
IL CAFFÈ DIGITALE
THE INNOVATION GROUP
NEWSLETTER
The Innovation Group
Innovating business and organizations through ICT
SPECIAL EDITION
CYBERSECURITY
SUMMIT 2020

**Sponsor**

**Partner Sponsor:**

**Gold Sponsor:**

**Media Partner:**

**Con il patrocinio di:**

# Sommario

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Usare l'Intelligenza Artificiale per la Cybersecurity

Intervista a

**Alessandro Monforte**

**Regional Sales Manager, Cloud Cyber Security Solutions, Cisco**

Sempre di più, come si è visto anche nell'ultimo periodo, con una recrudescenza degli attacchi informatici in contemporanea all'avanzamento della pandemia Covid-19, le aziende devono gestire uno Tsunami di minacce informatiche che colpiscono device fissi e mobili, con lo scopo di infiltrarsi nei sistemi core business ed esfiltrare informazioni sensibili. Una risposta efficace può però già oggi far leva sulle potenzialità dell'AI, che arriva a identificare e fermare le minacce laddove gli approcci tradizionali falliscono. Ne parliamo in questa intervista con Alessandro Monforte, Regional Sales Manager, Cloud Cyber Security Solutions, Cisco.

**Come vede evolvere nel breve periodo la situazione con riferimento alle minacce informatiche? Quali sono le tendenze a livello di malware? quali le caratteristiche e cosa puntano a colpire?**

Nell'ultimo periodo il numero di attacchi informatici è cresciuto enormemente, soprattutto con temi legati all'emergenza del Covid-19: basti pensare che i laboratori Cisco Talos di Threat intelligence, hanno misurato il 3 aprile 2020 115mila nuovi domini registrati con la parola corona o covid nel nome, e di questi 75mila (il 65%) erano malevoli.

Oggi le minacce sono collegate a due grandi famiglie di malware: da un lato i Trojan bancari, che possono colpire sia i dispositivi fissi che quelli mobili con lo scopo di sottrarre le credenziali di home banking o dati sensibili, e dall'altro lato il Cryptojacking. Con riferimento ai Trojan, si tratta di una minaccia rilevante, che sta crescendo ed è sempre più sofisticata. Molto spesso i trojan sono degli "zero day" – ossia sfruttano vulnerabilità nuove, mai incontrate prima, per cui non esistono ancora delle cure, come sta succedendo in questi giorni con la diffusione pandemica del coronavirus cinese: non avendolo mai visto prima, e non essendoci cura, è il panico.

In presenza di malware zero day, le soluzioni tradizionali come gli antivirus sono inefficaci perché non li riconoscono. Serve quindi far evolvere la difesa e ricorrere a soluzioni basate su tecniche di intelligenza artificiale (AI). I Trojan bancari sono molto evoluti nella capacità di esfiltrare informazioni sensibili, in particolare Emotet, un nome che oggi è sulla bocca di tutti, perché particolarmente malevolo e molto ostico. Nel 90% dei casi, Emotet infetta sia pc sia cellulari attraverso la classica mail di phishing, che sollecita il povero "cliente" a inserire i propri dati per la fatturazione, a specificare l'Iban del proprio conto, a loggarsi a una copia fasulla del sito della propria banca. Oggi viene preso di mira anche il cellulare, con il quale, dato lo schermo ridotto, le persone soffrono di una più bassa percezione sulla veridicità del sito. Nel secondo semestre del 2019, Cisco ha intercettato tramite le proprie soluzioni - solo

in Italia - 800.000 attacchi collegati a Emotet: il malware era presenti nel 90% dei casi in messaggi di posta elettronica.

**Per quale motivo questo malware è in forte crescita?**

Perché permette al cyber crime di ottenere un premio consistente se l'attacco ha successo. Noi abbiamo individuato per l'Italia 16mila domini malevoli da cui provengono questi attacchi. Un aspetto che rende Emotet molto insidioso è il fatto che è in grado di rilevare se si trova in un ambiente sandbox, ossia se ha colpito un utente vero oppure se è in un ambiente protetto (utilizzato per far detonare il malware e capire come si comporta). Il malware è dotato di meccanismi per rilevare se è in un ambiente virtuale come il sandbox. Inoltre, un'altra caratteristica che lo contraddistingue è il fatto di essere esso stesso veicolo per altri trojan, da utilizzare per vari scopi.

Cosa fare per bloccarlo? serve dotarsi di tecniche di AI e avere una soluzione in grado di avvisarti, nel momento in cui cadi nella trappola del phishing, che stai andando su un sito malevolo. Poichè questi domini malevoli cambiano in continuazione, non basta più una soluzione tradizionale basata su attacchi noti, servono invece algoritmi AI applicati a livello infrastrutturale che si accorgono che il dominio è stato registrato da una persona sospetta, quindi ragionevolmente è da evitare. In questo modo la navigazione viene immediatamente bloccata.

**Quindi la soluzione si presta bene alla protezione di tutti gli ambienti usati dagli utenti**

È una protezione pensata per tutti gli endpoint, device fissi e mobili. Nel caso del mobile, con uno schermo piccolo è più facile essere raggirati. Cisco ha sia soluzioni preventive sia di endpoint security: il trend che si è osservato di recente è quello che vede la difesa informatica scegliere soluzioni di detection e response intelligente sugli endpoint, con capacità di analisi retrospettiva. Se trovo il computer infetto, superata la prima linea di difesa, la soluzione EDR (Endpoint Detection e Response) grazie all'analisi retrospettiva è in grado di dire da dove è arrivato il malware e come si è propagato: informazioni utili per investigare e porre rimedio.

**Secondo trend importante?**

C'è una seconda importante famiglia di malware da tenere sotto attenzione: quella che caratterizza il fenomeno del cryptojacking. Il cryptomining di per sé sarebbe una pratica lecita: l'utilizzo di cicli di calcolo del PC per il mining, la produzione di criptovalute. Il cryptojacking è però diverso perché avviene all'insaputa dell'utente. L'unica cosa che si osserva, mentre la potenza di calcolo è "trafugata", è un rallentamento delle prestazioni del PC, che in quel momento sta producendo criptovalute. Il volume di attacchi cryptojacking nel primo semestre 2019 è stato di 53 milioni di attacchi a livello mondiale.

Il cryptojacking è anche questo piuttosto noioso: usa javascript, che è presente in ogni dominio visitato, per cui è molto semplice incontrare il malware che instilla questo codice malevolo nel browser. Non c'è signature di malware per questo attacco: se arrivo su un dominio con javascript infetto subito avviene l'infezione. Anche qui serve quindi l'AI per avvisare se un certo sito – correlato ad un altro malevolo – va evitato. Sono trend che riguardano molto da vicino i dispositivi mobili, per cui è importante che le aziende proteggano bene i device mobile dei propri dipendenti, cosa non semplice in ambiente BYOD. Servirebbe che anche i carrier pensassero di dotare le proprie offerte di un layer aggiuntivo di sicurezza.

C'è una seconda importante famiglia di malware da tenere sotto attenzione: quella che caratterizza il fenomeno del cryptojacking. L'unica cosa che si osserva è un rallentamento delle prestazioni del PC, che in quel momento sta producendo criptovalute. Il volume di attacchi nel primo semestre 2019 è stato di 53 milioni a livello mondiale.

**Parlando di gestione dei rischi cyber e della maturità raggiunta dalle aziende italiane, in passato la tendenza era piuttosto verso la prevenzione che non verso la capacità di detection e risposta. Sta cambiando qualcosa?**

Purtroppo, in Italia persiste una mentalità basata sull'assunzione "a me non capita", e quando capita, è il panico. Osservo ancora poca proattività nelle aziende, e la cybersecurity è vista come un costo piuttosto che come un'opportunità (oltre che una necessità). Abbiamo ospedali che colpiti da ransomware hanno chiuso i battenti per diversi giorni, o aziende produttive italiane che infettate da ransomware, soprattutto se si trattava di PMI, hanno fermato la catena di produzione, con un grave danno economico. Con competenze informatiche in molte PMI pari a zero, arriviamo

al paradosso per cui alcuni ritengono più conveniente pagare il riscatto piuttosto che investire in cybersecurity.

Nelle grandi aziende, abbiamo un CISO e sono presenti varie soluzioni. Il problema è qui che si arrivano a contare 10, 15 fornitori di cybersecurity nella stessa azienda, ognuno molto verticale, con tutta una serie di soluzioni che non si parlano, ognuna con una sua consolle di gestione diversa. Se voglio sapere come sono messo rispetto ad esempio a un'epidemia di ransomware in corso, la risposta sullo stato della sicurezza è complessa e non unificata, e servono in media 60 giorni per capire che si è stati attaccati e a mettere in piedi le contromisure. Invece l'incident response sarebbe un elemento fondamentale: come emerge anche dal recente "2020 CISO Benchmark Study" (sesta edizione dell'analisi annuale di Cisco volta a riportare le 20 priorità in ambito cybersecurity per il 2020), la complessità di gestione della cybersecurity, legata alla molteplicità di ambienti diversi presenti in azienda, mette a dura prova la resistenza dello staff di security.

*Fonte: 2020 CISO Benchmark Study, Cisco. Numero dei diversi security vendor utilizzati negli ambienti di sicurezza delle aziende (N = 2.800).*

Dai risultati della survey si ha che già oggi il 34% delle aziende hanno dato in outsourcing i servizi di incident response, mentre il 36% utilizza terze parti per l'analisi dei sistemi compromessi, una percentuale in crescita rispetto allo scorso anno. Bisognerebbe quindi premiare soluzioni molto integrate e soprattutto dotarsi di una consolle unitaria a cui accedere, inserire le informazioni sul malware e capire se sono stato colpito. In questo modo diventa più facile effettuare le corrette azioni di remediation.

**In conclusione, quali sono le priorità oggi?**

Bisogna mettere al sicuro il paese: per farlo, sarebbe fondamentale una maggiore collaborazione tra vendor di sicurezza e carrier in modo che questi riescano ad elevare la sicurezza a livello di sistema, attraverso le proprie offerte rivolte ai mercati residential e PMI, per colmare questo vuoto di tecnologia nei segmenti più esposti e con meno abilità tecniche.

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## GDPR compliance, come ottimizzarne la gestione

Intervista a

**Valentina Raineri**

**Privacy Engineer, OneTrust**

Da tempo le aziende si sono attivate sul fronte della compliance al GDPR, scoprendo però che per alcuni aspetti (gestione dei rischi, DPIA o Data Protection Impact Assessment, gestione del Registro dei trattamenti, Accountability) la complessità della gestione rendevano tutto il processo di mantenimento della compliance estremamente oneroso. Anche la recente emergenza legata alla pandemia Covid19 ha riportato in primo piano le esigenze di un corretto trattamento della privacy, considerando l'uso più esteso di trattamenti di dati personali, effettuati nell'ultimo periodo con un uso più intensivo di tracciamento delle persone in rispondenza a esigenze sanitarie o per facilitare il remote working.

Una proposta innovativa è quella della soluzione di compliance management offerta da OneTrust, di cui abbiamo parlato in questa intervista a Valentina Raineri, Privacy Engineer, OneTrust.

**Considerando lo stato dell'arte della compliance, quali sono le principali problematiche incontrate dalle aziende in base alla vostra esperienza?**

Un tema che incontriamo di frequente è come mantenere aggiornato il Registro dei trattamenti: molte società hanno dovuto adeguarsi velocemente al GDPR, per cui hanno creato un registro provvisorio, solo con le informazioni di base registrate su excel. Questa soluzione però rimane statica nel tempo. Serve invece un registro costantemente aggiornato, ma non è facile tenere traccia di chi ha fatto cosa e quando, e avere il testo finale disponibile per tutti. Con il nostro software, diventa molto più facile gestire questo processo.

**Come funziona in pratica la vostra soluzione?**

La nostra soluzione si esplica in varie fasi: nella prima, popoliamo la piattaforma in vari modi, ad esempio, importando direttamente tutti i dati già presenti in excel. Alcuni clienti, più all'estero che in Italia, sono già dotati di software per cui la nostra piattaforma – tramite un tool molto flessibile, un Open API framework - si collega a tutti questi sistemi. Un altro metodo che seguiamo è quello di inviare questionari alle persone del business che sono responsabili di processo e del trattamento di dati personali. In questo modo, riusciamo ad arrivare alla sorgente delle informazioni.

Dopo aver raccolto il dato, tramite la piattaforma è possibile compiere varie attività, il risk management, la DPIA. Il tutto con il fine di rispondere alla GDPR compliance, trattare correttamente i dati e mitigare i rischi, avendo on board il business, quindi collegandosi direttamente a diversi asset (ambienti applicativi) e trattamenti, e riuscendo sempre a capire come i diversi ambienti si collegano uno con l'altro e quali sono i dati personali coinvolti.

