White Paper

I motivi degli attacchi alle PMI

Come farsi odiare dai cybercriminali in 6 semplici mosse 2

Un problema che cresce ... 2
L'egalitarismo del cybercrimine ... 3
Sotto attacco da ogni direzione ... 3
Cybercrimine, conoscerlo per evitarlo ... 4
Il lato oscuro dei superpoteri ... 5
Aggiornarsi è la prima regola per sopravvivere ... 5
Mettici una parola buona ... 6

Glossario 7

Come farsi odiare dai cybercriminali in 6 semplici mosse

Oggi si parla tanto di **trasformazione digitale** e di **aziende digitalizzate**: un obiettivo verso il quale una PMI lungimirante dovrebbe puntare indipendentemente dal settore di attività e dalle dimensioni. Si tratta di un'evoluzione nell'impiego delle risorse informatiche che porta con sé indiscutibili vantaggi come maggiore flessibilità, ottimizzazione del lavoro e dei costi, integrazione delle catene produttive e commerciali, persino la dematerializzazione degli uffici come abbiamo potuto constatare nel corso della pandemia.

Insomma, potremmo dire che se fino a oggi abbiamo inserito l'informatica nelle nostre attività tradizionali un pezzo per volta per cercare di tenere il passo con la modernizzazione, ora è arrivato il momento di voltare pagina e diventare realtà "digital-first" nelle quali, per l'appunto, l'IT diventa il cuore e il cervello da cui ogni processo dipende a cascata.

La vita digitale delle PMI non è tuttavia immune dai rischi che questa epoca ci ha ormai abituato a dover affrontare. La **diffusione degli attacchi informatici** è andata crescendo negli anni fino a diventare un pericolo endemico di fronte al quale dobbiamo ragionare in termini di "quando sarò colpito" e non più di "se sarò colpito".

La trasformazione digitale significa anche questo: **saper vivere nel mondo virtuale** adottando i medesimi accorgimenti che siamo abituati a utilizzare nel mondo reale. Come non lasceresti mai la tua azienda con le porte aperte, i documenti critici in bella vista e il magazzino privo di qualunque antifurto, allo stesso modo è ora che applichi ragionamenti simili al tuo patrimonio informatico – dagli strumenti hardware alle applicazioni software fino ai dati e alle informazioni che, come tutti ormai giustamente ripetono, costituiscono "l'oro nero del XXI secolo".

Un problema che cresce

L'arrivo degli Anni Venti sarà ricordato per l'aumento esponenziale degli **attacchi ransomware** scatenati contro enti pubblici, organizzazioni e aziende di ogni tipo. Il tema è ormai ospite fisso dei media generalisti: avrai letto o sentito parlare tante volte di un ospedale, una banca o un'impresa di qualche genere che deve interrompere le proprie attività perché ha perso il controllo dei sistemi IT. Funziona così: un dipendente clicca su un allegato o un link studiato in modo tale da aprire la strada a codice malevolo che si innesta su PC e server allo scopo di crittografare (quindi rendere inutilizzabili) tutti i dati che vi trova, chiedendo quindi un riscatto in cambio della chiave di decifrazione necessaria a rendere nuovamente accessibili le informazioni.

Qualche vittima paga, per poi scoprire talvolta che la chiave di decifrazione non funziona o che il cybercriminale **scompare non appena ricevuti i soldi**; qualcun altro preferisce invece ripristinare l'intero ambiente IT dall'ultimo backup sicuro disponibile, attività che può richiedere anche settimane di tempo e che comporta sempre un certo **livello di rischio**.

Il fatto che sui media si parli di questo fenomeno solo quando colpisce realtà importanti come Trenitalia[1], l'Università di Pisa[2] o il sistema sanitario della Regione Lazio[3] non deve però trarti in inganno facendoti credere che il problema sia circoscritto solamente a vittime di un certo rilievo. Tutti sono infatti a rischio, tant'è vero che l'Italia è il terzo Paese al mondo per attacchi ransomware verificati[4] e ha addirittura conquistato, nel marzo 2022, il poco invidiabile primato di nazione europea maggiormente colpita[5].

