

## RAPPORTO CLUSIT 2020

La quindicesima edizione del Rapporto Clusit 2020 sulla sicurezza ICT, mostra una situazione drammatica su quasi tutti i fronti

*pag. 6-9*

## SPECIALE SMARTWORKING

*pag. 22*



### IN QUESTO NUMERO:

#### CYBER ATTACK

*pag. 6-9*

- Rapporto Clusit 2020: solo Coronavirus peggio del cybercrime

*pag. 10*

- Il rispetto della cyber security in azienda parte dall'alto

*pag. 11-13*

- I dati sono il capitale del futuro e vanno protetti

#### SOLUZIONI

*pag. 14-15*

- La sicurezza dei dati non strutturati

*pag. 16-18*

- Per la business continuity meglio lasciar perdere la scaramanzia

*pag. 19-20*

- CIE garantisce la sicurezza delle piccole e medie imprese

#### SPECIALE SMARTWORKING

*pag. 22-23*

- Come preservare la sicurezza nello smart working

*pag. 24*

- Crescono gli attacchi di phishing che sfruttano il Coronavirus

*pag. 25-26*

- Il decalogo per realizzare meeting di gruppo in sicurezza

*pag. 27*

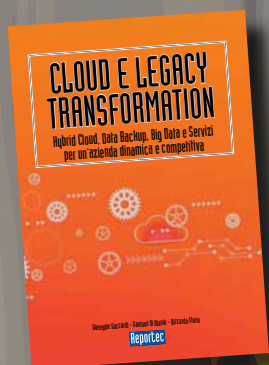
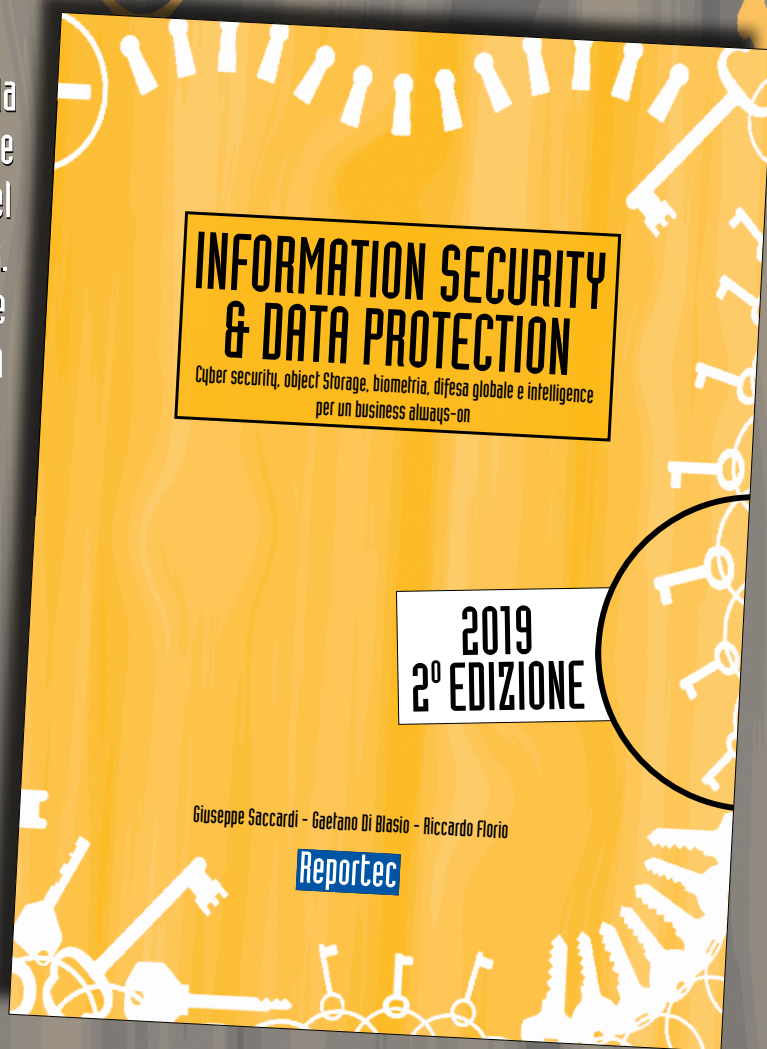
- Lo smart working richiede più sicurezza negli accessi

*pag. 28*

- Smart Working più semplice e sicuro con il desktop virtuale

# È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche  
**CLOUD E LEGACY TRANSFORMATION**

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

**Security & Business 51**  
marzo 2020

Direttore responsabile:  
Gaetano Di Blasio

In redazione:  
Giuseppe Saccardi, Paola  
Saccardi

Hanno collaborato:  
Riccardo Florio

Grafica: Aimone Bolliger  
Immagini: dreamstime.com  
[www.securityebusiness.it](http://www.securityebusiness.it)

Editore: Reportec srl  
Via Marco Aurelio 8  
20127 Milano  
tel. 02.36580441  
Fax 02.36580444  
[www.reportec.it](http://www.reportec.it)

Registrazione al tribunale  
n.585 del 5/11/2010

Tutti i marchi sono  
registrati e di proprietà  
delle relative società

## Un numero di Security e business pieno di virus

L'apertura di Security e business è destinata, come al di solito alla rubrica Cyber Attack, che raccoglie informazioni sui trend relativi alle minacce e agli attacchi. Ma la copertina di questo numero 51 non poteva che essere dedicata a uno speciale sullo Smart Working, un tema che è balzato agli onori di cronaca su tutti i media mondiali a causa della pandemia che tutti stiamo affrontando.

Lo smart working ha salvato molte imprese che hanno potuto mantenere alcune operazioni attive. Per molti è stata una "scoperta": ci sono casi di realtà che si erano opposte ad adottare il lavoro da remoto, soprattutto per una ritrosia naturale di molti imprenditori abituati a vedere i lavoratori seduti alle proprie postazioni, quale "misura" di produttività.

Molti non torneranno indietro, avendo sperimentato che "si può fare!"

Attenzione, però: si deve fare correttamente soprattutto dal punto di vista della sicurezza. I sistemi di protezione ci sono, ma vanno scelti e applicati correttamente, adeguatamente alle esigenze di ciascuna realtà.

Tornando, invece alla rubrica Cyber Attack, questa è dominata dall'importante quantità di dati che sono stati raccolti dagli esperti del Clusit e presentati in Marzo in un Security Summit on line, in tempi di Coronavirus.

Al riguardo ci sono solo notizie negative, che sanciscono ancora una volta la difficoltà nel fronteggiare i massicci attacchi destinati a qualsiasi dispositivo connesso. Non basta, infatti la crescita della consapevolezza sul problema della cyber security: restano comunque scarse le applicazioni di best practice e insufficienti gli investimenti in sicurezza, soprattutto se paragonati ai ingenti mezzi a disposizione del cybercrime, ormai foraggiato da veri e propri delinquenti senza scrupoli.

Lo dimostra anche le azioni che non hanno smesso di attaccare chi si trovava in difficoltà. Anzi, già a metà 2019, gli esperti del Clusit hanno segnalato che il settore della sanità è uno degli obiettivi più bersagliati.

# RAPPORTO 2020 INDAGINE AIPSI-CSWI SUL LAVORO FEMMINILE NELLA CYBERSECURITY IN ITALIA

AIPSI, l'Associazione Italiana Professionisti Sicurezza Informatica, è il capitolo italiano di ISSA, un'organizzazione internazionale no-profit di professionisti ed esperti praticanti.

Di recente è stata rilasciato il Rapporto finale 2020 sulla prima indagine via web condotta dal Gruppo di Lavoro CSWI di AIPSI sul lavoro femminile in Italia nel settore della sicurezza digitale e gratuitamente scaricabile per gli utenti (<https://www.aipsi.org/aree-tematiche/cswi-cyber-security-women-s-italy/rapporto-2020-cswi-aipsi.html>). Prima è necessario registrarsi al sito di AIPSI (<https://www.aipsi.org/registrati.html>).

L'indagine, basandosi su una libera ed anonima risposta via web ad un questionario on line, ha fornito significative indicazioni sulla situazione del lavoro femminile in Italia nell'ambito della sicurezza digitale, attingendo alle risposte fornite dalle dirette interessate.

A rispondere all'indagine sono state prevalentemente donne di giovane età (il 54% fino a 34 anni) e di istruzione a livello universitario (solo il 14%

non è laureata), prevalentemente tecnica (55%).

L'essere donna e svolgere una attività lavorativa impegnativa come quella della sicurezza digitale, interdisciplinare e in continua e rapida evoluzione, può comportare problemi nella vita personale e familiare, soprattutto se si hanno dei figli piccoli.

Il 52,6% delle rispondenti ha evidenziato difficoltà nel conciliare i tempi del lavoro con quelli della famiglia, soprattutto se si intende crescere professionalmente ed arrivare a posizioni di leadership tecniche e/o manageriali.

