportamento e predittiva, volte a rafforzare le policy di sicurezza inerenti lo scambio dei dati tra IT legacy e cloud (CASB: Cloud Access Security Broker), come ad esempio nel caso delle banche i cui dipendenti utilizzano Microsoft Office 365, la sicurezza su Web e quella della posta elettronica.

Approcciare la security attraverso un filtro human-centric, osserva Forcepoint, aiuta le organizzazioni a comprendere meglio gli indicatori del normale comportamento informatico e identificare

rapidamente attività e operazioni, quali la shadow IT, che rappresentano i maggiori rischi.

Il rafforzamento delle policy di sicurezza è stato perseguito con funzionalità che valutano il rischio di condivisione di file e di altre applicazioni cloud e proteggono dalla perdita di dati sensibili non archiviati nella rete aziendale, analizzando parametri quali il comportamento dell'utente e le caratteristiche dell'applicazione, per esempio i dati, il dispositivo e la posizione da cui si accede.

Microsoft 365 e Azure sicure con Forcepoint CASB

L'obiettivo di rendere sicure le attività in cloud e in ambienti quali Microsoft 365 e Azure si è concretizzato, come evidenziato, con il rilascio di ulteriori controlli di analisi comportamentale che semplificano la protezione.

Le funzionalità, disponibili per Forcepoint CASB, Forcepoint Web Security e Forcepoint Email Security, hanno l'obiettivo primario di fruire del cloud come motore per lo sviluppo del proprio business in modo sicuro e affidabile. L'obiettivo, per le specifiche soluzioni, è stato perseguito apportando aggiornamenti che comprendono rispettivamente:

- **Forcepoint Web Security:** funzionalità che consentono un controllo più granulare delle applicazioni cloud e bloccano

eventuali attività di shadow IT.

- **Forcepoint Web Security:** strumenti di migrazione in cloud che consentono agli utilizzatori di Forcepoint Web Security con installazioni locali di migrare in ambiente Cloud in qualsiasi momento.

- **Advanced Malware Detection (AMD) Powered by Lastline:** disponibile per le piattaforme on-premise e in Cloud Forcepoint Web Security e Forcepoint email security. L'integrazione della tecnologia AMD sandbox consente poi di proteggere in tempo reale gli utenti ovunque si trovino.



In pratica, la analisi comportamentali di Forcepoint CASB analizzano il comportamento dell'utente e le caratteristiche dell'applicazione, ad esempio i dati, il dispositivo e la posizione da dove si accede. A questo Forcepoint ha aggiunto una rinnovata User Risk Dashboard single-view che evidenzia sia le attività dei dipendenti che il potenziale impatto sul business basato sulle autorizzazioni che l'utente detiene all'interno dell'organizzazione. *

Per un'Industry 4.0 sicura servono soluzioni specializzate

Stormshield rende sicura l'interazione tra sistemi industriali tradizionali e l'information technology con prodotti e partnership

Il susseguirsi di cyber attacchi nell'ultimo anno ha portato all'attenzione del mondo industriale e dei servizi ad esso rivolti il fatto che un semplice incidente informatico può avere conseguenze catastrofiche, dall'interruzione della produzione alla chiusura di interi siti produttivi, dalla perdita di dati aziendali critici al danneggiamento della reputazione di un brand.

Il mondo produttivo si trova quotidianamente a confrontarsi con attacchi sempre più sofisticati, che evidenziano la difficoltà di aziende private come degli enti della PA di rispondere efficacemente a minacce di nuova generazione, come se i rischi informatici tangessero esclusivamente terzi.

È però assolutamente illusorio, mette in guardia Alberto Brera, Country Manager di Stormshield Italia, pensare che i cyber attacchi possano essere fermati del tutto. Le aziende devono però rinunciare al ruolo di spettatore passivo che si sono ascritte e prendere provvedimenti. Proteggere l'azienda con soluzioni adeguate ha di certo un costo, non nasconde il manager, ma tale investimento è necessario tanto quanto siglare una polizza assicurativa: la sicurezza IT va inquadrata come colonna portante di una strategia di governance aziendale contemplando tutti gli aspetti di natura tecnologica e organizzativa.



Alberto Brera, Country
Manager di Stormshield
Italia

Una protezione certificata UE, dal posto di lavoro alla rete

Per affiancarsi e supportare il mondo industriale nell'affrontare in modo sicuro il processo della Digital Transformation e le problematiche poste dalla crescente interazione tra OT (tecnologia operativa tradizionale) e l'IT (infrastruttura informatica), Stormshield ha sviluppato un portafoglio di soluzioni che affronta la cyber security su più livelli e ambiti aziendali. Esso comprende soluzioni di sicurezza punto-punto per la protezione delle reti (Stormshield Network Security), delle postazioni di lavoro (Stormshield Endpoint Security) e dei dati (Stormshield Data Security).

Come osserva l'azienda, si tratta di soluzioni di nuova generazione certificate dai severi enti europei preposti (EU RESTRICTED, e ANSSI EAL4+) e dalla NATO, atte a garantire la protezione delle informazioni strategiche, dei processi produttivi e di business in modo affidabile. Implementabili in qualsiasi tipologia di azienda, istituzione ed organizzazione, si rivelano ideali per la flessibilità con cui si adattano ad ogni esigenza e sono commercializzate attraverso una rete di distributori, integratori di sistema e operatori certificati in grado di erogare un qualificato servizio pre e post vendita.

Partnership per una Industry 4.0 sicura e a prova di obsolescenza

Il problema della sicurezza permea profondamente il settore industriale. Nonostante il crescente interesse per un'Industry 4.0, in Italia il settore manifatturiero sembra focalizzarsi primariamente su esigenze business quali la remotizzazione delle operazioni e del monitoraggio di sistemi esistenti, più che trasformarsi in industria di nuova generazione, e mettere in secondo piano valutazioni concernenti i rischi connessi a questa innovazione strategica.