A questo bisogna poi aggiungere il fatto che il ransomware è solo **uno dei numerosi tasselli di un puzzle informatico criminale** che comprende attività come spionaggio industriale, sottrazione di informazioni bancarie, impersonificazioni fraudolente, controllo di reti di computer per ulteriori attività illecite e così via. Una quantità di golose occasioni di guadagno per bande di personaggi senza scrupoli che esercitano una pressione sempre più forte sulle difese informatiche di tutti noi – e che purtroppo, numeri alla mano, dimostrano di non essere all'altezza della situazione.

1 Panorama, Trenitalia colpita da Hive Group, biglietterie ko per un ransomware, 2022
2 Cybersecurity360, Università di Pisa vittima di ransomware, pubblicati dati riservati, chiesto riscatto milionario, 2022
3 IlSole24ore, Attacco hacker alla Regione Lazio, indaga anche l'antiterrorismo, 2021
4 IlSole24ore, Italia sotto attacco hacker, ma mancano 100mila esperti di cyber security, 2022
5 SecurityOpenLab, Italia prima in Europa per attacchi ransomware, 2022

Tutto ciò non accade per caso, bensì per una scarsa diffusione culturale delle buone pratiche IT. Da noi la rivoluzione digitale è forse avvenuta troppo velocemente e disordinatamente per le nostre abitudini, e ora ne stiamo pagando il prezzo.

Tuttavia non è mai troppo tardi per darsi una bella svegliata e adottare alcuni semplici ma efficaci accorgimenti che possono renderci agli occhi dei cybercriminali un osso più duro del previsto e quindi non meritevole di ulteriori "attenzioni" che potranno essere rivolte con maggiori probabilità di successo verso bersagli più malleabili e impreparati.

Il primo passo è quello di **conoscere i punti deboli delle PMI** maggiormente diffusi e sfruttati dai cybercriminali. Una volta acquisita la consapevolezza degli errori che si compiono, avrai la chiave per chiudere fuori dall'IT aziendale coloro che non aspettano altro che colpirti.

L'egalitarismo del cybercrimine

Un errore che ti può costare molto caro è quello di **convincerti di essere immune** al problema perché ritieni che la tua attività non sia sufficientemente grande, famosa e potenzialmente remunerativa da giustificare lo sforzo di un attacco mirato. Questo atteggiamento, oltre a essere favorito dal fatto che i media comprensibilmente parlano dei cyberattacchi solo quando riguardano realtà note al pubblico, è legato al vecchio modo di lavorare "artigianale" dei pirati informatici, che un tempo si muovevano selezionando con cura la potenziale vittima per poi studiarla e, se possibile, colpirla con metodi ad hoc.

Oggi invece, come una vera azienda, il cybercrimine è un'attività economica su vasta scala che ottimizza tempo, lavoro e redditività automatizzando più possibile i vari passaggi operativi affidandoli sempre più spesso a squadre che si specializzano su specifiche fasi: ricerca delle vulnerabilità e produzione di codice pericoloso, diffusione del malware, gestione finanziaria e riciclaggio, commercializzazione su vasta scala di informazioni e accessi, e via dicendo.

Automazione e grandi numeri hanno una conseguenza che ti riguarda molto da vicino: nella maggior parte dei casi, infatti, i cybercriminali non selezionano più le loro vittime una per una, bensì "pescano a strascico" nell'infinito oceano di Internet con sistemi che iniettano automaticamente il codice malevolo negli ambienti IT di chiunque, per distrazione o leggerezza, abbocchi all'amo.

Una campagna di cyberattacchi quindi **non guarda in faccia a nessuno**. La tua azienda può essere grande o piccola, di successo o in difficoltà, ma la vera differenza la fanno l'atteggiamento prudente di chi ci lavora e il continuo processo di rafforzamento delle tecnologie di difesa.