Un altro aspetto non proprio positivo che è emerso dal sondaggio riguarda il fronte della retribuzione, dove le differenze di genere esistono: a parità di ruolo, responsabilità, competenza ed anzianità, il 38% delle donne rispondenti ha dichiarato di essere pagata meno degli uomini, e la stessa percentuale di esserlo in egual modo.

Altri aspetti negativi nella sicurezza digitale che



## PARTECIPA AL WEBINAR DI AIPSI

AIPSI organizza un webinar per presentare i dati più significativi emersi dall'indagine e per discutere, in una tavola rotonda con alcune delle donne più note in questo settore in Italia a livello istituzionale, accademico e industriale, come conciliare il tempo del lavoro con quello della vita personale, e su come migliorare nel futuro tale bilanciamento anche grazie a strumenti quali lo smart working.

Alla tavola rotonda del webinar parteciperanno:

- dott.a Nunzia Ciardi, Direttore del Servizio Polizia Postale e delle Comunicazioni
- dott.a Marella Folgori, Italy, Russia & CIS Sales Leader Security & Manageability Oracle
- dott.a Adriana Franca, Country Manager digi-Tree Italia
- dott.a Paola Generali, Presidente Assintel, Consigliera della Camera di Commercio MI, MB e LO, Managing Director GetSolution
- prof.a Donatella Sciuto, Prorettore Vicario del Politecnico di Milano, Professore ordinario di Architettura dei calcolatori e sistemi operativi
- avv.a Carla Secchieri, Consigliera CNF, VP FiiF-CNF, Coordinatrice corso DPO CNF-Ordine Ingegneri

La partecipazione al webinar è gratuita, ma è obbligatorio registrarsi:

<https://www.eventbrite.it/e/biglietti-webinar-cswi-aipsi-il-lavoro-femminile-nella-sicurezza-digitale-in-italia-101876405070>

Data e ora:

mar 21 aprile 2020 - h.17:30 - 19:00 GEST

hanno segnalato le rispondenti includono il tempo di lavoro necessario/richiesto, che risulta ben più alto delle canoniche 8 ore giornaliere a contratto, la mancanza di un team di lavoro supportivo e collaborativo, la non disponibilità di efficaci strumenti informatici per il supporto e l'automazione di parti del proprio lavoro, la mancanza di telelavoro/smart working. La maggior parte delle rispondenti vorrebbe inoltre avere maggiori e più approfondite competenze tecniche.

Ci sono fortunatamente anche aspetti positivi in questo ruolo. Per esempio, per la maggior parte delle rispondenti, questi riguardano la sua interdisciplinarietà, le varie opportunità e le sfide che impone. Tra gli aspetti del proprio ruolo che più soddisfano ci sono il mettere in sicurezza la propria organizzazione e l'utilizzo delle proprie capacità. Da evidenziare che il personale ritorno economico di questo lavoro è considerato rilevante solo da una piccola percentuale.

Il settore della sicurezza digitale che maggiormente sollecita l'interesse delle donne che hanno risposto è la compliance.

Per il prossimo futuro professionale le rispondenti vorrebbero essere più competenti, in posizioni di maggior responsabilità e potere, in aziende che hanno a cuore il bilanciamento dei tempi e investono nelle proprie risorse umane.

## RAPPORTO CLUSIT 2020: SOLO CORONAVIRUS PEGGIO DEL CYBERCRIME

*La quindicesima edizione del Rapporto Clusit 2020 sulla sicurezza ICT, mostra una situazione drammatica su quasi tutti i fronti*

*di Gaetano Di Blasio*

**G**li attacchi gravi continuano ad aumentare anno su anno: nel 2019: +91,2% degli attacchi rispetto al 2014. Ma è solo la punta di un iceberg, avvisa Alessio Pennasilico, membro del consiglio direttivo del Clusit, introducendo la presentazione del Rapporto Clusit 2020. Infatti, dall'analisi si evince che si registra un nuovo picco di crescita degli attacchi gravi: 1670, cioè il 7% in più nel 2019, rispetto al 2018. viene confermata, quindi la tendenza osservata a metà del periodo di rilevazione, all'orquando è stato presentato l'aggiornamento.

Vergognosa la pressione sul settore sanitario, che non accenna a diminuire, anzi gli attacchi a strutture della Sanità sono stati il (12% del totale degli attacchi, aumentati del 17% rispetto al 2018.

Tra i colpiti, diverse realtà anche in Italia, come sottolinea Sofia Scozzari, tra gli autori del Rapporto Clusit 2020.

Un dato che spicca è relativo alla crescita degli attacchi a "bersagli multipli": si tratta di ben un quarto degli attacchi compiuti



a livello mondiale.

Stupisce meno il sempre maggior utilizzo delle tecniche di Phishing e Social Engineering (+81,9% rispetto al 2018).

Più in generale, gli esperti del Clusit hanno rilevato 139 attacchi al mese da gennaio a dicembre 2019, colpendo sistematicamente, in ogni aspetto della società, della politica, dell'economia e della geopolitica, ha evidenziato Andrea Zapparoli Manzoni, uno degli autori del Rapporto Clusit 2020 e membro del Comitato Direttivo Clusit. Si tratta del 47,8% in più rispetto alla media dei 94 attacchi mensili registrati nel quinquennio

2014-2018.

Questi dati già di per se stessi impressionanti, sono una minima parte, perché non *Andrea Zapparoli Manzoni, membro del consiglio direttivo del Clusit*





*Sofia Scozzari, del Clusit.  
Alessio Pennasilico, membro del  
consiglio direttivo del Clusit*

comprendono gli attacchi tentati o bloccati e, per quanto significativo, il campione analizzato è inficiato dalla tendenza a non rendere pubblici gli incidenti.

Anche il GDPR (General Data Protection Regulation) nonché l'entrata in vigore della direttiva NIS, neo 2018, non hanno ancora dato evidenza di un miglioramento nelle pratiche per la sicurezza informatica. Peraltro, la consapevolezza delle istituzioni e degli utenti sta crescendo. Si tratta di fenomeni che per natura e dimensione travalicano i confini dell'IT e della stessa cyber security. Al riguardo, Zapparoni Manzoni ha affermato: «Ci troviamo di fronte a un vero e proprio cambiamento epocale nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi. Gli attaccanti sono oggi decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari ed unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging (e la mente dei loro utenti), su scala globale, 365 giorni all'anno, 24 ore al giorno». L'esperto è ancora più duro: « Viviamo ed operiamo



in una situazione di inaudita gravità in termini di rischi cyber, che mette a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi – online e offline – che su di essa fanno affidamento».

### **I dati principali sugli attacchi**

Gli esperti del Clusit, ormai dal 2014 hanno riclassificato gli attacchi in differenti livelli di impatto, sulla base di variabili di tipo geopolitico, sociale, economico, distinguendoli anche in attacchi diretti e indiretti. Nel 2019, gli attacchi andati a buon fine, sono stati, nel 54% dei casi, di impatto alto e critico, per il 46% di gravità media. Il cyber crime si conferma come principale causa degli attacchi gravi, essendo protagonista nell'83% dei casi. A questa categoria, d'altronde appartengono gli attacchi con l'obiettivo di estorcere denaro alle vittime, senza preoccuparsi di bloccare apparati medici e mettere a rischio la vita dei pazienti.

Più in dettaglio, gli esperti del Clusit hanno registrato il numero di attacchi di Cyber crime più elevato degli ultimi 9 anni, con una crescita del 162% rispetto al 2014 e del 12,3% rispetto al 2018.

Lo spionaggio attraverso sistemi telematici ha

registrato una crescita bassa: 0,5%, raggiungendo una quota del 12%, ma si ritiene che le informazioni in questo "comparto" siano insufficienti per aver un quadro veritiero.

Diminuiscono gli attacchi di Cyber Warfare, cioè la guerra delle informazioni, che è il 2% del totale. Si deve però considerare la gravità di questi attacchi che minano i presupposti della democrazia.

## Il destino delle vittime

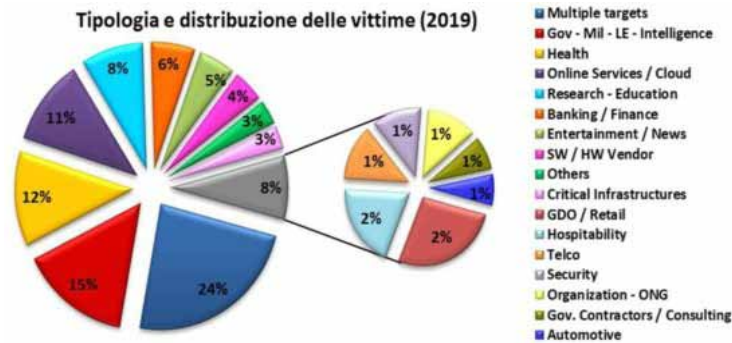
L'analisi del Clusit prosegue esplorando i settori maggiormente colpiti da attacchi gravi, in particolare, nel 2019 si è registrato un 24% del totale degli attacchi nella categoria Multiple Targets, cioè attacchi di vario tipo, accumulati dall'essere nel mirino di organizzazioni criminali, come su accennato, concentrati su una logica "industriale" tesa a massimizzare i guadagni.

