UniverseIT

www.universeit.blog

La cyber security a prova di PMI: semplicità e integrazione le parole chiave

Garantire la sicurezza informatica di un'azienda sta diventando una vera e propria impresa, tante sono le variabili e le minacce in grado di incidere sulle sorti dei nostri sistemi. Tuttavia, una volta acquisita una adeguata conoscenza dello scenario entro cui siamo chiamati ad agire, esistono alcune soluzioni di sicurezza integrate nelle piattaforme per la produttività, che possono semplificarci notevolmente la vita. A patto di agire con consapevolezza e avvalersi di una consulenza esperta nelle fasi di setup iniziale, affinché tutti i sistemi possano operare nel modo corretto.

Paper 2022

Sommario

Sommario

Cyber security: la difficile impresa di fronteggiare minacce in continua evoluzione

Negli ultimi anni abbiamo assistito ad una vera e propria escalation del crimine informatico, che si traduce nel sensibile aumento di minacce alla cyber sicurezza aziendale, dove un banale errore può spesso causare danni di notevole entità ai sistemi informatici, ai dati ed alla corretta erogazione dei servizi, mettendo, nei casi più gravi, in seria crisi le sorti del business.

Anche qualora l'azienda si dimostrasse sufficientemente solida nel reggere l'urto di un incidente di sicurezza informatica, rimarrebbero da scontare gli effetti indiretti di un possibile danno reputazionale. Non esistono scuse di sorta. Qualsivoglia possa essere la ragione, una realtà che non sa proteggere i propri sistemi, i dati sensibili dei propri clienti e non si dimostra capace a garantire i servizi che promette è destinata ad essere segnata dal marchio dell'inefficienza e dell'inaffidabilità. Un'onta spesso indelebile, o molto difficile da recuperare per un brand, che rischia di fare molto più male del danno economico diretto causato da un attacco.

Se le grandi realtà enterprise sono più esposte ai rischi in termini di sicurezza informatica, queste solitamente vantano un'organizzazione in grado di supportare interamente e in outsourcing le misure necessarie per garantire ai propri sistemi una sicurezza adeguata, sia in termini di prevenzione che di risposta ad un possibile incidente. A partire dalla formazione di un SOC (Security Operation Center) e di un IRT (Incident Response Team), che comportano competenze e risorse spesso al di fuori della portata di una PMI.

Tuttavia, non tutto è perduto. Agendo in maniera consapevole, anche nelle piccole realtà è assolutamente possibile implementare dei fondamentali di sicurezza capaci di adattarsi al continuo variare delle minacce provenienti dalla rete, e non solo. A partire dal 2020 una serie di eventi a livello globale ha creato un terreno molto fertile per il proliferare dell'attività del crimine informatico, incoraggiando moltissimo la sua diffusione.

Pandemia Covid-19: il lavoro in remoto e la fragilità degli endpoint

Nel marzo del 2020 il mondo intero è stato travolto dall'emergenza pandemica del Covid-19, che ha costretto una serie di lockdown, capaci di interrompere bruscamente le tradizionali relazioni per le attività di lavoro, formazione e vita sociale. Da un giorno all'altro, il mondo si è ritrovato a lavorare da casa, senza la possibilità di poter accedere agli uffici.

Questa contingenza ha dato luogo ad almeno due criticità nodali in fatto di sicurezza informatica. Da un lato, il dover garantire dall'esterno l'accesso ai dati presenti sui server aziendali, spesso risolto grazie a VPN o altre modalità di accesso e condivisione attraverso la rete internet. Dall'altro l'evidenza dei fatti, che ha visto i dipendenti lavorare

Cyber Security a prova di PMI

utilizzando dispositivi informatici personali o comunque collocati all'esterno del perimetro di sicurezza aziendale, con tutti i rischi derivati da un utilizzo improprio, in gran parte dovuto alla scarsa cultura in termini di cyber sicurezza. Gli endpoint, quando sprovvisti di adeguati sistemi di sicurezza o utilizzati in modo inopportuno, sono diventati l'anello debole della catena informatica dell'azienda e questo i cyber criminali lo sanno benissimo.