Ne è la riprova, evidenzia Stormshield, un test condotto nel 2016 che ha rivelato oltre 13.000 sistemi SCADA esposti su internet senza alcun controllo. A fronte del tipico ciclo di vita di un impianto, è un dato che nel 2017 non avrà subito grandi variazioni. Il problema è che i firewall tradizionalmente

specializzati nella prevenzione di incidenti informatici in una rete aziendale non sono in grado di interpretare i protocolli SCADA, né di individuare un eventuale traffico malevolo o non autorizzato su tali protocolli, dando luogo ad un quadro allarmante come quello

in grado di reagire proattivamente contro le minacce che nascono al crocevia tra l'automazione industriale e la rete informatica, con l'obiettivo primario di supportare concretamente le aziende manifatturiere a trasformarsi in Industry 4.0 in accordo al principio della



*Sni40, firewall industriale per la sicurezza dei sistemi IT e OT
Industry 4.0: investire sulla sicurezza*

evidenziato, ma evitabile con soluzioni di sicurezza adeguate.

Dello stesso parere di Brera è anche Gruppo SIGLA, partner di Stormshield, che operando da anni nel settore dell'automazione industriale presso principali aziende sia nazionali che multinazionali, osserva come queste reagiscano all'esigenza di aprirsi sempre più verso utenti ed applicazioni esterne, introducendo apparati che possano integrarsi a quelli esistenti, facendo quindi evolvere l'infrastruttura attualmente in uso per evitare di rinnovarla completamente. Un punto chiave della partnership tra il produttore e Gruppo Sigla è l'attenzione dedicata da Stormshield alla messa in sicurezza dei sistemi di produzione con una proposta di sistemi UTM/IPS sviluppati attorno al mondo SCADA,

sicurezza 'by design'.

Strategica per Stormshield al fine di abilitare un'Industry 4.0 a prova di cybercrime è anche la partnership con Schneider Electric, azienda specializzata nella gestione dell'energia e nell'automazione. La complementarità delle rispettive aree di competenza - quella di Stormshield nella protezione di reti, server e workstation, e quella di Schneider Electric in ambito OT - ha portato allo sviluppo di un prodotto di sicurezza flessibile, lo Stormshield Sni40, un firewall industriale "hardenizzato", specificamente progettato per far fronte alle esigenze di sicurezza dei sistemi IT e OT e quindi adatto ai diversi ambienti industriali, in cui Sni40 riconosce e fornisce protezione proattiva anche per il traffico dati SCADA. *

Business Always-On e dati critici al sicuro su Microsoft Azure

Con una nuova soluzione, Veeam consente di sfruttare Microsoft Azure per garantirsi la continuità operativa ed eliminare il costo di un sito di ripristino dedicato

Il business delle aziende dipende ormai fortemente dall'information technology, a cui si richiedono piani precisi atti a mantenere l'operatività qualora si verificino interruzioni di servizio. La realtà però è che, nonostante il rischio di danni economici e di immagine consistenti, per molte aziende le strategie per il backup e il ripristino volte a mettere in sicurezza la continuità del business non sono sostenibili, o si avviano a non esserlo: da un lato il costo di un sito di ripristino remoto per un sistema replicato, con hardware e software duplicati, è proibitivo a causa dell'elevata spesa in conto capitale; dall'altro il backup e il ripristino richiedono elevati investimenti in termini di tempo e risorse.

Una risposta all'esigenza di coniugare sicurezza e economicità l'ha ideata Veeam Software, specializzata nelle soluzioni per l'Availability for the Always-On Enterprise, con l'annuncio di Veeam Recovery to Microsoft Azure with Veeam PN (Powered Network).

È una soluzione on-demand, già disponibile, che ha l'obiettivo di assicurare una rapida continuità operativa e che include anche il nuovo prodotto gratuito Veeam PN, una soluzione software defined networking (SDN che elimina la necessità di creare VPN e semplifica la configurazione di rete quando si vuole creare un sito di ripristino su Microsoft Azure.

Dati al sicuro su Azure

Veeam Recovery to Microsoft Azure fornisce in pratica, ha evidenziato Veeam, un mezzo semplice e sicuro per il recupero dei carichi di lavoro on-premises su cloud pubblico. I responsabili IT possono avviare automaticamente un'istanza cloud Azure ed erogare in modo sicuro servizi a clienti, partner e dipendenti raggiungibili ovunque essi siano, il tutto senza dover sopportare gli investimenti necessari per realizzare in azienda un sistema ridondante di standby.

A livello funzionale la nuova soluzione, che viene fornita già pronta all'uso, abilita il ripristino cloud per i backup Veeam ed è arricchita come accennato da Veeam PN,



Albert Zammar, SEMEA
Vice President di Veeam
Software

una soluzione SDN per definire un sito di ripristino in Microsoft Azure. Veeam Recovery to Microsoft Azure con Veeam PN fornisce un recupero dati basato su cloud e permette di evitare le spese connesse alla costruzione e manutenzione di un sito remoto di ripristino di proprietà.

«Con Veeam Recovery to Microsoft Azure, i dirigenti e gli imprenditori possono dormire sonni tranquilli, sapendo che, in caso di disastro, l'azienda continuerà ad operare nel cloud pubblico, senza spendere una fortuna od occupare tutto il tempo del personale IT», ha commentato Danny Allan, Vice President Product Strategy di Veeam. Veeam Recovery to Microsoft Azure con Veeam PN è stato espressamente progettato per semplificare e automatizzare la configurazione di un sito di ripristino in Microsoft Azure riducendo la complessità delle implementazioni di VPN, indipendentemente dalle dimensioni delle aziende o dei service provider, e fornire un collegamento di rete sicuro tra le risorse IT locali e quelle in Azure mediante una connettività da sito a sito.

Veeam assicura la business continuity ai clienti di KPNQwest

Una conferma del livello di sicurezza e di business continuity garantite dalle soluzioni Veeam arriva dalla decisione di KPNQwest di adottarne le soluzioni per garantire la continuità operativa ai propri clienti.