A seguire, gli autori del Rapporto Clusit 2020 rilevano il settore pubblico attirare il 15% degli attacchi, in discesa del 19,4%), ma in questi non sono conteggiati gli attacchi alla sanità, che, che non è tutta pubblica e che nel suo complesso è il bersaglio per il 12% degli attacchi, crescendo del 17% rispetto al 2018.

Un boom è quello dei servizi online, che è colpito "solo nell'11% degli attacchi, ma registra un "promettente" + 91,15%.

La "classifica" prosegue con il settore della Ricerca e formazione scolastica (8% in calo dell'8,3%), con il finance (pure in calo del 10,2%)

Seguono i settori), bancario e assicurativo che quota



il (6% in ma in calo del 10,2%) ; intrattenimento/ informazione con il (5% in calo del 31,4%), Commercio e Grande Distribuzione Organizzata (2% degli attacchi, in crescita del 28,2%), e l'insieme di "Altri Settori" (3% del totale attacchi, +76,7%), Telecomunicazioni (1% del totale.

Da evidenziare, infine, un piccolo 1% degli attacchi rivolti ai Fornitori di Sicurezza Informatica, che cresce addirittura di un +325%.

## Le tecniche d'attacco

L'analisi degli esperti del Clusit svelano che gli attacchi utilizzati sono stati basati per il 44% dei casi, su Malware, in crescita del 24,8%. Tra questi il Ransomware ammonta al 46%; grazie a una crescita del 21% rispetto al 2018.

Confermata la tendenza dei cyber criminali a scegliere tecniche semplici. Mentre gli attacchi che sono imputabili a organizzazioni "vicine ai governi" storicamente usano tecniche più complesse, ma si stanno adattando, perciò si osserva la tendenza all'utilizzo di queste tecniche anche da parte di attori e state-sponsored.

Con il 19%, al secondo posto, fra le tecniche d'attacco, uno sconcertante "unknow", che però è calato del 22%.

Al contrario delle tecniche di Phishing e Social

Engineering in, gran spolvero con +81,9% rispetto al 2018, giungendo così a rappresentare il 17% del totale.

Facile immaginare che questi attacchi usano soprattutto la posta elettronica, vista la gran quantità di messaggi palesemente falsi, ma che, evidentemente sono efficaci.

Gli autori del Rapporto Clusit 2020 specificano, infatti che una quota crescente di questi attacchi basati su Phishing si riferisce "BEC scams", ovvero frodi via email che colpiscono in maniera specifica le organizzazioni con l'obiettivo di infliggere danni economici, con impatto spesso ragguardevole.

Sommando il resto delle altre tipologie di attacco utilizzate nel 2019 resta solo il 12,3% del totale.

### Prepararsi alla resilienza

Da segnalare, inoltre, un notevole aumento percentuale delle categorie "0day" (+50%) e "Account Cracking" (+53,6%), mentre sembrano scendere gli attacchi realizzati sfruttando vulnerabilità note (-28,8%), DDOs (-39,5%) e tecniche multiple/APT (-33,7%).

Si può notare che le categorie "infrastrutture critiche" e "strutture governative", hanno subito il maggior numero di attacchi che presentano un livello di Severity "Critical", insieme a "Banking/Finance" e altri; mentre le categorie con il maggior numero di attacchi con impatti di livello alto sono diretti principalmente alla sanità e, di nuovo, alle strutture governative.

Come sempre, il Rapporto Clusit 2020 si completa

con alcuni contributi, tra cui l'analisi della situazione italiana in materia di cyber-crime e incidenti informatici a cura di Fastweb, che presenta i dati relativi agli attacchi rilevati dal proprio Security Operations Center (SOC), cui si aggiungono i dati (qualitativi) sullo stato della sicurezza informatica nel Sud Italia" condotto dai ricercatori dell'Università degli Studi di Bari con Exprivia|Italtel.

Accurata, ovviamente, anche la consueta analisi di IDC Italia sul mercato italiano della Sicurezza IT, pure inclusa nel Rapporto Clusit 2020.

Concludiamo con un'osservazione degli autori del Rapporto Clusit 2020: "Dal punto di vista della distribuzione degli attaccanti che le hanno prese di mira, emergono differenze molto significative tra le aziende, il che conferma che ogni categoria di bersagli ha un suo particolare panorama di minacce dalle quali deve proteggersi. Di conseguenza non esistono soluzioni universali ma anzi, ogni settore dovrebbe schierare un mix di soluzioni difensive specifico.

Questa osservazione evidenzia, a nostro avviso, che occorre una strategia aziendale per la sicurezza e la protezione dei dati che deve basarsi su una logica mirata alla resilienza, cioè sulla capacità di "risollevarsi dopo una caduta.

Il Rapporto Clusit 2020 è stato presentato in diretta streaming il 17 marzo 2020, in una prima tappa "virtuale" del Security Summit sul cui sito si trovano gli aggiornamenti dei prossimi eventi. Sul sito del Clusit è possibile scaricare il rapporto, previa registrazione.



## IL RISPETTO DELLA CYBER SECURITY IN AZIENDA PARTE DALL'ALTO

*Manager e alti dirigenti aziendali sono un bersaglio crescente per gli attacchi phishing e devono essere i primi a dare l'esempio per la cyber security*

*di Giuseppe Saccardi*

A seguito della pubblicazione del report annuale Gartner 2019 CEO e Senior Business Executive Survey, si è rivelato importante analizzare le priorità dei dirigenti senior ivi intervistati.

A parte le preoccupazioni relative alla regolamentazione del commercio e al clima economico generale, i CEO vedono sempre più la necessità del business digitale come strumento per offrire nuovi prodotti e canali da cui generare ricavi, e come un modo per rafforzare la propria crescita.

L'82% degli intervistati, commenta in proposito Check Point, ha dichiarato di avere in corso un'iniziativa di management o un programma di trasformazione digitale, rispetto al 62% del 2018.

Un punto che si è evidenziato, ma di sovente trascurato, è che gli alti dirigenti dovrebbero dare l'esempio. Questo, purtroppo, si è dimostrato difficile ma portare la sicurezza informatica agli alti livelli sta diventando sempre più importante.

Come ci si può aspettare che i dipendenti si fidino del team dirigenziale, che si attengano alle loro regole o che prendano sul serio i problemi di sicurezza,

se i vertici non lo fanno?

Bella domanda, ma la risposta forse la si trova nel detto "per chi suona la campana". Si pensa sempre che suoni per gli altri, soprattutto quando si è al vertice di una istituzione.

### **La cybersecurity come priorità**

Il problema è che i manager e gli alti dirigenti sono un bersaglio crescente per gli attacchi phishing di social engineering.

Il Verizon Data Breach Investigations Report di quest'anno, riporta Check Point, ha mostrato che le minacce di social engineering che colpiscono i C-Level sono aumentate di 12 volte nel 2019, rispetto ai livelli del 2018.

Spesso gli attacchi phishing si sono presentati sotto forma di e-mail che sembravano passare da un alto dirigente a un altro.

E, poiché le azioni a breve termine di questi dirigenti di alto livello sono raramente messe in discussione, queste e-mail sono sempre più spesso vettore di attacchi mirati.

Quando è sempre più evidente che gli attacchi informatici costano alle organizzazioni milioni di dollari in perdita di entrate a causa dei danni al valore del marchio e alla reputazione, nonché dei tempi di inattività, la sicurezza informatica deve essere affrontata e presa sul serio in tutti gli aspetti del team dirigenziale.

Secondo studi recenti come quello di IBM sul Cost

of a Data Breach, il costo medio della violazione dei dati è aumentato del 12% negli ultimi cinque anni, e potrebbe ancora aumentare.

La sicurezza informatica deve essere di conseguenza indirizzata, suggerisce Check Point, ed adottata in tutti i livelli dell'azienda, e il consiglio al comparto dirigenziale è di dare priorità almeno alle seguenti aree: Adottare un approccio olistico alla sicurezza e

implementare un approccio proattivo che includa soluzioni preventive di sicurezza informatica. Con un'architettura integrata e una gestione centralizzata, è possibile bloccare in tempo reale sia le minacce note che quelle sconosciute.

Rendere la sicurezza informatica una priorità strategica in tutte le decisioni aziendali.

Aumentare la consapevolezza della sicurezza tra tutto il personale. Per fermare la quinta generazione di attacchi avanzati, è fondamentale tenere traccia delle attuali tendenze in materia di sicurezza e adottare un approccio completo e "Secure Your Everything" per proteggere tutte le aree di attacco – mobile, client, data center, cloud, rete e sistemi IoT. ❁

## I DATI SONO IL CAPITALE DEL FUTURO E VANNO PROTETTI

*Le conseguenze di una perdita dei dati, quali sono i principali fattori di rischio e cosa fare per non mettere in forse la sicurezza analizzato da Matrix42*

*di Giuseppe Saccardi*

I dati sono indispensabili per le aziende e questo fa sì che ci siano criminali informatici interessati per vari motivi a spiarlo, manipolarli o persino distruggerli.

