E-GUIDE

L'APPROCCIO MULTIDISCIPLINARE ALLA CYBER SECURITY

NETWORK DIGITAL 360

IN COLLABORAZIONE CON

accenture avanade Microsoft

L'APPROCCIO MULTIDISCIPLINARE ALLA CYBER SECURITY

L'approccio alla sicurezza informatica è oggi un tema che non può essere delegato semplicemente a un singolo "esperto" che si occupa esclusivamente degli aspetti di security. La sicurezza infatti permea varie dimensioni: dall'organizzazione aziendale, alla scelta delle soluzioni che vengono utilizzate.

1. LA CYBER SECURITY È UN LAVORO DI SQUADRA

La nuova declinazione della cyber security è **qualcosa di molto diverso da ciò a cui eravamo abituati fino a qualche anno fa**. Se nella prima decade del millennio si poteva pensare di garantire la sicurezza dei sistemi IT con antivirus e firewall, oggi il concetto di sicurezza copre una superficie più ampia, che comprende non solo la definizione degli strumenti di protezione, ma quella dei software utilizzati, delle policy, delle procedure e, in ultima analisi, la stessa organizzazione aziendale. In quest'ottica **l'approccio alla sicurezza informatica** è oggi un tema che **non può essere delegato semplicemente a un singolo "esperto"** che si occupa esclusivamente degli aspetti di security.

Si tratta piuttosto di un **approccio multidisciplinare**, in cui la sicurezza permea varie dimensioni: dall'organizzazione aziendale, alla scelta delle soluzioni (sia a livello IT, sia a livello di cyber security) che vengono utilizzate. Non è un caso che, in tema cyber security, nascano sempre più spesso partnership che coinvolgono aziende che operano in settori "confinanti". È proprio questa l'ottica in cui si muove la collaborazione tra **Accenture, Avanade e Microsoft**, nata anche con una focalizzazione specifica sul tema della cyber security con lo specifico obiettivo di mettere a fattore comune le proprie competenze per offrire una visione omnicomprensiva in ottica security.

AVANADE, ACCENTURE, MICROSOFT: TUTTE LE COMPETENZE CHE SERVONO PER LA CYBER SECURITY

accenture

Approccio flessibile che combina le strategie di cybersecurity, business continuity e enterprise resilience.

avanade

Approccio olistico alla protezione delle informazioni attraverso servizi di advisory, implementazione tecnologica e servizi di sicurezza gestita.

Microsoft

Più di 3.500 esperti di sicurezza globale e l'investimento annuale di 1 miliardo di dollari in ricerca e sviluppo.

I VANTAGGI DI UN'ALLEANZA STRATEGICA

- Focalizzazione sui servizi a valore aggiunto attraverso soluzioni orientate alla protezione di utenti, identità, dati e servizi.
- Personalizzazione delle soluzioni di sicurezza in linea con le priorità strategiche di business dei clienti.
- Competenza strategica di Advisory tecnologico.
- Supporto end-to-end alla realizzazione di business case integrati di trasformazione digitale.
- Forte orientamento all'innovazione attraverso l'implementazione di strumenti di intelligenza artificiale e machine learning.

Obiettivo sicurezza

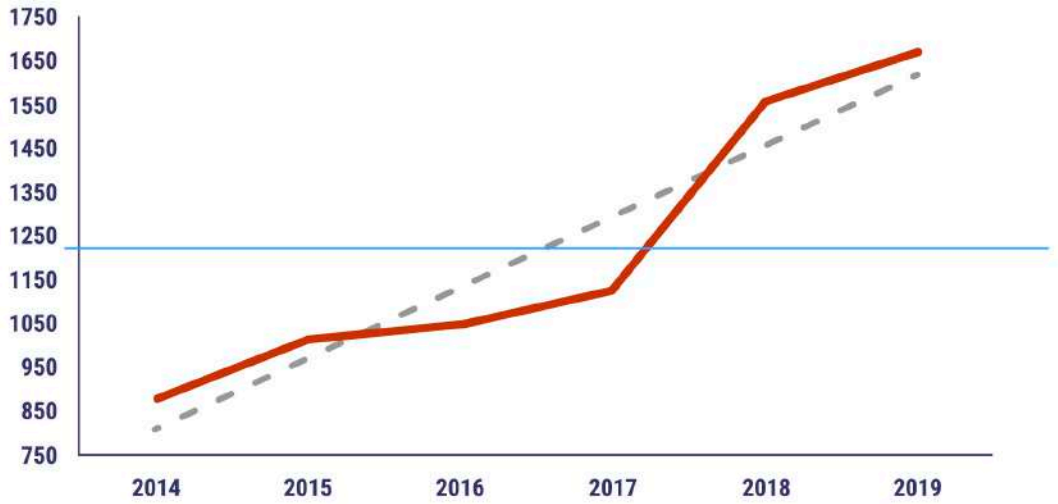
Quello della cyber security, in una manciata di anni, è diventato un tema caldissimo per qualsiasi azienda che tocca tutte le attività produttive. A contribuire a questa situazioni sono due fenomeni in particolare:

- il primo è quello della **digital transformation**, che interessa ormai le imprese di tutti i settori;

- il secondo è rappresentato invece dalla **costante crescita del cyber-crimine**, un "business" con un giro d'affari che nel 2018 è stato stimato in 1.500 miliardi di dollari. Una tendenza confermata anche dai primi dati emersi dal rapporto Clusit (marzo 2020), che nel 2019 registra un aumento di attacchi riusciti (1.670 casi denunciati, quasi il doppio rispetto al 2014) con una distribuzione assolutamente trasversale nei vari settori. Quelli più interessati, spiega il rapporto Clusit, sono il settore finanziario, quello delle strutture sanitarie, della ricerca e dei servizi online.

Il dato di fondo è che qualsiasi organizzazione, a prescindere dal settore in cui opera, è a rischio attacco. Il cyber-crime è un fenomeno che interessa tutti e che, stando alle stime più aggiornate, ha un costo per le organizzazioni di 600 miliardi di dollari a livello globale.

Non a caso lo stesso rapporto Clusit segnala, come elemento positivo, una maggiore attenzione da parte delle aziende al tema. “Il tema della sicurezza informatica è ormai assolutamente trasversale” conferma **Luba Manolova, Direttore della Divisione Microsoft 365 di Microsoft Italia.** “Qualsiasi impresa ha la necessità di mettere in sicurezza le sue infrastrutture IT per garantire la business continuity e tutelare il suo patrimonio, in particolare a livello di proprietà intellettuale”.



Numero di attacchi rilevati per anno (2014-2019).
Fonte: Rapporto Clusit 2020

Il tema della sicurezza informatica è ormai assolutamente trasversale e interessa tutti i settori del business.

Luba Manolova, Direttore della Divisione Microsoft 365 di Microsoft Italia

2. UNA NUOVA DIMENSIONE DELLA SECURITY

Il fatto che tutte le imprese, indipendentemente dal settore in cui operano, siano interessate dal tema cyber security non è l'unico elemento di novità con cui le aziende si devono confrontare. La logica stessa della sicurezza informatica, nel panorama attuale, è **molto più complessa rispetto al passato**. L'affermarsi delle tecnologie **cloud** e la diffusione del lavoro in **mobilità**, declinato secondo la logica del modern workplace e dello smart working, hanno infatti trasformato radicalmente la natura stessa delle architetture IT, rendendole non solo **più flessibili**, ma **anche con un perimetro meno definito**.

"L'approccio tradizionale che fa riferimento al perimetro non è più sufficiente" spiega **Fabio Vernacotola, Security Lead Italy di Avanade**. "Oggi i sistemi IT di un'azienda intersecano differenti piattaforme, come il cloud, e la loro messa in sicurezza richiede una visione più ampia. La logica della nuova cyber security deve infatti adeguarsi a un **nuovo panorama**, in cui non è più possibile pensare che tutto ciò che sta "dentro" può essere considerato affidabile mentre vada controllato solo ciò che arriva da "fuori".

Un perimetro meno circoscritto come quello delle moderne architetture IT, in cui lo scambio di dati e informazioni avviene tra dispositivi che spesso si trovano in mobilità e gli stessi servizi vengono erogati da piattaforme “esterne” come il cloud impone un cambio di prospettiva. “La logica è quella di un approccio **zero trust**” precisa **Gabriella Carrozza, Security Innovation Lead Europe di Accenture**. “L’organizzazione delle aziende punta sulla flessibilità sia sotto un profilo fisico, sia sotto un profilo di gestione dei processi produttivi. La security deve adeguarsi a questa filosofia per garantire un controllo efficace a livello IT”.