KPNQwest Italia, società nazionale che offre servizi di



telecomunicazioni su tutto il territorio italiano, ha scelto Veeam Backup Replication Enterprise Plus per supportare l'efficienza, la visibilità e la scalabilità su diversi ambienti IT, oltre a supportare i propri clienti nel percorso di Digital Transformation caratterizzato dalla disponibilità dei dati "Always On" e dalla rapidità di ripristino. KPNQwest Italia fornisce a migliaia di aziende italiane servizi di connettività in fibra ottica, data center e cloud computing ad altissima affidabilità e performance. Tali servizi sono erogati a partire da quattro data center di proprietà, ubicati presso il "Fiber Hub" italiano di via Caldera a Milano, ed attraverso una rete di accesso in larga banda nazionale.

«Ciò che ci contraddistingue nel settore dei Cloud Service Provider è l'alta specializzazione dell'infrastruttura. L'offerta KPNQwest Italia unisce l'affidabilità, la sicurezza, le prestazioni e la resilienza della propria infrastruttura di data center alle migliori tecnologie hardware e software per il cloud computing disponibili, per creare il

servizio di Virtual Data Center tra i migliori presenti sul mercato», ha osservato Matteo Flavi, product manager di KPNQwest Italia.

Tra le soluzioni per l'always-on sul mercato, ha evidenziato l'azienda, la soluzione Veeam è stata quella che si è rivelata più matura ed idonea per il mondo degli Internet Service Provider rispetto a soluzioni più complesse ma carenti di funzionalità fondamentali, come ad esempio il restore agentless su qualunque sistema operativo ed ancora di più per le ampie funzionalità di multi-cloud.

«Siamo orgogliosi di essere stati scelti da KPNQwest Italia per tante ragioni diverse. Ci hanno scelto per la nostra indiscussa superiorità tecnologica e perché moltissimi dei loro clienti, che utilizzavano già la soluzione Veeam, ne hanno promosso presso KPNQwest la semplicità, la scalabilità e la perfetta integrazione con gli ambienti multi-cloud. Questo per noi è un apprezzamento molto importante e ci lusinga molto», ha commentato Albert Zammar, SEMEA Vice President di Veeam Software. *

di
Giuseppe
Saccardi

La protezione fisica serve quanto quella logica



Le minacce alla sicurezza logica non devono trascurare quelle alla sicurezza fisica. Difendere gli ambienti e le persone è indispensabile quanto proteggere dati e applicazioni

La forte attenzione posta nell'ultimo anno alla sicurezza delle applicazioni e dei dati, a seguito di clamorosi cyber attacchi andati a buon fine nei confronti di aziende e operatori di levatura internazionale, oltre che l'avvicinarsi della data di entrata in funzione del GDPR, rischia di far passare in secondo piano la componente complementare della sicurezza logica (dati, applicazione, apparati) e cioè la sicurezza fisica.

Con il termine è da intendersi in senso lato la sicurezza di persone e beni materiali, come per esempio gli ambienti di lavoro, l'insieme di apparati, le server room, i data center e in generale quanto costituisce un asset materiale per un'azienda che può essere asportato o danneggiato.

Sicurezza a misura di ambiente

Se per un ambiente di smart o home working o dove si esercita la propria attività professionale le soluzioni presentano caratteristiche abbastanza omogenee, diverso è quanto si riscontra tra ambienti industriali o dedite ai servizi, dove standard di sicurezza, caratteristiche delle macchine, ampiezza degli ambienti sono notevolmente differenti. Cosa può essere necessario nel portfolio di un fornitore che si proponga come partner tecnologico? Vediamolo in sintesi.

Ambienti aziendali mono o multisito:

- Applicazione per la gestione centrale omnicomprensiva per un'architettura multi-sito.
- Una centrale di controllo ibrida flessibile adattabile alle diverse installazioni.
- Ampia gamma di sensori professionali le diverse esigenze e in grado di operare in rete fissa e/o mobile.

Istituti Finanziari

- Sistemi di rivelazione e antintrusione di Grado 3 in linea con gli alti standard di sicurezza richiesti dal settore.
- Sensori anch'essi di Grado 3, inclusi rivelatori professionali specifici come per esempio sensori sismici per la protezione di casseforti e installazioni bancomat.
- Software di gestione della sicurezza utilizzabile da piattaforma centralizzata e in grado di controllare tutti i sistemi relativi alla sicurezza.

Infrastrutture Critiche

- Sistemi di rilevazione di Grado 3 ad alti standard di sicurezza.
- Software di gestione centralizzato in grado di gestire e monitorare un'architettura multi-sito fortemente distribuita sul territorio urbano ed extraurbano.
- Sensori con caratteristiche professionali da interno ed esterno progettati per alti standard di sicurezza negli ambienti di uso più critici, come sicurezza e condizioni ambientali.

In sostanza, proteggere il business non è un qualcosa che deve limitarsi ai dati e al loro uso fraudolento, ma vuol dire anche, e in primis, proteggere l'ambiente fisico in cui questi dati sono custoditi o fruiti, si tratti dell'ufficio o dell'ambiente domestico dove si esercita sempre più lo smart working.

La Sicurezza con la S maiuscola dovrebbe quindi partire dalle persone e dalle cose e non puntare esclusivamente a proteggere i dati, per quanto questi siano importanti. Persone e cose costituiscono il vero valore strategico e umano dell'azienda e come tali vanno adeguatamente protetti e, per quanto concerne le persone, fatte operare in un ambiente che sia adatto al benessere personale, oltre che sicuro per quanto concerne i rischi fisici derivanti da una effrazione materiale.

Sicurezza, prevenzione, intervento

Garantire condizioni ambientali adatte e sicure è un compito però non sempre facile e presenta diversi aspetti da affrontare e considerazioni da fare.

In primis, quella che va fatta è una distinzione di cosa si intenda per sicurezza fisica perché una cosa è parlare di infrastrutture che permettono di rilevare quando vi è in atto un tentativo da parte di malfidati di introdursi in una abitazione, ufficio o stabilimento produttivo per trafugare beni o recare danni materiali che possono anche essere molto onerosi, un'altra è parlare di soluzioni che devono permettere un rapido

intervento del personale preposto privato o pubblico, per far sì che il tentativo non possa essere portato a termine con successo.

