

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

Distribuito gratuitamente con "Il Sole 24 Ore"



**Cyber security e
sicurezza ambientale**

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.



4 LA SICUREZZA LOGICA E FISICA

5 Trasformazione digitale e cyber-resilienza in azienda: a che punto siamo?

7 LA CYBER SECURITY AFFILA LE ARMI

8 Security Governance e gestione del rischio per la digital transformation

10 Come evitare che lo smart working sia una minaccia per le reti

12 Automazione che semplifica la rete aumentando la produttività

14 Un approccio trusted adattativo contro le minacce informatiche

16 Reti virtuali private e Zero Trust aumentano la sicurezza

18 Gli insegnamenti per la sicurezza da trarre dal COVID-19

20 Il 5G sta arrivando. Le implicazioni per la sicurezza

21 UNA SICUREZZA AMBIENTALE E FISICA

22 Al sicuro il telecontrollo della rete elettrica altoatesina di Alperia

24 Una protezione flessibile difende da minacce in continua evoluzione

27 Proteggere i dati aziendali accelera la digitalizzazione

28 Mettere al sicuro l'azienda richiede una accurata integrazione dei sistemi

Direction Reportec • anno XVII • numero 114 - giugno 2020

Direttore responsabile: Gaetano Di Blasio
In redazione: Giuseppe Saccardi, Gaetano Di Blasio, Paola Saccardi, Edmondo Espa
Grafica: Aimone Bolliger
Immagini Dreamstime.com

Redazione:
via Marco Aurelio, 8 - 20127 Milano
Tel 0236580441 - fax 0236580444
www.reportec.it
redazione@reportec.it

Stampa:
A.G.Printing Srl, via Milano 3/5
20068 Peschiera Borromeo (MI)

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.

LA SICUREZZA LOGICA E FISICA

La cyber security s'intreccia sempre più con la sicurezza fisica. Un importante e attualissimo esempio è relativo all'App Immuni, che fornisce uno strumento per contrastare la diffusione del contagio da Coronavirus, ma al tempo stesso preoccupa chi teme possa essere usata da malintenzionati per rubare dati personali. Si ritrovano, così temi importanti come la security by design. Cresce vertiginosamente lo sviluppo di app in generale e quelle dedicate alle esigenze legate alla pandemia, dalla gestione delle code alla prenotazione dell'ombrellone o del pranzo in spiaggia. Oppure app che permettono per esempio di ridurre le esigenze di contatto fisico nella registrazione e autenticazione quando si entra in azienda. Il vantaggio è che in caso di condizioni non idonee l'App invierà un allarme al responsabile del personale, che potrà così intervenire tempestivamente. L'automazione, con l'uso di machine learning o artificial intelligence stanno, del resto, dominando in tutti i settori e la cyber security non è da meno.

GDB



Trasformazione digitale e cyber-resilienza in azienda: a che punto siamo?

di Matthieu Bonenfant,
CMO Stormshield

Le aziende in grado di attuare un vero cambiamento sono nella posizione migliore per limitare l'impatto negativo apportato sul proprio business dall'attuale crisi pandemica

La trasformazione digitale, ormai considerata essenziale al fine di assicurare la continuità operativa di un'azienda, la competitività e la crescita del business, è da anni al centro dell'attenzione delle aziende ed ampiamente dibattuta.

Di conseguenza, si potrebbe ipotizzare che questo sviluppo delle organizzazioni e la trasformazione delle rispettive modalità operative siano ormai diffusi in tutto il tessuto economico e istituzionale, indipendentemente dal Paese, dal settore e dalla dimensione aziendale. Ma è poi davvero così? Non c'è una discrepanza tra ciò che si afferma e la realtà che concretamente si osserva? Nonostante le stime indichino che due terzi delle aziende abbiano fatto progressi in questo ambito nel corso del 2019 (da risultati illustrati in "Barometro della trasformazione digitale di Stormshield", una pubblicazione realizzata in collaborazione con "The Digital Factory"), la risposta a questa delicata domanda è chiara solo ora. Alla luce del periodo di lock-down appena trascorso, contrariamente alle loro stesse ipotesi, molte aziende erano ben lungi dall'essere sufficientemente preparate a passare alla modalità digitale al 100% da un giorno all'altro.

In effetti, questo periodo particolarmente critico ha costituito un vero e proprio banco di prova per verificare la reattività delle aziende e la loro cyber-resilienza. Nel corso delle nostre operazioni di supporto, abbiamo scoperto che molte infrastrutture

IT erano dimensionate per supportare il lavoro a distanza solo per al massimo un terzo dei dipendenti.

Un recente studio di Malakoff Humanis conferma questo dato, osservando che nel 2019 solo il 30% dei dipendenti del settore privato poteva optare per il telelavoro.

Una quota purtroppo insufficiente, in molti settori, a garantire la piena continuità operativa in situazioni critiche come quella che si è verificata.

Lo sviluppo delle organizzazioni è essenziale per sopravvivere

Durante il lock-down molte aziende hanno dovuto adattarsi alla mutata realtà e alle nuove esigenze nel modo di lavorare e cooperare, a volte con un'accelerazione forzata, e continuano a dipendere fortemente dalle tecnologie digitali.

Questo è stato fatto attraverso un massiccio aumento della capacità di telelavoro, la sostituzione di eventi fisici con eventi virtuali, la formazione sotto forma di e-learning, servizi di consulenza e telemedicina a distanza. In alcuni settori l'introduzione dell'online shopping con consegna a domicilio, altrimenti insolito, si è rivelata essenziale per la vendita di prodotti tra cui persino i pasti pronti. Quello che si evince dall'esperienza vissuta è che aziende che sono state in grado di attuare un vero cambiamento sono ora nella posizione



Matthieu Bonenfant, CMO di Stormshield

di prestazioni e produttività, ma chiaramente si configura come uno strumento per la sopravvivenza dell'azienda stessa. Dato questo stato di cose, è chiaro che le aziende devono consolidare o addirittura impostare un nuovo corso per una completa riorganizzazione e sviluppo.

Inoltre, il nuovo posizionamento strategico delle tecnologie digitali nel garantire la sostenibilità delle imprese e la continuità dei servizi pubblici evidenzia l'assoluta necessità di garantirne la tutela. Oggi più che mai, la sicurezza informatica deve essere una responsabilità collettiva cruciale

Trasformazione digitale: priorità assoluta per le industrie critiche

La trasformazione digitale, pur interessando tutti i soggetti, svolge un ruolo ancora più significativo nel garantire il corretto funzionamento delle infrastrutture critiche e operative, in particolare nei settori dell'energia, dell'approvvigionamento idrico, della difesa e della

migliore per limitare l'impatto negativo apportato dalla crisi che sta interessando l'intero globo sul loro business.

La trasformazione digitale, in un tale contesto, non rappresenta più solo una questione

sanità.

In questo contesto, è essenziale costruire infrastrutture in grado di far fronte a una vasta gamma di rischi, compresi i rischi informatici, che costituiscono una minaccia reale.

Ne è un preoccupante esempio l'aumento degli attacchi portati agli ospedali italiani durante la fase più critica della pandemia.

Le organizzazioni sensibili devono procedere alla trasformazione digitale e mettere la sicurezza delle loro infrastrutture al primo posto nella lista degli interventi da fare per continuare a compiere la loro missione vitale per milioni di persone.

Non dimenticare

Dopo la crisi, il pericolo principale sarà la convinzione di poter tornare ai metodi di lavoro precedenti e fingere che questa situazione eccezionale sia un unicum.

Tuttavia, lo shock che abbiamo vissuto deve aiutare a identificare più chiaramente le lacune che la tecnologia digitale può colmare, apportando miglioramenti in termini di continuità del business, gestione delle relazioni con i clienti, comunicazione interna ed esterna, aggiungendo valore ai prodotti e ai servizi che si offrono e mantenendo i collegamenti sociali quando è richiesta la distanza.

I progetti di trasformazione digitale e le relative questioni di sicurezza informatica non devono più essere visti come tematiche puramente tecniche, ma come una fonte di resilienza aziendale e una priorità assoluta per il management. ✱

LA CYBER SECURITY AFFILA LE ARMI

Con l'uso di machine e deep learning e lo sviluppo di soluzioni sempre più affidabili nella threat detection e nella capacità di risposta si risponde alle minacce

Security Governance e gestione del rischio per la digital transformation

Micro Focus promuove un modello di sicurezza esteso, predittivo e Zero Trust per proteggere dati, utenti e applicazioni

Micro Focus si è affermata negli ultimi anni come una protagonista nel settore della security. Una crescita avviata a partire dal 2017 con l'acquisizione della divisione software di HP Enterprise e, successivamente, ampliata e rafforzata attraverso un processo di estensione e integrazione delle soluzioni software, una riorganizzazione dell'offerta in famiglie di prodotti e altre acquisizioni strategiche come quella di Intersect, azienda che ha portato in dote soluzioni all'avanguardia di machine learning.

Oggi, Micro Focus propone un modello di sicurezza estesa, predittiva, intelligente, integrata, basata su security governance e gestione del rischio per accompagnare la transizione delle aziende verso un modello sicuro di digital transformation. L'approccio di Micro Focus è quello di una Zero Trust Security in cui nessun privilegio viene assegnato a priori e l'accesso a ogni risorsa aziendale deve essere motivato dalla propria attività lavorativa e il proprio ruolo.

