WHITE PAPER

NEXT-GENERATION SECURITY:

Le sfide che i CIO dovranno superare nel prossimo futuro.

LumIT
A DGS COMPANY

INDICE

3 Introduzione

4 Sicurezza informatica: lo scenario post-Covid

8 Next-Generation Security:
l'approccio "circolare" alla sicurezza informatica

10 Attacco alla nuvola

12 Another (data) breach in the web

13 Nelle terre sconosciute

14 Le opportunità della digital transformation

INTRODUZIONE

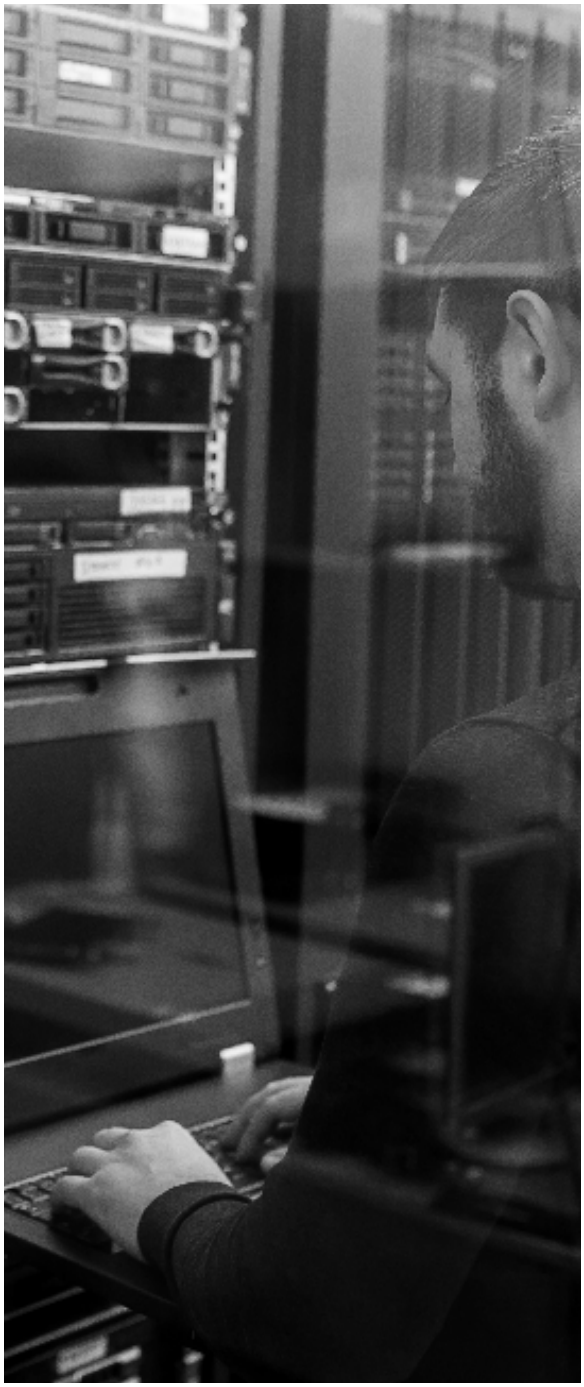
Inutile negarlo: **la comparsa della pandemia da SARS-CoV-2** ha scompigliato le carte un po' in tutti i settori, costringendo i vertici di migliaia di aziende in tutto il mondo a rivedere le strategie di sviluppo e le priorità che erano state stabilite quando né il Covid-19 né tanto meno la pandemia erano minimamente considerate. Tra tutti i reparti e dipartimenti, però, quello IT è stato particolarmente sovraccarico di lavoro. I CIO, e tutti i loro collaboratori, sono stati chiamati in prima linea sia per **garantire la continuità aziendale** sia per migliorare e implementare nuove strategie di difesa e protezione degli asset aziendali.