**Quali vantaggi si ottengono e quali riscontri avete dai vostri clienti?**

Tutto questo serve a ridurre la complessità del mantenimento di una soluzione di compliance al GDPR, riducendo le perdite di tempo, l'onerosità delle procedure e rendendo più efficace il processo. Osserviamo che spesso le informazioni sono mancanti: le persone del business sono all'origine del dato, se non ti interfacci direttamente con chi è responsabile del processo, spesso le informazioni non sono corrette, chiare o complete. La soluzione aiuta quindi ad ottenere una maggiore qualità del dato e un Registro dei trattamenti aggiornato, facilita e automatizza DPIA ricorrenti. Aiuta nella gestione dell'Accountability, perché mi dice chi ha fatto che cosa. Abilita una visione generale di tutti i dati personali trattati in specifici momenti del trattamento, compresi i fornitori legati a specifici aspetti del trattamento e agli asset / applicativi coinvolti.

**Con riferimento all'analisi del rischio, quali sono i vantaggi che si ottengono?**

L'analisi del rischio viene fatta sia inizialmente, quando si sta definendo un processo nuovo, sia in via ricorrente, con un risk assessment legato al DPIA o a un'analisi del rischio generale. In caso di trattamento di dati sensibili, l'analisi del rischio dice come mitigarlo, quali controlli e misure di sicurezza vanno implementate.

L'analisi del rischio è quindi un aspetto molto importante e delicato, centrale all'intera compliance: anche il Risk Management comprende aggiornamenti periodici, per cui è importante poter visualizzare il collegamento tra il rischio e i singoli trattamenti, oltre che poter, in caso di eventuale controllo del Garante, essere in grado di dimostrare che i rischi sono noti e sono state intraprese le corrette misure per mitigarli.

**La compliance al GDPR è stata una priorità per le aziende a partire da maggio 2018: vede ancora molto interesse oggi per gli aspetti collegati all'adeguamento?**

Il mercato Privacy è oggi tuttora molto attivo: lo dimostra il fatto, comunicato di recente, che OneTrust ha ricevuto – a compimento del suo primo funding round dello scorso luglio – finanziamenti per 210 milioni di dollari. Il mercato chiede infatti soluzioni complete, efficaci e facili da utilizzare per ridurre l'onerosità della compliance, che ha richiesto ad oggi un effort molto elevato.

Spesso i team che si occupano del GDPR nelle imprese sono legali con limitate competenze tecniche: importante quindi rendere il lavoro più semplice. È un mercato che vediamo crescere molto, e non solo per aspetti come data mapping, DPIA, gestione incidenti, ma anche per altri, come informative e consenso cookies. Non è un caso che siano state proprio queste mancanze a motivare le ultime sanzioni milionarie rivolte in Italia a ENI Gas e Luce e a TIM. Oggi le aziende stanno imparando che il vero valore sta nel potersi dire "Privacy First", nell'aver riconosciuto la priorità del Privacy by design nelle proprie attività.

**Parlando di incident management, quali aspetti caratterizzano la vostra soluzione?**

La forza del nostro modulo specifico per l'Incident Management sta nell'avere un punto centralizzato in cui gestire incidente di ogni tipo. Dove non c'è il processo di gestione dell'incidente, diventa molto utile dotarsi di un disegno del processo dell'incidente. Inoltre, grazie all'intelligenza del modulo OneTrust, nel momento in cui si inserisce o aggiunge incidente, si capisce – in base al Paese in cui mi trovo – qual è l'urgenza dell'incidente e quale deve essere la procedura da seguire, che cambia a seconda delle norme del singolo Paese.

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Cyber Risk Management 2020, a che punto siamo

A cura di
**The Innovation Group**

La pandemia da Coronavirus, a partire da fine febbraio 2020, ha messo i Responsabili della Security in una situazione completamente nuova, in cui la priorità è stata garantire la Safety delle Persone e la Resilienza e Continuità operativa del Business.

**CON LA SUA SURVEY ANNUALE SUI TEMI DEL CYBER RISK MANAGEMENT, TIG HA PUNTATO A MISURARE IL LIVELLO DI MATURITÀ RAGGIUNTO DALLE AZIENDE ITALIANE**

La risposta è stato un ricorso generale allo Smart Working, in uno scenario in cui i Rischi cyber diventavano giorno dopo giorno più numerosi (l'Italia è stata immediatamente presa di mira dagli Hacker con attacchi di Phishing e malware mirato) e il personale operativo da remoto richiedeva maggiori misure di sicurezza e supporto.

Il mondo che esce dalla pandemia da Coronavirus è profondamente cambiato: il Digitale è entrato in ogni ambito della vita personale, e la domanda di cybersecurity (oltre che di poter scegliere per la propria privacy) è oggi altissima. Con la sua survey annuale sui temi del Cyber Risk Management, The Innovation Group ha puntato a misurare il livello di maturità raggiunto dalle aziende italiane, facendo luce sulle sfide attuali, le frustrazioni e le speranze di chi lavora per la resilienza della propria organizzazione.

Dai risultati della survey "CYBER RISK MANAGEMENT 2020", condotta tra dicembre 2019 e gennaio 2020, si osserva una situazione complessa: le minacce cyber osservate dalle aziende sono numerose e la lista aumenta di anno in anno; in molti casi gli incidenti informatici subiti in conseguenza di attacchi cyber hanno conseguenze gravi; identità degli utenti ed endpoint aziendali sono gli ambienti più colpiti, ma i problemi non si limitano al perimetro noto dell'azienda, perché anche il cloud e l'Internet degli oggetti sono oggi vulnerabili.

La gravità della situazione richiede sempre di più il coinvolgimento del vertice aziendale su

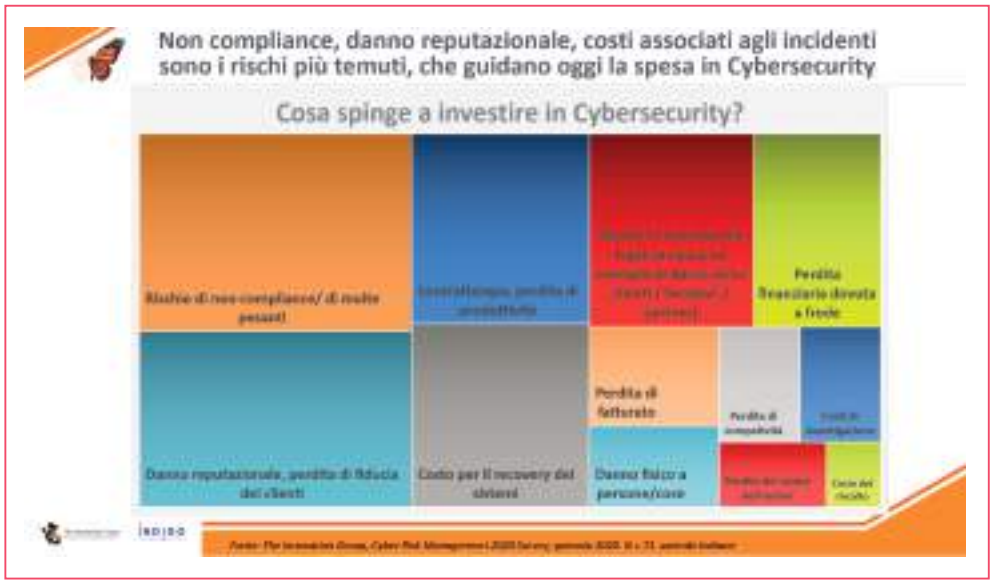
più fronti della cybersecurity; dall'altro lato, le aziende devono valutare attentamente quali sono gli impatti più gravi di un eventuale incidente, in modo da essere pronte ad affrontarlo.

## I principali Insight ottenuti dalla rilevazione di The Innovation Group

In termini di minacce osservate con maggiore frequenza, il Phishing lo è stato nel 2019 per il 71% delle aziende (+29% rispetto al 2017); a seguire, il Malware per il 58% (+12% rispetto al 2017) e il Ransomware per il 43% (-12% rispetto al 2017).

Solo l'8% delle aziende (il campione dei rispondenti è composto da realtà di tutti i settori e dimensioni) non ha osservato alcuna minaccia di cybersecurity. Un numero in diminuzione rispetto al 2017 (quando non aveva osservato minacce l'11% dei rispondenti).

Identità degli utenti ed Endpoint dell'azienda sono gli ambienti che più spesso sono stati coinvolti in incidenti cyber: rispettivamente nel 48% e nel 46% dei casi.




crittografando i dati (in mancanza di backup si rischia quindi di perdere del tutto) e rendendo le macchine inutilizzabili.

Parlando di quelli che sono i principali driver degli investimenti in Cybersecurity, va segnalato che il rischio di non compliance e multe pesanti è percepito dalle aziende come molto elevato, il 65% delle aziende lo considera uno dei principali driver per prendere provvedimenti in ambito sicurezza ICT. Segue a breve distanza il danno reputazionale, con possibile perdita di fiducia dei clienti, che è temuto da un 58% delle aziende. Altri impatti negativi che si temono, perché strettamente correlati ad incidenti di sicurezza, sono la perdita di produttività, il costo per il recovery dei sistemi e il rischio di controversie legali. L'eventuale costo legato a una richiesta di riscatto (ransomware) è invece all'ultimo posto (4% delle risposte). La diffusione del ransomware è purtroppo correlata a questo aspetto: gli attaccanti sanno bene che spesso le aziende preferiscono pagare il riscatto piuttosto che incorrere in tutti gli altri inconvenienti.

La rilevazione e la risposta in caso di incidente porta a dotarsi sempre più spesso di strumenti e servizi ad hoc: ai primi posti, Network Intrusion Detection (IDS, IPS) (66% delle risposte), Network traffic monitoring (62%), Log monitoring (60%), Endpoint Detection & Response (EDR) (52%).Al secondo posto però (35% delle risposte) la situazione appare già più grave, in quanto il blocco ai sistemi ha determinato la completa impossibilità di lavoro per gli utenti.

Analizzando nel dettaglio quali sono state le conseguenze tra chi ha avuto un impatto negativo da incidenti di cybersecurity, al primo posto (54% delle risposte) figurano i "leggeri disagi" per le persone.

Perdita di dati e mancata produttività delle persone sono quindi gli impatti con conseguenze economiche rilevanti: quelli che le aziende devono temere di più. Non è un caso che il Ransomware sia diventato un fenomeno così devastante: porta contemporaneamente ad entrambi gli effetti,

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Intervista con i CISO: cosa ha insegnato l'emergenza

Intervista a

**Fabio Gianotti**

**Chief Security Officer di UBI Sistemi e Servizi**

Il periodo dell'emergenza da Covid19 è stato per molti il momento in cui verificare (con uno stress test massivo) quale sarebbe stato il livello di resilienza aziendale, sul fronte di processi, persone e infrastrutture IT. Parlando di sicurezza, i responsabili di questo ambito hanno dovuto garantire, in tempi rapidissimi, il funzionamento e la conformità agli standard interni di un nuovo modello operativo basato sul distanziamento sociale di grandi numeri di persone.

Come è stata affrontata l'emergenza e cosa abbiamo imparato? Come guardare al futuro con una nuova consapevolezza e una maggiore tranquillità, avendo sviluppato ulteriori competenze e – ove richiesto – un upgrade tecnologico? E dove bisognerà ancora concentrarsi e innovare ulteriormente nel prossimo periodo? affrontiamo questi temi con Fabio Gianotti, CSO di UBISS.

**Come è stata affrontata l'emergenza? I sistemi informativi della Banca erano pronti a sostenere una forza lavoro collegata in gran parte da remoto?**

Il nostro vantaggio è stato che in effetti la Banca era già preparata: avendo per sua natura molti vincoli legati alla compliance a normative forti, la resilienza e la sicurezza dei processi sono da sempre una priorità, per cui l'operatività sicura da remoto era già possibile. Ad esempio, per il nostro SOC abbiamo una soluzione ibrida, per cui il 75% della workforce dedicata aveva già la possibilità di accedervi da remoto più giorni alla settimana. Anche tutto lo sviluppo del software è stato fortemente contaminato da aspetti di sicurezza negli ultimi anni. Questa forte informatizzazione ci ha permesso di mettere in piedi, in sole 2 settimane, oltre 10mila postazioni di lavoro virtuali (oltre quelle già date ai dipendenti).

Siamo arrivati in breve a punte fino a 10, 15mila accessi, per metà in VDI e per metà con VPN. Ci è bastato quindi adeguare le licenze, e le infrastrutture erano già pronte e resilienti per sopportare tutto questo.