Il dato di fatto purtroppo già sperimentato da migliaia di aziende di tutti i settori produttivi è che se

in un'azienda si verifica un incidente informatico, non è la sola produttività a risentirne ma ci possono essere ripercussioni sull'intero sistema informatico, e sino ad interessare i dipendenti stessi nel caso questo implichi una diminuzione della produzione e della quota di mercato aziendale.

Le perdite finanziarie osserva Matrix42, azienda impegnata nel rendere sicuri gli ambienti di Digital Workspace, non costituiscono tuttavia l'unica conseguenza negativa che le aziende sperimentano al verificarsi di una effrazione interessante i dati.

A queste si aggiungono i danni al brand derivanti dal dovere per legge denunciare pubblicamente le violazioni.

Bastano questi due aspetti, o dovrebbero bastare, per convincere le aziende a proteggere i propri dati come se si trattasse di un capitale prezioso, compito che può essere svolto tramite soluzioni atte a rendere la procedura allo stesso tempo più semplice e automatiche.

Nel vasto scenario dell'IT, suggerisce però Matrix42, l'attenzione principale dovrebbe essere rivolta ai dispositivi mobili a causa della loro, seppur relativa, vulnerabilità e dispersione sul territorio, due fattori che ampliano di conseguenza la possibile superficie di attacco da parte di malintenzionati.

D'accordo su questo la domanda che ci si pone è cosa fare, e da dove partire. I tre ragionevoli e condivisibili passi che Matrix42 suggerisce sono: valutare, proteggere e automatizzare. Vediamoli in dettaglio.

## **Valutare rischi e minacce per prevenire i rischi**

La considerazione di base degli esperti dell'azienda è che la protezione dei dati e le misure di sicurezza da attivare per la loro salvaguardia sono un obbligo, soprattutto dopo l'introduzione di normative come il GDPR.

Purtroppo i reparti IT hanno difficoltà nel gestire al meglio le criticità legate alla sicurezza informatica. In particolare, non sono poche le aziende che non risultano in grado di identificare i vettori di attacco alla loro infrastruttura IT e di conseguenza non sono in grado di stabilire delle misure di protezione adatte contro le minacce attuali e future.

Uno dei motivi può risiedere nel fatto che il mondo dei sistemi IT e dei modelli di lavoro è diventato

estremamente eterogeneo e nel rapido aumento del volume dei dati raccolti ed elaborati.

In sostanza, osserva, sarebbe la stessa crescente digitalizzazione a incorporare un vulnus che può causare un drastico incremento di rischi e minacce. La raccomandazione è quindi di prendere adesso le dovute precauzioni in vista di una possibile, o meglio certa, criticità dello scenario futuro.



## **Proteggere i dati dei dispositivi mobili**

Per il solo fatto che si spostano ed operano al di fuori del perimetro aziendale, i dispositivi mobili costituiscono il fattore di rischio maggiore in ambito informatico.

Su questi dispositivi, soprattutto se sono quelli di utenza privilegiata, sono archiviati e utilizzati un'ampia varietà di dati, spesso sensibili, che vengono scambiati sia all'interno che all'esterno della rete aziendale.

L'insieme variegato dei dispositivi mobili non si limita ai soli computer portatili, ma comprende anche tablet, smartphone, smartwatch, dispositivi IoT e altro ancora.

Le aziende devono quindi garantire un'attenta gestione centralizzata di ogni tipo di dispositivo IT per

evitare rischi per la sicurezza.

Se la sicurezza degli endpoint è parte integrante del concetto di IT e se al momento dell'installazione di nuovi dispositivi vengono attivate diverse misure di protezione, ne risulta un livello di protezione più alto. In questo modo, le modalità di cifratura sono messe in atto già durante o subito dopo l'installazione dei sistemi operativi e delle applicazioni.

Un discorso a parte, osserva Matrix42, meritano poi le interfacce. Le aziende dovrebbero monitorare e filtrare le interfacce dati in modo mirato, e se non sono necessarie Matrix42 raccomanda di utilizzare sempre un controllo delle interfacce per bloccarle.

### **Bloccare automaticamente le applicazioni non autorizzate**

Ad esempio, un sistema di controllo d'accesso audit-proof blocca l'attivazione involontaria di microfoni e telecamere, cosa che può evitare intercettazioni indesiderate delle conversazioni di lavoro, qualcosa di simile ai fuori onda televisivi e alle relative spiacevoli conseguenze.

Un altro suggerimento, ampiamente condivisibile, è che le aziende dovrebbero in genere bloccare tutte le applicazioni che non sono state esaminate dal reparto IT alla ricerca di vulnerabilità, incompatibilità e regolamentazioni delle licenze.

Questo significa permettere l'utilizzo delle sole applicazioni fornite dal reparto IT tramite una gestione centralizzata dei software. In questo modo, le aziende possono conoscere esattamente il numero di licenze di cui hanno bisogno, proteggersi da minacce

di malware ed evitare perdite di produttività, risparmiando tempo e denaro.

### **Soluzioni integrate con processi automatizzati**

Si è visto cosa fare, ma cosa non fare? Ad esempio le aziende dovrebbero evitare le applicazioni stand alone quando si tratta di scegliere una soluzione di gestione e sicurezza degli endpoint.

D'altra parte, suggerisce Matrix42, è consigliabile adottare soluzioni che possono essere combinate e ricorrere ad approcci integrati che possano migliorare l'efficienza e ridurre i costi amministrativi. Per poter proteggere in modo ottimale un sistema sin dal suo avvio, si possono anche utilizzare misure di protezione dei dati e contro i malware che generano automaticamente report sugli eventuali incidenti in un sistema di service desk, e che possono essere combinate con soluzioni di unified endpoint management e di asset management.

È un approccio che abilita e automatizza la distribuzione del software e il controllo dell'applicazione, e che permette di bloccare tutte le applicazioni che non sono state eseguite o installate dall'installatore preposto.

La protezione dei dati aziendali, rimarca Matrix42, è un punto essenziale per le imprese e il futuro risiede nell'automazione e nell'integrazione di varie soluzioni. È bene però evidenziare che la sicurezza dei dati non deve andare a scapito della produttività dei dipendenti e l'implementazione di una soluzione unificata e di processi ben coordinati è fondamentale. ❁

## LA SICUREZZA DEI DATI NON STRUTTURATI

*Micro Focus Voltage SmartCipher permette di proteggere i file non strutturati e i dati contenuti al loro interno, controllandone l'accesso e l'uso durante l'intero ciclo di vita*

di Riccardo Florio

Secondo IDC entro il 2025 il volume globale di dati ammonterà a 163 Zettabyte e l'80% di questi sarà di tipo non strutturato (Fonte: Data Age 2025: Don't Focus on Big Data; Focus on the Data That's Big, IDC, 2017).

Appare, quindi, evidente, come un numero sempre più ampio di dati aziendali critici siano contenuti all'interno di file di natura destrutturata e come la loro protezione rappresenti un'esigenza cruciale per i Chief Security Officer.

Un aiuto per rispondere a questa sfida è fornito da SmartCipher, il più recente tassello della famiglia di soluzioni Micro Focus Voltage per la protezione dei dati e la privacy, pensato in modo specifico per garantire la protezione e gestione dei dati non strutturati.

### **Sicurezza persistente su file e dati non strutturati**

Voltage SmartCipher permette di applicare ai file una protezione persistente, che li segue attraverso il loro intero ciclo di vita abilitando, nel contempo,

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



visibilità e controllo completo sul loro utilizzo attraverso qualsiasi tipo di piattaforma.

Questa soluzione utilizza una tecnologia brevettata per cifrare i dati in modo trasparente tramite un algoritmo AES-256 aggiungendo, nel contempo, policy di accesso e protezione sui file e sui dati contenuti al loro interno.

Attraverso un sistema centralizzato di "policy management" è possibile costantemente e in tempo reale individuare i file, monitorare il loro utilizzo e prevenire l'accesso non autorizzato per mantenerli sempre protetti, ovunque si trovino.

Da remoto è possibile applicare e aggiornare policy a livello di singolo file, sincronizzandole con i file che si trovano memorizzati sull'endpoint oppure su una piattaforma di collaborazione.

Voltage SmartCipher funziona in modo trasparente con qualsiasi tipo di dati, sia on premise sia in cloud. La tecnica di cifratura utilizzata consente, infatti, ai file protetti di rimanere agnostici rispetto al sistema operativo, alle applicazioni e all'utente, garantendone la protezione su qualsiasi piattaforma di collaborazione, inclusi e-mail e soluzioni in cloud come Microsoft One Drive, Dropbox, Box e altri.

"Il portafoglio di soluzioni Micro Focus Voltage protegge i dati sensibili e abilita controlli granulari,

riducendo il rischio di violazione della privacy - afferma Pierpaolo Alì, Director Southern Europe Security, Risk & Governance di Micro Focus -. 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."