«Le imprese di ogni tipo sono ormai obbligate a compiere una trasformazione digitale per poter competere in un mondo sempre più interconnesso, digitalizzato e intelligente - afferma Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus -. Micro Focus ha un approccio di sicurezza basato sulla governance e la gestione del rischio in cui le nuove tecnologie di intelligenza artificiale e machine learning forniscono il substrato per un'analisi intelligente, capace di rispondere in tempo reale a ogni possibile minaccia. Questo approccio è realizzato attraverso una gamma di soluzioni e tecnologie, organizzate in una serie di famiglie di prodotti che affrontano in modo completo le tre tematiche di protezione: dati, utenti e applicazioni.»



*Pierpaolo Ali, Director
Southern Europe Security,
Risk & Governance di
Micro Focus*

Governare il nuovo perimetro dell'identità

In un contesto dominato da forme di lavoro mobili e dal cloud, le identità degli utenti sono ciò che delinea il nuovo perimetro aziendale da proteggere e, in ambienti ibridi complessi, è sempre più facile perdere il controllo su tutti i privilegi di accesso alle risorse aziendali.

Le soluzioni Micro Focus NetIQ per la governance dell'identità e dell'accesso

risolvono questi problemi, consentendo di rilevare situazioni non conformi, bloccare qualsiasi tentativo di accesso non autorizzato ed effettuare azioni automatiche di correzione. Per esempio, NetIQ Identity Governance analizza automaticamente tutte le informazioni sui diritti degli utenti legate a sistemi, applicazioni e dati per identificare in tempo reale le situazioni in cui gli utenti hanno accesso non motivato alle risorse.

«Operare in sicurezza con una forza lavoro distribuita è diventato una necessità per la maggior parte delle aziende - puntualizza Ali -. In pochi mesi abbiamo osservato anni di innovazione nel modo di lavorare, accelerando il passaggio da quello che era considerato un modello ideale a una necessità. L'architettura Zero Trust e l'approccio integrato di security governance e risk management di Micro Focus offrono alle aziende le caratteristiche di flessibilità, sicurezza e capacità di adattamento di cui hanno bisogno».

Cifratura persistente dei dati, anche durante l'uso

Attraverso la famiglia di soluzioni Voltage Security, Micro Focus mette a disposizione gli strumenti per garantire una sicurezza persistente, consentendo di cifrare i dati quando sono archiviati, mentre vengono trasferiti e anche durante l'utilizzo grazie a tecnologie esclusive e brevettate.

Il più recente componente della famiglia è Voltage SmartCipher, che permette di applicare ai file una protezione persistente, che li

segue attraverso il loro intero ciclo di vita. Attraverso un sistema centralizzato di "policy management" aggiornabile da remoto è possibile individuare i file, monitorare il loro utilizzo e prevenire l'accesso non autorizzato per mantenerli sempre protetti, sia on premise sia in cloud. «Il portafoglio di soluzioni Micro Focus Voltage protegge i dati sensibili e abilita controlli granulari, riducendo il rischio di violazione della privacy - spiega Ali -. L'introduzione sul mercato di Voltage SmartCipher mette a disposizione dei nostri clienti la possibilità di gestire e proteggere in modo completo anche le informazioni sensibili contenute nei file non strutturati, mantenendo il costante controllo sul loro accesso e utilizzo. Tutto questo in modo trasparente per l'utente e senza creare discontinuità nell'ambiente di security preesistente».

Protezione intelligente dalle minacce

Alla difesa dalle minacce Micro Focus dedica ArcSight, una piattaforma di Security Information and Event Management (SIEM) di tipo modulare e integrata, adatta ad ambienti on-premise, cloud e ibridi e dotata della tecnologia Intersect di machine learning non supervisionato.

Intersect fornisce analisi rapide e accurate di rilevamento delle minacce, attraverso un meccanismo di attribuzione di indici di rischio individuali, definiti in base all'analisi del comportamento di un utente rispetto al suo modello esperienziale o a quello di utenti con un

profilo analogo.

«Grazie al machine learning - continua Ali - le attività di correlazione e sicurezza preventiva e prescrittiva risultano significativamente potenziate, abilitando una Security intelligence evoluta. L'Intelligenza artificiale porta le analisi a un livello di accuratezza superiore, mentre il modello di machine learning non supervisionato di ArcSight Intersect abilita un processo di adattamento dinamico automatico al mutare del contesto. In questo modo, non c'è bisogno di preimpostare riferimenti di confronto, che renderebbero il processo più statico e meno rapido nell'affrontare nuovi scenari».

Protezione del ciclo di vita delle applicazioni

L'ultimo tassello della protezione Micro Focus è la famiglia di soluzioni Fortify, che fornisce gli strumenti per affrontare in modo efficace e strutturato il processo di controllo delle applicazioni attraverso il loro intero ciclo di vita.

Le soluzioni Fortify Micro Focus forniscono gli strumenti per effettuare test di sicurezza applicativa in modalità statica e dinamica, garantire uno sviluppo sicuro e analizzare il codice per cercare vulnerabilità mentre è in esecuzione.

Fortify è inserita da sette anni di seguito tra i leader nel Gartner Magic Quadrant for Application Security Testing e ha ottenuto il punteggio più alto nel report 2020 Gartner Critical Capabilities for Application Security Testing per il caso d'uso Enterprise e il caso d'uso Mobile and Client. *

Come evitare che lo smart working sia una minaccia per le reti

Uno studio di CyberArk evidenzia che nello smart working il 77% dei dipendenti utilizza dispositivi personali non gestiti, con forti rischi per le credenziali privilegiate

La diffusione dello smart working sta permettendo a molte aziende di continuare ad essere operative anche in un momento di crisi come l'attuale, perlomeno per la componente del lavoro non strettamente legata a produzione di fabbrica e laddove la presenza fisica è indispensabile.

Se però in azienda si è abituati a comportamenti virtuosi per quanto concerne le procedure di sicurezza da osservare e nell'utilizzo degli strumenti informatici a disposizione, e si è soggetti a criteri di sicurezza e controlli informatici severi, questo può non esserlo quando ci si trova in ambito domestico e, di conseguenza, si può aprire la strada a comportamenti poco virtuosi e forieri di problemi.

In proposito i dati di recenti analisi sono auto-esplicativi e allarmanti. Un'indagine di CyberArk (cyberark.com/it), azienda con una presenza mondiale specializzata in soluzioni di sicurezza per la gestione dell'accesso privilegiato, ha infatti rilevato che le abitudini di lavoro da casa, compreso il riutilizzo delle password e la possibilità per i membri della famiglia di usare i dispositivi aziendali, stanno mettendo a rischio i sistemi critici e i dati sensibili delle organizzazioni.

L'indagine, ha spiegato CyberArk, si è posta l'obiettivo di valutare lo stato della sicurezza nell'attuale ambiente di lavoro remoto ed ha permesso di rilevare che:

- il 77% dei dipendenti utilizza per accedere ai sistemi aziendali dei dispositivi "BYOD", ovvero di proprietà personale, che per lo più non sono gestiti e risultano dunque insicuri.
- Il 66% dei dipendenti ha adottato strumenti di comunicazione e collaborazione come Zoom e Microsoft Teams, per i quali è stato recentemente segnalata la presenza di vulnerabilità di sicurezza, successivamente rimosse, ma indicative di come strumenti non controllati e gestiti centralmente possano essere molto pericolosi e aprire la strada al trafugamento di dati sensibili.

Non è tutto. Lo studio realizzato da CyberArk ha altresì rilevato che i rischi in cui può incorrere la sicurezza aziendale diventano ancora più elevati quando a lavorare in home working si tratta di genitori. Si tratta di persone che hanno

dovuto trasformarsi rapidamente in insegnanti, assistenti e compagni di gioco a tempo pieno, un contesto “multi funzione” per cui non sorprende che le buone pratiche di sicurezza non siano sempre in cima ai pensieri quando si tratta di lavorare da casa. In particolare, in un tale contesto caotico in quanto ad attività:

- Il 93% ha riutilizzato le password per applicazioni e dispositivi diversi.
- Il 29% ha ammesso di consentire ad altri membri della famiglia di utilizzare i dispositivi aziendali per svolgere attività scolastiche, ludiche o addirittura per lo shopping in rete.
- Il 37% salva in modo non sicuro le password nei browser sui propri dispositivi aziendali.

La corsa per offrire nuove applicazioni e servizi che consentono il lavoro a distanza, associata a connessioni non protette e pratiche di sicurezza pericolose, ha anche ampliato in modo significativo la superficie di attacco.

È quindi importante, osserva CyberArk, aggiornare le strategie di sicurezza per adattarsi a questo nuovo panorama dinamico di minacce, soprattutto quando si tratta di salvaguardare le credenziali privilegiate dei lavoratori remoti che, se compromesse, potrebbero lasciare scoperti i sistemi e le risorse aziendali più critiche.

Proteggersi dal furto di credenziali

Il problema del proteggere gli endpoint, soprattutto se remoti o accessibili a più utenti, deriva

anche dal fatto che su di essi sono spesso presenti i diritti di amministratore locale.