**Nell'ultimo periodo, quello che ha preoccupato molti è stata la possibile vulnerabilità degli endpoint: qual è stata la vostra risposta?**

Avendo adottato già quattro anni fa tutta la suite Office365, il cloud ci ha molto aiutato. Dal punto di vista della sicurezza, poi, da tre anni fruiamo di una soluzione CASB per la protezione degli accessi via API ai nostri servizi cloud.

Oggi tutti gli accessi alla intranet hanno una strong authentication con software token. Inoltre, sugli endpoint, tutti gli strumenti (antimalware, ecc.) permettono di tenere sotto controllo la situazione. Un ulteriore livello di sicurezza è quello che abbiamo aggiunto a settembre 2019, con una tecnologia israeliana di deception, grazie alla quale

riusciamo ad effettuare una completa analisi comportamentale degli utenti, a replicare la CX del collega e a prevenire eventuali movimenti laterali, verificando che le attività siano quelle corrette.

Questa soluzione che ci ha permesso di avere una notevole persistenza e capacità di prevedere la parte comportamentale: stiamo ora lavorando, per il futuro, a un concetto password less, ossia a un'autenticazione comportamentale, con schemi che vanno oltre rispetto alla realtà odierna di un oggetto per autenticarsi che l'attaccante può rubare.

**L'utilizzo di tecnologie avanzate di questo tipo richiedono però un'elevata "maturità" dal punto di vista della completa digitalizzazione e ingegnerizzazione di tutti i flussi?**

Assolutamente sì: nel nostro caso siamo partiti già da anni e ad oggi tutta la parte applicativa fruisce di un dato cifrato fino alle terze parti. Ossia, anche i fornitori che lavorano con noi devono seguire un nostro protocollo.

L'analisi comportamentale funziona bene se già avanti su questa strada, e ci insegna che non ci possiamo improvvisare: tutti i tasselli devono far parte di un framework, che nel nostro caso è quello del NIST. Il nostro piano strategico per la sicurezza del 2019 è entrato del resto a far parte integrante del piano industriale della Banca: un lavoro importante, che serve però a far capire bene cosa si può fare e cosa no.

**Se quindi l'esperienza della pandemia vi è servita a confermare la bontà delle scelte effettuate in passato, quali sono le conclusioni dopo questo "stress test" e di conseguenza i piani per il futuro per la cybersecurity?**

Le aziende enterprise hanno di default le infrastrutture necessarie per lo smart working, il tema è con che velocità si riesce a scalare. Noi avevamo già un modello per il lavoro da remoto, ma per adottarlo per tutti è servito soprattutto avere un piano di continuità operativa – che nelle banche è anche richiesto dalle norme. La pandemia è servita per noi a testare tutte le funzioni critiche dal punto di vista dell'operatività di remoto, allargando il perimetro della business resilience fino all'infrastruttura domestica.

Questa esperienza poi ha fatto capire all'azienda che il perimetro aziendale è sempre più liquido e allargato: di conseguenza anche le minacce possono arrivare da più canali che prima non si consideravano. Oggi con la disponibilità per tutti di strumenti mobile, le persone si rendono conto di essere molto più produttive. L'approccio di cybersecurity ora deve essere di tipo "anti-fragile", ossia basarsi su il concetto di analisi comportamentale e password less.

Le aziende enterprise hanno di default le infrastrutture necessarie per lo smart working, il tema è con che velocità si riesce a scalare. Noi avevamo già un modello per il lavoro da remoto, ma per adottarlo per tutti è servito soprattutto avere un piano di continuità operativa – che nelle banche è anche richiesto dalle norme.

# CYBERSECURITY SUMMIT 2020

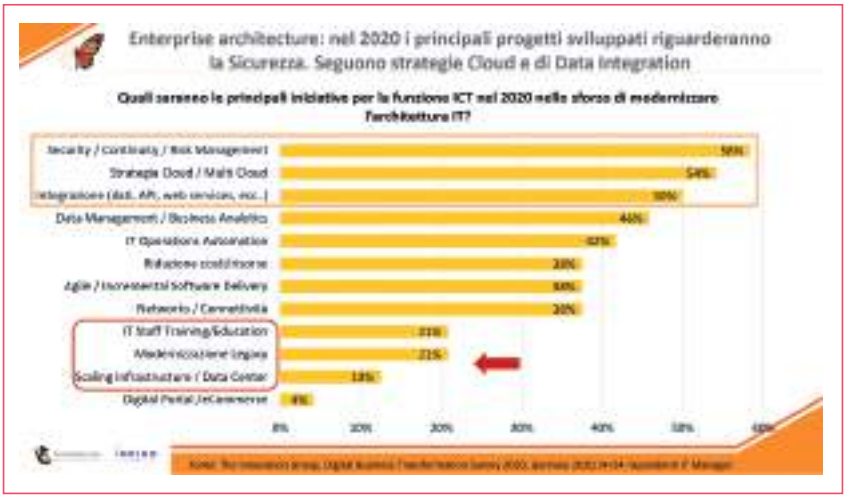
## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

### Quali saranno le conseguenze del Covid19 sulla Cybersecurity

**Elena Vaciago**
**Associate Research Manager, The Innovation Group**

La diffusione del coronavirus ha sospeso la vita delle persone e delle economie di ogni parte del mondo, ma il ricorso al digitale ha favorito la continuità delle relazioni e del lavoro: questo potrebbe portare a conseguenze importanti, nel prossimo periodo, sui progetti di sicurezza informatica.

Quando a inizio 2020, in The Innovation Group abbiamo analizzato i risultati della nostra survey annuale sui trend della Digital Trasformation, la "DBT Survey 2020", condotta tra dicembre 2019 e febbraio 2020 su un campione di 181 aziende italiane operanti nei diversi settori, è emerso che l'importanza della cybersecurity era già molto elevata: sostanzialmente al primo posto tra i progetti previsti per la modernizzazione degli ambienti IT, con un 58% di aziende che citavano queste iniziative. Poi, nel giro di poco tempo, molte cose sono cambiate. Con il diffondersi dell'epidemia, la priorità è stata quella di mettere in sicurezza il lavoro da remoto. Tanto più che gli attaccanti sono stati molto veloci e da subito, già da febbraio, hanno fatto evolvere le proprie tecniche per sfruttare le "debolezze" della situazione che si andava creando.

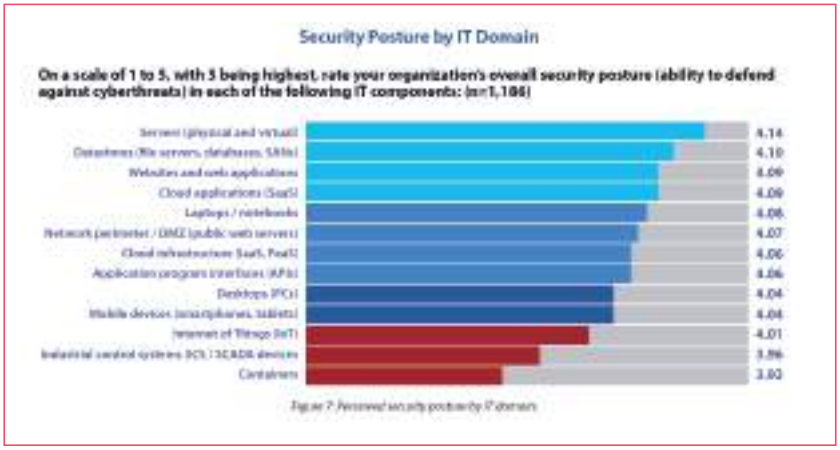



Come hanno dovuto reagire i team di IT security per adattarsi al nuovo contesto? Gli sforzi sono andati chiaramente in due direzioni principali. Da un lato supportare tutte le iniziative di smart working, assicurando la sicurezza di device, accessi e comunicazioni, in un contesto in cui il traffico e l'utilizzo di PC era profondamente mutato. Dall'altro lato, ma contemporaneamente, cercare di fermare o anticipare gli hacker, che si stavano muovendo verso una diversa superfice d'attacco e un "fattore umano" indebolito dalla distanza dall'ufficio e dal fatto di essere emozionalmente meno stabile. Quindi le priorità per la security sono diventate:

- Protezione della continuità delle attività

online (collaborazione, e-commerce ecc.) che durante il periodo sono diventate particolarmente critiche per l'operatività delle aziende.

- Sicurezza degli endpoint utilizzati da un gran numero di persone dalla propria abitazione (si stima ad esempio che negli USA si è passati da un 3% di aziende nel 2019 che aveva oltre i tre quarti della forza da lavoro in remoto, a una quota attuale del 75% delle aziende che lo ha permesso).
  E' dimostrato che gli hacker hanno cercato di arrivare alle reti enterprise sfruttando i punti deboli come quelli rappresentati da PC e reti WiFi domestiche.
- Messa in sicurezza di ambienti di collaborazione e meeting online, abbandono di strumenti "consumer" e investimenti in cloud security, per prevenire che questi diventassero il target degli attaccanti, come del resto è avvenuto (basta ricordare i fatti per la piattaforma Zoom), con sottrazione di credenziali e accesso a dati confidenziali condivisi dagli utenti.
- Sicurezza delle comunicazioni e degli accessi: si è osservato fin dall'inizio del lockdown un incremento molto elevato di collegamenti VPN, che ha però poi comportato complessità, trattandosi di ambienti che hanno proprie vulnerabilità, e in particolar modo, possono diventare essi stessi un punto critico da proteggere da attacchi esterni, assumendo di fatto un ruolo molto importante per la continuità del business. Sono state così individuate soluzioni per proteggere le VPN, come sistemi anti-DDoS o VPN tunneling con traffico direttamente al cloud, con servizi come cloud firewall o altro per ulteriore ispezione di sicurezza.
- Formazione delle persone e policy per il lavoro da remoto.
  L'emergenza ha costretto lo staff di security a focalizzarsi sul supporto alle persone alle prese con una situazione molto complessa, che dovevano collegarsi in gran numero da remoto alla rete aziendale, utilizzando device come PC e smartphone non sempre gestiti dall'azienda.
  La consapevolezza di un maggior numero di attacchi come phishing e malware rivolto alle persone, elemento più debole, ha costretto a intervenire con attività di formazione o policy e servizi di help desk per aiutare le persone a evitare di cadere nei tranelli degli hacker, o essere in grado di intervenire in caso di eventuali malfunzionamenti.




### Le scelte del team di security: oggi focus sulla gestione della crisi, domani nuove misure

Cosa ha insegnato questa esperienza? Innanzi tutto, va osservato che alcuni erano già pronti – con un'architettura moderna, un mix di soluzioni fisiche e virtuali, in alcuni casi una soluzione di smart working già testata – e di conseguenza, hanno potuto migrare con continuità e senza errori alla nuova configurazione.

L'utilizzo di soluzioni cloud-based si è dimostrato vincente in questo passaggio proprio per la rapidità e la scalabilità messa a disposizione: evitare perdite di tempo e ritardi ha permesso quindi in definitiva, a chi aveva un'infrastruttura IT moderna e resiliente, di evitare perdite del business, lungaggini sulla supply chain, annullare il rischio di perdere clienti e fatturato.

Dove invece le infrastrutture da adeguare erano in casa (firewall, VPN, VDI, sistemi di amministrazione multivendor, ecc.) lo staff IT si è trovato a dover risolvere tutta una serie di difficoltà, a identificare soluzioni alternative, a ridisegnare i collegamenti, a dover acquistare nuovi sistemi, ampliare la banda disponibile e quant'altro.

Ora che l'adeguamento è stato fatto, molte aziende prevedono di mantenere il nuovo status quo per tutto il resto dell'anno, ma cosa servirà adesso dal punto di vista della cybersecurity?

### L'emergenza Covid19 sarà l'occasione per modernizzare l'approccio alla sicurezza?

Purtroppo possiamo aspettarci che nei prossimi mesi, nei settori più colpiti dalla pandemia, ci saranno tagli ai budget IT e quindi anche una riduzione di risorse per investimenti in cybersecurity.