### I vantaggi di Voltage SmartCipher

Il primo immediato vantaggio offerto da Voltage SmartCipher è un aumento di visibilità e controllo sui file sensibili permettendo alle aziende di determinare quando, dove e come i singoli file sono acceduti e modificati e da chi, per fornire un ampio controllo e protezione sui dati non strutturati.

La possibilità di esercitare una gestione centralizzata delle policy consente di modificare i criteri di controllo e accesso in base all'evoluzione del valore e della riservatezza dei dati al passare del tempo. Le funzionalità integrate di rilevamento, classificazione, monitoraggio e reporting in tempo reale sui file e sui dati rendono, pertanto, SmartCipher una soluzione utile per migliorare le attività di audit e di verifica della compliance.

Inoltre, le funzionalità di protezione fornite da Voltage SmartCipher garantiscono attività di collaborazione sicure attraverso ambienti eterogenei senza richiedere alcuna modifica alle applicazioni o al sistema operativo, favorendo la realizzazione di ambienti IT ibridi sicuri.

Voltage SmartCipher può essere implementato in più fasi, in base alle esigenze delle aziende,

consentendo agli amministratori di mappare la posizione dei file e implementare la protezione su di essi senza introdurre alcuna discontinuità operativa. SmartCipher aggiunge protezione e gestione dei dati non strutturati al portafoglio Micro Focus di prodotti e soluzioni per la sicurezza, i rischi e la governance che include:

- ControlPoint: aumenta la visibilità dei dati non strutturati per migliorare la sicurezza, l'efficienza e la compliance;
- Data Privacy Manager: gestione e protezione della privacy lungo il ciclo di vita dei dati;
- NetIQ: policy di Identity e Access management in ambienti on-premises, mobili e cloud.
- Fortify: sicurezza delle applicazioni on-premises e on-demand durante l'intero ciclo di vita dello sviluppo del software.
- ArcSight: rilevamento delle minacce in tempo reale, analytics e investigazione su qualsiasi sorgente di dati.

Voltage SmartCipher è disponibile come prodotto in licenza per l'endpoint oppure in forma di abbonamento annuale. ❁



## PER LA BUSINESS CONTINUITY MEGLIO LASCIAR PERDERE LA SCARAMANZIA

*Per lo smart working e gli accessi privilegiati è meglio affidarsi a una sicurezza a più livelli e biometrica, non alla scaramanzia. I suggerimenti di CyberArk*

*di Giuseppe Saccardi*

I detti per riferirsi al momento attuale sono numerosi e risalgono ad epoche diverse. Extreme times call for extreme measures, dicono gli anglosassoni, mala tempora currunt, gli antenati latini, che ricorrevano anche al detto "in omnia pericula tasta ....". Facile immaginare a quale gesto scaramantico, ancora in voga, si riferissero. È comunque indicativo che di momenti critici nel passato l'umanità non è stata avara ma se siamo qui a parlarne vuol dire che li ha superati tutti.

Tornado all'oggi uno degli imperativi del momento, e dove più che dalla scaramanzia ci si attende un aiuto dalla tecnologia e dalla ricerca scientifica, è quello di come mantenere attivi i canali di comunicazione e cooperazione in un mondo fortemente, e verrebbe da aggiungere sin troppo, globalizzato. In sostanza, la domanda che ci si pone, osserva CyberArk, società specializzata nelle soluzioni che assicurino un business "always on", che ben si adatta al momento, è in che modo l'attuale tecnologia permette alle aziende di continuare ad operare in momenti come quello che si sta attraversando.

Posti di fronte ad una situazione imprevista le aziende hanno dovuto studiare come continuare a operare in un mondo virtuale, facendo leva sulla tecnologia per infondere stabilità e ridurre al minimo le interruzioni delle loro attività.

In questo, le tecnologie di collaborazione, come le conferenze web e il project management, consentono ai dipendenti di lavorare da casa, mantenendo l'operatività.

Quello che però si rivela essenziale è che strumenti e applicazioni utilizzati online siano sicuri e protetti, per evitare che aggressori possano sfruttare questi momenti di difficoltà per i loro fini ed aumentino ulteriormente la criticità per le aziende.

### **Il fattore tempo**

Fondamentale, in una economia globalizzata, fortemente interdipendente e dove il benessere sociale dipende dalla velocità con cui circolano merci e servizi, si delinea essere il fattore tempo.

La domanda che ci si pone allora è: le aziende stanno cercando di tenere il passo con i dipendenti che lavorano a distanza, ma in che modo possono farlo rapidamente? Una cosa è certa, in frangenti come questi la velocità e il tempismo, oltre che alle giuste decisioni, è tutto, e lo insegna la Storia.

Momenti di crisi anche profondi hanno poi portato ad un rapido sviluppo successivo, crisi di media intensità ma di lunga durata hanno richiesto alla società molto tempo per riprendersi.



Molte società, come le banche, hanno già attivato ad esempio i piani di continuità operativa che prevedono la possibilità per i dipendenti di lavorare da remoto. Tuttavia, molte aziende fanno fatica a mantenere le attività commerciali, soprattutto per problemi legati all'IT.

Rispetto all'epidemia di SARS del 2003, i progressi tecnologici stanno però permettendo a dipendenti e fornitori, e tutta la supply chain, di lavorare da remoto in sicurezza, fornendo l'accesso ad applicazioni e risorse mission critical al fine di supportare le attività quotidiane. Cosa che lascia ben sperare anche se la guardia va tenuta alzata.

### **I rischi dell'accesso remoto ad applicazioni mission critical**

Un fattore di rischio nel lavoro remoto e realizzato tramite infrastrutture disperse fisse e mobili, e relativi dispositivi di utente, è dato dal fatto che si moltiplicano i punti che possono essere fruiti da malintenzionati per superare le difese, entrare nei

sistemi e muoversi una volta entrati in ogni direzione. In pratica, ampliando la superficie esposta aumentano in modo esponenziale i rischi.

È una cosa sperimentata da tutti i grandi imperi che, oltrepassata una certa dimensione, non sono stati più in grado per limitazione tecnologica di far fronte ai nemici che ne penetravano in diversi punti le frontiere troppo estese.

In pratica, lo smart working distribuisce e amplia la superficie in cui si può lavorare, ma lo possono fare non solo i lavoratori ma anche i malintenzionati, che comunque sono pur sempre dei lavoratori, seppure sui generis e che sfruttano computer, cellulari e email per accedere ad applicazioni e dati critici dell'azienda.

Va poi considerato, osserva CyberArk, che molte imprese oggi si affidano a fornitori esterni per gestire porzioni della loro infrastruttura IT e, per farlo, queste organizzazioni devono disporre di un accesso privilegiato ai sistemi IT dell'azienda.

Tuttavia, l'estensione degli accessi privilegiati a

provider terzi può essere difficile quando ci si affida a sistemi di autenticazione e autorizzazione degli utenti convenzionali. I motivi sono svariati:

I tradizionali sistemi di gestione dell'identità e le soluzioni di controllo degli accessi, progettati per l'autenticazione dei dipendenti aziendali e dei dispositivi di proprietà dell'azienda, non sono adatti a garantire la sicurezza del personale di terze parti e dei dispositivi esterni.

La maggior parte delle aziende ha scarsa o nulla visibilità o controllo sull'accesso remoto alla rete aziendale. Fornire postazioni di lavoro a ogni fornitore non è una strategia applicabile e l'implementazione di VPN o agenti su laptop o desktop di un'altra azienda è spesso troppo oneroso da gestire per i team IT.

Personale e requisiti di accesso possono cambiare da un giorno all'altro, rendendo poco o punto praticabili i tradizionali schemi di gestione delle identità basati su ID utente e password.

Con un perimetro flessibile e una crescente dipendenza dalle attività in outsourcing, i team di sicurezza devono trovare modi innovativi per garantire ai fornitori esterni un accesso sicuro agli account privilegiati senza interrompere le operazioni.

Ce n'è per un SIO e un CIO, ma anche per il board aziendale, che in fin dei conti è responsabile ultimo della protezione dei dati aziendali, abbastanza per passare delle notti inquiete.

### **Autenticazione a più fattori e biometria la chiave per la sicurezza degli accessi**

Per dare una mano ad affrontare il momento difficile e nell'ambito della sua attività, CyberArk si è proposta di aiutare i suoi clienti a risolvere le esigenze di Business Continuity accelerandone il processo ed

estendendo la sua soluzione CyberArk Alero a fornitori e dipendenti che devono accedere ai sistemi critici interni.

Si tratta, nella sua essenza, di una soluzione che combina accesso Zero Trust, autenticazione biometrica a più fattori e provisioning just-in-time in un'unica soluzione erogata sotto forma di SaaS.

Tra gli obiettivi perseguiti dalla soluzione ed evidenziati dall'azienda, va annoverato che:

- Può essere configurata rapidamente per consentire alle aziende di mettere in sicurezza la propria infrastruttura IT e le informazioni sensibili.
- Mitiga i rischi per la sicurezza tramite un approccio Zero Trust Access. In pratica, assicura che i fornitori accedano solo a ciò di cui hanno bisogno.
- Non richiede VPN, agenti o password, e consente l'accesso dei fornitori attraverso sessioni tracciabili.
- Fornisce un accesso privilegiato senza password ai fornitori che hanno bisogno di accedere a sistemi interni critici.