Quest'ultimo aspetto, spesso e volentieri sottovalutato se non proprio ignorato negli anni precedenti, nel mondo del "new normal" assume un'importanza strategica. Per moltissime aziende, garantire la cyber security – e gli investimenti in questo settore – è diventata **una priorità assoluta**. Con i dipendenti a casa, infatti, il **perimetro funzionale dell'azienda si è esteso in maniera indefinita**, sino a raggiungere dimensioni difficilmente immaginabili non moltissimo tempo fa. Non solo: è cresciuto anche il numero e la varietà di dispositivi che devono connettersi alla rete aziendale, rendendo particolarmente complesso il compito di chi si trova a gestire gli accessi agli asset informatici aziendali.

Insomma, la pandemia ha stravolto le priorità delle aziende e, con esse, quelle dei CIO che, nei prossimi mesi e nei prossimi anni, si troveranno ad affrontare nuove sfide all'insegna della **Next-Generation Security**.

SICUREZZA INFORMATICA: LO SCENARIO POST-COVID

La pandemia ha ribaltato quelle che erano le priorità di un CIO. Soprattutto nell'ambito della **sicurezza informatica**. A partire dallo scorso marzo, infatti, i programmi di adozione dello smart working e del lavoro da remoto hanno subito una improvvisa, e per molti versi inattesa, accelerazione. Da un giorno all'altro centinaia di migliaia di persone si sono ritrovate a lavorare da casa, causando un sovraccarico di lavoro per i reparti IT aziendali.



I CIO, dunque, hanno dovuto velocemente ridefinire quali fossero le priorità aziendali. Come si legge nel report "*COVID-19 crisis shifts cyber security priorities and budgets*" di McKinsey, dall'inizio della pandemia **le minacce informatiche e i tentativi di attacco si sono moltiplicati**, facendo crescere la pressione sui reparti IT e di sicurezza informatica. Gli attacchi phishing, che consentono ai criminali informatici di impadronirsi delle credenziali di accesso a profili e account online, sono aumentati di sette volte nell'arco di poche settimane, costringendo le aziende a correre ai ripari.

Più in generale, nelle settimane immediatamente successive allo scoppio della pandemia e al "trasloco" nei salotti di casa di interi uffici, sono aumentati gli **attacchi di tipo "social engineering"** che, sfruttando diverse tecniche a metà tra lo psicologico e l'informatico, consentono di ottenere informazioni utili a penetrare senza troppa fatica all'interno di infrastrutture informatiche.

I Chief Information Officer, di concerto con chi si occupa di sicurezza informatica, hanno dovuto rivedere completamente i loro piani e le loro priorità. In particolare, ha iniziato ad affacciarsi il **concetto di Next-Generation Security**, ossia una sicurezza informatica "circolare", in grado di dare risposta nel medio e nel lungo termine a minacce di pericolosità e complessità crescente. Nell'immediato, invece, hanno adottato delle soluzioni di sicurezza che garantissero tanto gli endpoint dei dipendenti, quanto le infrastrutture informatiche aziendali.
Un approccio differente che avrà, inevitabilmente, delle **ripercussioni sull'intera organizzazione aziendale** nel medio e nel lungo termine. Per non farsi trovare impreparati alle sfide del futuro, infatti, le imprese dovranno **rivedere i loro piani strategici di crescita e sviluppo** e riallocare conseguentemente le risorse. Secondo una ricerca condotta tra i responsabili di sicurezza informatica in Italia, l'81% prevede che il Covid-19 cambierà il modo di operare delle loro aziende nel lungo periodo.

AUTOMAZIONE DELLA SICUREZZA INFORMATICA

L'universo della sicurezza informatica è oggi sin troppo complesso per poter essere gestito in autonomia e senza il supporto di strumenti adeguati. Il CIO e il suo team IT fanno così affidamento su piattaforme e soluzioni che siano in grado di **analizzare in tempo reale tutti gli eventi che accadono nella rete** e nei singoli endpoint, individuare e neutralizzare tutte le potenziali minacce all'infrastruttura informatica aziendale. Diventa quindi fondamentale adottare **soluzioni che consentano di automatizzare la cyber security**, così da essere sempre in grado di rispondere a eventuali attacchi o tentativi di intrusione nella rete.