Per mitigare il rischio CyberArk ha reso disponibile una specifica funzione di “deception” che migliora la soluzione CyberArk Endpoint Privilege Manager. In pratica, consente di rilevare rapidamente e di bloccare proattivamente gli attacchi in corso, di interrompere la catena di attacchi al punto di ingresso iniziale, di disporre di un modo per rintracciare gli aggressori, mitigare l’uso delle credenziali privilegiate e ridurre il tempo di permanenza.

«Il malware per furti di credenziali è disponibile velocemente e facile da implementare, inoltre, cosa ancora più importante, è estremamente efficace. Le tecniche di attacco stanno diventando sempre più diffuse ed efficaci per meglio comprendere i movimenti e la mentalità di un aggressore, permettendo al contempo di bloccare immediatamente e proattivamente



Massimo Carlotti, Pre-Sales Team Leader di CyberArk in Italia

il progredire dell’attacco», ha osservato Massimo Carlotti, pre-sales team leader di CyberArk in Italia.

Parte integrante della soluzione è una versione fruibile in modalità “Software as a Service” che ha l’obiettivo di consentire alle organizzazioni aziendali di ridurre il rischio di accessi amministrativi non gestiti sugli endpoint con sistema operativo Windows o Mac. Tra le funzionalità due sono molto utili:

- Elevazione e accesso Just-in-Time: le funzionalità Just-in-Time consentono di mitigare il rischio e ridurre l’impatto operativo abilitando a livello amministrativo l’accesso on-demand per periodi di tempo specifici, con un audit log completo e la possibilità di revocare l’accesso in caso di necessità.
- Applicazione dei Privilegi Minimi: implementando politiche di privilegi minimi, le organizzazioni possono ridurre la superficie di attacco, eliminare i privilegi di amministratore locale non necessari e consentire l’esecuzione di applicativi e processi strettamente indispensabili per eseguire l’attività richiesta e pertinente per quello che è il ruolo dell’utente.

A queste si aggiunge la possibilità di bloccare il furto delle credenziali. Consiste in una protezione avanzata che consente di rilevare e bloccare i tentativi di furto delle credenziali sugli endpoint, nonché di quelle memorizzate dal sistema operativo, le applicazioni IT e quelle di accesso remoto e dai browser web più diffusi. ❄

Automazione che semplifica la security e aumenta la produttività

Le varie aree della sicurezza di Cisco
accrescono la protezione e migliorano le
operation aziendali

Cisco sta investendo molto nella cyber security, che è un elemento distintivo nell'offerta, come ci segnala Fabio Panada, Senior Security consultant di Cisco, sottolineando come sia stata progettata per integrarsi efficacemente in tutte le quattro aree in cui opera l'azienda statunitense : sicurezza, networking, cloud e data center.

In ciascuna area si trovano soluzioni efficaci, ma il punto di forza principale si manifesta nella capacità d'integrazione delle singole soluzioni, in modo da costituire una vera piattaforma.

L'integrazione si apprezza particolarmente, sottolinea Panada, nell'interazione con le altre business unit di Cisco.

In pratica, ci spiega l'esperto, non si tratta di un prodotto da aggiungere alla dotazione di sistemi per la sicurezza, ma di uno "strumento" che si può calare nella realtà del cliente per rendere più efficace l'utilizzo di queste tecnologie.

Aggiunge Panada: «Siamo in un mondo sempre più connesso e i nostri clienti ci chiedono semplificazione per tutte le aree compresa la sicurezza: chiedono capacità di automazione, per abbassare i costi di gestione e orchestrazione per far "dialogare" tutte le componenti che sono all'interno della infrastruttura del cliente, la piattaforma che proponiamo soddisfa queste richieste».

Le aree di riferimento in termini di sicurezza: network security, cloud security, application security ed endpoint security, fanno tutte parte dell'offerta integrata, costruita con investimenti che, evidenzia Panada, hanno permesso di realizzare una piattaforma unica sul mercato con, alle spalle il gruppo di ricerca Talos, che va ad arricchire tutte le componenti della piattaforma.

In particolare, Talos fornisce molteplici servizi: da quelli informativi a quelli di incident response, handling, ricerca sulle vulnerabilità e altri. Inoltre aiuta a migliorare i prodotti.

Anni di investimento per aggiungere soluzioni, rileva ancora Panada sono concretizzati nella realizzazione di una piattaforma integrata, automatizzata, che ha coinvolto non solo la sicurezza ma anche gli altri ambiti di sviluppo in cui opera Cisco.

La recente piattaforma permette di risolvere alcuni problemi che i clienti devono

affrontare. Tra i primi, la profilazione delle tante soluzioni di sicurezza esistenti in azienda che spesso non sono armonizzare fra loro.

Per esempio un'importante semplificazione si ottiene nella threat response e l'analisi degli incidenti, grazie all'automazione di alcune attività, in particolare SecureX è in grado di raccogliere informazioni da vari strumenti, accedere al back office e creare in automatico alert o direttamente dei ticket, impostando work flow che aiutano a gestire l'operatività quotidiana,



Fabio Panada, Senior Security consultant di Cisco

non solo della security, ci illustra ancora Panada aiutandoci con un esempio.

Il Covid 19 ha portato un aumento di connessioni VPN.

La possibilità di analizzare il carico della VPN, monitorarlo, creare un ticket, se si registra un superamento di soglia, magari, Inviare una richiesta di provisioning di un nuovo terminatore VPN, può essere un workflow generato in modo completamente automatico.

Peraltro l'automazione della sicurezza è praticata da tempo in Cisco, anche attraverso analytics, nel back end, che consentono di analizzare in maniera trasparente i dati dell'infrastruttura . attraverso vari strumenti di machine learning, analizzando log di firewall, di mail e altro Permettendo analisi automatiche.

Gli attacchi cambiano in maniera continuativa, con vulnerabilità che vengono scoperte di continuo. Quando accade un simile caso le aziende si preoccupano, ma lo strumento di Cisco fornisce subito informazioni su quali e quanti dispositivi sono a rischio.

Varie piattaforme per la gestione di strumenti, quali console SIEM o sistemi MDM, nonché strumenti simili possono ottenere grandi benefici.

A qualunque azienda che acquista un prodotto Cisco Security, viene fornito SecureX gratuitamente. Questo vale anche per i clienti che dispongono di piccole soluzioni, come Umbrella, afferma Panada. Essendo SecureX cloud base, inoltre, non serve installare nulla. Non si tratta di un ulteriore strumento

da aggiungere all'infrastruttura, ma di una soluzione che i nostri clienti già hanno e possono usarla per semplificare, conclude Panada, lasciandoci con un esempio attuale che ben esprime le potenzialità operative e di business dell'automazione.

Office 365 in VPN si gestisce in automatico

Molte aziende utilizzano Office 365 accedendovi tramite una VPN (Virtual Private Network.) per una maggiore sicurezza. Non entriamo in dettagli tecnici, ma basti sapere che ciò genera un carico di rete potenzialmente importante, a seconda di quante email si spediscono e quali attività si svolgono. Cisco SecureX gestisce in automatico tutte le operazioni necessarie per ottimizzare la rete e garantire l'operatività e, di conseguenza, la produttività del dipendente. Una soluzione strategica per lo smart working.

Un altro automatismo semplifica il processo dei controlli per la sicurezza. In particolare, un addetto è tenuto a controllare l'informativa pubblicata quotidianamente sul portale del CERT (Computer Emergency Response Team) Italiano. Deve poi raccogliere gli indicatori di compromissione relativi all'informativa stessa, quindi deve confrontare tali indicatori per verificare se nell'infrastruttura dell'azienda ci sono elementi interessati dalla notifica e, infine applicare i rimedi necessari, qualora siano emerse criticità.

SecureX fa tutto ciò in tempi rapidissimi senza errori umani. ❁

Un approccio trusted adattativo contro le minacce informatiche

Libraesva protegge con efficacia le aziende dai pericolosi attacchi via mail con soluzioni dedicate al mondo enterprise

Libraesva si occupa da oltre un ventennio di sicurezza delle email. Ci sono voluti molti anni (e molti protocolli) per aggiungere meccanismi tecnici di sicurezza delle email lungo il tragitto tra il computer di origine e quello di destinazione. Nel panorama odierno, a preoccupare è il trend senza sosta delle minacce alle aziende e alle loro risorse, che va ben al di là del solo spam. Di fatto tutto ciò che viene veicolato tramite email può potenzialmente trasportare codice malevolo con caratteristiche molto diverse. Come ci spiega Paolo Frizzi, Ceo di Libraesva: «Gli strumenti per contrastare gli attacchi informatici ci sono, ma oggi la sfida è intercettare minacce mutevoli o sconosciute». Un dato di fatto è che la posta elettronica costituisce il veicolo privilegiato per gli attacchi usati contro ambiti business. Basti pensare ai molti Ceo presi di mira con truffe di tipo BEC (Business Email Compromise) apparentemente inviate da loro collaboratori fidati e volte a sottrarre ingenti somme di denaro. Libraesva parla di "Castello di Carte" per indicare quanto sia delicato l'equilibrio tra attaccanti e vittime, e quanto articolato sia il meccanismo che lo tiene in piedi. Lato difesa, la sfida per quanti si occupano di sicurezza informatica e di email security è ogni giorno elevata vista la facilità con cui gli attaccanti riescono a veicolare messaggi ingannevoli e malevoli, pur nel rispetto di tutti i protocolli di sicurezza aziendali. Specializzata in email security, Libraesva vanta un approccio innovativo nel settore che consente di rilevare e a disarmare gli attaccanti intervenendo sui vettori e sulle modalità di intrusione da questi prescelti e adattando la propria strategia per bloccare ogni attacco già in fase di prima analisi. Questo approccio è l'elemento vincente che, afferma Frizzi con orgoglio, ha portato «Palo Alto Networks a siglare un accordo a livello mondiale con Libraesva, di cui apprezza anche la puntualità e il basso livello di falsi positivi».