Le tecniche delle cybergang si evolvono infatti senza sosta, da un lato inventando nuovi approcci creativi per aggirare e raggirare le potenziali vittime, dall'altro studiando le vulnerabilità di sistemi operativi e applicazioni per trovare nuovi varchi sconosciuti da sfruttare per entrare negli ambienti IT altrui.

Per questo motivo non puoi pretendere di installare una soluzione per la sicurezza informatica e poi disinteressartene cullandoti in un falso senso di protezione. **La cybersicurezza cambia per rispondere a tipologie di attacco sempre nuove**, quindi è buona norma mantenersi aggiornati su quanto offre il mercato compatibilmente con il tipo di ambiente che possiedi e il budget che puoi dedicarvi, integrando di volta in volta quanto necessario o addirittura sostituendo le vecchie soluzioni quando ciò rappresenta la scelta più opportuna.

Suggerimento #1 – Chiediti sempre: come si sta evolvendo lo scenario della cybersicurezza? C'è qualcosa che posso fare in più per rafforzare le mie difese?

Sotto attacco da ogni direzione

Parliamo costantemente di cybercriminali e il nostro pensiero va automaticamente a loschi figuri incappucciati che smanettano alla tastiera da chissà quale remoto anfratto facendo perdere le loro tracce nei meandri di Internet. È un'immagine del tutto comune, un cliché favorito dal racconto dei media e da una certa cinematografia da un tanto al chilo, che rischia però di distrarre l'attenzione dalla realtà.

E la realtà ci dice che oltre un quinto degli attacchi[6] trova origine **all'interno delle stesse aziende**. Si tratta di personale, ex dipendenti, consulenti e fornitori che si rendono responsabili (anche se nella maggior parte dei casi in modo inconsapevole) di violazioni alla sicurezza e sottrazioni di dati sensibili.

Le motivazioni sono le più disparate: nei casi di involontarietà la causa va fatta risalire a disattenzione e scarsa consapevolezza, altrimenti la molla può essere sete di guadagno, spionaggio industriale, vendetta, persino attivismo politico (il cosiddetto *hacktivism*).

Anche in quest'ultimo caso commetteresti un errore a sottovalutare il potenziale problema pensando che non riguardi la tua attività, dal momento che l'ambiente IT della tua azienda può essere sempre usato per colpire indirettamente imprese, enti e organizzazioni con cui sei in rapporti. È la strategia di **sfruttare l'anello debole di una catena** per arrivare al vero obiettivo dell'attacco.

Questo significa che non puoi più considerare la cybersicurezza come se si trattasse di erigere un bastione virtuale al di fuori del quale stanno i cattivi mentre all'interno ci sono solamente i buoni. La realtà è che oggi non c'è più un "dentro" e un "fuori", e che anche il collaboratore più fidato può provocare danni di vasta portata – a maggior ragione in un'epoca in cui ormai è assolutamente comune lavorare all'esterno del rassicurante perimetro dell'ufficio, magari con computer e dispositivi personali che sono al di fuori del controllo dell'IT aziendale tradizionale.

La situazione si affronta in un solo modo: **sensibilizzando il personale** affinché operi sempre con attenzione evitando leggerezze e distrazioni, certo, ma anche facendo in modo che l'apparato di cybersicurezza di cui disponi **tenga sotto controllo ogni attività e ogni flusso di traffico** indipendentemente dall'origine.

Suggerimento #2 – Affronta il tema della cybersicurezza a 360 gradi evitando di lasciare singole sacche di immunità che potrebbero poi ritorcersi contro di te quando meno te lo aspetti.

Cybercrimine, conoscerlo per evitarlo

Abbiamo appena visto come una porzione significativa delle violazioni di sicurezza trovi origine all'interno delle aziende stesse. Le statistiche ci offrono un ulteriore dato su cui riflettere: il 60% degli attacchi di origine interna[7] è provocato infatti da semplice negligenza, il che significa mancanza di formazione e scarsa sensibilizzazione nei confronti della sicurezza.