Il nuovo paradigma della sicurezza si basa su un approccio zero trust. Il controllo dell’identità e degli accessi diventa fondamentale.

Gabriella Carrozza, Security Innovation Lead Europe di Accenture

Le minacce cyber richiedono capacità di analisi delle informazioni che le imprese non possono più affrontare da sole. Ma non è solo un tema di tecnologia e security frameworks: c’è bisogno di partner affidabili con competenza ed esperienza.

Fabio Vernacotola, Security Lead Italy di Avanade

IL REBUS DELLO SMART WORKING

L'adozione di un modello di lavoro flessibile, accanto agli indiscutibili vantaggi in termini di produttività e qualità della vita, porta con sé elementi di rischio per la cyber security che non possono essere sottovalutati. L'utilizzo di strumenti e servizi fuori dal perimetro aziendale, infatti, aumenta esponenzialmente la superficie d'attacco a disposizione di eventuali pirati informatici. Oltre ai normali strumenti di protezione (dai sistemi di Mobile Device Management ai collegamenti tramite VPN) è indispensabile definire e implementare policy specifiche per l'accesso ai dati e ai servizi.

Se l'utilizzo di sistemi MDM (Mobile Device Management) consentono di separare i dati e le applicazioni aziendali da quelli della sfera privata dei lavoratori, nel panorama attuale diventa indispensabile prevedere sistemi di gestione dell'accesso alle risorse cloud (CASB) che permettano di garantire la massima sicurezza nell'utilizzo degli strumenti di lavoro erogati attraverso la formula Software as a Service (Saas) ormai prevalenti nelle infrastrutture aziendali di grandi dimensioni.

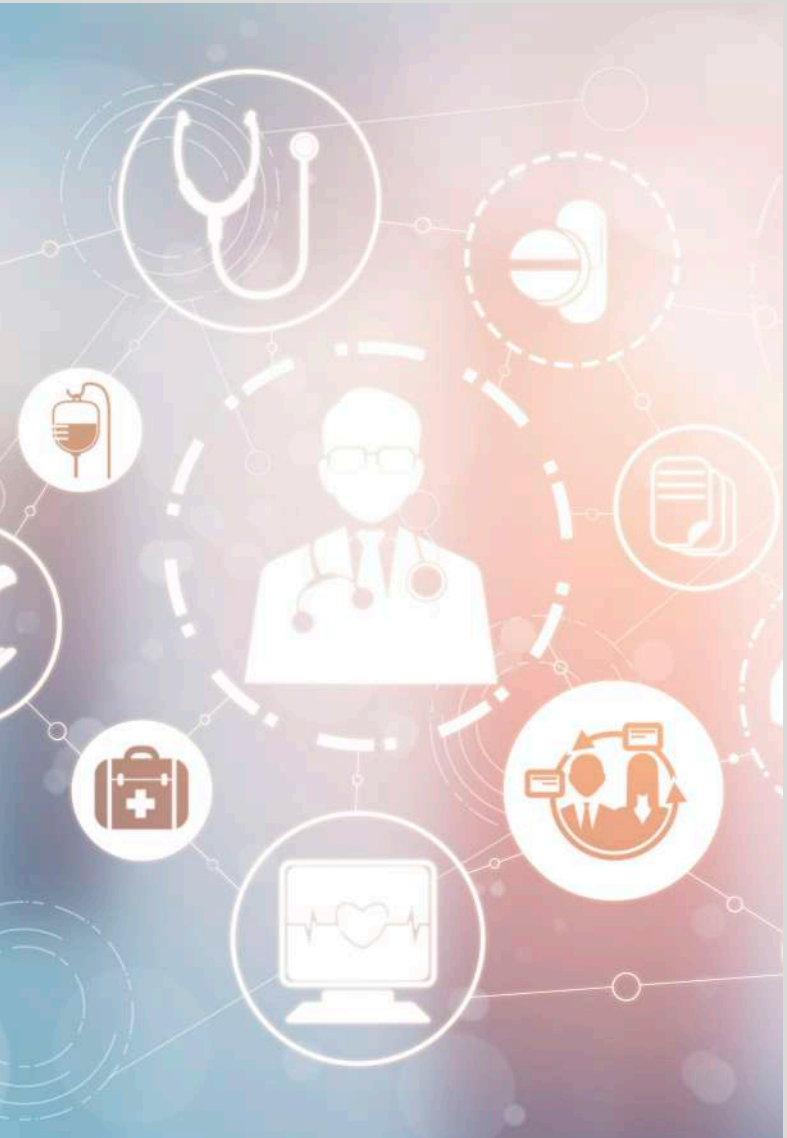
3. SICUREZZA SU MISURA

Date queste premesse, è evidente che **i servizi di cyber security devono adeguarsi alle specifiche esigenze dell'azienda**, attraverso un'attività di **assessment** basata sulla tipologia di attività, sui sistemi implementati e su una puntuale individuazione dei **servizi mission critical**.