I due sono piani del tutto diversi e richiedono tecnologie, soluzioni e approccio progettuale diverso, così come diverse sono le soluzioni atte a scoraggiare atti di questo genere.

Nel primo rientrano soluzioni come sensori, rilevatori, videocontrollo, telecamere ad alta definizione e in definitiva tutto quanto permetta di rilevare un tentativo di effrazione. Il secondo comprende soluzioni che da una parte devono allertare, tramite sistemi sicuri che non possono essere manomessi preventivamente fuori servizio siano essi fissi o mobili, i gestori della sicurezza in modo che possano prendere le decisioni operative più opportune in base a specifici protocolli di intervento e al livello di importanza dell'area in cui è in corso un tentativo di effrazione.

Complementare a questo però devono essere disponibili barriere fisiche (vetrate o porte antisfondamento, o altri sistemi atti a ritardare l'effrazione fisica in un'area protetta) in grado di trattenere l'attaccante fisico per il tempo necessario agli addetti alla sicurezza di intervenire sul luogo e bloccare il tentativo.

L'offerta sul mercato di soluzioni che rientrano in uno o nell'altro dei campi sopra esposti è ampia ma non sempre le due cose coincidono e sono presenti nel portfolio di prodotti e servizi della medesima azienda.

Va considerato che la sicurezza

fisica richiede approcci molto specializzati e chi ha esperienza nel produrre soluzioni come le videocamere ad elevata risoluzione, brandeggiabili e con capacità di visione notturna, non necessariamente ha anche la capacità di sviluppare soluzioni fisiche antieffrazione, o software di gestione in rete, o dell'insieme di oggettistica IoT di apparati intelligenti di rilevamento delle condizioni e di controllo dell'ambiente fisico, o di soluzioni per il controllo dell'accesso a sale riservate e così via.

La cosa è complicata anche dalla varietà di standard che sono andati sviluppandosi nei decenni passati che solo ora come complessità sta trovando una soluzione con la diffusione di dispositivi che possono collegarsi in modo nativo e trasmettere su rete IP e Internet, e da qui far uso del cloud sia per segnalare eventi che per ricevere comandi di attuazione di specifici compiti, ad esempio accendere o spegnere una telecamera, abilitare l'apertura di una porta, accendere la luce ed il riscaldamento in una sala riunioni, aprire e chiudere automaticamente un cancello o la basculante di un box dopo aver accertato che in vicinanza o al suo interno non siano presenti sconosciuti.

Definire gli obiettivi

I modi per proteggere ambienti riservati, siano essi domestici o aziendali o pubblici nel caso di aree quali parchi, giardini, strade o uffici aperti al pubblico,

sono compiti spesso non semplici. Questo sia per l'estensione delle aree sia per la diversità di oggetti e numero di zone o microzone che comprendono. Per esempio, una stanza può comprendere una o più porte, una o più finestre e se si vuole avere una segnalazione puntuale ognuna di queste deve poter essere trattata individualmente, cosa che richiede un dispositivo specifico, una segnalazione che permetta di individuare esattamente da dove un allarme è partito e così via, e a fronte di questo una diversa strategia di intervento, Ai fini della sicurezza, in previsione di un intervento e del valore di chi e cosa si trova al





suo interno, può essere utile avere installata una telecamera che permetta di vedere quali e quanti sono quelli che stanno cercando di forzare porta o finestra, in modo da avere una squadra di intervento predisposta opportunamente ed in numero adeguato. Così come i dispositivi di videosorveglianza devono essere in grado di rilevare le dimensioni di un essere vivente che entra nel campo d'azione per non allertare inutilmente il personale di sicurezza quando poi si tratta di un animale di piccola taglia.

Qualunque sia il caso da gestire e l'ambiente da proteggere, il primo passo da compiere, suggeriscono gli esperti del settore, è una adeguata analisi del rischio, analisi che deve stabilire una priorità dei beni materiali, degli ambienti e delle persone da proteggere, come rilevare e segnalare quando qualcosa non va e come fare e cosa installare per far sì che la protezione fisica regga sino all'intervento risolutore. In sostanza, prima di porre mano al progetto fisico dell'infrastruttura di sicurezza si deve procedere alla analisi globale del rischio e agli obiettivi che ci si prefigge di raggiungere.

L'analisi del rischio come punto di partenza

Quella dell'analisi del rischio non è però una fase di un progetto per la sicurezza fisica che può essere condotta in autonomia dalla società partner nella sicurezza.

È un compito che oltre che essere accurato richiede che lavorino spalla a spalla sia gli esperti del settore sia i responsabili del cliente, che alla fin fine è l'unico che può dare una valutazione oggettiva del valore dei beni e delle persone da proteggere in base al rischio che questi, in base alle funzioni e alle mansioni aziendali, possono correre. Peraltro, è nel corso dell'analisi del rischio che si può fare la iniziale distinzione tra i beni immateriali come i dati e quelli materiali.

Vi possono essere beni materiali che necessitano protezione, così come beni immateriali quali le informazioni, e ovviamente sono due tipi di protezione diversa che sono necessarie.

I parametri da considerare sono svariati, ad esempio se si tratta di un edificio in cui circolano solo persone interne o anche esterne, se è un edificio aperto al pubblico o è un building privato e così via. Si tratta di informazioni che devono essere raccolte in modo strutturato altrimenti si corre il rischio di non riuscire a fornire la protezione che serve all'utente.

Esiste poi una questione di fondo accennata. Sovente si è portati a pensare che un sistema antifurto serva ad evitare il furto stesso. Non è così o perlomeno non lo è se il tutto non è inserito in un approccio sistemistico corretto.

Il sistema antintrusione avvisa che c'è un intruso, poi che il furto venga evitato è tutta un'altra questione e questo non sempre viene ben spiegato ma è fondamentale.

Se ho un'opera d'arte importante non è che con la sola protezione volumetrica si evita che il quadro possa essere rubato. Certo, l'intruso viene rilevato ma l'intruso c'è ancora. Se però, una volta scattato l'allarme, non compio altri passi l'intruso se ne può andare con la tela arrotolata sotto il braccio.