A coordinare il tutto troviamo il SOC (Security Operation Center), una struttura che sia in grado di monitorare e individuare possibili "incidenti" di sicurezza, rispondere a questi incidenti mettendo in atto adeguate contromisure e sia in grado di effettuare la mitigazione delle vulnerabilità (ossia, sappia riconoscere falle e vulnerabilità nella rete e nei software utilizzati e realizzare delle patch che impediscano a criminali informatici di approfittarne).

Ma quali sono gli strumenti che il CIO può utilizzare per realizzare un SOC efficiente e funzionale alle necessità della propria azienda? Le soluzioni, com'è semplice immaginare, possono essere le più varie, ma tre su tutte sembrano poter garantire i risultati migliori:

SIEM. Acronimo di Security Information and Event Management, il SIEM è una piattaforma che raggruppa diversi software e strumenti che consentono al CIO e al team di sicurezza informatica aziendale di attuare un monitoraggio costante e puntuale di tutti gli eventi che accadono nella rete aziendale. Grazie ad algoritmi di intelligenza artificiale e machine learning, le soluzioni SIEM sono in grado di analizzare le informazioni raccolte (come i log di accesso alla rete o quelli relativi al comportamento dei singoli endpoint) e individuare comportamenti anomali e, dunque, possibili minacce;

SOAR. Acronimo di Security Orchestration, Automation and Response, il SOAR è una piattaforma che raccoglie dati provenienti da diverse fonti per analizzare, orchestrare e automatizzare la risposta a eventuali minacce di sicurezza. Gli strumenti SOAR possono essere utilizzati per individuare, e neutralizzare, minacce legate al phishing oppure analizzare le attività degli endpoint connessi alla rete e scoprire eventuali anomalie nel comportamento di uno di essi;

NAC. Acronimo di Network Access Control, il NAC è una piattaforma di controllo e gestione degli accessi in rete. Grazie a un NAC non sarà solo possibile impostare regole automatiche per consentire l'accesso a un endpoint "già conosciuto", ma si potranno analizzare i loro comportamenti e, in caso di anomalie, espellerli dal network aziendale o "neutralizzarli" per effettuare controlli mirati.

NEXT-GENERATION SECURITY: L'APPROCCIO "CIRCOLARE" ALLA SICUREZZA INFORMATICA

Nel lungo periodo, in particolare, dovremo attenderci un cambio di atteggiamento nei confronti della sicurezza informatica pressoché totale. Una vera e propria **"Rivoluzione Copernicana" del settore**, che porterà dall'avere un approccio passivo e attendista nei confronti delle minacce informatiche a un approccio proattivo e volto a mitigare il rischio informatico.

In ambito cyber security, la crisi sanitaria che stiamo vivendo ha accelerato l'adozione di un nuovo modello, che abbiamo chiamato di **Next-Generation Security**, caratterizzato da un approccio circolare alla protezione delle strutture e degli asset informatici aziendali. Nello specifico, la "sicurezza di prossima generazione" si compone di **quattro fasi** che si susseguono in una sorta di spirale senza fine.

SECURITY BY DESIGN

Volendo individuare un momento iniziale, potremmo dire che la Next-Generation Security prende il via con la **progettazione dell'intera infrastruttura informatica aziendale** e con la scelta delle soluzioni di sicurezza preposte alla sua protezione. Tutto, infatti, deve essere realizzato nell'ottica del **"Security by design"**: i principi della sicurezza informatica devono essere parte integrante del processo di progettazione e sviluppo, così da evitare che vengano a crearsi delle falle e delle vulnerabilità sin dall'inizio. Ciò comporta la revisione dei processi e dell'organizzazione, dell'infrastruttura informatica e la scelta di nuove soluzioni di sicurezza che consentano di migliorare la protezione dell'intero ecosistema aziendale.