Già adesso, l'attenzione dei responsabili per la cybersecurity si è probabilmente focalizzata sulla gestione dell'emergenza, con il conseguente abbandono di progetti che erano stati pianificati e che sono stati spostati più avanti nel tempo. Ma qual è oggi la percezione

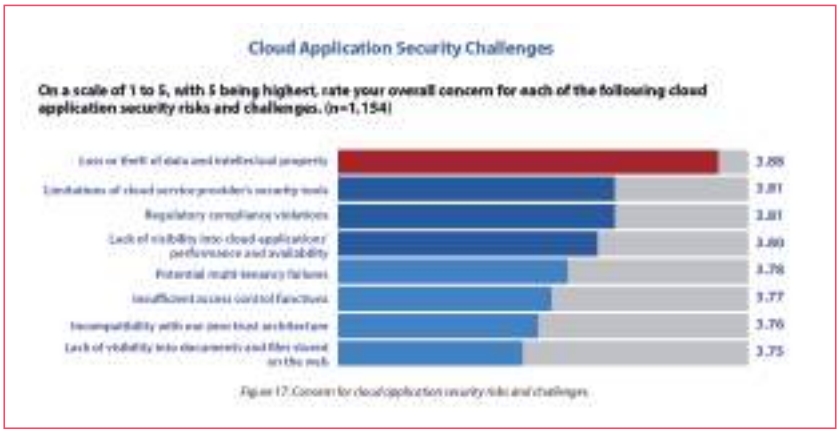
sul livello di sicurezza dei diversi ambienti e come questo cambierà dopo il Covid-19?

Fino a poco tempo fa, device come PC unmanaged e smartphone personali non si potevano certo dire del tutto al sicuro … la sicurezza ha sempre avuto particolare attenzione per la protezione delle risorse chiave centrali nelle organizzazioni.

Come mostrano i risultati del Cyberthreat Defense Report (CDR) di CyberEdge, un'indagine rivolta quest'anno a 1.200 professionisti e decision maker dell'IT security in aziende con oltre 500 addetti, in 17 diversi paesi e per 19 settori (pubblicata a marzo 2020 in modo da riportare anche i primi effetti della pandemia Covid19 sulle scelte di cybersecurity), si ha l'impressione che via via che ci si allontana dal datacenter, dai database, i file server e le applicazioni core, la sicurezza diventa una variabile sempre meno importante.

### Per gli ambienti cloud la percezione di sicurezza potrebbe essere mal riposta …

Un ambito su cui bisognerà sempre più indagare è quello della sicurezza nell'uso del cloud, perché per quanto in molti si dicano confidenti, in realtà questa potrebbe ben presto dimostrarsi una percezione errata.
Secondo quanto riporta il Cyberthreat Defense Report (CDR) di CyberEdge, i responsabili della cybersecurity sono oggi piuttosto preoccupati per tutta una serie di rischi connessi all'uso del cloud, tra cui ai primi posti appaiono



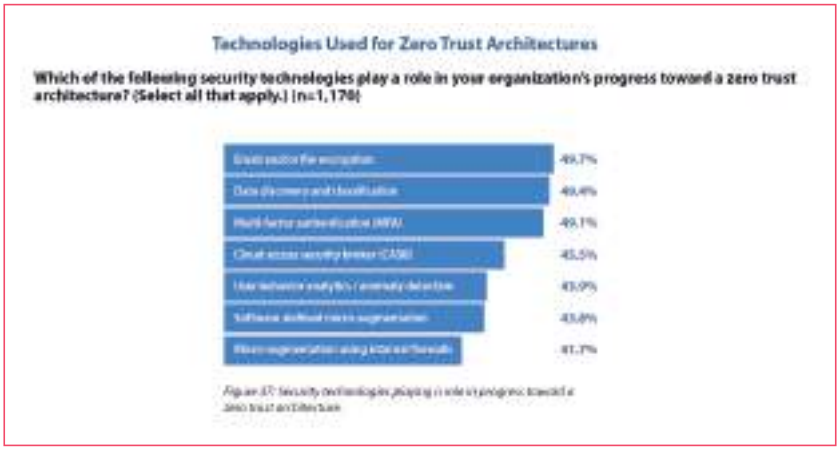

- Perdita o furto di dati e intellectual property
- Possibilità che le misure di sicurezza del cloud provider siano limitate
- Violazioni con conseguenze di non-compliance alle norme
- Scarsa visibilità sulle performance e la disponibilità delle applicazioni in cloud.

### Una risposta verrà dall'approccio Zero Trust?

In conclusione, quello che osserveremo nel prossimo futuro, a causa di una completa de-perimetrizzazione degli ambienti elaborativi, e della necessità di ripensare la difesa per essere in grado di proteggere asset, dati e collegamenti che si ridefiniscono in modo flessibile di giorno in giorno, sarà un sempre maggiore interesse per il modello Zero Trust.

Un'architettura di questo tipo per la cybersecurity si basa (come spiegato in un precedente articolo), sul concetto che qualsiasi persona o processo aziendale, indipendentemente da dove si collega (sulla rete interna o su internet), deve autenticarsi e stabilire un livello adeguato di "trust" per poter accedere alle risorse corporate.

La sfida per il disegno di un'architettura zero trust è quella di implementare sistemi di autenticazione molto efficaci, realizzare una micro-segmentazione delle reti e dei sistemi (in modo che se un attaccante è in possesso di credenziali pregiate, non può comunque muoversi attraverso più segmenti della rete), rendere in definitiva molto difficile l'accesso a dati e applicazioni se non si posseggono i corretti diritti.
La survey citata ha indagato quali sono le tecnologie che chi sta progredendo verso un'architettura di questo tipo ha già in essere, e tra queste appaiono: email e file encryption (49,7%), data discovery e classification (49,4%), multi-factor authentication (MFA, 49.1%), CASBs (45,5%), user behavior analytics / anomaly detection (43,9%), software-defined micro-segmentation (43,8%), micro-segmentation con firewall interno (41,7%).




Vedremo nei prossimi mesi, parlando di questi temi nella nostra Community, se queste scelte e questo trend sarà confermato anche per quanto riguarda gli indirizzi scelti dalle aziende italiane.

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

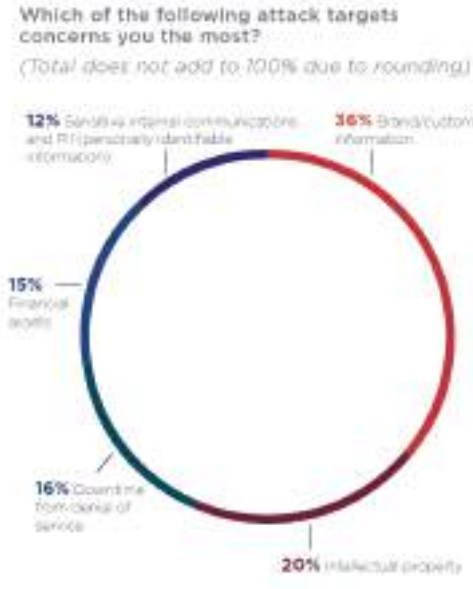
### L'AI può essere un valido aiuto per la sicurezza

**Elena Vaciago**
**Associate Research Manager, The Innovation Group**

Quello di un Security Officer non è certo un compito facile di questi tempi: si potrebbe sintetizzare in breve, "allocare risorse scarse nella risposta a minacce cyber crescenti". In nessuna altra parte del business tutto cambia alla velocità con cui questo avviene nella cybersecurity, e i dati sugli incidenti dimostrano che nessuno può dirsi totalmente al sicuro da un ransomware, da un attacco di phishing o altro.

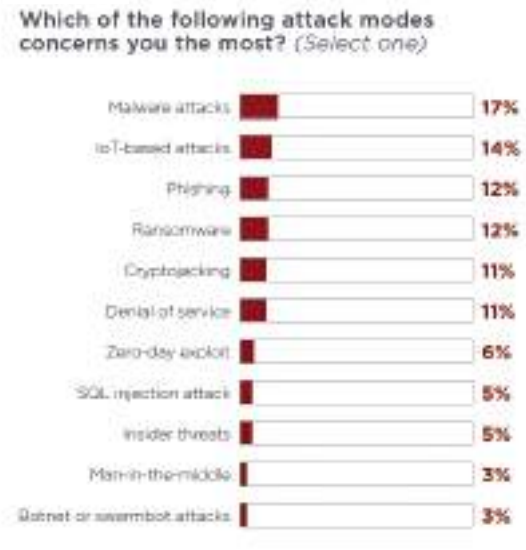
Lo scenario delle minacce cyber è oggi molto dinamico, e non sembra che le cose miglioreranno nei prossimi anni. Una recente ricerca di Forbes Insights ("Making Tough Choices. How CISOs Manage Escalating Threats And Limited Resources"), con interviste a 200 CISO, ha messo in evidenza che 8 manager della security su 10 si aspettano un escalation dei rischi cyber nel prossimo futuro: un 21% inoltre afferma che le capacità degli attaccanti (siano essi singoli hacker che agiscono per proprio profitto, o gruppi collegati a operazioni state-sponsored, o ancora singoli dipendenti poco accorti o poco onesti) cresceranno rapidamente nel prossimo periodo, molto di più che non le capacità dell'azienda di tenere il passo nella difesa e nella risposta.

Sembra quindi che in un gran numero di situazioni, chi guida la Cybersecurity sia alla ricerca di nuovi approcci, avendo verificato con mano che quelli attuali sono poco efficaci. Lo sforzo maggiore è diretto alla protezione di ambiti prioritari per la stessa sostenibilità del business. La salvaguardia dei dati dei clienti e della reputazione del brand sale quindi al primo posto (è scelta da un 36% dei rispondenti), seguita, da un 20% di rispondenti, dalla proprietà intellettuale.




Fonte: 2019 FORBES INSIGHTS, "Making Tough Choices. How CISOs Manage Escalating Threats and Limited Resources"

Presi dalla difficoltà quotidiana di combattere le minacce più comuni e già note, i CISO non sembrano quindi in grado di anticipare o prepararsi per le evoluzioni delle minacce a più lungo termine.




Fonte: 2019 FORBES INSIGHTS, "Making Tough Choices. How CISOs Manage Escalating Threats And Limited Resources"

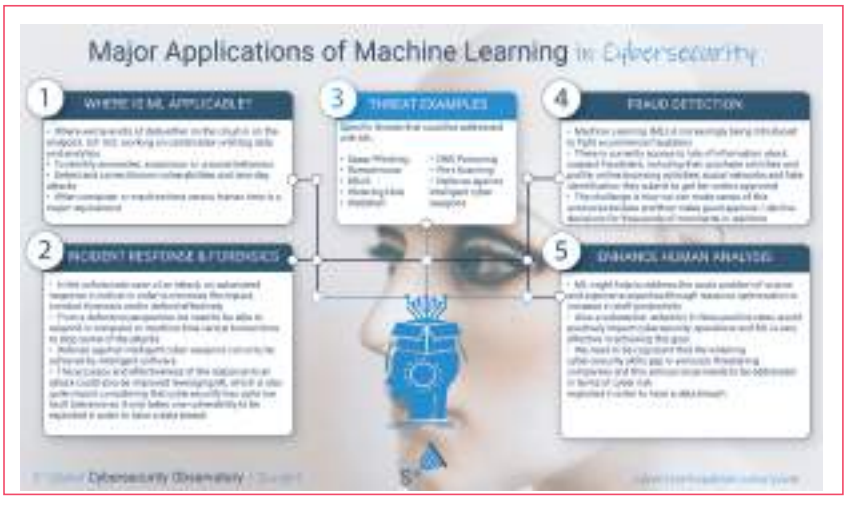
Bisogna tener presente che i trend con cui appaiono le nuove minacce o i nuovi schemi di attacco sono legati strettamente alla scoperta di nuove vulnerabilità, e su questo fronte, un trend che già oggi preoccupa molto (il secondo posto nella figura successiva) è quello degli attacchi originati da botnet IoT, milioni di device infettati (router, webcam, device medicali, wearable, sistemi industriali, ecc.) che sono utilizzati dagli attaccanti per sferrare attacchi di scala molto superiore al passato.

Quali sono gli ostacoli che i Security Officer incontrano nella battaglia quotidiana contro tutti questi rischi? Al primo posto viene indicato il budget inadeguato, seguito dalla mancanza di sufficiente supporto da parte del Top management, dalla mancata cooperazione con altre aree del business, dal poco tempo a disposizione per la formazione delle proprie persone, fino alla mancanza di risorse con skill adeguati nel far fronte ai temi della cybersecurity.