Da qui emerge l'importanza di un efficace servizio di analisi che preveda che obiettivo ci si pone, con un approccio che permetta di creare una infrastruttura che segnali l'intrusione e che allo stesso tempo resista per il tempo necessario a permettere l'intervento della Sicurezza. Naturalmente quello che vale per beni materiali vale a maggior ragione per la protezione delle persone fisiche. Se nel processo di raccolta delle informazioni, dell'analisi del rischio e della determinazione degli obiettivi manca qualcosa il sistema potrebbe, e a ragione, non funzionare. *



Con SiMPNiC la sicurezza dell'ambiente business e home diventa smart

SiMPNiC di CTS Group è una soluzione per il benessere ambientale che rende sicuri e confortevoli gli ambienti home e di smart working

Il benessere e la sicurezza dell'ambiente di lavoro in tutte le sue forme, compreso quello domestico vista la diffusione e l'interesse crescente per lo smart e l'home working, si sta imponendo all'attenzione di aziende e professionisti.

A garantire qualità dell'ambiente e sicurezza ci ha pensato CTS tramite il suo marchio SiMPNiC, società che ha tra i suoi i partner ingegneristici e distributori nazionali CIE Telematica, azienda italiana che opera da oltre vent'anni nel settore delle soluzioni e infrastrutture di rete di accesso fisse e mobili e del controllo del territorio.

La linea di prodotti dedicata al benessere ambientale e alla sua sicurezza comprende un'ampia gamma di soluzioni IoT per migliorare sia il comfort sia la sicurezza e rendere smart e controllabile via rete e smartphone l'ambiente in cui si vive o si lavora. La gamma di apparati e dispositivi IoT intelligenti comprende CPE per collegamenti su reti fisse e wireless, videocamere di controllo, smart plug con diverse tipologie di presa e



gateway per videocamere. Distribuiti per l'ambiente domestico o di smart working permettono di tenerlo sotto controllo, così come di controllare lo stato di accensione o di spegnimento di apparati elettronici, con il tutto che può essere gestito tramite gateway da remoto e la possibilità di ricevere remotamente e tramite dispositivi mobili segnalazioni sul verificarsi di eventi fuori dall'usuale o potenzialmente pericolosi (per esempio fughe di gas, effrazioni e così via). Un ruolo chiave nell'erogazione del servizio di gestione lo assumono gli iCPE, che sono dei gateway IoT multiservizio che operano tramite il protocollo Z-Wave e che costituiscono una piattaforma aperta che permette di sviluppare soluzioni di smart Home/Office ad hoc.

Sicurezza dell'ambiente innanzi tutto

Uno degli obiettivi chiave di SiMPNiC consiste nel rendere sicuro l'ambiente, intento perseguito tramite un meccanismo di sicurezza rafforzata che permette di realizzare una infrastruttura di controllo distribuita che protegge sia le persone sia le cose e le informazioni sensibili.

Il sistema assicura una protezione di classe Telco ottenuta tramite il ricorso a protocolli di sicurezza nella comunicazione tra gli oggetti che supervisionano l'ambiente, chiavi di sicurezza e soluzioni atte a garantire la privacy dei dati.

La sicurezza si estende sino a comprendere la prevenzione di disastri ambientali dovuti al malfunzionamento di oggetti o a guasti dei servizi pubblici fruiti. Tra i controlli di prevenzione disponibili vi sono ad esempio la gestione automatizzata dell'energia, il rilevamento di perdite di gas o idriche, la rilevazione di fumi o eccessiva CO2. Al momento della rilevazione viene automaticamente segnalato l'evento e vengono avviate in automatico le procedure di prevenzione necessarie. ✱

Data Protection e videosorveglianza per una maggiore sicurezza

L'importanza di componenti affidabili, come gli hard drive WD nella realizzazione di soluzioni critiche per le imprese

Si fa un gran parlare di sicurezza, anche perché siamo in campagna elettorale, ma il dibattito è spesso superficiale, mentre in ambito tecnologico occorre andare in profondità per cogliere la differenza tra una soluzione supportata da un prodotto adeguato e quella che si basa su sistemi all'avanguardia, progettati per un'elevata affidabilità e alte prestazioni.

Un sistema per il controllo video di un'azienda, un ufficio o una casa deve garantire la qualità delle riprese e la registrazione continua. Gli hard disk per la videosorveglianza di Western Digital sono stati progettati per un utilizzo a tutti i livelli.

Le unità WD Purple, in particolare, sono state progettate e costruite, ci spiegano presso WD, per sistemi di sicurezza ad alta definizione, destinati a funzionare ininterrottamente (24 ore al giorno per 7 giorni la settimana). Non a caso sono in grado di supportare fino a 64 telecamere e sostenere un tasso di workload (cioè la quantità di dati trasferiti da un hard disk a un altro), che arriva fino a 180 TB all'anno. Cioè, precisa Davide Vento, Business manager Italy and Greece, Storage Devices dept di Western Digital, un tasso tre volte superiore a quello tipico di un'unità desktop.

Si tratta di sistemi che sono stati ingegnerizzati appositamente per la videosorveglianza, dotati, infatti, di un software di storage specifico per questa applicazione e potenziato da una tecnologia esclusiva di WD, pronta per supportare l'Ultra-HD, chiamata AllFrame 4K.

Quest'ultima migliora lo streaming ATA per limitare la perdita di fotogrammi, ottimizzare in generale la riproduzione del video e aumentare il numero di alloggiamenti di hard disk supportati all'interno di un NVR (Network Video Recorder).

Scalabilità, affidabilità e durata

Sono caratteristiche che consentono di creare e installare un sistema di sicurezza affidabile su misura per le proprie esigenze di business e destinato a durare nel tempo. A tal proposito, evidenzia Vento, le unità WD Purple sono realizzate con componenti anti-ossidazione, al fine di garantire l'attività anche in ambienti



Davide Vento, Business Manager Italy and Greece, Storage Devices dept di Western Digital

difficili. Inoltre, il già ricordato supporto fino a 64 telecamere consente di espandere il sistema, qualora si dovesse allargare il perimetro da sorvegliare.

