Cybersecurity: l’anno che sta finendo e l’anno che verrà

Ci avviciniamo alla fine di un anno molto difficile, che ha stravolto radicalmente sia le abitudini personali che il modo di lavorare di milioni di persone. Tanto per citare numeri notissimi, nel periodo del primo lockdown abbiamo assistito ad un incremento radicale del lavoro da remoto: ad aprile di quest’anno i lavoratori che si sono trovati in questa condizione erano 4 milioni con un incremento quasi di circa 3 milioni rispetto all’anno precedente. In pratica, si tratta del 18,5% della forza lavoro con un potenziale di crescita fino al 35,7% pari ad 8,2 milioni di lavoratori[1]. È perfino superfluo sottolineare che tipo di impatto possa avere questa nuova condizione di vita e di lavoro su tutti noi: è una discussione rimbalza in ogni momento su tutti i media, da quelli tradizionali a quelli digitali.

Oltre al lavoro da remoto, abbiamo acquistato online molto di più di prima (quasi il doppio rispetto al corrispondente periodo dell’anno precedente) e siamo ricorsi ad Internet anche per servizi “sensibili” come i servizi sanitari. Di conseguenza, si è di molto ampliata la superficie esposta al cybercrime che ha intensificato le sue attività attraverso il veicolo principe, ovvero, le e-mail di phishing che in molti casi – per far leva sulla preoccupazione del momento – sono state subdolamente predisposte con contenuti legati al Covid-19.

La nuova condizione generata dalla crisi pandemica ha, quindi, un impatto significativo anche su chi si occupa di cybersecurity, che dall’inizio della crisi è stato impegnato a cercare di mantenere in piedi controlli di sicurezza disegnati per un mondo che all’improvviso è cambiato radicalmente. Si tratta, quindi, di capire quanto le tecnologie utilizzate per realizzare questi controlli si siano rivelate adatte a

supportare l’evoluzione che si è resa necessaria nello scenario di crisi pandemica.

Vediamo con ordine. Sicuramente, per le aziende questa nuova situazione ha comportato la necessità di adeguare le proprie infrastrutture di accesso e di collaborazione sia in termini di capacità che (spesso) in termini di funzionalità. Possiamo dire chi aveva già adottato soluzioni cloud per la gestione del lavoro d’ufficio (documenti, posta, chat, videoconferenza) è riuscito ad essere pronto più velocemente di chi, invece, alla data aveva queste infrastrutture realizzate on-premise. Le aziende cloud-based non hanno avuto problemi di scalabilità e, inoltre, hanno potuto abilitare ulteriori controlli di sicurezza con semplici configurazioni. Possibili esempi di ulteriori controlli sono: aggiungere elementi di irrobustimento delle procedure di accesso (come, ad esempio, aggiunta di un secondo fattore di autenticazione), oppure, usufruire di strumenti come le sandbox o i sistemi di URL filtering utili a rendere più sicure le e-mail che – come abbiamo visto – sono il principale veicolo di attacco.

In questo frangente, quindi, il cloud ha dimostrato di poter fornire vantaggi in termini di scalabilità, semplicità e velocità troppo rilevanti per essere ignorati, anche dal punto di vista della sicurezza.

Facciamo un esempio: nella prima settimana di settembre tante aziende sono state interessate da una campagna di phishing generata a partire da mail «reali» scambiate in precedenza dai destinatari di tale campagna con clienti o fornitori, probabilmente derivate da breach dei medesimi. La campagna aveva l’obiettivo di diffondere il malware Emotet, testa di ponte per il ransomware Ryuk o per il banking trojan Trickbot. La particolarità di questa campagna è stata quella di usare tecniche di social engineering piuttosto evolute, in quanto le mail di phishing apparivano come reply a mail effettivamente inviate dal mittente ad una sua controparte. Questo caso testimonia l’aumento della complessità delle campagne di

attacco che tentano di sfruttare l'aumento esponenziale della superficie digitale nel periodo Covid. Di fronte a campagne di questo tipo è indispensabile: a) avere controlli di sicurezza adeguati e facilmente configurabili; b) avere il giusto livello di visibilità sugli end-point e sulla rete; c) addestrare le persone a riconoscere le e-mail di phishing attraverso le quali arrivano i tentativi di propagazione di queste minacce. Viceversa, il rischio di dover sopportare impatti rilevanti dovuti – ad esempio – alla propagazione di un ransomware è veramente elevato; ma questa, nel 2020, è una storia vista più di una volta.