Il valore di una relazione con l'Adaptive Trust Engine

Ad apportare un ulteriore livello di sicurezza in contesti business, Libraesva ha ideato ATP - Adaptive Trust Engine: un meccanismo che assegna una sorta di punteggio al livello di fiducia in una comunicazione. L'idea di base parte

dall'analisi dello storico di una relazione. In buona sostanza, vengono considerate anche le interazioni che costituiscono un rapporto nel tempo tra mittente e ricevente con il quale viene calcolato un valore della fiducia attribuita a una comunicazione.

È facile comprendere che un "first time sender" è uno sconosciuto e come tale desta attenzione, così come è intuitivo che un messaggio arrivato da un abituale fornitore possieda un valore di fiducia più alto.

Tale matrice di fiducia viene costruita sia a livello di persone, cioè considerando la storia tra due indirizzi di posta, sia a livello di organizzazione.

Per esempio: «Siamo in grado di distinguere quando un utente riceve una comunicazione per la prima volta dall'azienda ACME, riconoscendo che con ACME sussiste uno storico di interazioni, magari con altri impiegati, alzando il punteggio. Si possono considerare anche altre triangolazioni con ACME ed elevare il livello di fiducia» spiega uno degli esperti Libraesva.

Nell'Adaptive Trust Engine, di recente rilascio, Libraesva aggiungerà già questa estate ulteriori sistemi per raffinare il valore di fiducia e per identificare anomalie nella spedizione dei messaggi.

Altro tema critico è quello della pertinenza. Capita di spedire un messaggio all'utente sbagliato, tant'è che varie organizzazioni aggiungono un "footer" nell'email, chiedendo di cancellare il messaggio qualora sia arrivato al destinatario errato. Di fatto si tratta

comunque di una fuoriuscita di contenuti, magari non grave, comunque più o meno imbarazzante. Con la prossima evoluzione estiva, l'Adaptive Trust Engine di Libraesva potrà valutare le email in uscita, sempre in base ai valori di fiducia, chiedendo all'utente di verificare i corretti destinatari prima di far partire la mail. La soluzione si propone dunque di agire nel processo di relazioni sociali mediate dal mezzo email su cui fanno leva in maniera esponenziale gli attaccanti per perpetrare i loro attacchi.

Il disarmo alle minacce informatiche è un lavoro condiviso

Sia che le email siano in transito tra caselle di posta sia che siano già archiviate, è fondamentale mantenere alta l'attenzione alla sicurezza. Le soluzioni di email security della società italiana, con



Paolo Frizzi, CEO di Libraesva

sedi a Lecco e a Londra, operano su tutte le tipologie di file e allegati - pdf e formati Office i più comunemente usati - agendo sul loro codice prima che raggiunga la casella di destinazione.

Nel mondo enterprise così come nella pubblica amministrazione, con le molte comunicazioni trasmesse quotidianamente e l'elevata sensibilità dei dati in queste contenuti, è comprensibile quanto sia importante poter adottare un approccio di prevenzione contro le minacce efficaci.

Frizzi spiega come «Con il nostro approccio preventivo e non solo reattivo, siamo in grado di salvaguardare la reputazione e l'integrità aziendale, con riguardo anche ai requisiti dell'attuale normativa vigente. I nostri strumenti di "deep inspection" dei contenuti email, sia in transito sia archiviati, cooperano con le infrastrutture IT esistenti, consentendo allo stesso tempo a ogni singolo utente di accedere alle proprie risorse "in quarantena" in totale sicurezza».

Il manager ribadisce un concetto fondamentale: «Le minacce odierne fanno leva in misura crescente su logiche di ingegneria sociale per propagarsi nei sistemi aziendali - reti, cloud, pc e dispositivi mobili. È quindi imprescindibile che sia adottato oggi un approccio collaborativo e che vi sia una consapevolezza condivisa tra tutti i livelli e i reparti aziendali sui rischi che tali minacce rappresentano in termini di produttività e quindi anche economici per poter vincere insieme questa importante sfida di sicurezza».



Reti virtuali private e Zero Trust aumentano la sicurezza

La diffusione del cloud pubblico e dello smart working richiedono nuovi approcci alla sicurezza. Quali e con che benefici lo ha illustrato SolarWinds

La diffusione del cloud pubblico e il crescente ricorso allo smart working imposto da nuovi modelli nel lavorare e cooperare, impongono un profondo ripensamento della postura aziendale per quanto concerne la cyber security e il come garantirla.

Ai problemi usuali, e di per sé già complessi, connessi alla protezione del perimetro aziendale e ai dispositivi e applicazioni che racchiude, si sono sommati quelli relativi ad ambienti distribuiti, alla mobility e al massiccio ricorso allo smart working.

È uno scenario in forte evoluzione che ha reso evidente come le usuali strategie di salvaguardia dei dati, delle applicazioni e degli utenti non risultino più in grado di fornire una protezione adeguata.

Come sia possibile migliorare la sicurezza e la sua gestione lo abbiamo chiesto a Tim Brown, VP Security di SolarWinds MSP (www.solarwindsmsp.com/it), un'azienda globale con sede in Texas che sviluppa software di gestione IT rivolto primariamente agli MSP e che fornisce una sicurezza su più livelli tramite il ricorso all'intelligenza collettiva e ad una spinta dall'automazione.



Tim Brown, VP Security di SolarWinds e SolarWinds MSP

GS: Cos'è cambiato nell'ultimo anno nell'ambito della sicurezza e protezione dei dati?

TB: Nel corso dell'ultimo anno il panorama delle minacce ha subito un'evoluzione e i criminali informatici ora agiscono in modo più mirato e strategico. Nel mondo sono stati registrati attacchi ai danni di ospedali, città e infrastrutture. I criminali sono diventati più perseveranti, organizzati e alla ricerca di infiltrazioni di maggiore portata che offrono opportunità di guadagno più elevate.

GS: In questo preoccupante scenario come dovrebbe essere gestita o articolata l'infrastruttura IT per la protezione e la sicurezza dei dati e delle applicazioni aziendali?

TB: Nel mondo ibrido odierno, è fondamentale per le imprese adottare un approccio che ponga al centro dati e applicazioni. Si tratta di quello che spesso chiamiamo un modello di sicurezza "zero trust". Con questo approccio, ciascuna applicazione viene considerata singolarmente con la relativa protezione, mentre l'impresa viene considerata come l'insieme di queste applicazioni. È necessario implementare criteri rispettati da tutte le applicazioni, in modo da poter continuare ad utilizzare tutte quelle applicazioni on-premise e SaaS impiegate dalla maggior parte delle aziende.

GS: Come può essere posto in atto in azienda un modello "zero trust"?

TB: L'implementazione di un modello zero trust non può essere immediata, ma è comunque fondamentale ora che la maggior parte delle persone lavora da casa e non più all'interno del perimetro aziendale, cosa che in passato permetteva di affidarsi a un livello di sicurezza di base predefinito. Ora invece gli utenti accedono alle reti aziendali da nuovi dispositivi e nuovi luoghi. Questo aspetto rende l'identità un fattore cruciale per il modello zero trust. In assenza di un perimetro di rete ben definito, i rischi vanno ricollegati a singoli utenti, dispositivi e applicazioni.

GS: In sintesi, che benefici fornisce il modello zero trust e perché le aziende dovrebbero preferirlo a quelli sinora adottati?

TB: Le imprese che si sono preparate a implementare questo nuovo modello saranno molto più in grado di affrontare con successo la situazione attuale rispetto a quelle che si sono sempre affidate a una VPN per garantire l'accesso di tutti i dipendenti a ogni sistema.

GS: Smart working e mobilità stanno influenzando in modo significativo il problema di come garantire la protezione e la sicurezza dei dati.

Quali sono le applicazioni business critical più a rischio di cyber attacchi e come possiamo proteggere queste applicazioni e gli endpoint?

TB: Diventa fondamentale implementare più livelli di protezione. Gli utenti amministrativi e quelli che ricoprono ruoli con accesso a dati sensibili dovrebbero poter contare su una protezione maggiore rispetto agli utenti generici. Lo stesso modello va implementato per le applicazioni: l'azienda deve individuare le risorse più importanti, vale a dire applicazioni, dipendenti e processi. Quali siano le risorse business critical dipende dalla singola azienda, ma individuarle è fondamentale per garantire un'adeguata riduzione del rischio.