AUTOMATIZZARE LA SICUREZZA

Il secondo passaggio prevede l'implementazione di soluzioni tecnologiche che consentano di **automatizzare la sicurezza informatica**. In questo scenario, l'intelligenza artificiale e il machine learning rivestiranno un ruolo di primaria importanza, consentendo di alleggerire il carico di lavoro dei team di sicurezza. Gli algoritmi di AI e apprendimento automatico, infatti, si occuperanno di analizzare automaticamente il traffico della rete aziendale, andando a individuare le minacce informatiche, indipendentemente dal fatto che si presentino sotto forma di malware o di tentativo di attacco phishing.

APPROCCIO PROATTIVO E PREDITTIVO

Il terzo passaggio riguarda il già citato cambiamento di approccio, che dovrà essere **proattivo e "predittivo"**. Ovviamente, ciò non vuol dire che si sarà in grado di prevedere quando e come avverranno gli attacchi. Semplicemente, i CIO dovranno essere in grado di implementare misure di sicurezza che mettano al riparo dalle varie tipologie di attacco che potranno interessare l'ecosistema informatico aziendale.

TEST E SIMULAZIONE

Infine, sarà necessario verificare che tutte le soluzioni adottate siano in grado di proteggere l'infrastruttura tecnologica. La quarta fase, dunque, sarà quella di **test e simulazione**, che permetta di creare dei "falsi attacchi" e valutare se le risposte che arrivano dai sistemi di difesa siano quelle inizialmente attese.

ATTACCO ALLA NUVOLA

L'incremento del lavoro da casa e dello smart working ha portato a un **aumento dell'utilizzo di soluzioni e piattaforme cloud**, che consentono ai dipendenti sia di accedere a postazioni di lavoro "virtualizzate" sia di continuare a svolgere riunioni e incontri anche se ci si trova a decine (se non centinaia) di chilometri di distanza l'uno dall'altro. La "nuvola", dunque, è diventata una sorta di ufficio virtuale nel quale i dipendenti si recano ogni mattina sfruttando i loro dispositivi informatici (PC e smartphone).

Lo spostamento sul cloud, però, ha aperto un nuovo vastissimo fronte nella lotta al crimine informatico. Secondo diverse ricerche, nei mesi di picco del lockdown e della pandemia gli **attacchi alle infrastrutture cloud sono cresciuti del 630% anno su anno**, mostrando che il collegamento alla nuvola possa rappresentare l'anello debole dell'intera "catena informatica" aziendale.

Capire il perché di questo aumento non è affatto complicato. Prima di tutto, dal cloud passano informazioni di grande valore, come **documenti ufficiali dell'azienda, segreti industriali e dati personali di utenti e dipendenti**. Il cloud, poi, può rappresentare la chiave di accesso alla rete aziendale, anche se dovesse essere ospitata su un cloud privato anziché pubblico. La brutta abitudine di condividere e utilizzare la stessa password – o una semplice variazione della stessa – per diversi account favorisce il compito dei criminali informatici, che potranno provare ad accedere alla LAN aziendale con lo stesso nome utente e la stessa chiave d'accesso che si utilizza per il cloud pubblico.

Le piattaforme cloud, poi, **possono essere utilizzate anche come "esca"** per schemi di attacco e truffa condotti attraverso campagne spam e phishing. Negli ultimi mesi sono stati intercettati migliaia e migliaia di messaggi di posta elettronica che invitavano i dipendenti a scaricare le nuove versioni degli applicativi cloud oppure a effettuare un nuovo login per testare nuove funzionalità.

I CIO, dunque, **dovranno fronteggiare veri e propri "assalti" alla nuvola**, utilizzando sia strumenti e piattaforme di sicurezza (come vedremo tra poco, ad esempio, sarà necessario utilizzare dei software che garantiscano una migliore gestione degli accessi alla rete aziendale, che permettano di individuare e bloccare immediatamente eventuali "intrusi"), sia attraverso un percorso di formazione che aiuti a migliorare la consapevolezza dei dipendenti e li porti a individuare con facilità eventuali minacce a loro rivolte.