Stante il rispetto di standard minimi di sicurezza applicabili in qualsiasi ambiente, la definizione degli strumenti necessari per garantire la protezione dei dati e dell'attività richiede in definitiva un **processo di analisi e pianificazione estremamente accurato** attraverso un coordinamento con le figure più rilevanti in azienda, sia a livello manageriale, sia a livello tecnico. Insomma: un approccio "maturo" alla cyber security **non può prevedere una ricetta standard**, ma porsi obiettivi che devono essere perseguiti attraverso strategie differenziate e adeguate alle esigenze dell'impresa.

A contribuire a questa visione è anche la normativa in materia di sicurezza, a partire dal Regolamento Generale sulla Protezione dei Dati (GDPR), che impone quella che possiamo definire una “obbligazione di risultato”. In altre parole, nel quadro normativo attuale quello che viene chiesto alle imprese non è di mettere in campo strumenti standard predefiniti, ma di **garantire la sicurezza del dato adottando tutte le precauzioni necessarie**, caso per caso. “Il tema della regolamentazione ha ormai assunto un ruolo di primo piano” conferma Fabio Vernacotola di Avanade. “L’introduzione di un principio di responsabilità ha rappresentato un vero punto di svolta sia per quanto riguarda l’attenzione alla cyber security, sia per quanto riguarda le modalità in cui viene declinata”.

LA CYBER SECURITY NEL SETTORE MEDICALE



In ambito healthcare, il tema della sicurezza informatica ha specifiche criticità legate sia alla sensibilità dei dati trattati, sia alle peculiarità delle infrastrutture IT e dei dispositivi utilizzati.
Sotto il primo profilo, le imprese si trovano a dover considerare il tema dell'adeguamento a normative stringenti (a partire dal "nuovo" GDPR) che impongono l'adozione di una estrema attenzione per la protezione della privacy dei pazienti.
Da un punto di vista tecnico, invece, il tema caldo è quello della "fragilità" dei dispositivi medicali, spesso gestiti attraverso sistemi legacy, la cui sostituzione o aggiornamento è resa difficile (o impossibile) da problemi di compatibilità.
Uno scenario in cui è indispensabile l'adozione di soluzioni specifiche, a partire da una rigorosa segmentazione della rete, una gestione accurata degli accessi e la previsione di sistemi di protezione specifici per i dispositivi a rischio.

4. UN PROCESSO MULTIDISCIPLINARE

In quest'ottica diventa evidente come sia impossibile separare la fase di assessment dalla scelta delle soluzioni (sia quelle direttamente dedicate alla sicurezza, sia quelle più genericamente implementate a livello IT) e dalla loro gestione. Sono aspetti che si intrecciano e che richiedono competenze specifiche, attraverso un approccio integrato. "La **tecnologia che forniamo come Microsoft è un fattore abilitante**" conferma Luba Manolova. "La sua implementazione a livello di sistemi richiede però una definizione puntuale delle procedure e delle strategie per integrarli nei processi aziendali. Per farlo servono partner che siano in grado di fornire servizi di advisor adeguati".
Insomma: la logica della **security by design** deve ispirarsi a un approccio di tipo sistemico, in cui l'adozione di soluzioni tecnologiche si accompagnano a procedure di business adeguate e policy rigorose che consentano di proteggere il dato aziendale in ogni fase. In definitiva, non si tratta di individuare un "esperto" per ogni settore, ma di **affidarsi a soggetti che hanno competenze trasversali in grado di vedere il quadro d'insieme** e proporre le soluzioni più adeguate per le necessità dell'impresa.

"La collaborazione tra chi sviluppa le soluzioni tecnologiche e chi ha le competenze per implementarle, anche a livello di organizzazione dei processi, rappresenta un valore aggiunto fondamentale nel settore della cyber security" conferma Gabriella Carrozza di Accenture.