NEL MARZO DEL 2020 IL MONDO INTERO È STATO TRAVOLTO DALL'EMERGENZA PANDEMICA DEL COVID-19, CHE HA COSTRETTO UNA SERIE DI LOCKDOWN, CAPACI DI INTERROMPERE BRUSCAMENTE LE TRADIZIONALI RELAZIONI PER LE ATTIVITÀ DI LAVORO, FORMAZIONE E VITA SOCIALE. DA UN GIORNO ALL'ALTRO, IL MONDO SI È RITROVATO A LAVORARE DA CASA, SENZA LA POSSIBILITÀ DI POTER ACCEDERE AGLI UFFICI.

QUESTA CONTINGENZA HA DATO LUOGO AD ALMENO DUE CRITICITÀ NODALI IN FATTO DI SICUREZZA INFORMATICA.

La trasformazione digitale aumenta fisiologicamente la superficie di attacco

Ancor prima dell'emergenza pandemica, le aziende avevano intrapreso un'azione di innovazione e modernizzazione dei propri processi, ai fini di rinnovare la propria efficienza complessiva e la propria competitività sul mercato. Le conseguenze a livello globale del Covid-19 hanno accelerato una dinamica già in previsione, nota ai più come trasformazione digitale.

Il crescente impiego di soluzioni digitali, sia on-premise che in cloud, sta comportando un sensibile aumento di applicazioni e dispositivi connessi alla rete, che a loro volta costituiscono una vera gallina dalle uova d'oro per i cybercriminali, pronti a colpire con ransomware, phising, esfiltrazione dei dati, furto delle credenziali di accesso ai servizi e molte altre forme ostili alla sicurezza informatica di qualsiasi azienda, a prescindere dalla sua dimensione.

Il cybercrimine è in costante aumento non soltanto per quanto concerne il volume di attività malevolo, ma anche nell'evoluzione dei propri modelli di business. Non è un caso che sul dark web si assista ad una crescente diffusione del Cybercrime-as-a-Service, che prevede ad esempio il noleggio di kit ransomware con cui personalizzare i propri attacchi senza disporre di competenze informatiche molto elevate. Tale dinamica ha consentito una rapida escalation della base criminale, con tutto ciò che ne consegue in termini di sicurezza a livello globale.

Cyber Security a prova di PMI

Geopolitica e tensioni internazionali: l'aumento di tossicità informatica a livello globale

Ad aggravare ulteriormente il pesante quadro fin qui descritto ci pensano le crescenti tensioni a livello internazionale. Il drammatico conflitto tra Russia e Ucraina ha contribuito a portare all'attenzione del gran pubblico una cyberwar che ormai da diversi anni vede una sorta di tutti contro tutti tra i vari stati, continuamente impegnati a finanziare in maniera non ufficiale azioni utili a sabotare infrastrutture, rubare dati ed entrare in possesso di informazioni strategiche delle nazioni avversarie.

Probabilmente vi chiederete cosa possa c'entrare una guerra cibernetica che si gioca tra nazioni in tutt'altro contesto geografico e operativo rispetto alla nostra PMI. Osservazione corretta. E di fatto non vi sarebbe ragione di credere che una nazione possa interessarsi delle sorti di una piccola azienda, se al di fuori delle supply chain legate ai servizi fondamentali e alle infrastrutture critiche. Se non fosse che gli effetti dei continui attacchi alle infrastrutture critiche e alle aziende strategiche nell'economia dei vari paesi producano una quantità impressionante di materiale malevolo, che viene diffuso in rete e diventa capace di colpire praticamente chiunque. Questo vale soprattutto per quanto concerne la minaccia del nemico pubblico numero uno: il ransomware, con gli annessi cryptolocker, in grado di paralizzare le organizzazioni nell'utilizzo di dati e sistemi.