CYBER SECURITY AWARENESS: IL LATO UMANO DELLA SICUREZZA INFORMATICA

Non va mai dimenticato, però, che nello scenario descritto il fattore umano acquista un'importanza sempre crescente. Secondo molti analisti, infatti, il vero anello debole della catena della sicurezza informatica è rappresentato proprio dalle persone: gli **attacchi basati su tecniche di social engineering** aumentano a ritmo esponenziale, con i criminali informatici che preferiscono "hackerare" le persone anziché i software. Per questo motivo acquista sempre maggiore importanza il tema della **cyber security awareness**: è necessario che tutti gli utenti aziendali acquisiscano nozioni di sicurezza informatica, per riconoscere le minacce più frequenti.

È fondamentale, dunque, che **le aziende investano in "cultura della sicurezza informatica"**, affinché aumenti la consapevolezza dei rischi che si corrono quotidianamente navigando online. Anche la più semplice delle operazioni – come la lettura di un messaggio di posta elettronica, il download di un file di testo allegato a una mail o cliccare su un link – può causare danni a volte irreparabili. Un esempio su tutti: nella stragrande maggioranza dei casi le infezioni da ransowmare, che hanno causato miliardi di dollari di danni in tutto il mondo, partono proprio dal download di un file allegato a un messaggio di posta elettronica da parte di un dipendente distratto o poco "consapevole".

Ma cosa vuol dire, esattamente, **aumentare la cyber security awareness** degli utenti aziendali? Tutto passa da un'attenta formazione del personale, che deve essere in grado di riconoscere quelle che sono le minacce principali – le infezioni malware, gli attacchi phishing e le tecniche di ingegneria sociale, solo per citarne tre – e sapere come difendersi. Antivirus e antimalware da soli, per quanto potenti ed efficienti possano essere, non sono più in grado di assicurare un elevato livello di sicurezza: è necessario che chi siede di fronte a un PC (o tiene in mano uno smartphone) sia consapevole di tutto ciò che accade e che può accadere nell'universo informatico e si comporti di conseguenza.

ANOTHER (DATA) BREACH IN THE WEB

Gli attacchi agli applicativi cloud riguardano, direttamente e indirettamente, anche una delle altre sfide che i CIO dovranno affrontare sin dai prossimi mesi: la difesa dei dati – aziendali, dei dipendenti e dei clienti – dai tentativi di furto. I **data breach** (letteralmente "violazione dei dati") sono uno dei maggiori pericoli nel breve e medio periodo, indipendentemente dal settore nel quale l'azienda è attiva. E, specialmente se si opera in un mercato europeo, i furti di dati possono costare moltissimo, sia da un punto di vista economico sia da un punto di vista commerciale.

Il GDPR non prevede un tetto massimo per **le sanzioni applicabili in caso di violazione**: se il reato commesso è grave (come l'omissione di una privacy policy) si può arrivare a pagare il 4% del fatturato annuo mondiale. Aziende come Google o Amazon, se dovessero risultare colpevoli di violare il GDPR, potrebbero essere chiamate a pagare multe per miliardi di euro. Secondo il Data Breach Cost Calculator di IBM, **un furto di dati costa mediamente 3,82 milioni di dollari**, ai quali devono però aggiungersi anche i costi "indiretti".

Il furto di informazioni avrà, infatti, **anche un ritorno di immagine negativo**. La percezione che gli utenti avranno del brand cambierà inevitabilmente, con ripercussioni a livello commerciale. Insomma, i data breach possono avere un'onda molto lunga e difficile da controllare e valutare fino a fondo. Per questo i CIO dovrebbero progettare e attuare **azioni di detection and response**, che aiutino a individuare per tempo eventuali violazioni dei dati e impedire che queste abbiano un ritorno negativo sul business aziendale.