Da questo punto di vista, le statistiche parlano chiaro: la richiesta di figure con skill sulla cybersecurity è in continuo aumento e non trova risposta nel mercato del lavoro. Entro il 2021, potrebbero esserci fino a 3,5 milioni di job vacanti sui temi della cybersecurity, e il personale attivo in questo ambito lavora oggi già al massimo delle proprie capacità, fino a 52 ore alla settimana senza mai fermarsi. Una situazione non proprio ideale, se si considera che gli attaccanti scelgono weekend e festività come periodi ideali per portare a termine i propri attacchi …

Vista la situazione, nel report di Forbes si ipotizza che un aiuto concreto possa arrivare dall'implementazione di algoritmi AI basati su tecniche di Machine Learning per aiutare lo staff deputato alla cybersecurity ad essere più efficiente nel proprio lavoro: le tecniche di ML permettono infatti di dotare di ulteriori capacità lo stack tecnologico per la difesa e la risposta cyber, e di apprendere nel tempo a:

- riconoscere un attacco avanzato che è sfuggito alle normali procedure di difesa
- identificare comportamenti anomali analizzando il traffico di rete (ad esempio, attività di cryptomining, di remote file execution, tentativi di attacco brute force)
- analizzare le configurazioni, ricercare vulnerabilità nel software
- offrire soluzioni anti frode, tramite l'individuazione di tentativi anomali di accesso ai sistemi
- fornire un'identificazione sicura (tramite voice/video recognition)
- categorizzare un attacco sulla base del livello di rischio corrispondente
- rispondere più efficacemente in caso di incidente in corso.




## Come dovrebbe cambiare il ruolo della Security in azienda?

Nel tempo, dovrebbe essere sempre più chiaro che una buona Security Posture, una strategia efficace di protezione e risposta agli eventi cyber, rappresenta un valore importante per l'azienda nel suo complesso: questo sarà sempre più vero con l'accresciuto ruolo della tecnologia per il business. In particolare, quello che dovremo aspettarci per il futuro è un maggiore orientamento alla detection e alla

risposta, piuttosto che non alla prevenzione di incidenti di cybersecurity. Sempre di più infatti ci si renderà conto che attacchi, incidenti e data breach non possono più essere evitati: quindi una reazione veloce diventerà sempre più centrale nelle strategie delle aziende. E' quanto emerge anche dalla ricerca: il budget andrà sempre più nella direzione di incrementare le capacità di risposta.


Con questo scenario ben in mente, è chiaro che le risorse andranno sempre di più dirette a

- gestire le priorità sul fronte della Protezione (es. quali dataset sono più critici, ecc.)
- incrementare le capacità di Detection
- investire sulla Response, preparandosi a rispondere bene e velocemente.

Anche da questo punto di vista, l'AI sarà fondamentale. Se pensiamo con quale velocità riesce a diffondersi un malware come NotPetya, è evidente che nessun "umano" è in grado di tenere il passo: solo una tecnologia come AI e ML può individuare la minaccia e bloccarla immediatamente, prima che l'attacco si diffonda con successo.

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

### Gli attacchi ransomware evolvono e chiedono milioni

**Elena Vaciago**
**Associate Research Manager, The Innovation Group**

Gli hacker hanno di nuovo preso di mira una realtà in prima linea nella lotta all'epidemia. Fresenius, il più importante istituto ospedaliero privato in Europa, tra i maggiori fornitori di prodotti e servizi di dialisi molto richiesti per la pandemia Covid19, è stata colpita da un attacco ransomware che ha messo in crisi alcune delle sue attività.


Con 300mila dipendenti in 100 paesi nel mondo, la società vanta un 40% del market share dei servizi di dialisi negli USA, e per questo motivo, l'evento potrebbe avere conseguenze rilevanti durante la pandemia da Covid-19.

Secondo quanto è stato reso noto sul sito KrebsOnSecurity, un dipendente, che ha chiesto di rimanere anonimo, ha raccontato come nella sua sede siano stati isolati dei PC e come l'attacco cyber abbia colpito tutte le attività nel mondo. All'origine dell'attacco sarebbe stato individuato il ransomware Snake, un ceppo di malware relativamente nuovo, che colpisce soprattutto grandi organizzazioni prendendo in ostaggio i loro sistemi in attesa del pagamento di un riscatto in bitcoin.

Secondo quanto confermato dalla stessa società, preso atto dell'incidente sono state avviate tutte le misure per contenerlo, e sono state informate le autorità.

Non è il primo attacco che riguarda organizzazioni sanitarie dall'inizio dell'emergenza Covid-19: già ad aprile l'Interpol aveva avvisato della crescita dei tentativi di attacco contro organizzazioni e infrastrutture in prima linea contro l'avanzare dei contagi. Come visto in passato, gli hacker non si sono fermati neanche nel corso di un'emergenza sanitaria globale.

Gli attacchi di tipo Ransomware (che prevedono la richiesta di un riscatto in cambio della restituzione di dati che sono stati crittografati dal malware) hanno visto negli ultimi anni una crescita impressionante in tutto il mondo: se nel 2016 era stato stimato che ogni 40 secondi un'azienda cadeva vittima di un attacco ransomware[1], questo tempo si è oggi ristretto a 14 secondi, ed

è previsto arrivare a 11 secondi entro il 2021[2]. Questa statistica tra l'altro non considera gli attacchi rivolti a singoli individui, ma solo alle aziende.

## Come stanno evolvendo gli attacchi Ransomware

A partire dal 2019, si è osservata una mutazione delle tecniche scelte per gli attacchi Ransomware, che sono passati da un modello basato sull'invio massivo di mail di phishing, a forme di attacco mirate a specifiche organizzazioni. Partendo da un'infezione iniziale, a cui segue una fase di studio dell'azienda (che può durare anche 6 mesi), le attività malevole sono volte a raggiungere gli asset più sensibili. Gli attaccanti si muovono lateralmente nei sistemi interni, alla ricerca di dati da trafugare o di sistemi critici da bloccare (ad esempio la produzione nel caso di aziende manifatturiere), quindi a creare il danno maggiore. In alcuni casi, questo porta gli attaccanti a chiedere riscatti da milioni di euro.

A metà febbraio Manheim Auctions, la più grande casa d'aste di auto all'ingrosso nel mondo, con 145 filiali tra Nord America, Europa, Asia e Australia, è stata colpita da un attacco ransomware con una richiesta di riscatto per 30 milioni di dollari, una delle più alte finora registrate. Principale target dell'attacco, come ha comunicato il 14 febbraio la stessa Manheim Auctions, è stata la filiale Australiana, che ha dovuto rinunciare a tutti i sistemi informativi in seguito al ransomware: anche le vendite online sono state azzerate.

## Un caso celebre, l'attacco Ransomware alla Norsk Hydro

In seguito all'incidente originato da un attacco ransomware, alla Norsk Hydro (uno dei principali produttori globali di alluminio), nel marzo 2019 in molte delle 170 fabbriche le linee produttive sono state fermate e si è dovuti passare da attività automatizzate a manuali.

Ad essere colpita è stata soprattutto la divisione dell'alluminio estruso, sia in Europa, sia negli USA: in ultima analisi, sono state colpite le attività di 35mila dipendenti in 40 paesi, con il blocco di migliaia di PC e server.

Sulla base delle investigazioni, si è scoperto che tutto era cominciato 3 mesi prima, quando un dipendente aveva aperto una mail infetta proveniente (in teoria) da un cliente noto. In questo modo gli attaccanti hanno infettato i primi sistemi, con il ransomware LockerGoga, e da lì si sono mossi nella rete. Per rispondere all'attacco, l'IT ha dovuto prontamente spegnere la rete aziendale e i server per evitare il propagarsi del malware.

Come riporta la figura, il messaggio lasciato dagli hacker non faceva presagire niente di buono … in ogni modo, il management di Norsk Hydro ha deciso che non avrebbe pagato il riscatto.

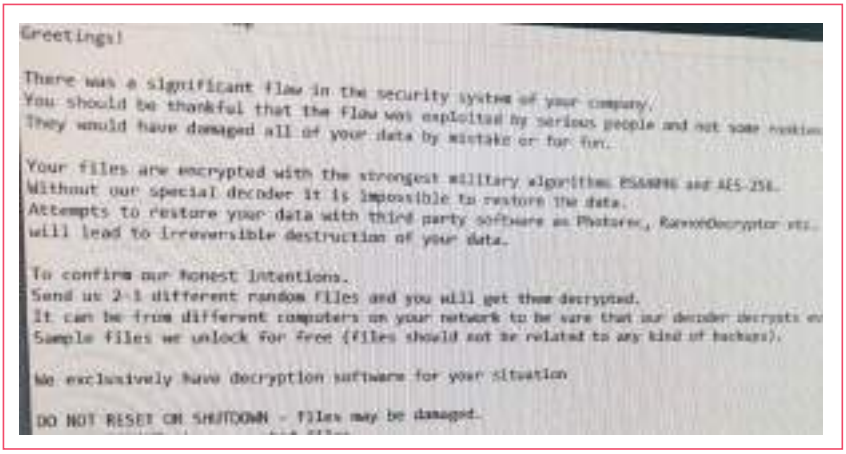
Il costo del recovery è però lievitato rapidamente: nel primo trimestre, l'impatto economico è stato valutato intorno ai 40 milioni di dollari, e successivamente, nel trimestre successivo, altri 35 milioni di dollari, quindi quasi 75 milioni di dollari in soli 6 mesi.

L'impatto maggiore come detto è stato subito dalla divisione Extruded Solutions. Il costo riflette principalmente la perdita di fatturato, dovuta al blocco della produzione, oltre che i costi per il recovery dell'IT e per i servizi di sicurezza acquistati nel periodo.

Dopo una settimana dall'attacco ransomware, la maggior parte dei sistemi e degli impianti produttivi erano tornati all'attività normale (anche se in alcuni casi ricorrendo ad attività manuali), solo nella divisione Extruded Solutions l'operatività è stata ridotta al 70, 80% per un periodo più lungo.

L'IT si è prodigata per riportare in operatività i sistemi, inizialmente isolando il malware (in modo da prevenirne la diffusione), poi recuperando i dati dai sistemi di back-up. La società aveva anche una cyber insurance con AIG, per recuperare almeno in parte le perdite subite.

Il costo registrato da Norsk Hydro avvicina questo caso a quello di altri produttori, come la società di trasporti danese Maersk (una perdita tra i 200 e i 300 milioni di dollari in seguito al ransomware NotPetya) o il produttore di beni farmaceutici UK Reckitt Benckiser, che sempre per NotPetya ha perso 129 milioni di dollari.




## Quali sono le fasi di un attacco Ransomware avanzato?

Gli attacchi di questo tipo stanno diventando sempre più sofisticati. Malware già esistente viene riutilizzato in modalità nuove, o viene combinato con nuovi malware in grado di sfruttare vulnerabilità non note. Le tecniche degli attaccanti sono in continua trasformazione, per ridurre le possibilità di essere riconosciuti e fermati, e anche per massimizzare i ritorni.

Se la maggior parte degli attacchi si

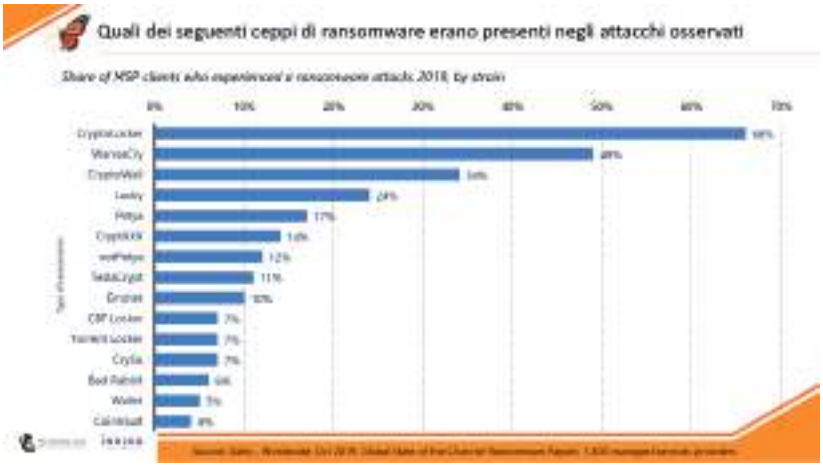
rivolge a regioni o a demografie, in alcuni casi gli attacchi (detti Advanced Ransomware Threats, ART), sono molto mirati e puntano ad ottenere il massimo profitto in operazioni che coinvolgono un target molto selezionato. Un ART si sviluppa in fasi successive (Cyber Kill Chain):