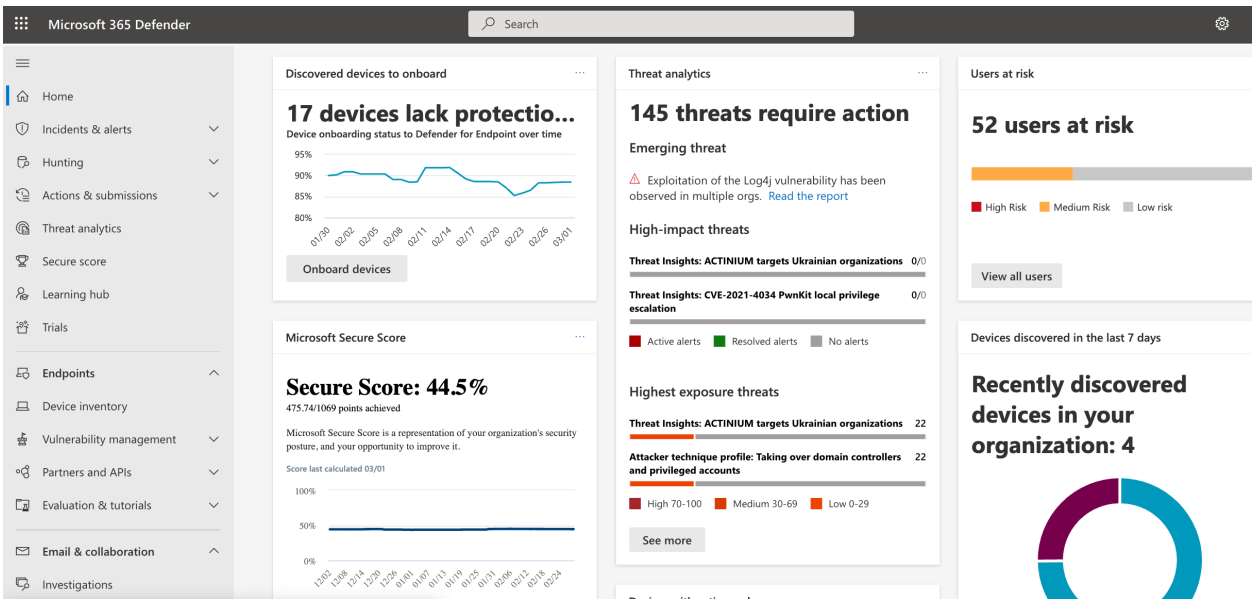
GLI EFFETTI COLLATERALI DELLE CYBERWAR COSTITUISCONO UNA ULTERIORE MINACCIA PER LE AZIENDE, CHE NESSUNO PUÒ PERMETTERSI IN ALCUN MODO DI SOTTOVALUTARE.

Cyber Security a prova di PMI

Una soluzione semplice e integrata: Microsoft Security Center (Microsoft 365 Defender)

In un contesto che vede una grandissima varietà di minacce all'orizzonte, pronte a colpire approfittando di una falla anche minima ai sistemi di sicurezza, la difficoltà maggiore per un dirigente d'azienda è capire da dove iniziare. Si tratta di una situazione molto diffusa ed assolutamente comprensibile, in quanto la situazione a cui far fronte non è oggettivamente semplice da inquadrare, ancor prima che da gestire.

Chi ha già subito una minaccia informatica o chi non l'ha ancora subita, ma sta semplicemente cercando di approfondirne il contesto per non farsi trovare impreparato, sarà sicuramente stato bombardato da un ventaglio di opzioni e soluzioni, tutte valide e per certi versi indispensabili. Le tradizionali soluzioni "legacy" come Antivirus, Antispam e Firewall sono oggi inefficaci per fronteggiare le nuove tipologie di attacco informatico nel contesto aziendale e sono state sostituite o affiancate da nuove soluzioni come: Endpoint Detection & Response, Anti-phishing, Threat Intelligence, Vulnerability Scan, Security Awareness, la cui terminologia sta diventando di uso comune. È evidente come, soprattutto per una PMI, non sia immediato orientarsi in questo ventaglio di tecnicismi.



L'interfaccia principale di Microsoft 365 Defender riepiloga le news e i principali alert, per offrire una visibilità generale dei sistemi aziendali in termini di sicurezza informatica.

Cyber Security a prova di PMI

Per far fronte a questa esigenza diffusa, le piattaforme di produttività integrano sempre più spesso soluzioni di cybersecurity che consentono di automatizzare un'ampia varietà di situazioni, che finiscono per diventare il miglior alleato per proteggere le infrastrutture IT della piccola e media impresa italiana.