NELLE TERRE SCONOSCIUTE

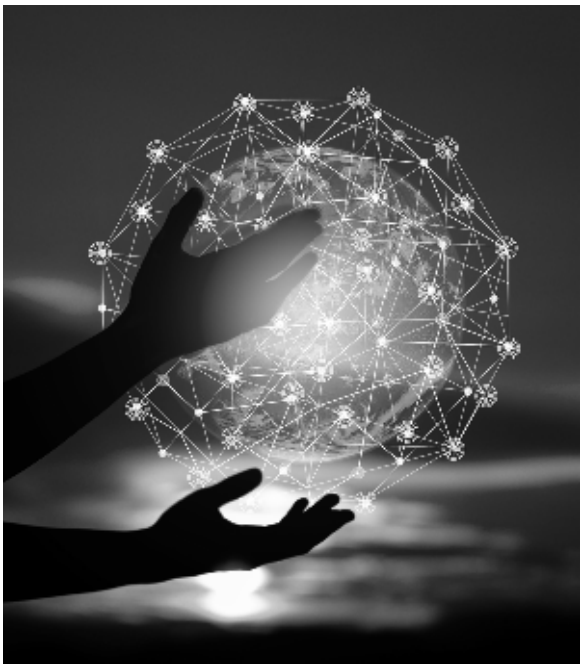
I Chief Information Officer, però, si troveranno ad affrontare anche sfide oggi sconosciute e difficilmente prevedibili. Il Covid, in questo senso, è esemplare. È fondamentale comprendere che la questione **non è tanto se mai si verrà attaccati, ma quando ciò accadrà**. E farsi trovare pronti. In questo scenario, l'intelligenza artificiale e l'apprendimento automatico giocheranno un ruolo chiave.

Gli algoritmi di AI e Machine Learning, infatti, si occuperanno sia delle operazioni di detection and response, sgravando gli addetti alla sicurezza informatica delle operazioni ripetitive e "noiose", sia di individuare nuove minacce non ancora conosciute. Utilizzando **algoritmi euristici**, le piattaforme e gli applicativi di sicurezza informatica saranno in grado di riconoscere nuove tipologie di attacco e di bloccarle, in attesa che un operatore in carne e ossa possa verificare se si tratti di una minaccia vera e propria o di un falso allarme.

LE OPPORTUNITÀ DELLA DIGITAL TRANSFORMATION

Bisogna però ammettere che il panorama non è tutto a tinte fosche: a fronte di così tante sfide, la digital transformation offre ai CIO (e alle aziende, ovviamente) un numero elevatissimo di opportunità di crescita e sviluppo. È fondamentale, però, che le soluzioni che garantiscono i maggiori vantaggi siano implementate in maniera adeguata all'interno dell'infrastruttura informatica aziendale. Anche il più piccolo degli errori, infatti, potrebbe consentire a un criminale informatico un'apertura da utilizzare per accedere alla LAN aziendale e trafugare segreti industriali oppure informazioni su dipendenti e utenti.

Ritorniamo, dunque, al concetto di **Security by design** che, come detto, funge da apripista al modello della sicurezza circolare della Next-Generation Security. Affinché tutto funzioni alla perfezione e si sia in grado di far crescere la propria azienda grazie alla digital transformation è necessario che i concetti della sicurezza informatica vengano tenuti in considerazione tanto nella fase decisionale quanto in quella operativa e realizzativa. Le aziende **dovranno investire in "cultura della sicurezza"**, non solo a livello di strumenti da utilizzare nella fase di automation, ma anche sul fronte della formazione del personale. Come detto, la consapevolezza su quanto accade in Rete acquista un'importanza sempre maggiore nell'ottica della protezione delle properties aziendali. E solo attraverso la giusta "awareness" sarà possibile sfruttare a pieno le opportunità che la trasformazione digitale offre a tutte le aziende.



SE VUOI SAPERNE DI PIÙ

CONTATTACI

VIA MILANESE 20
20099 SESTO SAN GIOVANNI

INFO@LUMIT.IT
SALES@LUMIT.IT

WWW.LUMIT.IT