Fonte: Lockheed Martin, The Cyber Kill Chain Framework

- Studio del target: l'attaccante comincia a raccogliere informazioni sull'organizzazione, le mail dei dipendenti, o qualsiasi altra informazione sui dipendenti (ad esempio, disponibile sui social media) per risalire al loro ruolo e alle loro attività nell'organizzazione. Nel "dossier" creato intorno all'azienda target, vengono riportati anche i collegamenti con partner, fornitori, consulenti e terze parti, perché anche questi dettagli saranno utilissimi per sferrare l'attacco.
- Penetrazione: in questa fase, un attacco di spear phishing o whaling viene rivolto a singoli target dell'azienda. Grazie alle informazioni ottenute nella fase precedente di social engineering, la mail sembra credibile a chi la riceve, aumentando quindi molto le probabilità di far scaricare un primo malware che andrà a installarsi sul PC del malcapitato.
- Fortificazione: l'attaccante nasconde le proprie tracce e instaura una serie di meccanismi per assicurarsi l'accesso per il futuro al device, oltre che per diffondere nuove infezioni. In alcuni casi un attaccante può anche mettere in sicurezza il device, in modo che non possa cadere in mano a un altro attaccante, che potrebbe creare un disturbo per le successive attività.
- Infiltrazione: in questa fase, gli hacker puntano ad acquisire le credenziali di altri utenti, in modo da poter accedere ad asset di maggiore valore, tra i quali anche i backup e i sistemi di archiviazione, che sempre più spesso gli attaccanti prendono di mira in modo che il ransomware sia poi ancora più efficace e distruttivo.
  Di nuovo, la conoscenza pregressa dell'organizzazione aiuta l'hacker a mappare processi e ruoli delle persone, cercando di bypassare controlli tecnici e capire ancora meglio le procedure di sicurezza e di incident response presenti in azienda. In questa fase cominciano anche ad essere esfiltrati dati che possono essere venduti (monetizzati) oppure essere riutilizzati per attività successive. Tra i dati più spesso colpiti, le credenziali degli utenti.
- Saccheggio: gli attaccanti modificano quindi i processi di backup, in modo sempre nascosto agli utenti. Ad esempio, cambiano le configurazioni dei dati da archiviare, cosicché il processo di backup sembra proseguire, ma in realtà avviene con dati diversi da quelli che dovrebbero essere salvati. Oppure possono modificare il software, introducendo degli errori nelle routine in modo che l'eventuale restore dei dati diventi impossibile da portare a termine. O ancora, potrebbero modificare la documentazione, cosicchè il team deputato al restore potrebbe incorrere in problemi nell'individuare i file corretti per il recupero dei dati.


- Riscatto: in questa fase, gli attaccanti lanciano il ransomware contro una serie di data store che contengono le informazioni target. Anche la data dell'avvio dell'attacco

ransomware è scelta in modo che l'impatto sia il più disastroso possibile: alcuni esempi sono, appena prima di un annuncio importante, durante una fusione o un'acquisizione di azienda, vicino a un audit. Si possono usare varie tipologie di ransomware (le famiglie sono numerose, come riportato nel grafico successivo), l'importante è che l'unico ad avere in mano le chiavi per decriptare i file è l'attaccante stesso.




Gli attaccanti più evoluti, una volta crittografati i file e fatte scomparire le chiavi, riescono anche ad eliminare ogni traccia del proprio passaggio nei sistemi dell'azienda colpita. In alcuni casi, si mantengono però delle possibilità di accesso, per poter tornare una seconda volta: ed è proprio quello che si osserva in questi giorni. Grandi aziende che sono nuovamente colpite dal attacchi ransomware nel giro di qualche mese.

Pitney Bowes, colosso globale attivo nelle spedizioni postali, con oltre 11mila dipendenti e un fatturato 2019 pari a 3,2 miliardi di dollari, ha subito un secondo attacco ransomware nel giro di soli 7 mesi.


L'incidente è venuto alla luce a inizio maggio, dopo che la banda di ransomware Maze aveva pubblicato un post sul blog in cui affermava di aver violato e crittografato la rete dell'azienda.

Nell'ottobre 2019, Pitney Bowes aveva subito un primo attacco, con il ransomware Ryuk. Entrambe le cyber gang Ryuk e Maze sono varietà di ransomware "gestite dall'uomo" (Human Operated Ransomware). Queste tipologie di infezioni si verificano dopo che gli hacker hanno violato la rete di un'azienda e assunto il controllo manuale del malware, con lo scopo di espandere l'accesso al maggior numero possibile di sistemi interni. Il gruppo Maze, a differenza di quello che usa Ryuk, si è specializzato nei leak di dati: è molto attivo e probabilmente responsabile di molti casi recenti, Chubb, Cognizant, Bouygues Construction, Southwire, la città di Pensacola. Un portavoce di Pitney Bowes ha dichiarato che l'intrusione è stata individuata subito e non ci sarebbero sistemi crittografati in aggiunta al leak di informazioni.

Il significato di tutto questo è che dopo un incidente così grave, bisogna assolutamente "sanificare" tutti gli ambienti. Il danno procurato dagli Advanced Ransomware Threat spesso è molto elevato, impedisce la stessa ripresa delle attività per molti giorni, e di conseguenza gli attaccanti arrivano a chiedere riscatti da milioni di dollari, commisurati a quanto l'azienda dovrà spendere per riprendere piena operatività.

Poiché solo poche, grandi organizzazioni sono in grado di rimettersi in piedi da sole, affrontare tutti i costi ed evitare di pagare il riscatto, è naturale che molti di questi incidenti rimangono nascosti da chi li ha subiti, e ha dovuto pagare per riottenere i propri dati. Bisogna però essere consapevoli che pagare il riscatto equivale a "finanziare" un'industria criminale che utilizzerà questi fondi per proseguire le proprie attività, colpire altre aziende (o la stessa che ha già pagato), rendere i propri attacchi sempre più evoluti, efficaci, distruttivi. Fino a colpire infrastrutture critiche, come un ospedale, un'azienda energetica, una rete nazionale.

[1] Security Bulletin by Kaspersky Lab, December 2016

[2] Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, Cybersecurity Ventures, Oct. 21, 2019

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Zero Trust, cresce l'adozione del modello

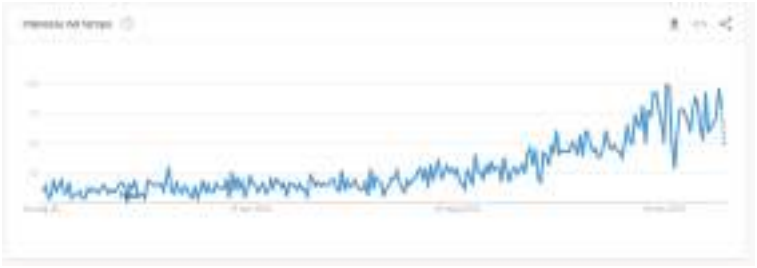
**Elena Vaciago**
**Associate Research Manager, The Innovation Group**

Il modello Zero Trust (Zero Trust Network, Zero Trust Architecture) è stato ideato nel 2010 da John Kindervag, allora Principal Analyst presso Forrester Research, sulla base della considerazione che non è più possibile permettere il "Trust" digitale finora prevalente nelle aziende, ossia, la fiducia per cui qualsiasi attività svolta "entro il perimetro" è sicura e quindi permessa.

Negli ultimi anni è infatti cambiato tutto: una volta, bastava essere in sede e utilizzare un sistema collegato alla rete, automaticamente si aveva il permesso di accedere alle applicazioni. Oggi ognuno lavora da dove vuole, usa device diversi, si collega da reti diverse: tutto il paradigma dell'IT è cambiato.

Il modello Zero Trust (un tema che sta registrando un interesse sempre più importante, come dimostra anche la figura successiva) punta a ripensare controlli e misure di sicurezza, ma a distanza di 10 anni dalla sua introduzione, solo oggi comincia ad essere applicato in un numero ancora basso di organizzazioni, nonostante le architetture tradizionali di security si siano già da tempo dimostrate inadeguate nel far fronte ad attacchi sempre più sofisticati.

Vediamo quali sono le cause che limitano l'impiego più diffuso di questa strategia, andando per passi successivi.



L'interesse per questa visione è oggi sicuramente molto elevato, come mostra l'andamento del Google Trend.

### Innanzi tutto, cosa significa Zero Trust?

Il Zero Trust è un concetto di sicurezza secondo il quale tutto quello che avviene negli ambienti utilizzati dall'azienda deve essere verificato: un'attività è permessa solo se si può escludere che sia il risultato di un'intrusione malevola nei sistemi.

La strategia con questo modello di sicurezza è speculare rispetto al passato, perché parte dal presupposto che non bisogna fidarsi di nessuno.

Quindi, non permette alcun accesso alla rete se non si è verificato chi è; se non si sa tutto del device con cui ci si collega; se non si dispone dell'autorizzazione ad accedere a particolari sistemi, dati, applicazioni.

## Da dove nasce Zero Trust? Guardiamo ad alcune statistiche …

Secondo il 2019 Data Breach Study di Ponemon Institute, il costo medio di un data breach è oggi di 3,9 milioni di dollari (era di 3,6 milioni di dollari 2 anni fa), e la dimensione di un data breach è in media di 25.575 record (rispetto ai 24.000 record di 2 anni fa). Inoltre, il tempo che intercorre tra il momento in cui avviene l'incidente e il contenimento dello stesso, è cresciuto del 4,9% tra il 2018 e il 2019: oggi si attesta su 279 giorni, di cui 206 per la fase iniziale di individuazione del breach (gli attaccanti riescono ad essere presenti per molto tempo inosservati nei sistemi e sfruttano questo periodo per conoscere meglio il proprio target e quindi colpirlo nel modo più dannoso) e 73 giorni per la risoluzione dell'incidente.

Oggi è noto il fatto che prima si riesce a individuare e quindi fermare un attacco, minore sarà il costo finale da sostenere. Si tratta di un costo che le organizzazioni devono affrontare su un periodo di tempo sempre maggiore: secondo la ricerca, il 67% il primo anno, il 22% nel secondo anno e l'11% negli anni successivi.

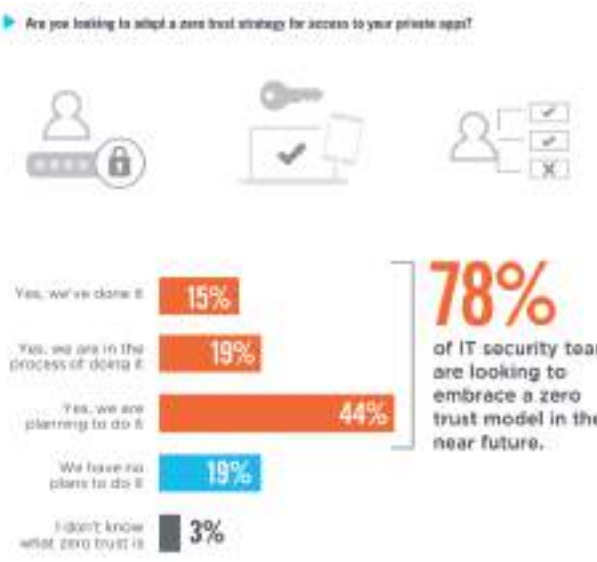

Fonte: "The longtail costs of a data breach", 2019 Data Breach Study, di Ponemon Institute e IBM Security

È stato misurato anche che il settore che deve affrontare il costo maggiore per record perso, in un eventuale data breach, è il mondo sanitario. Secondo la rilevazione annuale di Verizon (2019 Data Breach Investigations Report), basata quest'anno sull'analisi di 41.686 incidenti di sicurezza, di cui 2.013 con data breach conclamato, i settori che registrano un maggior numero di data breach sono stati il settore pubblico, sanitario, finanziario. Inoltre, è cresciuto negli ultimi anni, a causa anche degli attacchi ransomware, il numero di PMI che subiscono queste frodi, oggi rappresentano il 43% dei data breach. Anche secondo Ponemon, analizzando come cambia il costo di un data breach al variare della dimensione delle organizzazioni, le più grandi arrivano a spendere in media 5,11 milioni di dollari (un costo medio di 204 dollari per dipendente), mentre le media (tra i 500 e i 1.000 dipendenti) hanno un costo medio di 2,65 milioni di dollari, quindi un costo per dipendente molto più alto (3.533 dollari a dipendente). Questo semplice calcolo dimostra quanto una piccola azienda rischi molto di più, rispetto a una grande, di non essere in grado di riprendersi economicamente dopo un attacco cyber di impatto rilevante.