Comunque, volendo dare un aiuto al detto scaramantico latino con comportamenti pratici, CyberArk suggerisce ai dipendenti che lavorano da casa di mantenere i dispositivi mobili e i computer portatili al sicuro con password e crittografia, utilizzare la cifratura, l'autenticazione a più livelli e il blocco delle sessioni per proteggere i dati e, non ultimo, mantenere hardware e software aggiornati e dotati delle più recenti patch.

La tecnologia aiuta di certo, ma di aiuto è di sicuro anche il buon senso. ❁

## CIE GARANTISCE LA SICUREZZA DELLE PICCOLE E MEDIE IMPRESE

*I firewall della serie Check Point 1500 forniti da CIE Telematica prevengono le minacce, migliorano la sicurezza della mail e abilitano una protezione zero-day*

*di Giuseppe Saccardi*

**S**e per una grande azienda che dispone di un team dedicato di sicurezza e capacità di investimenti il problema di come organizzare il lavoro e la protezione dei dati se non semplice è perlomeno gestibile, ben più critica è la cosa quando si tratta di una media o piccola azienda.

Quello delle PMI è un contesto dove raramente si dispone del know how e dei budget per approntare progetti che prevedano la selezione di soluzioni adatte alle specifiche esigenze produttive e settoriali, realizzare confronti e tantomeno impianti di test e di valutazione in campo.

Un aiuto alle PMI è quello offerto da CIE Telematica, società di ingegneria indipendente con esperienza trentennale nelle reti fisse e mobili e nella sicurezza che ha selezionato un portfolio di prodotti adatti a rispondere alle esigenze specifiche di cyber security delle PMI.

Tra le piattaforme selezionate da CIE Telematica vi sono ad esempio i firewall di nuova generazione Check Point SMB della serie Check Point 1500. Sono

dei gateway ad alte prestazioni che sono stati sviluppati dall'azienda specializzata con l'obiettivo di fornire un elevato grado di prevenzione delle minacce, migliorare la sicurezza della posta elettronica e abilitare una protezione di tipo zero-day.

In pratica, ha osservato Luigi Meregalli, general manager di CIE Telematica, si tratta di una soluzione che consente di rispondere agli eventi di sicurezza in tempo reale tramite anche un portale di gestione unificato. Permette anche di disporre in mobility e gestire la propria sicurezza tramite una apposita app mobile.

A livello di portfolio di soluzioni disponibili i gateway di sicurezza della serie 1500 estendono ulteriormente la famiglia di dispositivi di sicurezza per piccole imprese già disponibile, prodotti a cui hanno aggiunto protezioni di sicurezza a più livelli in un fattore di forma compatto da 1 unità rack adatto



*Luigi Meregalli – CIE Telematica*

per ambienti quali quelli delle PMI ma in grado di assicurare la protezione di fino a 300 utenti, realtà tipiche queste di una filiale anche di medie dimensioni o di piccoli uffici.

Come evidenziato, il firewall dispone di targa di robuste caratteristiche operative. In particolare:

- È consigliato da NSS (National Security Strategy)
- Presenta una frequenza di blocco del 100%.
- Provisioning Zero Touch out-of-box ,
- App mobile per la sicurezza in viaggio
- Portale di gestione unificato

«Check Point è un fornitore leader di sicurezza, quindi ci siamo rivolti alle loro offerte. Check Point Small Business Appliances ci offre sicurezza di livello aziendale in una soluzione di sicurezza all-in-one» ha dichiarato Trevor Rowley, amministratore delegato della società di software per la gestione aziendale Optix. ❁



*Security gateway per PMI distribuiti da CIE Telematica*

# È disponibile il nuovo libro **SMART & DIGITAL TRANSFORMATION**

## **SMART & DIGITAL TRANSFORMATION**

*Aziende, ambienti produttivi e città sono sempre più  
Smart, ma si deve garantire flessibilità, always-on,  
sicurezza e accesso al multcloud*

Giuseppe Saccardi

**Reportec**

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

# COME PRESERVARE LA SICUREZZA NELLO SMART WORKING

*I consigli pratici di Forcepoint per permettere ai dipendenti di lavorare da remoto in sicurezza e con adeguate prestazioni di rete*

*di Giuseppe Saccardi*

Lo scenario di queste settimane, sperando che si tratti di settimane e non di mesi, ha messo a dura prova i comparti IT delle aziende che si sono trovati a dover gestire un numero sempre maggiore di dipendenti in smart working.

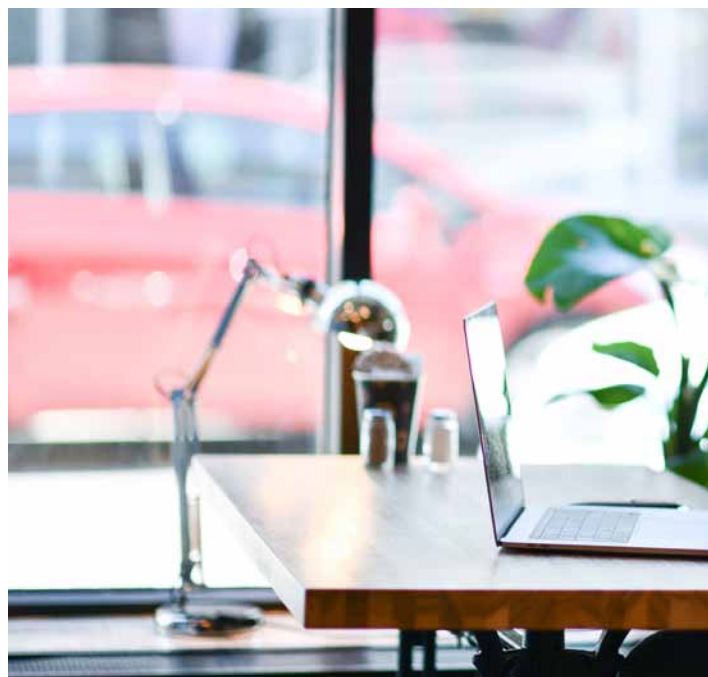
In risposta alla situazione globale, le aziende si sono dovute attrezzare per tutelare i propri dipendenti e, in molti casi, si sono attivate per implementare gli strumenti necessari per permettere ai lavoratori di proseguire le attività in smart working.

Ma come procedere o, parafrasando un termine molto in uso di questi tempi, che protocollo appare corretto seguire?

Un elenco di punti lo suggerisce Forcepoint, società molto attiva nella sicurezza informatica a livello mondiale, che ha stilato alcuni consigli pratici per permettere i di lavorare in sicurezza da remoto.

## **Seguire le disposizioni di emergenza o i piani di business continuity**

L'attuale contingenza rappresenta un banco di prova (se ne sarebbe fatto a meno volentieri ma tant'è) per gli strumenti informatici e la sicurezza della rete. In



tal senso appare necessario:

- Identificare i diversi flussi di lavoro a seconda del reparto: è fondamentale per capire quali applicazioni sono necessarie ai singoli dipendenti per svolgere il proprio lavoro.
- Attivare lo smart working a rotazione per un numero limitato di persone o sedi: è consigliabile al fine di testare l'accesso alla rete aziendale per dipartimento o tipologia di lavoro.
- Sviluppare un piano strutturato per comunicare con i propri dipendenti è importante: programmare fin dall'inizio come verranno inviati gli aggiornamenti e analizzare se è necessario suddividere le comunicazioni a livello di dipartimento, di reparto o di regione è essenziale per evitare rallentamenti.



### **Eeguire il test della soluzione di sicurezza sia dal punto di vista degli accessi che della capacità**

La chiave, evidenzia Forcepoint, è riuscire a valutare se la soluzione installata è in grado di supportare il crescente numero di lavoratori in smart working.

- Quali sono i dispositivi locali, le applicazioni cloud e gli ambienti ibridi di cui i dipendenti hanno bisogno per svolgere il proprio lavoro?
- La piattaforma Single Sign-On utilizzata ha un livello di sicurezza adeguato? In caso contrario, quali sono le criticità da affrontare?
- Per quanto riguarda le applicazioni cloud: quelle utilizzate dai dipendenti hanno livelli di flessibilità adeguati? È possibile estenderne la portata a centinaia o addirittura migliaia di nuovi utenti?

### **Verificare la sicurezza e il livello dei servizi VPN**

La connessione VPN è un elemento fondamentale per proteggere persone e dati. A maggior ragione se le aziende devono far fronte ad un elevato numero di dipendenti che accedono alla rete da remoto.