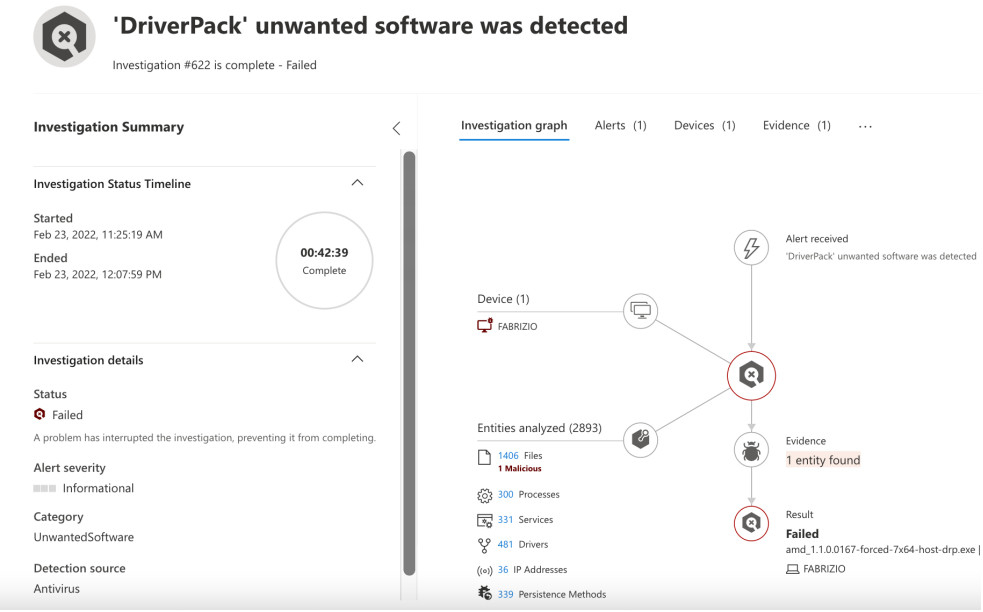
Tali soluzioni spesso non sono note ai più, vengono enfatizzate molto meno rispetto alle piattaforme principali, eppure si rivelano strumenti di straordinaria efficienza, soprattutto in termini di semplicità d'uso. È il caso di Microsoft Security Center, da qualche tempo integrato in Microsoft 365, in cui si configura quale modulo opzionale.

Microsoft Security Center, di recente rinominato Microsoft 365 Defender, consente di gestire una vasta serie di funzionalità specifiche per la sicurezza informatica, attraverso una dashboard semplice ed intuitiva, accessibile anche per chi non possiede competenze specialistiche in maniera di sicurezza.

Endpoint Security: la sicurezza in tempo reale di dispositivi client e server

La protezione degli endpoint rappresenta il punto nodale di qualsiasi strategia di cybersicurezza aziendale. La scansione e il rilevamento in tempo reale di vulnerabilità e minacce consentono un adeguato livello di protezione, compensando anche qualche errore di condotta da parte degli utenti. Microsoft Defender offre le funzionalità di quello che in ambito consumer è da tempo noto come software antivirus e nel contesto enterprise è ormai più frequente annoverare quale EDR (Endpoint Detection and Response).

Microsoft Security Center riesce a generare automaticamente la lista degli endpoint connessi, con tutti i dati relativi agli utenti, all'attività, rilevando la presenza di possibili minacce, a loro volta categorizzate secondo un criterio di potenziale criticità.



Microsoft Security Center consente di ricostruire in modo analitico la kill-chain di un attacco. Grazie a funzionalità avanzate di monitoraggio e prevenzione è possibile ricostruire l'esatta sequenza delle azioni rilevate nel contesto di un incidente o di un evento sospetto.