GS: Il cloud rappresenta un'opportunità, ma da alcuni è ritenuto anche un rischio. Quali misure sono necessarie per

proteggere dati e applicazioni in un cloud storage privato e pubblico, ad esempio Office 365, e quali applicazioni sono più a rischio?

TB: Una delle prime cose da tenere sempre presente circa applicazioni cloud pubbliche è proprio il fatto che sono pubbliche, ovvero accessibili da chiunque; pertanto non va mai utilizzata solo la password per proteggere l'accesso utente. Ad esempio, Microsoft 365 (noto in precedenza come Office 365) supporta l'accesso condizionale, che rappresenta una forma di autenticazione a più fattori; questo approccio va sempre implementato per garantire un ulteriore livello di sicurezza. Per tutte le applicazioni cloud pubbliche è importante capire come vengono protetti i dati e chi vi ha accesso. La condizione ideale è quella in cui il cliente è responsabile della chiave di crittografia, mentre il fornitore non ha accesso ai dati anche se si verifica una violazione della sicurezza.

GS: Quale ruolo ricopre un sistema di gestione moderno e quali servizi o funzionalità sono necessari?

TB: Un sistema di gestione moderno deve prendere in considerazione l'ambiente ibrido e offrire un unico pannello di controllo da dove gestire tutte le applicazioni cloud e on-premise. Inoltre, deve garantire l'implementazione e il rispetto di opportune policy di sicurezza in egual modo su tutti i sistemi, segnalando e documentando i rischi associati a un determinato ambiente. *

Gli insegnamenti per la sicurezza da trarre dal COVID-19

WatchGuard ha identificato otto suggerimenti per i responsabili dei team IT per garantire la sicurezza e pianificare la continuità aziendale nel perdurare della pandemia

Quella in corso è una pandemia di proporzioni mai viste per l'impatto che sta avendo sul mondo produttivo. Le aziende si sono rapidamente mobilitate per far fronte alla minaccia e il numero di persone che lavorano da casa è più elevato che mai, dando una forte accelerazione all'adozione dello smart working, che ha alleviato il negativo impatto sul mondo aziendale ma che espone a rischi in termini di sicurezza.

Una delle problematiche derivanti dall'avere una forza lavoro operativa a distanza, osserva in proposito WatchGuard (watchguard.com/it), azienda specializzata nello sviluppo di soluzioni per la sicurezza e continuità del business aziendale, è che le probabilità di essere vittima di attacchi informatici aumentano significativamente.

«Con il lavoro da remoto, le probabilità che un dipendente sia vittima di attacchi informatici aumentano significativamente - spiega Francesco Pastoressa, Marketing Manager Secur & Nordics di WatchGuard Technologies - poiché si è sprovi-

sti delle protezioni offerte dalla rete aziendale principale. È tempo che le aziende si preparino in maniera ragionata e strutturata ad affrontare gli aspetti di sicurezza legati a remote working o smart working, in quanto modelli che si avviano ad essere permanenti e non più parentesi emergenziali legati alla contingenza della recente epidemia di Covid-19. Promuovere attivamente all'interno dell'azienda la cultura della sicurezza, stabilendo standard e aspettative, parallelamente all'implementazione di tecnologiche come la VPN, l'autenticazione a più fattori, i filtri DNS e così via, sono alcune tra le azioni che le aziende e i responsabili dei team IT dovranno intraprendere per garantire la continuità del business». Senza i benefici intrinseci alle protezioni offerte dalla rete aziendale, i dispositivi degli utenti in



Francesco Pastoressa, Marketing Manager Secur & Nordics di WatchGuard Technologies

mobilità o all'esterno dell'azienda possono infettarsi senza che l'IT aziendale ne venga a conoscenza e, di conseguenza, diventare un punto di propagazione dell'infezione quando si riconnettono alla rete. A ciò si aggiungono altre sfide derivanti dal sovraccarico delle VPN e da problemi di larghezza di banda. Cosa fare in questo scenario? WatchGuard ha stilato otto suggerimenti per superare queste sfide.

Inventariare e valutare le risorse

Per molte aziende il passaggio al telelavoro è avvenuto repentinamente e non c'è stato il tempo di provvedere a una pianificazione adeguata. Ora è il momento di verificare e valutare le nuove necessità di accesso alla rete e di considerare le implicazioni a livello di sicurezza. Per le persone che prima non lavoravano da casa, può, invece, essere utile stilare un inventario di tutti i dati e le applicazioni a cui accedono regolarmente. Partendo da questo, sarà possibile stabilire a quali sistemi devono avere accesso, chi ha la necessità di accedere e quale sia il modo migliore di fornire questi accessi.

Stabilire le aspettative e comunicarle

È probabile che per molti dipendenti dell'azienda quella in corso sia la prima esperienza di telelavoro. È quindi il momento giusto per comunicare la policy aziendale e chiarire quali sono le aspettative nei confronti di chi lavora da remoto.

Promuovere una cultura per la sicurezza

I responsabili della sicurezza aziendale devono favorire l'apertura di canali di comunicazione in modo che se un dipendente si rende conto di qualcosa che potrebbe costituire una minaccia si senta autorizzato a segnalarlo sapendo che riceverà la dovuta attenzione.

Autenticazione a più fattori

È consigliabile implementare l'autenticazione a più fattori per tutti gli utenti, così da autenticarli in modo completo ogni volta che si connettono alla rete. Ciò consentirà di proteggere l'accesso alle applicazioni e agli ambienti cloud a cui i telelavoratori possono accedere direttamente da Internet.

Estendere l'accesso alla VPN agli utenti prioritari

Affinché i dipendenti mantengano la stessa produttività lavorando da remoto è essenziale una connessione sicura alla sede principale dell'azienda e alle applicazioni critiche. Le reti private virtuali (VPN) aggiungono un livello di sicurezza alle reti private e pubbliche, consentendo a persone e organizzazioni di inviare e ricevere dati via Internet in modo sicuro.

Garantire la sicurezza dai clic pericolosi

Con i dipendenti che lavorano da casa, è possibile che i computer portatili aziendali vengano utilizzati anche per una serie di attività personali di navigazione in rete e controllo dell'e-mail. I filtri DNS in

cloud permettono di bloccare le connessioni e limitare l'accesso ad aree di Internet rischiose.

Endpoint liberi da malware

Sebbene le soluzioni antivirus per gli endpoint intercettino molte delle minacce, non hanno alcun potere contro il malware elusivo zero day che spesso si osserva. Le soluzioni di rilevamento e risposta per gli endpoint non solo rilevano queste minacce avanzate, ma sono in grado di neutralizzarle e riportare al normale funzionamento il dispositivo infettato agendo al 100% da remoto.

Controllare il WiFi

Per chi abita in zone residenziali ad alta densità di tutti i dispositivi Wi-Fi, inclusi citofoni, console di giochi e dispositivi IoT, possono costituire un punto di vulnerabilità sfruttabile da vicini malintenzionati. È opportuno prendere in considerazione l'adozione di access point certificati in ambiente wireless attendibile, come WatchGuard AP225W suggerisce l'azienda, per conferire al reparto IT aziendale una esaustiva visibilità sulle prestazioni dei client e della rete, in modo da poter supportare al meglio i telelavoratori, e preconfigurare gli access point per facilitarne l'utilizzo da parte degli utenti domestici. Perché tutto ciò è importante, osserva WatchGuard? Perché una robusta sicurezza IT dimostra a dipendenti, clienti e altri soggetti importanti che l'azienda è in grado di operare anche in situazioni senza precedenti, come quella attuale. ❁

Il 5G sta arrivando. Le implicazioni per la sicurezza

5G tra opportunità e sfide alla cybersecurity: come prevenire e proteggersi dalle minacce secondo Sophos

Il 5G, le cui prime implementazioni sono già al centro della scena in ambito laptop e cellulare, diventerà una componente imprescindibile di ogni luogo di lavoro, anche in considerazione del boom dei device IoT pensati per cavalcare questa nuova rivoluzione.

Di conseguenza, la diffusione del 5G rappresenterà una nuova opportunità per gli hacker ed è fondamentale chiedersi come ci si possa proteggere dai nuovi rischi.

La mancanza di visibilità con il 5G continuerà ad essere un problema, come lo era stato con il 3G e il 4G, reso ancor più complesso dalla velocità e della possibilità di trasmettere esponenzialmente più dati. Nella migliore delle ipotesi ciò che sarà possibile vedere in un ambiente 5G sarà se un dispositivo lo stia utilizzando ma non ci sarà alcuna visibilità su ciò che viene effettivamente trasmesso, rendendo difficile individuare attività sospette.

Per ovviare a questa problematica, le aziende possono richiedere che i dispositivi IoT che vengono utilizzati siano collegati al wi-fi aziendale, al fine di ottenere un maggiore



Marco D'Elia, Country Manager di Sophos Italia

controllo sul traffico e intercettare attività indesiderate.

«Siccome non è possibile decifrare ciò che viene trasmesso, risulta incredibilmente difficile individuare gli attacchi mentre stanno accadendo. Per questo motivo Sophos ha messo a punto alcuni accorgimenti per rendere le proprie reti più sicure», spiega Dan Marco D'Elia, Country Manager di Sophos Italia (sophos.it), multinazionale operante nella sicurezza di ultima generazione. Naturalmente, le aziende non devono evitare di utilizzare dispositivi con 5G solo perché ci sono potenziali rischi per la sicurezza bensì adottare le precauzioni necessarie per proteggere la propria infrastruttura IT senza rinunciare


ai vantaggi di tale tecnologia.