L'EMERGENZA IOT NEL SETTORE INDUSTRIALE

La diffusione di sistemi di automazione e la cosiddetta Industria 4.0 hanno aperto un nuovo fronte di lavoro nella cyber security. I dispositivi "intelligenti" utilizzati per la produzione manifatturiera, infatti, hanno caratteristiche particolari che richiedono una diversa strategia di difesa rispetto ai normali endpoint. Si tratta di device con una limitata capacità di calcolo e di memoria, spesso equipaggiate con sistemi operativi "minimalisti" (in alcuni casi decisamente obsoleti) derivati da Linux e sui quali non è possibile installare un software antivirus.

L'unica soluzione, quindi, è quella di proteggerli attraverso un controllo minuzioso del traffico dati e delle funzionalità attive. Altro lavoro per il SIEM che in ambiti come questi diventa quindi indispensabile.

5. PREVENZIONE: GESTIRE GLI AGGIORNAMENTI

Secondo i dati Clusit 2020, l'8% degli attacchi rilevati nel corso del 2019 ha fatto leva su vulnerabilità conosciute. A questo dato, però, è necessario aggiungere quella porzione di attacchi classificati come generici "malware", che sfruttano falle di sicurezza per le quali erano già disponibili patch al momento della violazione.

Il tema del **patch management**, nel panorama attuale, rimane in sostanza **uno degli aspetti più "caldi" a livello di prevenzione**. A renderlo particolarmente delicato è lo stesso meccanismo di individuazione delle vulnerabilità e il sistema di bug bounty. Si tratta di uno strumento preziosissimo, che vede impegnati centinaia di ricercatori di sicurezza che operano in collaborazione con gli sviluppatori software per individuare bug e falle di sicurezza all'interno di software e appliance, ma che impone alle aziende di agire con tempestività per applicare le patch.

La puntuale pubblicazione dei bug attraverso il sistema CVE (Common Vulnerabilities and Exposures) ha infatti l'effetto collaterale di aprire una finestra all'interno della quale i cyber criminali possono contare su una sorta di "assist" per portare i loro attacchi a compimento. In pratica, dal momento della pubblicazione dei dettagli di una vulnerabilità (e del contestuale rilascio della patch che la corregge) si apre una fase critica, in cui i pirati hanno l'occasione di sviluppare facilmente un exploit in grado di sfruttare la falla di sicurezza. L'obiettivo, quindi, è quello di essere in grado di applicare gli aggiornamenti con la massima rapidità attraverso un sistema di patch management gestito e processi rigorosi che consentano di applicarlo puntualmente.

PATCH MANAGEMENT: SECURITY VS. IT

In tema di prevenzione, le attività di patch management finiscono per collocarsi in una situazione di conflitto con le attività del dipartimento IT. Il motivo è semplice: se in una prospettiva di cyber security l'implementazione degli aggiornamenti dovrebbe essere effettuata in una logica vicina al "as soon as possible", gli amministratori IT hanno invece la tendenza a dilatare i tempi, puntando a verificare eventuali incompatibilità prima di applicare le patch. La semplice introduzione di una forma di coordinamento tra i due ambiti rappresenta, di per sé, un livello di ottimizzazione delle procedure che può migliorare notevolmente il livello di sicurezza in azienda.

6. NON È ORDINARIA AMMINISTRAZIONE

L'attività di hardening non si esaurisce nella semplice applicazione di aggiornamenti. In molti casi, la sua declinazione nel contesto reale pone una serie di problemi tecnici e richiede competenze specifiche, che i "normali" amministratori IT non sempre posseggono. L'attenzione per la security, per esempio, passa anche dalla definizione delle configurazioni più adeguate, individuate sia in base all'ecosistema in cui si collocano, sia alle specificità dei servizi erogati. "Nel caso in cui ci si trovi di fronte a infrastrutture particolari, per esempio con una presenza di macchine con sistemi legacy, l'attività di patch management deve essere **affiancata da un'attività di mitigazione del rischio** portata avanti attraverso una puntuale impostazione dei software di sicurezza" conferma Fabio Vernacotola di Avanade.