La capacità, per questo, non è un problema, grazie alle unità WD Purple da 8 e 10 TB, pensati per i carichi dei video in 4K. Più in generale, le unità sono realizzate con la tecnologia HelioSeal, giunta alla quarta generazione e collaudata sul campo (di 15 milioni di unità fornite fino allo scorso aprile).

L'affidabilità è testimoniata, peraltro, dai numerosi test d'integrità funzionale cui WD sottopone i propri prodotti prima di commercializzarli. A questo si aggiunge l'ampia knowledge base maturata negli anni.

Inoltre gli hard disk WD Purple sono stati progettati per la compatibilità, proprio per consentire di aggiungere capacità al sistema di sorveglianza rapidamente e senza interruzioni. Grazie all'ampia serie di case e chipset supportati è più semplice configurare la soluzione NVR o DVR (Digital Video Recorder) più adatta alle proprie esigenze.

La data protection con gli hard disk WD Gold

Le soluzioni per la salvaguardia dei dati variano secondo le esigenze specifiche di ciascuna applicazione e necessità aziendale. WD fornisce ogni tipo di supporto e tecnologia storage (hard disk, SSD, NAS e altri sistemi per data center di ogni dimensione), per aiutare imprese e persone a usare e proteggere i dati. Gli hard drive WD Gold presentano



caratteristiche avanzate con una capacità di supportare workload a elevate prestazioni: fino a 10 volte il tasso gestito dall'hard disk di un desktop, sostengono presso la casa madre.

Si tratta, infatti di una soluzione "enterprise class", che presenta caratteristiche di efficienza energetica e prestazioni elevate. Una soluzione progettata per un utilizzo tipicamente destinato a server aziendali, ambienti di data center, sistemi di storage aziendali, data warehousing e datamining, NAS aziendale.

Ampia la scalabilità offerta da questa famiglia di hard disk da 3,5 pollici, che presenta unità da 1 TB fino a 12 TB, con la capacità di gestire workload fino a 550 TB all'anno, secondo quanto comunicato dalla casa madre.

Come abbiamo premesso l'affidabilità è una delle caratteristiche che fa la differenza, specialmente quando si parla di salvaguardia dei dati: gli hard disk WD Gold forniscono livelli di durabilità e affidabilità elevati: fino a 2,5 milioni di ore di MTBF (Mean Time Between

Failure- tempo medio tra un guasto e un altro), realizzato pensando alla necessità di gestire operazioni 24x7 in ambienti esigenti.

Per questo gli hard disk WD Gold sfruttano soluzioni all'avanguardia. Di quella HelioSeal si è già accennato, ma la gamma WD Gold impiega anche le tecnologie RAFF e Dynamic fly-height. La prima include un'elettronica sofisticata che controlla l'unità e corregge le vibrazioni lineari e rotazionali in tempo reale. In questo modo si ottiene un significativo miglioramento delle prestazioni in quegli ambienti, per esempio ad alta densità, che comportano vibrazioni più elevate di quelle che percepiamo nei pc.

La tecnologia Dynamic fly height, invece, si preoccupa costantemente di regolare l'altezza della testina per ogni azione di lettura e scrittura, in modo da assicurare sempre le massime prestazioni, ridurre gli errori e massimizzare l'affidabilità. Inoltre, un sistema con due attuatori per il posizionamento della testina, migliora l'individuazione delle tracce dati. Più precisamente, l'attuatore primario provvede al posizionamento generale, affidandosi ai principi elettromagnetici degli attuatori tradizionali. L'attuatore secondario utilizza un movimento piezoelettrico per posizionare le testine con la massima accuratezza. Infine, i WD Gold dispongono di un sistema per il ripristino degli errori limitati nel tempo (TLER) specifico per RAID. Questo permette di ridurre i lunghi blocchi della macchina, dovuti ai processi di ripristino da errori dell'hard disk tipici delle unità desktop. *

Salvaguardare la privacy a dispetto del visual hacking

di
Gaetano
Di Blasio



Il visual hacking è una realtà

3M mette in guardia sugli aspetti fisici della riservatezza dei dati, compresi anche nel GDPR

Vi è parso che lo sconosciuto seduto al vostro fianco sul Frecciarossa stesse sbirciando il monitor del vostro desktop, ma poi, scuotendo la testa vi siete dati del paranoico continuando a lavorare. Ebbene potreste pentirvene.

Gli attacchi mirati opera del cyber crime prevedono una prima fase comune che consiste nella raccolta di informazioni utili a scoprire quali sono i punti di vulnerabilità per penetrare le difese del bersaglio, tipicamente un'azienda. È una fase fondamentale per scegliere gli strumenti dell'attacco e l'informazione che viene cercata primariamente consiste nelle credenziali per accedere ai sistemi informatici di un'impresa.

Proprio username e password che il mobile worker digita per lavorare da remoto, per esempio in viaggio.

Sono tecniche chiamate di social engineering, molto più diffuse di quanto si creda. L'indagine intitolata "Public Spaces Interview Study", realizzata a fine 2017 dal Ponemon Institute e sponsorizzata da 3M ha rivelato che l'87% dei sempre più numerosi "mobile worker" ha sorpreso qualcuno guardare il monitor del proprio notebook da dietro le loro spalle, in uno spazio pubblico.

Un video o una bella fotografia potrebbe aver suscitato della semplice curiosità indiscreta, ma una pagina del foglio elettronico?

Il cosiddetto "Visual hacking" sta crescendo e tre su quattro mobile worker intervistati dal Ponemon Institute affermano di essere preoccupati per questa minaccia, ma la consapevolezza di un problema è solo l'inizio, dopo occorre la soluzione. Eppure oltre la metà degli interpellati ammette di non fare nulla per proteggere le informazioni mentre lavorano in luoghi pubblici.

Sempre gli analisti di Ponemon, nei loro studi sul visual hacking hanno rilevato che il 91% degli attacchi visuali va a buon fine. Inoltre, il 52% dei dati sensibili di un'azienda perde la sua riservatezza poiché viene visualizzato da un impiegato interno non autorizzato.