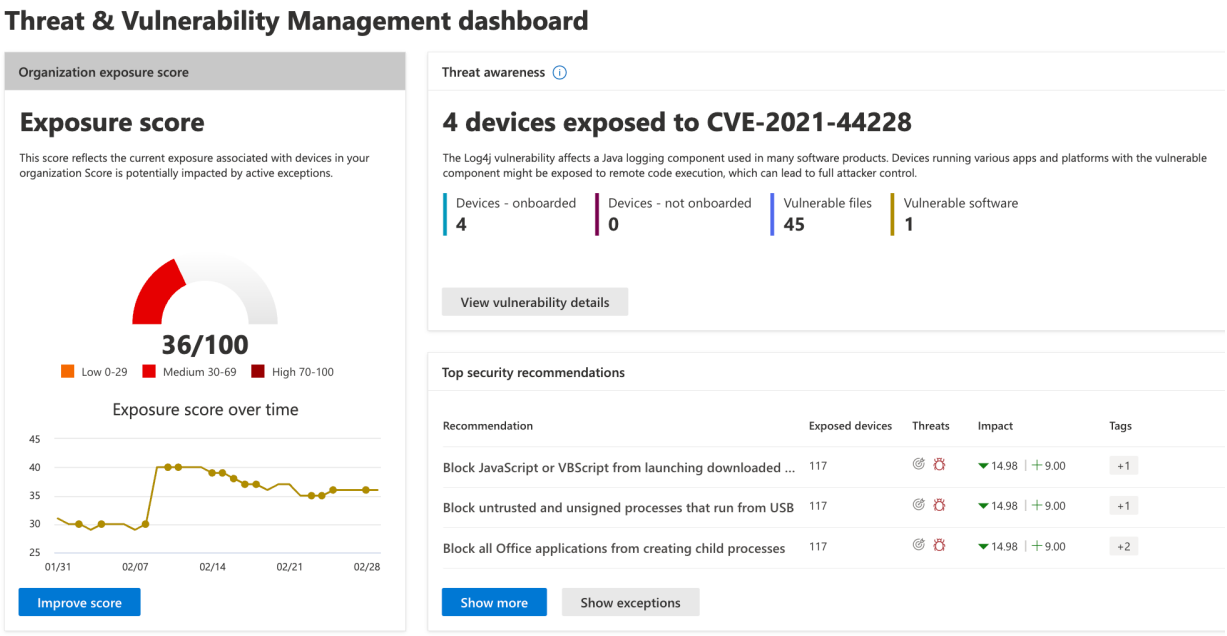
Cyber Security a prova di PMI

Email Security: come difendersi da link e allegati pericolosi

Le mail continuano a costituire uno dei principali vettori per le infezioni virali e il furto di dati di accesso ai servizi. Un clic nel punto sbagliato consente infatti ai vari malware di penetrare in maniera pressoché indisturbata di penetrare all'interno dei sistemi aziendali. Allo stesso modo, gli utenti possono rimanere vittima di attacchi phising sempre più sofisticati. Microsoft Security Center consente di effettuare un'analisi approfondita delle attività di Exchange e del traffico lato client, controllando la presenza di allegati e codice potenzialmente dannosi.

Threat & Vulnerability Management: come individuare le vulnerabilità della rete

Le vulnerabilità di rete costituiscono una delle opportunità più ghiotte per un cybercriminale interessato ad infiltrarsi all'interno del perimetro di sicurezza informatico di un'azienda. Microsoft Security Center è in grado di effettuare un semplice vulnerability assessment della rete aziendale, notevolmente automatizzato ed in grado di garantire un ottimo livello di dettaglio, soprattutto per quanto concerne le esigenze di una PMI.



Il risultato di una scansione eseguita da Microsoft Security Center sui device presenti nella rete aziendale. In automatico vengono rilevate le possibilità criticità, con una descrizione sintetica della minaccia e indicazioni sulla magnitudo.

Cyber Security a prova di PMI

Threat Intelligence: conoscere la propria esposizione rispetto alle minacce globali

Microsoft Security Center è in grado di automatizzare una serie di funzioni che coincidono con la threat intelligence, una disciplina che consiste nel raccogliere informazioni utili a prevenire gli attacchi informatici, per strutturare ed affinare le strategie difensive. Si tratta di un processo basato in particolar modo su conoscenza e strategia, perfettamente funzionale a piccole e medie realtà come le PMI.

Microsoft Security Center offre ad esempio un servizio costantemente aggiornato in merito alle principali minacce attive a livello globale, con notizie ed approfondimenti che rimandano all'approfondita letteratura sull'argomento presente sui vari portali e blog di sicurezza di Microsoft. Tale rassegna consente anche al personale non altamente specializzato di essere al corrente delle attività malevole più rilevanti e diffuse, in modo da formare una cultura e un sentimento pratico nei confronti delle minacce alla sicurezza informatica che potrebbero colpire l'azienda.

Security Awareness & Attack Simulation: educare gli utenti a difendersi al meglio

Microsoft Security Center consente di svolgere delle simulazioni di attacco nei confronti delle vulnerabilità individuate nella rete, ai fini di preventivare le modalità che gli attaccanti potrebbero utilizzare per penetrare all'interno del perimetro di sicurezza informatico delle aziende. Anche in questo caso, una semplice soluzione integrata consente di svolgere un servizio solitamente demandato ad operazioni ben più complesse ed onerose.