Quando **concedi a un collaboratore l'accesso** al tuo sistema informatico lo rendi indubbiamente produttivo – difficile oggi svolgere il proprio lavoro restando isolati dall'ambiente IT – a patto che sia stato adeguatamente addestrato per adoperarlo nel modo corretto e con le dovute attenzioni. In caso contrario ti stai portando a casa un rischio direttamente proporzionale alla quantità di autorizzazioni e privilegi assegnati a quell'utente e alla importanza dei dati e delle applicazioni a cui è in grado di accedere.

Ricordati che i cybercriminali fanno sempre **affidamento sull'atteggiamento sbadato e disattento** delle loro potenziali vittime. Una piccola distrazione non è magari sufficiente a provocare problemi irreparabili, ma sommandosi a tante altre piccole distrazioni quotidiane può offrire a un malintenzionato l'appiglio necessario per violare con successo i tuoi sistemi informatici.

C'è poi un'altra questione che viene spesso sottovalutata o addirittura ignorata, ed è quella che riguarda la **capacità del personale stesso di contribuire alla difesa** dell'ambiente IT aziendale. La cosa funziona in questo modo: ogni tentativo di intrusione o di attacco provoca un'alterazione della routine quotidiana legata ai sistemi informativi. Può trattarsi di un fenomeno appariscente come un'improvvisa campagna di phishing altamente mirata piuttosto che di segnali più soft come un rallentamento dei tempi di risposta di un database, qualche insolito errore di accesso, una macchina che svolge un'attività imprevista in un orario insolito o in modo scoordinato dai sistemi da cui dipende.

In ogni caso, si tratta di qualcosa che un occhio attento può aiutare a evidenziare contribuendo a bloccare l'attacco nelle sue fasi iniziali. Per farlo, tuttavia, occorre che il personale venga formato e sensibilizzato in modo da rilevare questi avvenimenti insoliti. È un passo in più rispetto al normale addestramento all'utilizzo

6 Forbes, The Frontline Is Your First Line Against Insider Threats, 2021

7 Ponemon, 2018 State of Cybersecurity in Small & Medium Size Businesses

dei sistemi informativi, ma può essere un'arma segreta di grande efficacia nella continua sfida lanciata dai cybercriminali.

Suggerimento #3 – Dedica regolarmente tempo e risorse a formare, aggiornare e sensibilizzare i tuoi dipendenti sull'uso dei sistemi IT anche al di là dello stretto ambito operativo dei singoli.

Il lato oscuro dei superpoteri

La sicurezza impone oggi che non vi sia sistema che possa essere adoperato senza credenziali che identifichino l'utente. E una volta identificato, l'utente viene ammesso a fare o meno determinate attività sulla base del suo profilo individuale. Detto in altre parole: ogni utente si trascina una serie di autorizzazioni che dipendono dall'attività e dalle responsabilità di ciascuno.

La **corretta gestione dei profili individuali** è uno dei pilastri che permettono di configurare e mantenere adeguatamente un ambiente informatico. Tuttavia non è raro imbattersi in casi in cui le regole di accesso vengano scavalcate affidando a un determinato utente una serie di permessi supplementari rispetto a quelli a cui avrebbe normalmente diritto.

Questo può avvenire per diversi motivi quando i tecnici preposti non hanno il tempo (o le competenze) per affrontare correttamente la richiesta urgente di un utente che deve effettuare un'attività insolita, magari in sostituzione di un collega o per poter aggirare errori o limitazioni di un'applicazione. Per comodità si finisce con l'attribuire privilegi di accesso **superiori al necessario**, spesso dimenticandosi di ripristinare il livello di autorizzazione corretto una volta conclusa l'emergenza.

Scorciatoie del genere sono quanto di più pericoloso si possa fare in un ambiente IT. Un utente che si ritrovi di colpo con privilegi più elevati del solito potrebbe involontariamente provocare danni incalcolabili perché non conosce le procedure che regolano i maggiori poteri affidatigli, senza considerare che qualsiasi errore compiuto alla tastiera ha ovviamente un impatto tanto più ampio e profondo quanto più estesi sono i diritti concessi all'utente.