Fonte: Verizon 2019 Data Breach Investigations Report

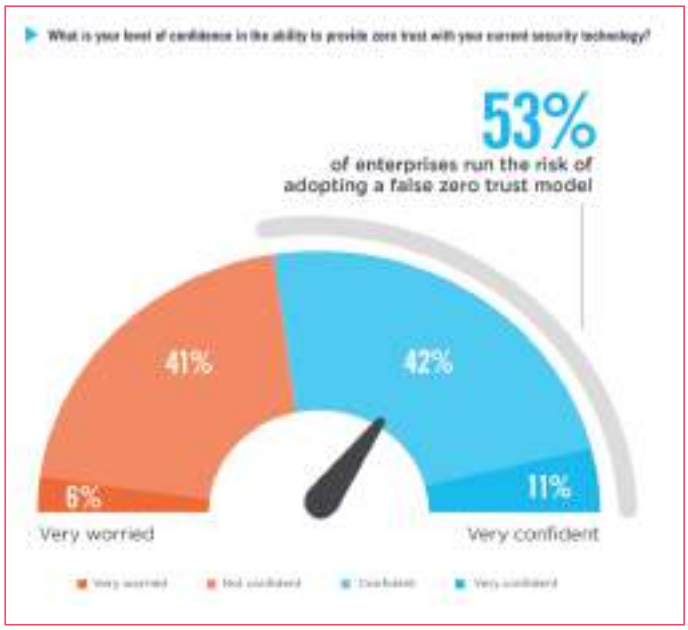
Quindi nonostante in tutto il mondo si spenda sempre di più in sicurezza (a livello globale gli investimenti sono previsti arrivati a 42 miliardi di dollari a fine 2020), i data breach sono più diffusi, le perdite sempre più elevate, il numero di record persi sempre maggiore: è evidente guardano questi numeri che l'approccio alla security che stiamo tutti seguendo non risulta molto efficace.

## Come procede l'adozione del modello Zero Trust?




Quanto sono effettivamente interessati a questo modello i Security Manager? secondo una survey pubblicata lo scorso febbraio da Cybersecurity

Insiders ("Zero Trust Progress Report"), parlando di accesso alle app aziendali, circa i 2 terzi degli intervistati (professionisti di cybersecurity) ha detto di essere intenzionato ad adottare il modello zero trust per verificare le identità delle persone: solo un 15% però lo sta facendo già oggi, gli altri sono in corso di adottarlo o lo pianificano.




Il problema quindi è come passare dalle buone intenzioni all'applicazione concreta: gli aspetti di implementazione di un modello di questo tipo sono ancora molto critici. Sempre secondo la stessa survey, le aziende si dividono in 2 tra chi è confidente di poterlo fare con le attuali tecnologie e chi no.

Il problema sta dalla parte di chi è più tranquillo. Un'eccessiva confidenza nelle proprie capacità e nella disponibilità pregressa di tecnologie "abilitanti" può portare in realtà all'insuccesso del progetto. Il vero problema nell'adozione di Zero Trust, come sarà spiegato in seguito, è che non si può ricondurre unicamente alla tecnologia: quello che serve veramente è un cambio di mentalità e una revisione estesa dei processi di sicurezza da adottare in azienda.

## Come fermare i data breach? È possibile farlo con Zero Trust?

Come detto in precedenza, il punto di partenza del modello Zero Trust è tener presente che la difesa al perimetro della rete non è più sufficiente: la dimostrazione di questo viene dal fatto che alcuni dei più gravi data breach registrati negli ultimi anni sono stati svolti dagli hacker aggirando la difesa dei firewall aziendali. Una volta entrati nella rete, gli hacker sono riusciti a muoversi negli ambienti interni senza incontrare alcuna resistenza. Il problema è che oggi moltissime "porte" rimangono aperte, il muro difensivo è diventato un colabrodo: se il successo di Internet è legato al fatto che ciascuno può condividere con chiunque altro qualsiasi informazione in qualsiasi momento, il risultato è che nessuno è più al sicuro.

L'altro problema è che molti dei dati aziendali sono già oggi "fuori dalle mura": il datacenter tradizionale è stato sostituito da una moltitudine di repository in cloud, anzi, in multi-cloud, e questi a loro volta sono condivisi sia da interni, sia da esterni all'organizzazione, con applicazioni e device che vi accedono da ogni parte del mondo.

## La tecnologia e l'architettura di una strategia Zero Trust

Il modello Zero Trust si basa su varie tecnologie e metodologie per riportare in sicurezza gli ambienti IT dell'azienda.

- Un ruolo importante è assegnato alla segmentazione della rete: se si divide una rete in vari segmenti logici, per l'attaccante diventa più difficile un eventuale movimento laterale una volta avuto accesso interno. La micro-segmentazione è una tecnica più nuova che estende il concetto al suo estremo, creando segmenti di rete a livello di singole macchine o workload individuali.
- Serve poi un enforcement granulare degli accessi per singoli utenti (approccio identity-based) che sono verificati (Trust) sulla base della loro location, del device che usano e di altri dati per controllarne l'identità, assegnare quindi l'utilizzo di una certa macchina o di una certa applicazione. Ma è anche possibile verificare contestualmente che il device con cui stanno accedendo è sicuro, è aggiornato e monitorato. Per far questo, un modello Zero Trust fa ricorso in modo esteso a tecnologie già note (multifactor authentication, IAM, orchestration, analytics, encryption, scoring, file system permissions), e su policy di governance del tipo Least Privilege, PAM, che assegnano gli accessi sulla base del ruolo e del task.
- Un altro approccio che fa parte del modello è quello noto come Software-Defined Perimeter (SDP). La maggior parte delle offerte SDP si basano su un software client, un controller e un gateway, con lo scopo di offrire accesso remoto a single applicazioni interne (quindi "restringendo" il perimetro alle applicazioni). In questo modo si riduce anche il ricorso alle VPN.

In realtà, si tratta di tecnologie e misure di sicurezza che le aziende utilizzano già da anni: dove sta quindi la differenza? L'approccio Zero Trust non risiede tanto nelle tecnologie, quanto nei processi e nella mentalità che richiede, e nella comprensione molto più fine dei carichi di lavoro delle persone, oltre che del

comportamento effettivo delle applicazioni e dei servizi in esecuzione su ciascun sistema.

## Cominciare a utilizzare Zero Trust per il cloud

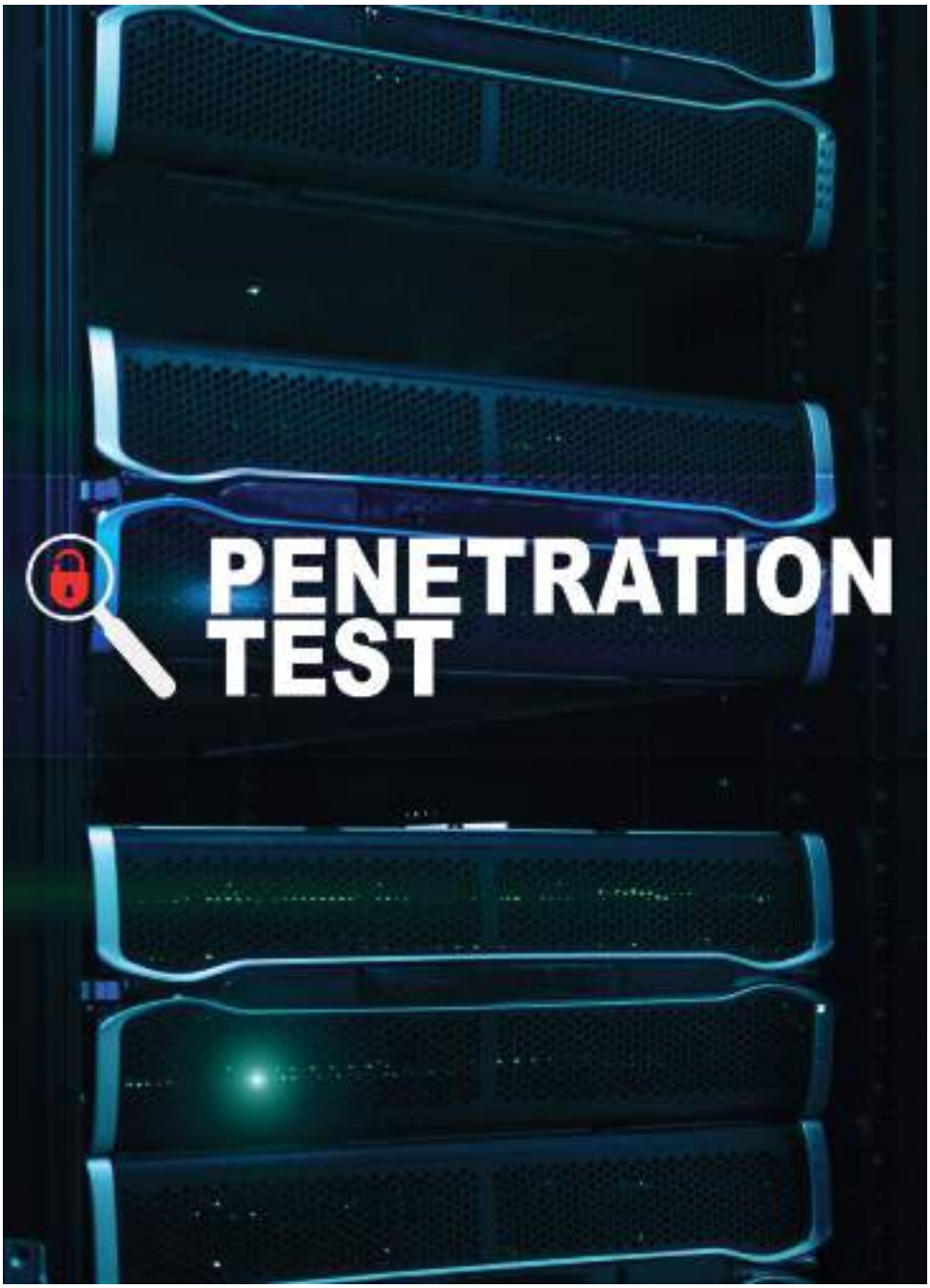
Come viene oggi detto da più parti, un buon banco di prova per questo modello è il cloud, che oltre a essere un ambiente greenfield, in cui la sicurezza va tuttora disegnata, è anche un esempio di come si stanno modificando le modalità operative e di come deve quindi essere adeguata la cybersecurity.

In architetture cloud ibride, una micro-segmentazione granulare (per massima visibilità a livello di traffico di rete, carichi di lavoro, configurazioni applicative) e l'automazione di policy per presidiare in maniera dinamica tutto l'insieme dei carichi di lavoro (ovunque essi si trovino), permette alle organizzazioni di innalzare veramente, by design, il livello di sicurezza. Adottare una micro-segmentazione Zero Trust permette di consentire solo il flusso di traffico tra i sistemi e le connessioni approvate, indipendentemente dall'ambiente in cui si trovano. Il modello viene così inserito nei sistemi virtuali tramite l'hypervisor e garantisce controllo, scalabilità, dinamicità del disegno della sicurezza.

## Perchè le aziende ritardano nell'implementazione di Zero Trust?

Gran parte del ritardo nell'adozione di Zero Trust va attribuito al technical debt dei sistemi legacy e delle architetture di sicurezza tradizionali, che è molto difficile migrare al nuovo approccio. Proprio per questo molti cominciano ad adottare il modello per il cloud: lì non c'è legacy e si possono utilizzare i servizi di security-as-a-service (SaaS). Il passaggio degli ambienti legacy è più lento, non trova grandi vantaggi nei modelli SaaS.

Dal punto di vista dei costi, Zero Trust non dovrebbe costare di più rispetto alle soluzioni tradizionali, anzi, beneficerebbe di un maggiore consolidamento e merge di sistemi diversi di sicurezza. Ma di sicuro, nuovi costi sono legati alla formazione delle persone, a nuove competenze e strumenti da portare in azienda. Inoltre, la conoscenza puntuale dei workload e di quali accessi abilitare, può rappresentare un grande ostacolo a livello di disegno della soluzione, e non andare incontro alla filosofia vigente oggi in molte aziende, piuttosto liberali sul fronte delle autorizzazioni e degli accessi. Quello che si teme infatti è che un approccio di questo genere possa rallentare il business. La soluzione sta probabilmente nella possibilità di identificare l'approccio più consono per la singola organizzazione: vedremo nei prossimi anni, dall'analisi di singoli casi concreti, come ognuno avrà individuato il percorso migliore per la propria realtà.



# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Ricerca TIG: come è stata gestita l'emergenza Covid-19

A cura di
**The Innovation Group**

Dall'inizio dell'epidemia Covid-19, tutte le aziende si sono trovate nella situazione di dover far fronte a una crisi molto grave, che ha avuto impatti diretti sulla stessa continuità del business, e a cui tutti hanno risposto con procedure d'emergenza.