La sicurezza dei sistemi, infatti, si garantisce anche attraverso una **corretta impostazione** dei sistemi e dall'attività di **virtual patching**, l'applicazione cioè di tutti quegli accorgimenti (per esempio la definizione di regole a livello di firewalling) che consentono di bloccare gli attacchi collegati a vulnerabilità note. "Come sviluppatori di software ci impegniamo a migliorare e aggiornare costantemente i nostri prodotti" sottolinea Luba Manolova di Microsoft Italia. "La loro efficacia è però subordinata a una corretta applicazione e impostazione da parte degli utenti. Ricorrere a un servizio gestito consente di avere la migliore garanzia di mantenere un adeguato livello di sicurezza sulle piattaforme".

Autenticazione

In una realtà in cui il perimetro IT dell'azienda è sempre più sfumato e il lavoro in mobilità rappresenta ormai una quota consistente dell'attività produttiva, il puntuale controllo dell'attività di ogni singolo utente diventa un pilastro fondamentale nella gestione della cyber security. Dai sistemi **MDM (Mobile Device Management)** alla definizione di sistemi di autenticazione "robusti", il tema della gestione dell'attività degli utenti ha acquisito un ruolo di primo piano.

"Gestire in maniera adeguata gli accessi ai servizi e ai documenti aziendali permette di ridurre notevolmente la superficie d'attacco" conferma Fabio Vernacotola di Avanade. "Oltre alla gestione dei device, è fondamentale avere a disposizione tutti gli strumenti che consentano una verifica dell'identità, come l'adozione di sistemi di **autenticazione multifattore** e piattaforme di gestione come **Azure Active Directory**". Ancora una volta, però, la semplice adozione di strumenti adeguati non esaurisce il tema. "Per gestire l'accesso dei dati, soprattutto in ambito enterprise, è indispensabile definire policy, ruoli e privilegi a livello di gestione utente" spiega Gabriella Carrozza di Accenture. "Avere la certezza che ogni utente abbia accesso solo ai servizi e alle informazioni cui ha diritto di accedere è il primo, fondamentale, passo per garantire la sicurezza dei dati".

Visibilità e trasparenza

L'evaporazione del concetto di perimetro e la nuova declinazione del concetto di protezione dei dati sono alla base di un cambio di prospettiva a livello di cyber security che ha portato a concentrarsi, oltre che sulla prevenzione, sulla logica del **detect and response**.
In altre parole, oltre all'impegno per correggere le vulnerabilità e garantire il massimo livello di sicurezza dei sistemi, è indispensabile essere in grado di individuare con tempestività un eventuale attacco e agire con altrettanta velocità per contenerlo.

La chiave, in questa prospettiva, è l'utilizzo di sistemi **SIEM (Security Information and Event Management)** che consentano di analizzare in tempo reale tutto ciò che succede all'interno dei sistemi. Il mantra della cyber security moderna, quindi, è quello di avere la massima trasparenza e visibilità all'interno della rete, per riuscire a individuare immediatamente qualsiasi anomalia che possa rappresentare l'indizio di un attacco in corso. "Il controllo tramite SIEM non deve limitarsi ai dispositivi on premise" specifica Fabio Vernacotola di Avanade. "Nello scenario moderno, buona parte dei servizi e delle risorse sono erogati tramite cloud. È fondamentale, di conseguenza, adottare un approccio integrato che permetta di avere la massima visibilità anche di questa dimensione".

BLOCCARE LE TRUFFE? SERVONO POLICY E PROCEDURE

Se la tecnologia può bloccare malware e minacce informatiche, quando si parla di truffe la soluzione arriva, più che dagli strumenti di analisi, dall'adozione di procedure ispirate alla logica della cyber security. È il caso delle BEC (Business Email Compromise), le truffe attraverso le quali i cyber criminali utilizzano account di posta elettronica compromessi per ingannare i dipendenti dell'azienda e sottrarre cospicue somme di denaro. Lo schema è semplice quanto efficace e prevede come primo passo la violazione dell'account email di un dirigente. Utilizzando l'accesso alla posta elettronica della vittima, i truffatori inviano un messaggio in cui impersonano il manager e dispongono un pagamento apparentemente legittimo, spesso diretto a un fornitore abituale.

Le coordinate bancarie incluse nell'ordine di pagamento, però, fanno riferimento a un conto corrente controllato dai pirati. Secondo l'FBI, questa truffa avrebbe permesso ai cyber criminali di rubare 1,7 miliardi di dollari nei soli Stati Uniti. Per mitigare i rischi, il Federal Bureau of Investigation suggerisce di adottare procedure di verifica per ogni pagamento disposto attraverso strumenti informatici.