- Per garantire una adeguata connessione VPN e la continuità delle operazioni, è necessario quantificare il numero di dipendenti che si collegherà da remoto e moltiplicarlo per 2.
- Quali applicazioni deve utilizzare il marketing? Quali sono, invece, quelle per gli sviluppatori, il finance e la contabilità? Come anticipato al punto 1, attivare lo smart working a rotazione per i diversi comparti è un ottimo sistema per testare il livello di sicurezza e capacità richiesti da ognuno di essi.
- Per ottimizzare i servizi VPN è consigliabile creare connessioni "private", a seconda delle prestazioni, dei diversi dipartimenti e della tipologia di lavoro svolto. Ad esempio, è possibile creare una VPN specifica a cui i membri del team di contabilità possano accedere durante le attività di fine trimestre.

Le situazioni di emergenza possono capitare: è proprio per questo che le aziende sviluppano piani di continuità aziendale. L'importante, nota Forcepoint, è riuscire a sfruttare al meglio queste occasioni per testare gli strumenti e le tecnologie a disposizione. La verifica delle connessioni VPN e una soluzione di sicurezza in grado di coprire tutte le applicazioni e i device necessari per lavorare da casa, sono essenziali per garantire la produttività e tutelare i dipendenti in questo difficile momento. ❁

# CRESCONO GLI ATTACCHI DI PHISHING CHE SFRUTTANO IL CORONAVIRUS

*Mentre l'intero pianeta affronta l'emergenza sanitaria, mette in guardia Barracuda Networks, gli hacker sfruttano le discussioni via email e sul web*

di Giuseppe Saccardi

**N**ella lotta ai cybercriminali non si deve mai calare la guardia, nemmeno e viene da dire soprattutto nei momenti più critici. Dimostrazione è che crescono e diventano sempre più sofisticati gli attacchi di phishing che sfruttano l'emergenza Coronavirus.

In proposito, segnala la società, i ricercatori di Barracuda hanno segnalato il verificarsi di un costante aumento del numero di attacchi via email collegati al Coronavirus dilagato dalla Cina da gennaio scorso e osservato un recente picco in questo tipo di attacco, in crescita del 667 per cento dalla fine di febbraio.

Tra l'1 e il 23 marzo, ad esempio, Barracuda Sentinel ha rilevato 47.825 attacchi spear phishing email: 9.116 di questi rilevamenti erano collegati al Coronavirus, il che rappresenta circa il 2 per cento degli attacchi.

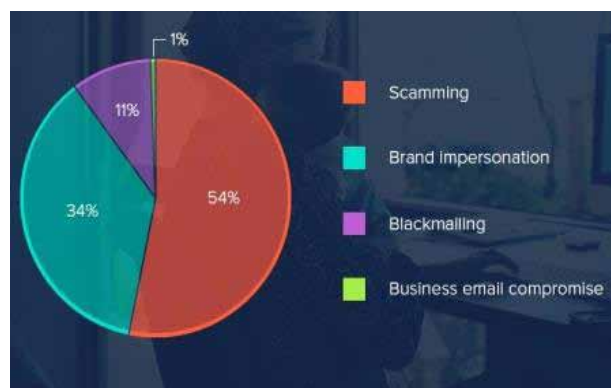
Per fare un raffronto, a febbraio sono stati rilevati 1.188 attacchi email relativi al Coronavirus e a gennaio solo 137. Sebbene il numero complessivo di questi attacchi sia ancora basso rispetto ad altri, la minaccia sta crescendo rapidamente.

## Come proteggersi?

Cosa fare per proteggersi dai malintenzionati? Vediamo cosa suggeriscono gli specialisti di Barracuda. Anche se le email di phishing che sfruttano il Coronavirus sono nuove, valgono comunque le stesse precauzioni di sempre per la sicurezza della posta elettronica:

Diffidare di qualsiasi email che cerchi di indurre gli utenti ad aprire allegati o a cliccare sui link. Le soluzioni anti-malware e anti-phishing possono essere particolarmente utili per impedire a email e payload dannosi di raggiungere i destinatari predestinati, ma anche con tali protezioni in atto si dovrebbe sempre usare cautela poiché nessuna soluzione è efficace al 100%.

Fare attenzione a tutte le comunicazioni che sostengono di provenire da fonti dalle quali normalmente non si ricevono email. Questi sono probabilmente tentativi di phishing. Mentre ricevere email relative al coronavirus da liste di distribuzione legittime a cui si appartiene sta diventando frequente, le email



di organizzazioni dalle quali non si ricevono regolarmente messaggi dovrebbero essere esaminate attentamente.

Usare cautela con le email provenienti da organizzazioni con cui si comunica regolarmente. La brand impersonation è piuttosto diffusa negli attacchi email relativi al coronavirus; è necessario quindi fare attenzione quando si aprono email che si prevede di ricevere da una determinata organizzazione. Ciò è particolarmente vero per coloro che operano nel settore sanitario poiché vengono presi di mira dagli attacchi informatici che approfittano della pressione derivante dalla gestione di un flusso enorme di casi di coronavirus.

Cercare enti di beneficenza affidabili e donare direttamente. Una tattica comune delle truffe legate al coronavirus è la richiesta di donazioni per aiutare le persone colpite dalla pandemia. Per evitare di

cadere vittima di uno di questi attacchi, non rispondere alle richieste via email di donazioni. Invece, è meglio individuare enti di beneficenza conosciuti e donare direttamente a loro per essere sicuri che i fondi finiscano dove possono fare del bene piuttosto che nelle mani dei truffatori. È anche altamente improbabile che qualsiasi organizzazione benefica legittima richieda donazioni attraverso i portafogli Bitcoin, quindi vedere questo in un'email dovrebbe essere un campanello d'allarme.

«Cerchiamo di rendere il mondo un posto più sicuro. Crediamo che ogni organizzazione meriti l'accesso a soluzioni di sicurezza di fascia enterprise cloud-enabled, semplici da acquistare, implementare e utilizzare. Proteggiamo email, reti, dati e applicazioni con soluzioni innovative in grado di crescere e adattarsi al crescere delle esigenze dei nostri clienti. Oltre 150.000 organizzazioni in tutto il mondo si affidano a Barracuda per proteggersi da rischi ai quali non sapevano neanche di essere esposte, affinché possano concentrarsi sulla crescita del proprio business» ha osservato Barracuda. ❁

## IL DECALOGO PER REALIZZARE MEETING DI GRUPPO IN SICUREZZA

*Pur di connettersi nel modo più veloce e comodo possibile, si trascurano aspetti importanti per la sicurezza. I dieci consigli di Kaspersky per proteggersi*

di Giuseppe Saccardi

**D**iverse app utilizzate per i meeting di gruppo, diventate popolari nelle ultime settimane, si sono scontrate, negli ultimi giorni, con alcuni problemi legati alla sicurezza informatica. È quello che evidenzia e su cui mette in guardia Kaspersky.

Ad esempio, osserva, l'aumento di popolarità di

applicazioni come HouseParty e Zoom ha destato l'interesse anche da parte dei criminali informatici mettendo in evidenza i possibili rischi legati all'uso di queste piattaforme.

David Emm, Principal Security Researcher di Kaspersky ha condiviso alcuni consigli su come proteggersi quando si utilizzano applicazione per le conferenze di gruppo, che siano con i propri cari o di lavoro.

«... Spesso, pur di connettersi nel modo più veloce e comodo possibile, si trascurano però alcuni aspetti molto importanti. Fatta la premessa che ciascun utente ha la possibilità di decidere quanto della propria vita privata desidera rendere pubblica online, è importante sottolineare che prima di condividere qualsiasi cosa in rete è importante farsi delle domande e tenere a mente qualche regola. Questo consentirà agli utenti di potersi connettere al web in modo sicuro e di rimanere in contatto con i propri car» ha osservato Emm.

### **Le domande da porsi prima di scaricare un'applicazione**

Da dove trae i propri guadagni l'applicazione che intendiamo scaricare? Se l'app è gratuita, il prezzo da pagare molto probabilmente saranno le informazioni personali degli utenti. È importante quindi controllare i permessi richiesti dalle app e verificare quali dati vengono raccolti, memorizzati e riutilizzati. I dati trasmessi dall'applicazione vengono criptati? Tenersi informati sulle tattiche di social engineering. Come si fa a sapere che le persone con cui veniamo in contatto utilizzando l'app siano realmente



### **I dieci consigli per utilizzare qualsiasi tipo di applicazione**

- Controllare con molta attenzione le impostazioni di privacy e sicurezza
- Utilizzare password uniche e complesse per tutti gli account online
- Porre dei limiti a ciò che può essere visto e condiviso
- Non dare la propria fiducia a qualcuno senza aver fatto prima delle verifiche. Verificare con i suoi contatti che l'identità di chi vi ha contattato/o inviato un link su un'applicazione sia reale
- Disattivare le funzioni che non vengono utilizzare o che non sono necessarie per abilitare l'accesso (ad es. microfono, accesso alla telecamera, ecc.).
- Non condividere ciò che non si vuole rendere pubblico e visibile a tutti
- Segnalare gli abusi
- Proteggere tutti i vostri dispositivi con un prodotto di sicurezza Internet affidabile
- Installare gli aggiornamenti del sistema operativo e delle applicazioni non appena disponibili
- Se si tratta di riunioni di lavoro, attenersi all'app raccomandata/fornita dalla vostra azienda e non alla vostra app preferita per le video call di gruppo.

chi dicono di essere? Come possiamo verificare le informazioni o i link ricevuti?