- Il 5G può rappresentare una backdoor alla rete aziendale, pertanto è necessario assicurarsi che non ci sia alcun punto cieco impossibile da controllare e predisporre interventi tempestivi ove necessario.

- Identificare i dispositivi non gestiti nella rete. È una grande sfida se i dispositivi comunicano solo attraverso il 5G, ma diventa più semplice se viene utilizzato anche il wi-fi, poiché sarà possibile individuarli attraverso una scansione della rete. Utilizzando una soluzione EDR e attraverso un'apposita query, sarà più semplice rilevare eventuali device non gestiti.

- In mancanza d'altro, utilizzare la crittografia e i controlli di accesso che assicurano comunque un buon livello di sicurezza ai dati all'accesso ad essi.

«Nell'implementare nuove infrastrutture e servizi appare fondamentale avere ben chiari i potenziali nuovi rischi. In definitiva, l'avvento del 5G ribadirà ulteriormente la necessità di una protezione a tutti i livelli dell'ambiente IT, un approccio dal quale le aziende potranno trarre benefici già nell'immediato» conclude il country manager di Sophos Italia. ❁



UNA SICUREZZA AMBIENTALE E FISICA

In parte per le esigenze sviluppatesi in seguito alla pandemia, una crescente attenzione è stata rivolta agli aspetti fisici della sicurezza. In particolare, sono state sviluppate applicazioni che aiutano i dipendenti a seguire le regole imposte per ridurre il rischio di contagio, come il vincolo di rispettare le distanze. Sembra banale, ma occorre considerare la difficoltà di chi è abituato a muoversi in ambienti familiari, dovendo porre attenzioni nuove.

App recenti rendono più semplice gestire all'interno di uffici privati, pubblici e commerciali, fattori quali la distanza, la temperatura, la densità fisica delle persone.

In aiuto stanno arrivando soluzioni che, basate sulla intelligenza artificiale e dispositivi IoT, consentono di effettuare automaticamente e in tempo reale una serie di controlli, invitando utenti e clienti, anche con la proiezione di messaggi visivi, a correggere il proprio comportamento o a pilotarlo in modo corretto.

Al sicuro il telecontrollo della rete elettrica altoatesina di Alperia

Alperia, provider di energia, ha adottato le soluzioni Kaspersky per proteggere i sistemi di telecontrollo della rete elettrica per 280 mila utenti altoatesini

Alperia, azienda altoatesina nata nel 2016 dalla fusione di due importanti società energetiche locali, oggi gestisce 34 centrali idroelettriche, 6 centrali di teleriscaldamento e oltre 8.600 km di rete elettrica e 700 punti di ricarica elettrica che forniscono energia elettrica e gas a 280 mila utenti.

La divisione Telecommunications e Teleconduction di Alperia Group, guidata da Sandro Moretti, gestisce i sistemi di trasmissione dei dati di produzione e le telecomunicazioni. Il team di 13 persone ha la responsabilità delle RTU (Remote Terminal Unit), dei datacenter, dell'operatività delle sale di controllo e della rete di collegamento verso le due realtà del gruppo di produzione (Alperia Greenpower) e distribuzione (Edyna) di energia elettrica.

L'esigenza di Alperia di trovare un partner strategico di sicurezza informatica è nata dalla necessità di proteggere un sistema molto complesso e in particolare di proteggere i sistemi di telecontrollo dedicati alle centrali di produzione ed alla rete di distribuzione, preposta all'erogazione di energia elettrica dei suoi utenti in Alto Adige.

Era quindi fondamentale individuare una soluzione che consentisse di inserire, all'interno del perimetro della gestione dei sistemi di telecontrollo, un sistema di sicurezza contro gli attacchi informatici più evoluto del classico endpoint e, soprattutto, dedicato all'ambito OT.

Una caratteristica imprescindibile per proteggere gli ambienti industriali è, infatti, quella di utilizzare soluzioni espressamente pensate per questi sistemi che siano in grado di offrire la massima protezione senza rischiare di interrompere il funzionamento di macchine fondamentali per la fornitura dei servizi.

Dopo un'attenta analisi delle soluzioni disponibili sul mercato, specificamente dedicate agli ambienti industriali, Alperia ha trovato la risposta in Kaspersky Industrial CyberSecurity (KICS), una soluzione progettata specificamente per la protezione dei diversi livelli delle infrastrutture industriali, fra cui i sistemi di automazione SCADA, DCS, PLC, MES, postazioni di engineering e connessioni di rete.



*Morten Lehn, General
Manager Italy di
Kaspersky*

Una caratteristica distintiva di questa soluzione è l'implementazione di un approccio olistico per garantire la sicurezza informatica delle imprese industriali e delle infrastrutture critiche.

Grazie alla flessibilità e versatilità delle impostazioni la soluzione può essere configurata a seconda delle esigenze e adattarsi ai requisiti dell'ambiente ICS specifico. E' un approccio che prevede non solo la protezione degli endpoint industriali, ma anche l'uso di tecnologie di monitoraggio passivo per identificare le anomalie e rilevare possibili intrusioni nella rete.

Gruppo di lavoro congiunto

Installare una soluzione di sicurezza su sistemi che devono essere sempre attivi non è semplice. Alperia e Kaspersky (kaspersky.it) hanno per questo costituito un gruppo di lavoro congiunto per realizzare il miglior set-up possibile della soluzione.

«La collaborazione è stata la strada giusta da percorrere per raggiungere il nostro obiettivo. L'idea di avere una task force con i tecnici di Kaspersky a disposizione in azienda ci ha permesso di personalizzare il prodotto e cucirlo su misura sulla nostra realtà. Sono convinto che in casi come questo si debba andare oltre il classico rapporto cliente - fornitore e puntare a un rapporto di partnership più esteso. Per questo stiamo prendendo in considerazione l'idea di fare un contratto di service con Kaspersky che vada oltre l'assistenza sul prodotto e si configuri come una



Impianto di generazione elettrica di Alperia

fornitura di consulenza su tutto il perimetro della rete», ha dichiarato Sandro Moretti, Division Manager Teleconduction & Telecommunication di Alperia.

A fine del 2018, per alcune settimane, la soluzione KICS for Nodes è stata messa in esercizio su alcune macchine al fine di verificare non solo gli effetti sulla loro operatività ma anche per comprendere quali fossero le esclusioni da impostare e le ottimizzazioni da integrare.

In Alperia tutti i sistemi sono ridondati. Inizialmente, quindi, la soluzione è stata installata solo su una delle due macchine ridondate - quella principale - in modo da disporre di un backup solido in caso di criticità, senza rischiare impatti sulla produzione in caso di problemi.

Dopo aver superato positivamente diversi stress test e aver verificato che il nuovo sistema non rilevasse eventuali falsi positivi e non avesse delle interazioni che potessero rallentare gli applicativi e bloccare alcuni servizi fondamentali, Kaspersky Industrial Cybersecurity è stato implementato e reso completamente operativo su circa 40 server di Alperia. «Siamo davvero molto orgogliosi di essere stati

scelti da una realtà così innovativa e orientata al futuro nell'ambito della fornitura di energia come Alperia - ha commentato Morten Lehn, General Manager Italy di Kaspersky-. Per Kaspersky non è una sorpresa che aziende che erogano servizi essenziali come l'energia elettrica stiano prestando sempre più attenzione alla protezione delle infrastrutture che sono chiamate a gestire. L'aumento dei dispositivi connessi e la crescente digitalizzazione delle infrastrutture delle reti di pubblica utilità, porta con sé tante opportunità, ma anche un aumento esponenziale dei rischi. Gli incidenti informatici a livello industriale sono tra quelli più pericolosi, perché possono determinare interruzioni nella produzione e causare tangibili perdite economiche, oltre ad essere complessi da risolvere. Soprattutto quando l'incidente si verifica in settori critici e vitali, come quello dell'energia. Guardando al futuro, continueremo a lavorare per fornire soluzioni di sicurezza informatica su misura che tengano conto delle esigenze aziendali in continua evoluzione di ogni industria».



Una protezione flessibile difende da minacce in continua evoluzione

FINIX ha reso disponibili soluzioni che difendono le infrastrutture IT e controllano la fruizione degli spazi commerciali in aderenza alle normative anti Covid

Nell'attuale contesto lavorativo, in cui la necessità di rispondere all'emergenza sanitaria ha spinto all'adozione dello smart working, è di vitale importanza la tutela della sicurezza dei dispositivi e dei dati e, non ultimo, il controllo degli spazi fisici per quanto riguarda le persone che li frequentano.

«Nel campo della sicurezza informatica e della digital transformation la nostra azienda può vantare, da un lato, le soluzioni di Fujitsu, di cui siamo gli unici distributori in Italia, dall'altra l'esperienza maturata dalla capillare presenza sul territorio e un canale indiretto di vendita con una storia pluridecennale. Con particolare riferimento alla nostra offerta in ambito security, il nostro obiettivo è di ampliarla con soluzioni di innovative aziende italiane e internazionali», ha osservato Danilo Rivalta, CEO di FINIX Technology Solutions.