Il secondo punto cruciale su cui sono stati impegnati gli specialisti di cybersecurity è stato quello relativo all'accesso da remoto. Più o meno tutte le aziende si sono riversate ad aumentare la loro capacità di accesso dall'esterno che prima era dedicata ad una quota tutto sommato limitata di dipendenti. Quindi, creazione di nuovi collegamenti VPN o aggiunta di capacità alle VPN esistenti che implica, a seconda dei casi, un'attività realizzativa piuttosto intensa (ad esempio, distribuzione di client VPN e di certificati digitali e configurazione del secondo fattore di autenticazione via OTP) che è commisurata anche al numero di collegamenti da creare che, per alcune aziende, ha raggiunto le decine di migliaia di unità. Insomma, un problema anche in termini di mantenimento e gestione.

In tanti casi, poi, l'apertura verso l'esterno è avvenuta in situazioni in cui e aziende non erano pronte, ovvero, non avevano attuato all'interno le corrette pratiche di segregazione in termini di raggiungibilità sia di reti che di applicazioni, altro controllo fondamentale che in molti casi si è dovuto realizzare ex-novo. Se poi aggiungiamo il fatto che le tecnologie che realizzano le VPN non sono esenti da pecche (nel recente passato molte di queste hanno manifestato vulnerabilità critiche), allora, si delinea completamente quello che è successo. Tante aziende hanno aperto all'esterno

in fretta, gestendo complessità tecnologica e organizzativa e non avendo filtrato a monte quello che deve essere esposto alla singola utenza che si connette. Quindi, una situazione preoccupante, specialmente quando le credenziali di accesso alla VPN – nella logica del SSO – sono anche quelle che danno accesso al PC ed ai servizi aziendali. Insomma, le VPN sono punti di criticità da controllare per bene.

Che cosa succederà il prossimo anno? Probabilmente nulla di diverso da quanto abbiamo già visto. Molti dei trend di cui abbiamo discusso si consolideranno e diventeranno permanenti. La superficie esposta non diminuirà e l'accesso da remoto alle infrastrutture aziendali rimarrà un punto critico.

Di seguito le mie previsioni: ma è un gioco, o forse no.

Ci sarà un incremento dell'adozione di servizi Cloud sia in ambito interno che di business; questa tendenza darà molti vantaggi in termini di semplicità e agilità ma richiederà un'attenta gestione da parte degli uomini che si occupano di cybersecurity. Un proliferare disordinato di presenza in cloud è di per sé una criticità.

Le VPN saranno progressivamente sostituite da servizi cloud SASE (Secure Access Service Edge) che offrono sia il servizio di accesso sicuro senza richiedere l'installazione di client sul PC, che servizi di configurazione che consentono di restringere l'accesso alle risorse aziendali per gruppi di utenti o per singoli utenti.

Spariranno le password, sostituite da modalità di accesso biometrico eventualmente supportate da app su mobile.

Proseguirà l'adozione di tecnologie AIML (Artificial Intelligence & Machine Learning) applicate all'analisi di Big Data; e speriamo che questo approccio in ambito cybersecurity inizi a mantenere le promesse fatte già da qualche anno.

Note

[1] Fonte “Rapporto annuale ISTAT – capitolo 3”

Articolo a cura di **Marcello Fausti**



Il Dott. Marcello Fausti è attualmente responsabile della CyberSecurity del Gruppo Italiaonline.

Nei 10 anni precedenti, è stato responsabile della IT Security di TIM con responsabilità della protezione delle infrastrutture critiche; dello sviluppo e gestione dei sistemi a supporto dell’Autorità Giudiziaria; della gestione del Security Operation Center, della gestione del processo di ICT Risk Management e dello sviluppo delle contromisure di sicurezza per la gestione operativa dei piani di sicurezza. È stato, inoltre, responsabile del Security Lab di TIM. In precedenza ha lavorato nel gruppo Olivetti come direttore marketing e business development di una società di system integration attiva sul mercato dei large account e come marketing manager della divisione PA della capogruppo.

È certificato CISM, PMP, COBIT, ITIL, ISO20000.

https://www.ictsecuritymagazine.com/articoli/cybersecurity-lanno-che-sta-finendo-e-lanno-che-verra/