Occorre ricordare anche come un utente ad alte credenziali sia la vittima preferita di qualsiasi cybercriminale: un conto infatti è colpire con malware o virus qualcuno che lavora al computer con possibilità operative minime, altra cosa invece quando lo stesso accade a un utente che gode di privilegi superiori.

Il codice malevolo infatti "gira" all'interno delle macchine con lo stesso livello di autorizzazioni dell'utente che ne è stato infettato consentendone l'ingresso; per questo motivo si adotta generalmente il principio per cui a ogni utente vengono concessi sempre e solo i diritti minimi necessari affinché possa svolgere il proprio lavoro. Meno sono i privilegi concessi, minore è la superficie di attacco esposta ai malintenzionati.

Suggerimento #4 - Oltre a sensibilizzare il tuo personale su questo argomento, fai eseguire verifiche periodiche sui privilegi di accesso di tutti gli utenti, compreso tu stesso.

Aggiornarsi è la prima regola per sopravvivere

Se usi un qualsiasi dispositivo digitale, che sia un PC piuttosto che uno smartphone, conoscerai bene quegli avvisi che di tanto in tanto compaiono per suggerirti – no, a volte sembra quasi per ordinarti – di eseguire gli aggiornamenti disponibili per il sistema e le applicazioni.

È vero, le **procedure di aggiornamento** sono una noia: lo scaricamento dei pacchetti influisce sulla velocità della rete e la successiva installazione fa rallentare la macchina e di conseguenza il lavoro, per non parlare della necessità di dover spegnere e riavviare il sistema (magari più volte) per completare tutta la sequenza. Sempre che il sistema riparta correttamente senza brutte sorprese perché magari l'ultimo aggiornamento ha introdotto qualche incompatibilità hardware o software che costringe a sospendere il lavoro che si stava facendo – il lavoro vero, quello produttivo – per cercare di capire come aggirare il problema o ripristinare la macchina a una situazione regolarmente funzionante.

Ti sbagli di grosso però se pensi che la soluzione migliore per evitare tutto questo sia quella di ignorare gli aggiornamenti e dare retta al proverbio "se funziona, non c'è motivo di cambiarlo". Infatti gli aggiornamenti non vengono rilasciati per un capriccio o per una strategia di marketing delle software house, bensì sono una parte fondamentale del lavoro di costante miglioramento dei prodotti per aggiungervi ulteriori funzionalità. Soprattutto, però, neutralizzano le vulnerabilità che man mano vengono scoperte dagli sviluppatori o dagli stessi utilizzatori.

Inutile dirlo, le vulnerabilità sono oro per i cybercriminali perché, adeguatamente sfruttate, rappresentano il varco di accesso ad applicazioni, sistemi e reti. Quindi, se vuoi che il tuo ambiente non venga regolarmente violato con facilità, una strategia di aggiornamenti ben studiata può aiutarti a svolgere questa essenziale attività minimizzando nel contempo le interruzioni, i rallentamenti e gli imprevisti che possono sempre esserci.

Oggi esistono in commercio **soluzioni che possono automatizzare** le procedure di aggiornamento intervenendo quando più opportuno (per esempio quando il carico di lavoro è minore e il traffico di rete più scarso o assente, in genere di notte o nei week-end) e addirittura simularle preventivamente così da evitare incompatibilità inaspettate.

Suggerimento #5 - Inizia con un censimento di tutti i tuoi sistemi e dispositivi, poi predisponi un piano di aggiornamenti regolari: è la prima linea di difesa contro i malintenzionati.

Mettici una parola buona

I dati aggiornati al 2022 ci dicono che nel **Dark Web**, quella sorta di web nascosto nel quale sguazzano criminali di ogni tipo, cyber e no, **sono in vendita 24,6 miliardi di credenziali**[8] con un incremento del 64% rispetto al 2020. Sono informazioni frutto di una lunga serie di violazioni di siti e database che periodicamente colpiscono organizzazioni grandi e piccole: siti e-commerce, portali web, servizi online, aziende tradizionali, università, ospedali, enti pubblici e via dicendo.