7. L'IMPORTANZA DEI DATI

Il legame tra dati e sistemi di analisi evoluti è doppio.

Da un lato, l'utilizzo di **machine learning e AI** consente di estrarre dai log di sistema le informazioni indispensabili per **monitorare la rete e reagire a eventuali attacchi**. Dall'altro, un'ampia disponibilità di dati permette di **addestrare in maniera più efficace gli algoritmi di intelligenza artificiale** utilizzati per l'analisi.

"La nostra piattaforma SIEM **Azure Sentinel** può sfruttare un patrimonio di informazioni amplissimo, stimato in più di 8.000 miliardi di eventi registrati al giorno" spiega Luba Manolova di Microsoft Italia. "I risultati si vedono: l'adozione di un sistema di analisi basato sull'intelligenza artificiale istruito attraverso questi dati ci ha permesso in soli 12 mesi di ridurre del 50% i tempi necessari per l'analisi delle minacce".

Una tecnologia che si sta sviluppando in maniera prepotente e che consente di mettere a disposizione degli esperti di sicurezza tutti gli strumenti che gli servono per eseguire analisi approfondite e monitorare costantemente lo stato dei sistemi. "Lo sviluppo di sistemi di machine learning e intelligenza artificiale rappresenta un enorme salto di qualità per la cyber security" prosegue Luba Manolova. "La possibilità di sfruttare una piattaforma ampia come quella a cui ha accesso Microsoft rappresenta un valore aggiunto che ci consente di sfruttare al massimo le opportunità offerte da queste tecnologie".

Il fattore umano

I sistemi SIEM rappresentano uno strumento prezioso, che consente da un lato di raccogliere, organizzare e analizzare i dati, dall'altro di automatizzare la risposta per mettere in campo un primo argine a eventuali attacchi. Nell'ottica della detection and response, però, un ruolo fondamentale è rivestito dal **SOC (Security Operation Center)** cui è affidata la gestione del SIEM e dell'attività di contrasto ai cyber attacchi.

"Per qualsiasi azienda di medie o grandi dimensioni è indispensabile poter contare sull'assistenza di un centro in grado di offrire una gamma molto più ampia di competenze e tecnologie rispetto ai tradizionali SOC. In tal senso il nuovo Cyber Fusion Center di Accenture è attivo in ambito di Ricerca & Sviluppo su servizi di ultima generazione, quali l'applicazione di Intelligenza Artificiale e Machine Learning per il rilevamento degli attacchi, metodologie e strumenti per analisi di malware avanzati, ricerca e utilizzo di informazioni di threat intelligence e sviluppo di sistemi di automazione nella risposta ai cyber attack" spiega Gabriella Carrozza di Accenture. "Si tratta di servizi che oggi possono essere erogati anche in remoto, mettendo in campo processi di collaborazione con i team interni che gestiscono le infrastrutture IT e interagendo con l'azienda in una logica di co-creazione nello sviluppo di nuove strategie e soluzioni". Anche in questo ambito, infatti, la chiave per la predisposizione di un sistema di sicurezza adeguato passa inevitabilmente per la definizione di procedure di response che consentano di ottimizzare tempi ed efficacia dell'azione. "Quello della security è un settore in cui non si può improvvisare" conferma Fabio Vernacotola di Avanade. "Per garantire un livello eccellente di difesa servono diversi fattori: l'implementazione di strumenti efficaci, una gestione puntuale e un'organizzazione meticolosa di policy e procedure a livello aziendale".

L'ATTIVITÀ DI INTELLIGENCE A LIVELLO DI SOC

Uno dei compiti del team di esperti all'interno di un SOC è quello di fornire un supporto "strategico" nel contrasto all'attività dei cyber criminali. È quella che viene definita "attività di intelligence" e che prevede un monitoraggio continuo per intercettare le attività di hacker e pirati informatici prima che questi possano portare a termine i loro attacchi. Questa forma di controllo consente sia di individuare le nuove minacce quando sono ancora in una fase "embrionale", sia di rilevare le attività preparatorie di pianificazione e raccolta di informazioni da parte dei cyber criminali in vista di un attacco mirato all'azienda.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38

20125 - MILANO

TEL. 02 92852785

MAIL: MARKETING@DIGITAL4.BIZ