Il GDPR e la data privacy

La raccolta di ogni genere di dati personali relativi a clienti, prospect o dipendenti è esplosa nell'era delle "data driven enterprise", diventando uno strumento critico per il business. I lavoratori mobili non dovrebbero conservare informazioni sensibili sui propri dispositivi, ma certamente vi accedono tramite essi e, usandoli, li visualizzano sui monitor.

Tutto ciò dovrebbe portare le imprese a valutare con attenzione ogni rischio concernente il trattamento dei dati. Il GDPR (General Data Protection Regulation) è chiaro su questo punto: non si possono ignorare i rischi legati alla sicurezza dei dati, anche in termini di sicurezza fisica. L'articolo 24 del GDPR delinea la responsabilità di un'organizzazione nella salvaguardia dei dati nell'implementare misure tecnologiche e organizzative appropriate, al fine di assicurare e dimostrare una gestione dei dati personali corretta.

L'articolo 32 va oltre, specificando che, nel valutare il livello appropriato di sicurezza, il responsabile deve considerare i rischi rappresentati dal trattamento e utilizzo dei dati, in particolare per proteggerli da distruzione accidentale o illegittima, perdita, alterazione, rivelazione del dato (cioè perdita della riservatezza), o accesso non autorizzato, trasmissione del dato, memorizzazione o altra elaborazione.

Il regolamento europeo sulla data protection pone particolare enfasi sulla prevenzione da accessi non autorizzati alle informazioni, includendo la visualizzazione del dato anche da parte di individui interni ed esterni all'organizzazione.

In altre parole, è previsto che un dato debba essere accessibile solo da personale autorizzato alla sua visualizzazione. Il rischio che un'informazione possa essere carpita anche semplicemente per osservazione è dunque concreto anche in ufficio e le imprese devono tenerne conto, nel dimostrare la propria compliance al GDPR.



Effetto filtrante per la vista laterale

Filtri 3M Privacy contro gli hacker visivi

3M mette a disposizione un'ampia gamma di filtri da applicare ai monitor di qualsiasi dispositivo, dai grandi formati per le workstation fino a tablet e smartphone. Realizzati grazie a una tecnologia ottica avanzata che garantisce privacy visiva e protezione degli schermi, questi filtri costituiscono una difesa dal visual hacking, fornendo protezione contro i danni fisici e l'abbagliamento dello schermo.

Grazie alla tecnologia Microlouver i filtri privacy di 3M oscurano completamente la visione laterale, mentre l'utilizzatore godrà la massima nitidezza dell'immagine dall'angolo di visualizzazione centrale.

Il vicino sul treno o il collega indiscreto vedranno solo uno schermo nero o color oro.

Diversi i modelli disponibili per soddisfare le multiple esigenze del mercato

Ci sono i filtri 3M Privacy Nero con e senza cornice, compatibili con un'ampia gamma di portatili e di monitor esterni, hanno un lato lucido ed uno satinato che aiuta a

ridurre i riflessi. Seguono i filtri 3M Privacy Oro senza cornice (che mantengono tutte le caratteristiche del filtro Nero, fornendo in media il 25% di nitidezza in più rispetto quest'ultimo). A ciò si aggiunge una speciale superficie lucida che proietta uno schermo di un vivido color oro per una privacy superiore. Sono considerati l'ideale, da 3M, per gli schermi ad alta risoluzione.

Per i computer portatili dotati di funzione touch sono stati progettati i filtri 3M Privacy Nero, che forniscono una maggiore risposta tattile, anche grazie al filtro più sottile prodotto dal costruttore, a effetto vellutato e rappresentano la soluzione migliore, a detta dei tecnici 3M per gli schermi ad alta risoluzione con maggiore densità di pixel. Tutti i filtri 3M Privacy possono essere applicati, per garantire la riservatezza e facilmente rimossi ogniqualvolta si vogliono condividere i contenuti.

Le pellicole protettive 3M Privacy per i telefoni, invece, sono progettate per essere usate all'occorrenza: nell'orientamento verticale garantiscono la privacy e in quello orizzontale consentono di condividere lo schermo. L'applicazione è semplicissima e con tecnologia stay-clean si evita l'accumulo di polvere e sporco sui bordi.

Va segnalato che sono possibili personalizzazioni per dispositivi di marche e dimensioni diverse: sul sito di 3M è presente un selettore di prodotto che, in base al vostro dispositivo, individua i filtri compatibili.



Proteggere l'ambiente per proteggere il business e le persone

RISCO ha sviluppato soluzioni per la protezione di ambienti office e di smart working che mettono in sicurezza beni materiali ed immateriali e garantiscono da intrusioni

Proteggere il business non è solo questione di antivirus. La sicurezza deve prendere per prima cosa in considerazione le persone e i beni di un'azienda, garantirne la protezione e, in caso di necessità, un intervento rapido del personale preposto. È questo che RISCO ha posto alla base della sua vision per la sicurezza, sia che si tratti di una PMI sia di una grande azienda, di un centro commerciale od ospedaliero, di un impianto produttivo o un istituto finanziario. Nata col marchio Rokonet nel 1978, RISCO Group si è evoluta nel tempo affermandosi oggi, ha illustrato Ivan Castellan, che ne dirige la sede italiana, come società indipendente di livello globale nello sviluppo e commercializzazione di un'ampia gamma di soluzioni di sicurezza, impianti antifurto ad alte prestazioni, rivelatori e accessori. Il portfolio comprende tecnologie integrate che spaziano dalle connessioni wireless al cloud e allo smartphone e permette di proteggere le aree riservate da intrusioni e allertare immediatamente il personale di vigilanza.

Copertura diffusa e capillare

Chiave delle soluzioni RISCO è il poter realizzare un'infrastruttura di protezione che può coprire l'intera azienda e le sue aree esterne, oltre a permetterne il controllo automatizzato tramite sensori, videocamere e attuatori, controllabili da un unico centro o tramite app su smartphone mediante il cloud RISCO.