Quello della cybersecurity è di certo un campo dell'IT che necessita di soluzioni innovative. Basta considerare che a marzo 2020 i soli attacchi ransomware sono aumentati del 148% rispetto al mese precedente; ed è in questa arena che FINIX (finix-ts.com) si propone di assumere un ruolo primario.



Danilo Rivalta, CEO di FINIX Technology Solutions

«In questi mesi abbiamo lavorato per individuare le migliori soluzioni di cybersecurity da offrire alle imprese e ai clienti nazionali: è il caso di Morphisec, per la protezione del punto più vulnerabile di una azienda, l'endpoint, che rappresenta l'elemento più critico di una soluzione di smart working. La soluzione che proponiamo rende l'endpoint praticamente inattaccabile ed è stato nominato 2020 Technology Pioneer dal World Economic Forum», ha evidenziato Rivalta.

Morphisec, il futuro della sicurezza avanzata

Morphisec è una soluzione che affronta il problema della sicurezza informatica con un approccio di nuova concezione - Moving Target Defense (MTD) - in grado di proteggere l'intera organizzazione end-to-end da minacce avanzate come attacchi fileless e zero day, exploit in-memory e ransomware avanzato.

Di derivazione militare, opera in base all'assunto che un target in movimento è più difficile da attaccare di uno fisso e sfrutta lo spostamento, la distribuzione e la crittografia dinamica dei dati in memoria per renderne più difficile l'attacco o il furto.

La maggior parte delle soluzioni di antivirus presenti sul mercato si focalizzano su un processo che prevede prima il riconoscimento della minaccia e solo successivamente il blocco della stessa. Morphisec al contrario, osserva FINIX, prima ancora di identificare il tipo di minaccia, le blocca attraverso la citata tecnologia brevettata MTD, in grado di trasformare lo spazio di memoria, spazio che, in quanto statico, costituisce il principale obiettivo degli attacchi evoluti.

Prevenire le minacce

La peculiarità di Morphisec risiede nell'approccio attivo nella prevenzione delle minacce tramite la trasformazione continua dello spazio di memoria. Numerosi i benefici che apporta:

- Blocco di minacce avanzate e zero-day: Previene zero-day e attacchi avanzati senza la necessità



Ulisse mantiene sotto controllo gli spazi, la temperatura e il comportamento dei visitatori

di una conoscenza preliminare della forma, del tipo o del comportamento della minaccia.

- Applicazione di patch virtuali: Protegge l'infrastruttura dagli exploit della vulnerabilità quando le patch non sono ancora disponibili.
- Protezione unica delle infrastrutture IT: protegge dagli attacchi server Windows e Linux, endpoint, desktop virtuali come VMware Horizon View e Citrix e carichi di lavoro in cloud.
- Implementazione semplice: l'implementazione non presenta conflitti di sistema o di manutenzione, non richiede di configurare o aggiornare database, firme o regole, log o avvisi da analizzare.
- Nessun impatto sul sistema: opera come agent stateless leggero con ingombro minimo, privo di componenti run-time e di conseguenza senza impatto sulle prestazioni.

«Morphisec porta all'interno della

cybersecurity un concetto innovativo puntando sulla prevenzione contro gli attacchi più evoluti, inclusi gli APTs, zero day e ransomware. Ha il vantaggio di poter essere implementata facilmente nell'infrastruttura di sicurezza esistente di un'azienda per costituire uno stack di prevenzione semplice e altamente efficace», ha osservato Rivalta.

Ulisse controlla gli spazi e i rischi sanitari del retail

Se con Morphisec si è proposta di controllare i rischi cibernetici, con la soluzione Ulisse FINIX ha pensato al controllo ambientale e dei rischi sanitari.

Nella sua essenza, Ulisse è una soluzione sviluppata per supportare le aziende che hanno esigenze di controllo accessi e, al tempo stesso, ottenere più informazioni possibili nell'analisi dei dati relativi al comportamento dei visitatori e facendo leva sull'IoT e l'AI.



Ulisse regola gli accessi in sicurezza alle aree

Nell'attuale situazione, in cui banche, negozi, uffici e servizi ad alta affluenza si trovano a dover affrontare sfide significative, gli ingressi sicuri e contingentati sono diventati un'esigenza impellente per integrare la ripresa del business con le esigenze di salute pubblica.

A questo si aggiunge una complessità in più per il comparto Retail, che deve integrare tecnologie legacy con lo sviluppo di nuove soluzioni di trasformazione digitale. Per far fronte a queste esigenze FINIX ha scelto di portare sul mercato la soluzione Ulisse, che poggia su un sistema di analisi dei flussi di persone negli spazi fisici basato su di un modello brevettato.

«L'analisi dei comportamenti all'interno degli spazi, anche commerciali, sarà sempre più fondamentale. Il motore di auto machine-learning in cloud, insieme ai modelli di analisi comportamentale creati sulla base dei dati raccolti giornalmente, analizza

questa immensa mole di informazioni e suggerisce azioni migliorative in real time. Per questo motivo siamo particolarmente soddisfatti che una tecnologia come Ulisse sia entrata all'interno del nostro hub di innovazione» ha commentato Rivalta.

Funzionalmente Ulisse utilizza una tecnologia basata su sensori IoT a bassa complessità e algoritmi di Intelligenza Artificiale, mediante i quali è possibile ricavare tutta una serie di KPI propri delle attività dei clienti.

I sensori rilevano i flussi di persone tanto all'interno quanto all'esterno di uno spazio fisico, identificano eventi di affollamento e inviano in tempo reale i dati e le coordinate spaziali al sistema di proiezione che, in maniera dinamica, visualizza pattern luminosi o messaggi visuali sul pavimento del negozio.

Il proiettore, integrato nella scocca principale di Ulisse, abilita un

sistema di comunicazione dinamica in tempo reale che attraverso mappature di luce suggerisce al visitatore un comportamento adeguato volto a favorire il distanziamento e contingentare gli accessi nel caso in cui ci sia un numero eccessivo di persone.

Una termo-camera, inoltre, permette di implementare un sistema di screening che può rilevare la temperatura sui flussi di visitatori con un margine di errore di 0,5 gradi Celsius. Sistemi di rilevazione della temperatura a distanza sono anche in grado di controllare eventi critici sul territorio per prevenire il diffondersi di epidemie. Questo tramite un motore di auto-machine learning sul cloud per il consolidamento e l'analisi della vasta quantità di dati raccolti sul campo.

A livello funzionale la soluzione è indipendente dall'infrastruttura IT dei clienti, cosa che si traduce in facilità di implementazione e la disponibilità di configurazioni flessibili

Gli obiettivi di FINIX non si limitano però ad individuare nuove soluzioni ma sono più ampi.

«Il nostro obiettivo è di rafforzare ulteriormente la nostra posizione come centro di eccellenza negli ambiti di Cybersecurity, IoT e Artificial Intelligence. Vogliamo essere un centro di competenza non cattedratico, ma pratico e ricco di contenuti. E farlo anche attraverso scouting di aziende e start-up italiane particolarmente capaci che abbiano ideato o con cui ideare altre soluzioni innovative», ha spiegato Rivalta. ❁

Proteggere i dati aziendali accelera la digitalizzazione

di
Giuseppe
Saccardi

SB Italia coniuga security e smart working in progetti di digitalizzazione: dalla firma remota alla sicurezza di dati e accessi, alle applicazioni in cloud

Negli ultimi mesi la maggior parte delle aziende è stata costretta a mettere i propri dipendenti e collaboratori in smart working. È però importante distinguere tra un'azienda che lavora in home working e una azienda davvero digitale. Se i processi sono rimasti analogici, si può affermare di avere la forza lavoro in home working, ma non si può dire che l'azienda sia diventata digitale.

La possibilità di approvare e firmare digitalmente, di poter accedere alle informazioni aziendali organizzate come patrimonio dati digitale con un solido sistema di protezione, di tracking, sicurezza e controllo: tutti questi sono esempi di funzionalità, strutture dati e applicazioni che definiscono un'azienda digitale.

Se da un lato la digitalizzazione, abbinata a un sistema di sicurezza efficace, è ormai condiviso essere un percorso che va fatto in tempi rapidi, dall'altro per attuarla servono competenze difficilmente reperibili in toto all'interno di un'azienda; si parla di competenze su un ampio numero di tecnologie e soluzioni a cui si devono

affiancare capacità di comprendere i processi e padroneggiare le metodologie. Per questo diventa importante il ruolo del system integrator che si affianca all'azienda in questo percorso di digitalizzazione.

«Noi, come SB Italia riscontriamo che anche se le esigenze sono spesso apparentemente le stesse o simili, ogni azienda ha le sue peculiarità e deve definire la strada più adatta alla sua specifica natura. Un importante aiuto lo fornisce il system integrator che per definizione integra competenze diverse su più tecnologie e si pone come un elemento di collegamento tra tecnologia, processi e realtà del cliente. Dispone di una vista "orizzontale", conosce più soluzioni che possono risolvere l'esigenza ed è in grado di indirizzare il cliente a scegliere quella ottimale valutando pro e contro sia tecnologici che

economici», evidenzia Massimo Missaglia, Amministratore Delegato di SB Italia.