Ricordarsi che niente e nessuno può considerarsi al sicuro al 100%. Anche se pensiamo di non essere interessanti per un criminale informatico, siamo tutti potenziali vittime degli hacker interessati alle app.\*

## LO SMART WORKING RICHIEDE PIÙ SICUREZZA NEGLI ACCESSI

*I punti critici dello smart working e i rischi per la sicurezza in cui si può incorrere se non si controllano i requisiti illustrati da Rich Turner di CyberArk*

*di Giuseppe Saccardi*

L'emergenza Coronavirus ha spinto molte organizzazioni ad adottare pratiche di smart e remote working in un'ottica di continuità di business. Anche se obbligato, si tratta tuttavia di un approccio che richiede si ponga attenzione dal punto di vista della sicurezza.

Poiché il numero di dipendenti che lavorano a distanza aumenta rapidamente, fornire loro un accesso sicuro ai sistemi, alle applicazioni e ai dati provenienti dall'esterno della rete aziendale comporta spesso complicazioni.

Senza una connessione internet privata, gli utenti remoti che richiedono l'accesso a sistemi critici devono affidarsi a una combinazione di VPN, MFA e soluzioni di controllo dell'accesso remoto per potersi autenticare e accedere a ciò di cui hanno bisogno. Il problema è però, osserva Rich Turner, EMEA VP di CyberArk, che i tradizionali sistemi di enterprise identity management e le soluzioni di controllo degli accessi, solo per fare un esempio, sono progettati per autenticare i dipendenti e i dispositivi di proprietà dell'azienda e non sono del tutto adatti a

garantire la sicurezza del personale di terze parti e dei dispositivi esterni.

In pratica, è il punto del manager, possono essere facili da aggirare e non sono progettati per fornire un accesso granulare, spesso essenziale per utilizzare le risorse interne più importanti di un'organizzazione.

Peraltro, anche disponendo di un ampio margine di tempo per pianificare e implementare una soluzione – cosa che date le circostanze la maggior parte delle aziende non ha avuto – garantire l'accesso remoto è un compito difficile per molti.

È inoltre importante considerare, aggiunge Turner, che i requisiti di accesso e in particolare per le terze parti, possono cambiare sostanzialmente da un giorno all'altro o da una settimana all'altra, rendendo impraticabili i ricorsi ai tradizionali schemi di gestione dell'identità basati su user ID e password.

Ma, viene da dire, questo è un caso in cui, se piove,



*Rich Turner - EMEA VP di CyberArk*

piove sul bagnato. Questo perché buona parte se non la maggior parte delle aziende ha una visibilità o un controllo ridotto o del tutto assente sull'accesso remoto alle reti proprietarie, il che rende più difficile identificare e bloccare eventuali malintenzionati. Quando si verificano situazioni critiche che generano un senso di preoccupazione a livello umano, spesso si aggiungono rischi informatici con i cybercriminali impegnati a capitalizzare sulle paure della gente. Non per nulla la stessa OMS ha lanciato un

allarme sull'incremento degli attacchi di phishing legati direttamente al Coronavirus.

Cosa si può fare?

Con un perimetro che non esiste più e una crescente dipendenza dalle attività a distanza, i team operations e sicurezza IT devono ripensare la protezione, esplorando modalità innovative per garantire ai lavoratori esterni da remoto un accesso sicuro senza interrompere l'operatività, è il suggerimento di Turner. ❁

## SMART WORKING PIÙ SEMPLICE E SICURO CON IL DESKTOP VIRTUALE

*I nuovi ThinOX4PC e ThinMan di Praim abilitano lo Smart Working sicuro da ogni postazione e con qualsiasi dispositivo*

*di Giuseppe Saccardi*

**M**obilità, flessibilità, facilità di implementazione e di manutenzione, sicurezza, eccetera sono di certo caratteristiche molto importanti per le aziende in cerca di soluzioni a sostegno dei loro collaboratori che lavorano da remoto e a sostegno dei nuovi paradigmi di lavoro come il Nomad Work, lo Smart Working o la mobilità tra sedi e postazioni. Il problema è però come passare dalla teoria alla pratica ottimizzando gli investimenti e minimizzando i rischi di trovarsi in casa una piattaforma che si rivela poi poco adatta e flessibile.

Una risposta l'ha ideata Praim con le soluzioni VDI di desktop virtuali abbinate a un software che consente



### **Comunicazione sicura con il protocollo Web Socket**

Uno degli aspetti critici nello smart working è quello posto dalla amministrazione dei dispositivi e dalla sicurezza dei dati trasferiti da e verso remoto.

In pratica, servono gli strumenti necessari per la configurazione, la gestione e il monitoraggio dei Thin Client remoti, incluso in questo insieme anche un protocollo di comunicazione sicuro per la connessione

del server centrale, come il di ThinMan Server, agli endpoint remoti.

Il problema di un protocollo sicuro è critico, osserva Praim. Questo perché gli utenti remoti devono disporre della connettività di rete necessaria per raggiungere le risorse aziendali ed essere coperti in modo efficace, anche se non in sede, per quanto concerne gestione, monitoraggio e sicurezza.

Detto altrimenti, agli amministratori viene chiesto di garantire la sicurezza fornendo flessibilità agli utenti anche quando questi si spostano o si connettono da casa ma, non potendo conoscere ogni singolo ambiente da cui gli utenti si collegheranno,

di affrontare le sfide citate più tranquillamente a partire dall'amministratore IT sino all'utente finale.

In pratica, ha evidenziato l'azienda, una soluzione come il suo nuovo ThinOX4PC consente ad esempio di trasformare qualsiasi dispositivo in un Thin Client aziendale sicuro, facilmente controllabile e che può essere gestito attraverso un unico pannello di controllo.

Recentemente, inoltre, la società ha anche rilasciato delle nuove funzionalità, sia su ThinOX4PC che nella console di gestione ThinMan Server, funzionalità indirizzate a favorire e semplificare la gestione "end-to-end" degli utenti remoti.

devono fornire strumenti e linee guida semplici per garantirne l'operatività.

Per renderlo possibile Praim ha sviluppato uno specifico protocollo di comunicazione che ha l'obiettivo di semplificare notevolmente la comunicazione fra le soluzioni Thin Client Praim e ThinMan Server. Tramite il nuovo protocollo Web Socket Secure i prodotti Praim, tra cui ThinOX, Agile4PC, Agile4Pi e ThinOX4PC, possono comunicare con ThinMan Server salvaguardando la sicurezza delle comunicazioni.

Peraltro, evidenzia Praim, il nuovo protocollo fornisce funzionalità aggiuntive per la comunicazione tra gli endpoint Praim e ThinMan Server. Le funzionalità includono:

- Connessioni sempre attive verso ThinMan
- Maggiore visibilità dello stato dei client
- Flessibilità nella scelta del certificato di sicurezza
- Configurazione di rete meno onerosa

Per quanto concerne la sicurezza, in particolare, la crittografia su Web Socket è resa possibile utilizzando i certificati SSL. L'implementazione Praim di Web Socket sicuri nella comunicazione fra Thin Client e ThinMan consente nello specifico di adottare certificati SSL ottenibili con Let's Encrypt, oppure altri originati direttamente dalla propria infrastruttura PKI aziendale.

Numerose le possibilità di utilizzo evidenziate da Praim. Tra queste:

- Telelavoro: gli utenti remoti possono lavorare ovunque, purché dispongano di una connessione Internet e possano connettersi a ThinMan utilizzando la porta 443.

- Service provider: un service provider è in grado di gestire più gruppi di sistemi client da un unico pannello di controllo in cloud.
- Gestione dei dispositivi in mobilità: i dispositivi come i laptop sono pensati per spostarsi tra reti e postazioni di lavoro diverse. Il nuovo protocollo di comunicazione lo abilita senza la complessità della configurazione di rete ed evitando problemi agli amministratori IT e agli utilizzatori finali.
- Accesso remoto semplificato: l'accesso remoto e la comunicazione con i servizi interni sulla rete aziendale sono tradizionalmente realizzati con una connessione VPN. Tramite il protocollo di comunicazione sicura con ThinOX4PC e Agile4PC, la comunicazione con la rete aziendale interna è semplificata dalla comunicazione sempre attiva e crittografata con il server ThinMan.

In sintesi, riassume Praim, con il nuovo protocollo di connettività sicuro Web Socket integrato nei software Praim e il nuovo configuratore WiFi per ThinOX4PC, si viene a disporre degli strumenti necessari per una connettività senza interruzioni e disponibile su qualsiasi dispositivo.

Combinando le due soluzioni software Praim ThinMan e ThinOX4PC, qualsiasi dispositivo può essere trasformato in un Thin Client e qualsiasi luogo trasformarsi in una postazione di lavoro collegandosi al desktop virtuale aziendale. ✨