Ma se le vittime di queste violazioni provvedono a resettare immediatamente tutte le password dei loro clienti e utenti non appena si accorgono della sottrazione delle credenziali, il problema permane per tutti coloro (e non sono pochi) che per comodità tendono a riutilizzare più volte la stessa coppia nome utente / password su più siti e servizi differenti.

I cybercriminali infatti hanno sviluppato da tempo dei semplici programmi che tentano di forzare automaticamente l'accesso ai siti desiderati semplicemente **provando tutte le credenziali** rastrellate altrove facendo proprio leva sulla pigrizia di chi le ricicla più volte.

Ma non è tutto: le analisi che periodicamente vengono svolte su questi stessi dati dagli specialisti in sicurezza confermano anno dopo anno la malsana tendenza delle persone a usare **password molto semplici** ("abcdef", "123456", "password", "qwerty" sono solo alcuni esempi) o comunque facilmente indovinabili.

Ecco, la tua attenzione dovrebbe essere rivolta anche a questo importante aspetto della sicurezza. Dotarsi di password non banali (più lunghe sono e meglio è) e soprattutto uniche, esclusive: una password diversa per ogni accesso.

Per facilitarti la vita puoi usare un **password manager**, una piccola applicazione che ti suggerisce le nuove password quando le devi creare, le memorizza e te le ricorda al momento più opportuno. Molti browser incorporano funzionalità simili, ma ovviamente limitandosi alle credenziali dei siti web. Un password manager indipendente può aiutarti anche a tenere traccia di PIN e codici di carte di credito, token o chiavette, domande di sicurezza e così via.

Alcuni password manager possono anche essere usati contemporaneamente su più dispositivi (PC, telefoni...) in maniera sincronizzata, il che è una bella comodità per avere le informazioni che ti servono in qualunque momento.

Suggerimento #6 - Definisci una strategia operativa per le tue password in modo che siano sempre diverse, difficili da indovinare e variate periodicamente. Usa un password manager per semplificarti la vita.

Come vedi, puoi rafforzare la tua sicurezza osservando semplici accorgimenti che puoi mettere in pratica da solo. Se vuoi sfruttarli al massimo, approfondirne le possibilità e magari integrarli al meglio con il tuo ambiente IT specifico, il tuo Managed Service Provider o MSP è in grado di fornirti tutta la consulenza di cui hai bisogno.

La sua esperienza quotidiana gli permette infatti di essere sempre aggiornato sulle ultime tendenze cybercriminali e sulle relative contromisure, così da suggerirti le pratiche migliori da seguire affinché tu possa usare i tuoi sistemi nel modo più semplice e pratico possibile con la tranquillità di chi sa come farsi odiare dai malintenzionati digitali.

8 Digital Shadows, Account Takeover in 2022

Glossario

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

Malware – Combinazione dei termini inglesi "malicious" (malevolo, pericoloso, illecito) e "software". Indica l'insieme degli strumenti software che i cybercriminali utilizzano per entrare nei computer delle loro vittime, assumerne il controllo in modo parziale o integrale, propagarsi all'interno della rete colpita ed effettuare attività illecite come la sottrazione di dati personali o sensibili, lo spionaggio, l'invio di messaggi di posta indesiderata o il blocco crittografico dei dati a scopo di riscatto. Ognuna di queste attività assume una propria denominazione, come spyware, spamware, ransomware ecc.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, concettualmente simili ma accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

Spam – Messaggi indesiderati solitamente a carattere pubblicitario che rappresentano una porzione significativa del traffico mondiale di email. In molti Paesi l'invio di spam è reato e comunque quasi sempre contrario alle politiche d'utilizzo ammesse dagli Internet Service Provider. Per questo motivo, nonché per gli altissimi volumi di messaggi (anche alcuni miliardi) spediti da una normale campagna spam, i cybercriminali preferiscono effettuare l'invio attraverso computer di ignari utenti su cui sia stato precedentemente installato malware che ne permetta il controllo a distanza.