Il riepilogo di una simulazione di attacco condotta da Microsoft Security Center: un momento essenziale per aumentare la consapevolezza del personale senza rischiare alcun danno effettivo sui propri sistemi (credit: Microsoft)

Cyber Security a prova di PMI

Threat Hunting: analisi avanzata e investigazione forense

Il threat hunting è una disciplina fondamentale nell'ambito della cybersecurity, che utilizza un approccio proattivo nel combinare tecnologie ed attività di threat intelligence per individuare e bloccare attività malevoli all'interno della rete aziendale.

Microsoft Security Center, grazie alla sua elevate visibilità nei confronti dei processi e dei device attivi riesce ad individuare facilmente eventuali attacchi, notificandoli e/o bloccandoli prima che siano in grado di estendere al propria minaccia al punto da provocare danni seri al sistema. Molto spesso gli attaccanti nascondono la loro presenza all'interno delle macchine strategicamente più rilevanti, per esfiltrare dati o preparare la fase manifesta della loro offensiva.

Il threat hunting corrisponde ad una fase decisamente impegnativa nelle attività di cybersicurezza aziendale. La capacità di svolgere I presupposti fondamentali grazie ad una suite di sicurezza integrata costituisce un vantaggio significativo sia in termini economici che organizzativi.

UNA BUONA INVESTIGAZIONE DI BASE DA PARTE DEL PERSONALE IN-HOUSE CONSENTE DI COLLABORARE IN OUTSOURCING CON PERSONALE ALTAMENTE SPECIALIZZATO SOLTANTO QUALORA VENISSE RILEVATO UN PROBLEMA DI COMPLESSA SOLUZIONE, COME LA PRESENZA ALL'INTERNO DELLA RETE DI UN'ATTACCANTE CHE SI SOSPETTA ESSERE MOLTO PERICOLOSO.

SIEM (Security Information and Event Management): monitoraggio e correlazione di tutti gli eventi di sicurezza in azienda

Tra le funzioni più apprezzate di Microsoft Security Center vi è l'integrazione con Microsoft Sentinel, che agisce come un semplice ma efficace SIEM (Security Information and Event Management), ossia uno strumento in grado di centralizzare la raccolta e la gestione di tutti i log relativi alla rete, agli endpoint e agli applicativi eseguiti sui sistemi aziendali, ai fini di poterli analizzare in tempo reale per rilevare minacce o comportamenti sospetti.

L'impiego di Microsoft Security Center consente pertanto di avere a disposizione il monitoraggio di un SIEM senza dover in primo luogo ricorrere a soluzioni complesse o gestite da remoto da servizi altamente specializzati. I moderni IDS (Intrusion Detection Systems), fondamentali per l'attività dei SIEM, sono in grado di effettuare un'analisi comportamentale attraverso l'analisi dei log. Ciò è ad esempio molto utile per rilevare delle anomalie macroscopiche, come una macchina che tenta di accedere ad un server senza averne motivo o in orari incompatibili con le operazioni prefissate.

Cyber Security a prova di PMI

Un licensing su misura per le PMI e servizi di consulenza accessibili

Il capitolo costi di una soluzione come Microsoft Security Center costituisce uno degli aspetti più interessanti, soprattutto per quelle PMI che intendono strutturarsi a livello di cybersicurezza, pur non avendo a disposizione le risorse e le competenze interne necessarie per assicurarsi le soluzioni di mercato leader in ogni applicazione verticale.

Esso risulta compreso con alcuni piani di Microsoft 365 o è comunque acquistabile quale modulo aggiuntivo a pochi euro ad utente al mese. Ciò costituisce un interessante vantaggio strategico per valutare una suite di sicurezza informatica che, all'atto pratico, è in grado di risolvere con successo le esigenze operative in termini di sicurezza della maggior parte delle PMI. Chi attualmente dispone delle soluzioni Business o Enterprise potrebbe avere già inclusi nei propri piani parte di questi servizi, dovendo nel caso semplicemente abilitarli.

UNA CARATTERISTICA ESSENZIALE DI UNA SOLUZIONE INTEGRATA COME MICROSOFT SECURITY CENTER È DATA DALLA SUA DISPONIBILITÀ IN CLOUD. TUTTO FUNZIONA SENZA DOVER INSTALLARE ASSOLUTAMENTE NULLA IN LOCALE E SUI VARI DISPOSITIVI. È SUFFICIENTE LOGGARSI DA REMOTO IN MICROSOFT 365 ADMIN CENTER PER POTER GESTIRE OGNI FUNZIONE DELLA SUITE DI SICUREZZA.