Per ottimizzare controllo ed interventi l'area da proteggere può essere suddivisa in decine di microzone, costituite anche da una singola finestra o una porta, che può essere chiusa od aperta in modo automatico, o inviare un allarme se forzata. La protezione può essere rafforzata anche tramite videocamere ad alta risoluzione e applicazioni di gestione software che permettono di evitare i falsi allarmi generati ad esempio in aree esterne ed interne dalla presenza di animali o oggetti in movimento di piccola dimensione, grazie anche a tecnologie proprietarie quali la VPT (Variable Pet Threshold), SRT (Sway Recognition Technology) e DTC (Digital Correlation Technology)



Ivan Castellan, Branch
Manager Italy

Con RISCO Cloud è possibile un controllo ovunque ed in ogni momento

Le soluzioni di sicurezza RISCO coprono dalle PMI al grande impianto



aspetti che richiedono approcci diversi», evidenzia Castellan.

Ma c'è un altro punto su cui RISCO mette in guardia e che costituisce uno degli aspetti salienti dell'analisi: la differenza tra rilevazione di una intrusione e furto di beni.

«Il sistema antintrusione ha lo scopo di rilevare ed avvisare che c'è un intruso ma di per sé non impedisce che un furto vada a termine. Non sempre viene evidenziato ma è un aspetto fondamentale. Perché ciò venga impedito devo compiere altri passi progettuali ed organizzativi e includere nelle variabili anche cosa devo fare a livello di sicurezza per dar tempo al personale preposto di intervenire», spiega Castellan.

Per rispondere in modo esaustivo alle diverse esigenze il portfolio RISCO comprende soluzioni quali:

- Centrali di controllo per PMI, centri uffici, centri commerciali o logistici centrali anche distribuiti.
- Rilevatori commerciali e industriali a standard di grado 2 e 3.
- Controlli accessi per installazioni professionali mono-sito o multi-sito tramite reti fisse, mobili e cloud, mono o multiutente.
- Gestione tramite SynoSYS™ Integrated Security and Building Management, che gestisce in modo intelligente gli apparati e i rilevatori

connessi. Include mappe sinottiche e supporta sistemi di antintrusione, controllo accessi, antincendio e TVCC anche di terze parti.

- Applicazioni per smartphone e web basate su cloud
- Video verifica con validazione degli eventi da remoto.

Soluzioni per grandi installazioni e per PMI

Per rispondere alle diverse esigenze RISCO ha sviluppato diverse soluzioni di sicurezza.

ProSYS Plus è un sistema di grado 3 per grandi progetti scalabile fino a 512 zone che permette di integrare dispositivi di sicurezza cablati, radio e via RISCO Bus. È fruibile tramite un versatile sistema di licenze che, osserva Castellan, riduce il costo del progetto e permette tramite web, smartphone e cloud di gestire e monitorare il sistema in qualsiasi momento e luogo. Integra l'intera gamma RISCO di rivelatori per interno ed esterno, commerciali ed industriali, telecamere IP via cloud, e permette la verifica video degli allarmi e video Live HD.

LightSYS 2 è un sistema ibrido per le PMI dotato di una centrale di grado 2 e controllabile via smartphone. Gestisce sino a 50 zone.

Axeplus è invece un sistema di controllo accesso scalabile basato su cloud e personalizzabile, ideato per ambienti muti sito, senza limiti per numero di porte o utenti gestiti. Tutte le soluzioni sono gestibili tramite SynoSYS e, tramite cloud, con applicazioni Web e smartphone, è possibile disporre di una visione continua della situazione dei sistemi da ovunque. *

Oltre alla gestione diretta da parte dell'utente, le soluzioni di sicurezza si prestano, per come sono state concepite e tramite il cloud, anche ad essere fruito come servizio erogato da partner specializzati.

Partire dall'analisi del rischio

Quello che però fa la differenza tra un sistema di sicurezza efficace e il semplice assemblaggio di dispositivi è l'attenzione verso i servizi, l'analisi globale del rischio e gli obiettivi che ci si prefigge. «L'analisi del rischio è il primo passo da compiere e deve essere effettuata accuratamente e con professionalità dagli installatori professionisti della Sicurezza congiuntamente al cliente, analizzando quale è l'asset da proteggere, come è strutturato, le aree e i beni coinvolti e i rischi a cui al momento può andare incontro. Quello che evidenziamo è anche che ci sono due diversi tipi di beni da proteggere, quelli materiali e quelli immateriali come i dati, due



Atahotel Expo Fiera

Via Giovanni Keplero 12

20016 Pero (Mi) –

13-14-15 marzo



Security Summit è la manifestazione dedicata alla sicurezza delle informazioni, delle reti e dei sistemi informatici che, da anni, appassiona i partecipanti con contenuti e approfondimenti sull'evoluzione tecnologica del mercato.

Giunto alla X edizione il Security Summit si è imposto, ed è riconosciuto dal mercato, come l'Evento di eccellenza nel panorama italiano grazie all'alta qualità dei relatori e alla numerosa partecipazione di pubblico sempre più qualificato.

Anche nel 2018 si confermano questi valori: una struttura articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici.

Certificata dalla folta schiera di relatori (più di 500 sono intervenuti nelle scorse edizioni) provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 15.000 partecipanti, e sono stati rilasciati circa 10.000 attestati validi per l'attribuzione di oltre 16.000 crediti formativi (CPE).

La manifestazione vede impegnati in prima persona gli esperti del Clusit per la parte dei contenuti e Astrea sul fronte organizzativo per le quattro tappe annuali: quest'anno si parte dalla tre giorni di **Milano**, in programma presso l'Atahotel Expo Fiera il 13, 14 e 15 marzo con un'agenda articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici, a partire dalla presentazione del **Rapporto Clusit 2018 sulla sicurezza ICT in Italia e nel mondo**.

La partecipazione a Security Summit è gratuita, previa registrazione al sito securitysummit.it, dove sarà a breve disponibile il programma della tre giorni milanese.

Security Summit ha il patrocinio della Commissione Europea e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazione e della rete.

Organizzato da



www.securitysummit.it