SB Italia (www.sbitalia.com), si

identifica in questo ruolo e sono numerosi i clienti che si sono affidati a lei nel loro percorso di innovazione digitale, come per esempio il Gruppo San Donato, Mondadori, PwC Italia, Randstad Italia, Schneider Electric.

«Il modello con cui lavoriamo, che vede da un lato un referente commerciale unico che interagisce con il cliente, ne conosce le specificità e le esigenze, e dall'altro i team verticali dedicati per area con competenze approfondite delle soluzioni tecnologiche, ci consente di fornire ai clienti un supporto efficace nell'individuare e realizzare le soluzioni migliori per la singola azienda: dalla firma remota di ogni genere di contratto, alla messa in sicurezza dei dati e dei documenti aziendali, dalla disponibilità in cloud di ogni genere di applicazione con garanzia di protezione degli accessi e dei dati, alle applicazioni di intelligenza artificiale e alle analisi predittive» osserva Missaglia. ❁



Massimo Missaglia, AD di SB Italia

Mettere al sicuro l'azienda richiede una accurata integrazione dei sistemi

Combinare smart working e business continuity è un compito arduo che richiede il supporto di un esperto system integrator. È quello che ha fornito Personal Data a Veritas e Zignago

L'accelerazione impressa alla trasformazione digitale delle aziende come conseguenza diretta della situazione pandemica in corso a livello globale ha fatto emergere il problema della carenza di personale altamente specializzato in grado di progettare e gestire le piattaforme informatiche che, dal cloud alla mobility e alla security, abilitano lo smart working e ne garantiscono la fruizione in modo sicuro per dati, applicazioni e dispositivi.

Se dotarsi di conoscenze specifiche risulta però difficile anche per una grande azienda o corporate, tanto più lo è quando si tratta di una piccola o media azienda, che dispone di budget più limitati e ha maggior difficoltà a reperire sul mercato personale specializzato e costoso.

Una soluzione, osserva Personal Data (personaldata.it), è ricorrere a un system integrator che sappia coniugare in modo ottimale i diversi paradigmi che confluiscono nella "digital revolution" in atto e sappia altresì calarli nel contesto operativo e tecnologico di una specifica azienda, del suo settore di mercato e della sua disponibilità di budget.

Personal Data possiede, in tema di system integration, un background di conoscenze che risale al 1981, quando la società è stata fondata a Brescia con la missione di fornire, tramite business unit specializzate, soluzioni infrastrutturali personalizzate per la gestione, la virtualizzazione, la sicurezza e la business continuity dei sistemi di information technology. Dal 2012 la società è diventata parte di Project Informatica, società specializzata nei servizi e nelle soluzioni di Information e Communication Technology



Giuliano Tonolli, amministratore delegato di Personal Data, Gruppo Project



Ecologia e cura dell'ambiente tra i servizi del Gruppo Veritas

per le imprese e a capo del Gruppo Project, che ad oggi ha acquisito il 70% del capitale e ne ha ampliato ulteriormente il campo d'azione e la gamma di servizi forniti al mondo aziendale.

Il caso Veritas, un'esperienza concreta con partner di rilievo

Uno dei motivi del successo di Personal Data, ha osservato Giuliano Tonolli, amministratore delegato di Personal Data, Gruppo Project, e dei risultati ottenuti nel corso degli anni in numerose realizzazioni di rilievo, è stata l'accurata scelta dei partner tecnologici con cui operare e progettare soluzioni IT all'avanguardia, partner che comprendono società di caratura

internazionale come Trend Micro e Citrix.

Un esempio concreto è quanto realizzato da Personal Data per Veritas, una multi-utility veneta che per dimensioni e fatturato si posiziona tra le maggiori in Italia con 120 tra sedi direzionali, operative, impianti e depositi.

La multi-utility, tramite l'intervento di Personal Data e il suo ricorso a tecnologie Trend Micro, ha messo al sicuro dai cybercriminali e blindato dispositivi endpoint, server e reti.

In un contesto di minacce che si sono rivelate essere sempre più evolute e preoccupanti per il potenziale impatto su una azienda che eroga servizi, e ancor più sui suoi clienti, Veritas era alla ricerca

di un partner tecnologico in grado di fornire e supportare soluzioni di cyber security che disponessero e consentissero il patching virtuale dei sistemi e migliorassero le prestazioni sulla parte endpoint, gateway e posta elettronica, tutti obiettivi per i quali le soluzioni precedentemente adottate si erano dimostrate non del tutto soddisfacenti.

La stretta e proficua cooperazione degli esperti di Personal Data e di Trend Micro con il team IT di Veritas ha permesso di ideare ed attuare una strategia di protezione su misura, che ha posto in sicurezza sia la parte server che la parte endpoint tramite il ricorso a caratteristiche di machine learning e behavioural monitoring, e la parte

di rete tramite l'analisi in profondità degli eventi.

Quello che ha convinto Veritas della validità della soluzione proposta da Personal Data per rafforzare la postura aziendale nella security, soprattutto in una fase di forte adozione dello smart working, sono state in particolare le caratteristiche di leggerezza lato client, le capacità di individuare i movimenti laterali degli attacchi e delle possibili intrusioni, oltre alla possibilità di proteggere i sistemi legacy grazie a caratteristiche che hanno permesso di implementare robuste capacità di difesa, dando anche garanzie di consistenti ritorni economici.

Quanto attuato per Veritas sul fronte sicurezza ha trovato un parallelo in quanto realizzato per la multi-utility sul piano della gestione delle postazioni di lavoro e della diffusione dello smart working.

La collaborazione in questo campo dell'IT tra Personal Data e Veritas risale a oltre dieci anni fa quando Personal Data, riconosciuta come Citrix Platinum Solution Advisor, aveva realizzato con Veritas una prima sperimentazione di Digital Workspace. In quel primo contesto la soluzione Citrix aveva assicurato agli utenti remoti facilità d'uso e una velocità di esecuzione che aveva permesso alle applicazioni di far fronte alle esigenze operative della società.

Quando si è concretizzata nei mesi scorsi l'esigenza di dare una spinta ulteriore al lavoro agile, Personal Data ha di nuovo supportato

Veritas nel progetto di consolidamento dello smart working facendo ricorso ad un'esperienza sul campo testimoniata da oltre 3000 postazioni di lavoro che nel recentissimo passato ha rapidamente attivato per numerose aziende italiane.

Ad oggi la soluzione e l'infrastruttura approntata permettono ogni giorno di servire oltre 600 utenti senza che questi abbiano la percezione di disporre di prestazioni diverse a seconda del dispositivo usato o del luogo da cui lavorano.



La sede del Gruppo Zignago

«La gamma di tecnologie di workspace intelligente implementate negli anni, su cui si è deciso di puntare molto, hanno permesso a Personal Data di migliorare l'esperienza dei dipendenti di molte imprese e di rendere il loro modo di lavorare più smart e agile. Il grande insegnamento è stato l'adattamento alle esigenze, per evitare in qualsiasi modo la crisi», ha commentato Tonolli.

Il caso Zignago

Un altro caso che ha visto concretamente all'opera Personal Data è quello offerto dal Gruppo Zignago, costituito da società venete che operano nel settore vetrario, vinicolo e dell'energia e con una consolidata presenza in diverse

parti del mondo, tra cui Francia e Stati Uniti.

La holding ha di recente sentito la necessità di rinnovare l'infrastruttura IT a seguito del maggior impegno richiesto e ha optato, tra le prime ad adottare una tale soluzione, per il passaggio a SAP HANA in modalità TDI (Tailored Datacenter Integration).

L'obiettivo del Gruppo Zignago consisteva nel voler disporre di prestazioni elevate per lo storage dei dati che potessero essere certificate e mantenute nel tempo al variare delle esigenze di business.

Gli obiettivi prefissati sono stati successivamente ottenuti tramite il supporto tecnico e progettuale di Personal Data, che ha permesso al Gruppo Zignago di

concretizzare un incremento delle prestazioni relativamente all'I/O dei dati tra il settanta e l'ottanta per cento.

Dopo aver valutato con Personal Data quale potesse essere la soluzione migliore al fine di assicurare l'interfacciamento della piattaforma IT con SAP HANA, il gruppo di lavoro congiunto ha optato per l'adozione di una soluzione NetApp in MetroCluster con storage completamente di tipo flash.

L'infrastruttura che ne è risultata si configura come un sistema ad alta disponibilità e di disaster recovery centralizzato per tutti gli uffici distribuiti del gruppo sia in Italia che all'estero e ha soddisfatto del tutto le esigenze del Gruppo Zignago. ❁

È disponibile il nuovo libro
**INFRASTRUTTURE ICT,
CLOUD E MULTICLOUD**



Chiedi la tua copia dell'e-book scrivendo a:
shop@reportec.it • Il prezzo del libro è di 20 euro (iva inclusa)

È disponibile il nuovo libro
**IL FUTURO DEL WORKSPACE
E DELLO SMART WORKING**



Chiedi la tua copia dell'e-book scrivendo a:
shop@reportec.it • Il prezzo del libro è di 20 euro (iva inclusa)