La semplicità d'uso di Microsoft Security Center ne consente la gestione anche al personale IT in-house non dotato di una formazione specialistica nell'ambito della cybersicurezza. Nel caso in cui tali competenze non fossero disponibili all'interno dell'azienda, è decisamente auspicabile avvalersi di una consulenza esterna soprattutto nelle fasi di setup iniziale, in modo da accertarsi che l'aggregazione di tutte le risorse coinvolte avvenga in maniera corretta, affinché Microsoft Security Center possa garantire la visibilità in tempo reale che ci attende dal monitoraggio della rete, degli endpoint e degli applicativi aziendali.

L’impatto positivo dei casi di utilizzo di Microsoft Security Center: tra problemi risolti e una crescente fiducia nei sistemi di sicurezza integrati

Grazie ad una piattaforma di sicurezza le aziende possono in breve tempo toccare con mano alcuni dei vantaggi più evidenti di una soluzione di cybersecurity cloud based come Microsoft Security Center.

La prima parola chiave è visibilità. Grazie ad un sistema integrato, è possibile mappare tutti gli endpoint client e server attivi nella rete aziendale. Detto così, potrebbe apparire banale, ma conoscere con precisione la costituzione del parco macchine di un’azienda attiva da diversi anni diventa un’operazione tutt’altro che scontata, che oggi può essere risolta in maniera quasi del tutto automatica.

La visibilità si esprime anche nella conoscenza in tempo reale dei processi attivi sui vari dispositivi, aggregando una serie di informazioni decisamente utili e di facile lettura, disponibili attraverso report e insight, per aiutare i CIO e i dirigenti a prendere decisioni più consapevoli in una materia naturalmente complessa come la sicurezza informatica. Un decisore potrà ragionevolmente dedicare e giustificare un budget per la cybersecurity, se conosce nel dettaglio i vantaggi concreti che ne derivano.

Una funzione particolarmente utile di Microsoft Security Center è il modo con cui effettua la scansione degli endpoint. La conoscenza delle minacce presenti sui dispositivi è infatti categorizzata secondo criteri di criticità. La valutazione del rischio costituisce un elemento essenziale anche dal punto di vista psicologico, onde evitare di entrare nel panico di fronte ad un alert indistinto. Il sistema è in grado di indicare quali sono i fattori di a cui è necessario dedicare un’attenzione elevata, a fronte di altri meno prioritari, in funzione di una minor nocività della minaccia o di una bassa probabilità che si verifichi un vero e proprio incidente.

Cyber Security a prova di PMI

La tecnologia è solo una parte del problema: il ruolo della formazione della cultura della sicurezza in azienda

Una soluzione di sicurezza integrata come Microsoft Security Center rappresenta una formidabile opportunità per dotare le PMI di una strumentazione adeguata in materia di cybersicurezza. Tuttavia, nemmeno se prendessimo, funzione per funzione, la più evoluta risposta presente sul mercato, riusciremmo a garantire la totale sicurezza soltanto grazie al software.

NON DOBBIAMO MAI DIMENTICARE CHE I PRINCIPALI ATTORI DELLA SICUREZZA INFORMATICA IN AZIENDA SONO LE PERSONE. GARANTIRE AI DIPENDENTI UN'ADEGUATA FORMAZIONE IN FATTO DI CYBERSECURITY NON SI LIMITA ALL'APPRENDIMENTO DELLE FEATURE DI UN SOFTWARE O ALLE MODALITÀ CON CUI VA UTILIZZATO UN DETERMINATO ENDPOINT. OCCORRE PARTIRE DAL MINDSET.

È necessario capire le logiche che determinano la governance dei dati in condizioni ragionevolmente sicure, onde scongiurare i grossolani errori di condotta che potrebbero vanificare, in certi casi, anche gli sforzi delle più efficienti soluzioni di sicurezza aziendale.

Tali meccanismi devono diventare innati, nel contesto di una formazione continua, che si svolge in gran parte grazie ad un atteggiamento collaborativo, in cui ogni figura va coinvolta e responsabilizzata nella maniera più opportuna.