Sicurezza e futuro digitale per competere sul mercato

01/02/2022 3024 volta/e

L'interconnessione di macchine e impianti all'IT della fabbrica e a Internet pone la cybersecurity tra le principali sfide del nostro tempo.

12 specialisti raccontano perché la cybersecurity sia una sfida per ogni impresa vincente: i pareri degli esperti Acronis, Aton IT, Ermes, ESA Automation, Fortinet, Kaspersky, Microsoft, Semperis, ServiTecno, Siemens, Trend Micro e Vectra AI.

di Luca Munari

L'interconnessione di macchine e impianti all'IT della fabbrica e a Internet pone la cybersecurity tra le principali sfide del nostro tempo. Quali sono le esperienze e le soluzioni efficaci in ambito industriale per la protezione dalle minacce emergenti? Le imprese che hanno visto aumentare a livello mondiale gli attacchi, con una crescita del 125% nel primo semestre del 2021 rispetto allo stesso periodo del 2020, a quali scenari possono far riferimento per incrementare in sicurezza la Digital Transformation? Ecco il punto di vista di alcuni esperti.

È NECESSARIA PIÙ AUTOMAZIONE

Con la diffusione della pandemia Covid-19, tutti hanno dovuto adattarsi a una routine molto diversa e piena di sfide a cui pochi erano preparati. Questo ha cambiato completamente anche il panorama della sicurezza nel 2021. Ecco tre tendenze che probabilmente definiranno il panorama della cybersecurity nel 2022. Il ransomware è uno dei cyberattacchi più redditizi, al momento. E si espanderà ulteriormente insieme a MacOS e Linux, così come a nuovi ambienti come sistemi virtuali, Cloud e OT/IoT. Tutto ciò che è collegato a una rete raggiungibile è un potenziale bersaglio. Questo porterà sempre più a conseguenze e impatti nel mondo reale, e quindi anche a una maggiore richiesta di regolamenti e sanzioni ufficiali.

Le e-mail malevole e il phishing in tutte le varianti sono ancora ai massimi storici. Non ci aspettiamo che l'AI prenda completamente il sopravvento sulle e-mail di phishing nel 2022, ma ci aspettiamo una maggiore automazione e informazioni personalizzate dalle varie violazioni dei dati, rendendole più efficaci. Nuovi meccanismi contro OAuth e MFA continueranno a generare profitto per gli aggressori, permettendo loro di prendere il controllo degli account, nonostante i piani di aziende come Google di autoiscrivere 150 milioni di utenti alla 2FA. Con il prezzo del Bitcoin ai massimi storici, gli attacchi stanno aumentando e gli utenti finali continueranno a lottare con attacchi di phishing, infostealer e malware. Oltre a questi attacchi, ci aspettiamo di vederne di più contro gli smart contracts direttamente, con attacchi che colpiranno i programmi delle criptovalute. Ci aspettiamo anche che gli attacchi contro le app Web 3.0 saranno più frequenti nel 2022. (*Candid Wüest*, Acronis)

Candid Wüest, VP Cyber Protection Research di Acronis.

I PROCESSI FANNO LA DIFFERENZA

Gli attacchi hacker che colpiscono le aziende crescono con una percentuale a due cifre, al punto di posizionare il nostro Paese al secondo posto in Europa. Solo nel 2020 le aziende colpite da un ransomware sono state il 31%; di queste, il 34% si è vista crittografare i propri dati, perdendone la disponibilità, spessissimo avendoli ancora al loro posto, e di queste ultime il 14% ha pagato il riscatto, sperando di riaverne la disponibilità (The state of ransomware 2021). ATON IT, che pone particolare attenzione alla Business Continuity per garantire il ripristino dei dati in caso di perdita con soluzioni customizzate, pone l'accento sulla necessità di acquisire nuova consapevolezza sui reali livelli di rischio affidandosi ad esperti del settore.

Intervenire in modo strutturato sulle aree aziendali, individuando quali processi attuare per tornare operativi in tempi brevi, diventa fondamentale per la continuità aziendale a tutela del business dell'azienda stessa. In tema di backup dei dati e dei sistemi, ATON IT presenta una soluzione completa basata su tecnologia Acronis, che permette di gestire in modalità Cloud o Private Cloud l'intero servizio di backup e di Disaster Recovery as a Service, pianificando e stratificando i processi di backup direzionandoli sia localmente che su spazi Cloud, direttamente gestiti dal vendor o dal cliente. Sfruttando la tecnologia di Imaging e di Instant Restore di Acronis, è possibile ripristinare l'operatività di un sistema attaccato verificando e garantendo compliant con le policy aziendali, un RPO minimo di 15' e un failover rapido e automatico dell'ambiente di produzione.

La tecnologia, da sola, non basta. Ciò che conta è il pensiero alla base della soluzione tecnologica e il processo di produzione, supporto e commercializzazione. La selezione del partner tecnologico è alla base dei nostri processi aziendali, per garantire ai clienti le migliori soluzioni in termini di servizi e professionalità.

L'esternalizzazione dei processi di cybersecurity verso realtà che fanno di questo il proprio core business è la risposta più efficace a una crescita coordinata e collaborativa tra domanda e offerta nell'industria italiana moderna. (*Alessandro Valenza*, ATON IT)

Alessandro Valenza, Innovation Manager di ATON IT.

GIOCARE D'ANTICIPO

A fronte dell'evolversi del panorama informatico, il perimetro di vulnerabilità a cui le imprese sono esposte si è esteso enormemente e stiamo assistendo a una marcata evoluzione degli attacchi informatici, sia in termini di volumi che di complessità. Se nel passato assistevamo ad attacchi che puntavano a compromettere l'operato aziendale facendo leva sulla vulnerabilità delle sue infrastrutture, oggi puntano con decisione alla risorsa più debole, il dipendente dell'azienda stessa, che rappresenta la via d'ingresso più accessibile per estendere poi l'attacco all'intera organizzazione. Inoltre, attraverso fenomeni come il web tracking, gli hacker conoscono gusti e abitudini dell'utente e quasi sempre anche suoi dati sensibili, potendo costruire così attacchi estremamente mirati e con altissime probabilità di successo.