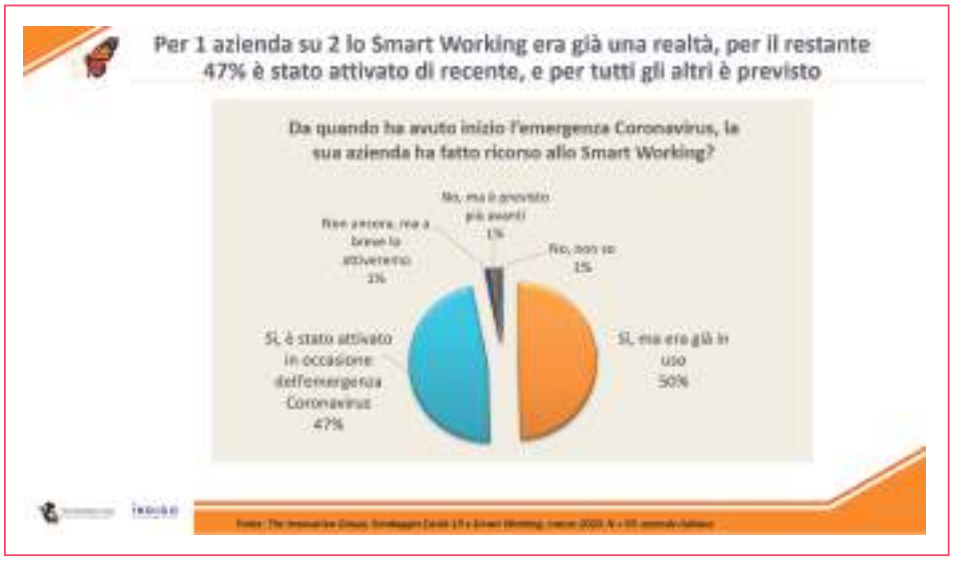
Misure specifiche per la protezione sanitaria della forza lavoro (come mascherine e guanti), distanziamento sociale, barriere in plexigas nei luoghi di contatto con il pubblico, e soprattutto, aspetto che è diventato prioritario per tutti a partire dal lockdown generale di fine marzo, operatività da remoto.

Oggi tutti parlano di Smart Working, ma vista la situazione, in realtà sarebbe meglio parlare di Remote o Home Working.

Quali sono state le conseguenze dell'emergenza e come hanno risposto le aziende italiane per preservare la continuità operativa?

Per rispondere a queste domande, The Innovation Group ha lanciato nella settimana del 25 marzo un sondaggio (subito dopo il Decreto del 24 marzo con cui venivano bloccate sia la circolazione delle persone sia moltissime attività) a cui hanno risposto 99 aziende, dei diversi settori e con diversi ruoli.

Dalle risposte è emerso che metà dei rispondenti utilizzavano il lavoro Agile già in precedenza, mentre l'altra metà lo ha attivato in occasione della pandemia da Covid-19: da segnalare però che le aziende che hanno risposto al sondaggio hanno anche dichiarato di avere percentuali diverse di persone che lavorano da remoto (solo un terzo oltre l'80% della forza lavoro), con orari lavorativi diversi.



Una conseguenza diretta dell'emergenza Covid-19 è stata quindi l'accelerazione della digitalizzazione dei processi aziendali, anche se con velocità e profondità di applicazione che variavano da caso a caso.

Se alcuni ambiti dell'impresa risultano infatti già informatizzati e quindi «smaterializzati» dal luogo di lavoro, altri sono ancora molto lontani da questa situazione. Inoltre, alcune aree, in primis le vendite, l'amministrazione, il servizio al cliente, hanno anche fruito – nei giorni dell'emergenza – di un «recupero di operatività» grazie a un maggiore ricorso di tutti (anche di clienti e partner) ai canali digitali.


La sicurezza è un tema importante, che si è posizionata ai primi posti tra gli investimenti richiesti dallo Smart Working.

Come emerge dal sondaggio, le aziende affermano di aver implementato numerose misure di sicurezza per i remote workers, innanzi tutto VPN (77% del campione), oltre ad anti-malware (68%) e formazione ad hoc (61%).

I rischi che vanno considerati nel momento in cui il lavoro è svolto da una postazione remota sono quelli associati a un ambiente che è by default meno protetto rispetto a quello dell'ufficio: collegamenti wireless, rete domestica non protetta, router potenzialmente già infettati, utilizzo di device personali o BYOD.

Le aziende sono chiamate, dalla compliance ma anche dal buon senso, a garantire che i dati aziendali, le applicazioni e le credenziali degli utenti siano protetti, le procedure basilari rispettate. Va anche considerato che gli hacker si sono prontamente adeguati alla situazione, sfruttando ogni occasione buona per portare a termine con successo i propri attacchi.

# CYBERSECURITY SUMMIT 2020

## GARANTIRE LA CONTINUITÀ DEL BUSINESS IN TEMPI DI PANDEMIA

## Il Crisis Management nei giorni del Covid-19

Intervista a

**Stefano Scoccianti**

**Enterprise Risk Manager, Gruppo Hera**

Quali sono le strategie che le aziende devono attuare per contenere i rischi in caso di pandemia? Come riorganizzare il lavoro, a cosa prestare attenzione in ogni fase dell'emergenza, quali criticità tenere presente nel momento in cui la forza lavoro viene isolata e continua ad operare in autonomia da remoto? Ne abbiamo parlato con STEFANO SCOCCIANTI, Enterprise Risk Manager, Gruppo Hera.

**Quali sono state per voi le misure fondamentali per contenere i rischi nel corso dell'emergenza creata dalla Pandemia Covid-19?**

Nell'ultimo anno e mezzo nel Gruppo Hera è stato avviato un processo di integrazione e ampliamento del modello di crisis management, un quadro di riferimento, dal punto di vista della governance e dei processi, per la gestione delle diverse categorie di crisi classiche (dall'interruzione di servizio, all'evento disastroso come un incendio, alla crisi reputazione, per fare degli esempi), assegnando un ruolo centrale al Comitato di crisi.

Questo è stato pensato a fronte di eventi che richiedono per rilevanza, intensità e strumenti di gestione, una focalizzazione specifica e straordinaria del gruppo e delle sue risorse, quindi attivabile quando l'evento travalica per importanza l'ambito circoscritto e gestibile a livello di singola attività di business.

Il Comitato, che comprende il vertice aziendale e le figure chiave di importanti filiere aziendali, ha il compito di attivare i piani di gestione della crisi che, per capirci, vanno al di là degli ordinari piani di emergenza di cui le aziende e i loro impianti sono dotati.

Nel caso della pandemia Covid-19, ci siamo trovati a gestire appunto una crisi non settoriale, non relativa ad un solo ambito del business, ma estesa a tutta l'organizzazione in tutte le sue componenti.

Naturale quindi che andasse trovata una risposta trasversale e coerente per tutta l'azienda.

Abbiamo attivato fin dal 21 febbraio, quindi dalla scoperta del primo focolaio, un comitato tecnico che si è riunito costantemente nelle prime settimane, in modo da inquadrare e strutturare l'approccio di crisis management tenendo conto di due grandi ambiti di presidio e gestione dei rischi:

- predisposizione di piani di continuità operativa, in coerenza con vari scenari evolutivi di severità della crisi individuati;
- misure di prevenzione e protezione innovative per la safety delle risorse.

Abbiamo quindi strutturato piani di continuità operativa per gestire tutti i possibili scenari per tutte le filiere aziendali, cosicché quanto c'è stato il lockdown generale non siamo stati colti impreparati.

Sostanzialmente, in poco più di 1 settimana di lavoro, intenso, trasversale, abbiamo definito i piani di gestione, collegati alla situazione del momento ma tenendo anche conto di una possibile escalation della crisi e implementato molte delle misure di prevenzione e protezione.

Operativamente, è stato piuttosto impegnativo realizzare in tempi rapidissimi le misure di protezione per i dipendenti più esposti, come ad esempio le barriere in plexiglas per i colleghi che lavorano a contatto con il pubblico, negli sportelli a cui rivolgersi per i nostri servizi. Sempre per limitare il rischio di contagio tra i colleghi, abbiamo organizzato la sanificazione degli ambienti e diradato le presenze nelle mense, stabilendo distanze tra i posti e una turnazione per i pranzi.

**Quali le misure in particolare per il lavoro da remoto?**

Da metà marzo è partito anche questo aspetto. Prima ci eravamo concentrati su aspetti come turnazioni e segregazione logistica, squadre da dislocare su diversi luoghi di lavoro, in modo da ridurre la possibilità di contaminazioni tra diverse squadre, fino ad avere in campo (ad esempio per i telecontrolli) singole persone isolate dal resto dei colleghi. Vi era comunque già una quota di colleghi in modalità remote.

Poi, nel momento del lockdown generale, tale quota è cresciuta notevolmente rappresentando una percentuale elevata delle risorse non impegnate sul campo o in impianti, grazie all'utilizzo di collegamenti e tools adeguati.

Questo è diventato nel corso delle settimane il nostro modo di lavorare, le comunicazioni sono state rese disponibili in ogni momento, mediante strumenti di condivisione e file in sharing. Dal punto di vista dell'IT, per garantire le attività in remoto, abbiamo velocizzato i processi di acquisto di PC portatili a fronte di una base disponibile già molto elevata, al fine di massimizzare le possibilità di lavoro da remoto per i colleghi (avendo scartato dall'inizio di consentire l'utilizzo del PC domestico privato).

Va detto che la situazione attuale, di remote working, ha trovato terreno fertile grazie alla preparazione effettuata negli anni precedenti da Hera nell'ambito del progetto di smart working rivolto a circa il 20% della forza lavoro.

Con l'emergenza Covid-19, è stato identificato e svolto un percorso per una popolazione significativa: sostanzialmente oggi le sedi si sono svuotate.

Riguardo invece ai colleghi che si occupano di manutenzione (per definizione remotizzati) oggi, per evitare contatti diretti e incrementare la sicurezza, la loro partenza avviene da casa (con il mezzo aziendale per l'intervento a disposizione sotto casa).

Possono muoversi ed espletare la loro attività senza passare presso la sede, prendendo in carico l'intervento tramite tablet, senza bisogno di consegna fisica di ordinativi del lavoro da effettuare e quindi contatti diretti.

**Si è parlato molto in questo periodo di rischi di filiera e di problematiche collegate alla Supply Chain nei giorni del Covid-19: qual è la sua esperienza su questo tema?**

Considerando 3 ambiti di supply chain rilevanti in tale contesto (ICT, DPI e fornitori di servizi per le filiere di business), sulla parte ICT, essendo partiti per tempo e in gran parte già strutturati, non abbiamo registrato particolari criticità. Invece, come per molti altri, nell'ambito dei dispositivi di protezione ci sono state difficoltà: pur disponendo di nostre dotazioni di DPI, come strategia prudenziale abbiamo scelto di garantirci un livello di disponibilità adeguato alla situazione.

Abbiamo dato corso ai contratti di fornitura esistente, pur nelle difficoltà e nelle incertezze di contesto, ed abbiamo anche attivato nuovi canali di fornitura grazie al nostro procurement.

Infine, sulla terza categoria di fornitura, ossia i partner locali sulle attività di esercizio, manutenzione, pronto intervento su reti e impianti, avendo partnership molto consolidate, abbiamo risolto le criticità che si presentavano tramite una maggiore cooperazione e coordinamento di tutti gli attori, operando nei limiti pervisti dalle disposizioni normative che si sono susseguite. Il nostro ufficio acquisti ha agito come osservatorio interno per valutare e individuare soluzioni per superare eventuali criticità per i vari cluster di fornitori, attivando ove possibile anche strumenti a sostegno della filiera. In questo momento non abbiamo segnali di criticità acute, ma c'è da dire che il nostro settore, essendo quello dei servizi essenziali, non è mai stato bloccato, e anche le catene di fornitura hanno continuato ad operare.

**Cosa cambierà nei prossimi mesi?**

Hera sta già predisponendosi per affrontare le settimane e i mesi che ci attendono, pur nelle incertezze riguardo alle modalità di ripartenza. Sicuramente una componente significativa sarà costituita dalle modalità di lavoro da remoto, componente importante per modulare il ritorno al new normal, e un ruolo rilevante sarà svolto dai vincoli che saranno imposti per il distanziamento sociale.

La dotazione di mascherine potrà diventare un elemento chiave di protezione, così come prassi attivate in queste settimane lato sanitizzazione e igienizzazione. Potranno inoltre rendersi necessarie ulteriori misure per garantire livelli adeguati di sicurezza ai colleghi.


# IL CAFFÈ DIGITALE

## ISCRIVITI ALLA NEWSLETTER MENSILE!

RICEVI GLI ARTICOLI
DEGLI ANALISTI DI THE
INNOVATION GROUP
E RESTA AGGIORNATO
SUI TEMI DEL MERCATO
DIGITALE IN ITALIA!

COMPILA IL FORM DI REGISTRAZIONE SU

**www.theinnovationgroup.it**