WHITE PAPER

La cyber security come strumento di business

—

Come raggiungere i risultati aziendali garantendo la continuità operativa

CYBEROO

Indice

Abstract

Gli attacchi alla cyber security sono sempre più frequenti, mirati ed efficaci. I cyber criminali non agiscono più in modo indiscriminato, colpendo a caso: **ora hanno obiettivi precisi, sanno chi attaccare e, soprattutto, quali danni possono causare** perché consapevoli di quanto possano valere dati e informazioni per un'organizzazione.

Non solo. I rischi evolvono e non è più solo il riscatto – richiesto nel caso dei ransomware – a spaventare aziende ed enti pubblici, ma anche la **minaccia di diffondere quanto sottratto in rete.** Insomma, gli effetti derivanti da un attacco sono importanti **sia come costi, sia come danno d'immagine** e possono essere talmente devastanti da impedire a un'impresa di risollevarsi.

La cyber security deve, perciò, essere considerata un elemento fondamentale dell'ecosistema aziendale, in grado di **assicurare la continuità del business.** Trascurare l'aspetto della sicurezza informatica è il primo passo per offrire il fianco al cyber crime, perché, al contrario di quanto si possa pensare, **oggi nessuna azienda è immune agli attacchi.**

Lo stato della cyber security

Sono sempre più frequenti ed eclatanti le notizie di attacchi a enti, istituzioni, aziende o strutture sanitarie, che mirano a rendere inaccessibili i dati. Solitamente, **l'obiettivo è puramente economico:** ottenere il pagamento di una certa cifra per consentire al legittimo proprietario di tornare in possesso delle informazioni sottratte. Questa pratica nello specifico è tipica dei ransomware, una particolare tipologia di malware ormai tristemente nota. In altri casi, l'attacco può avere un **intento di carattere strategico** e, quindi, può prevedere azioni mirate alla distruzione dei dati o alla scoperta di segreti industriali, se non addirittura di Stato.

Comunque sia, si evidenzia **un'importante evoluzione nelle attività del cyber crimine:** gli attacchi sono sempre più precisi e vengono messi in atto con tecniche altamente sofisticate. Alla base, inoltre, c'è **una struttura criminale ben organizzata.** Come anticipato, non si tratta più di azioni su larga scala, portate avanti affidandosi alla legge dei grandi numeri: oggi, l'obiettivo è ben definito e viene studiato con grande accuratezza.

La riprova arriva dai dati del **Rapporto Clusit** di marzo 2022: è stato rilevato, infatti, che **gli attacchi a impatto elevato sono passati dal 50% nel 2020 al 79% nel 2021.** La natura di questi fenomeni è sempre più spesso legata al cyber crime: **l'86% dei casi nel 2021 (+5% rispetto al 2020) è stato sferrato da gruppi criminali.** A seguire, lo spionaggio (in ogni sua forma), che è la causa dell'11% di queste attività.

Tra le tecniche, **a farla da padrone è il malware, che viene usato nel 41% dei casi.** Seguono quelle che il Rapporto Clusit identifica come tecniche sconosciute (21% dei casi), che "battono" le vulnerabilità (15,6%, +60% rispetto al 2020). Il Rapporto precisa che l'alta percentuale di attacchi dovuta a "tecniche sconosciute" è principalmente legata al fatto che molti attacchi (un quinto del totale) diventano di dominio pubblico a seguito di un "data breach". In questo caso, le normative impongono una notifica agli interessati, ma non li obbligano a fornire una descrizione precisa delle modalità dell'attacco (che normalmente, quindi, non viene dettagliata).

Dati alla mano, **il cybercrime può fare affidamento sull'efficacia del malware** - che oggi viene prodotto industrialmente a costi decrescenti - **e sullo sfruttamento di vulnerabilità (note o meno), per colpire più della metà degli obiettivi (quasi il 57% dei casi).**

Il cyber crimine, oggi, prende di mira soprattutto **obiettivi governativi/ militari** (15% del totale, +36,4% rispetto al 2020), **il settore informatico** (14% dei casi, +3,3% rispetto al 2020) **e la sanità** (13% dei casi, ma in crescita del 24,8% nel 2021).

I pericoli di un perimetro aziendale sempre più ampio

Durante la pandemia da Covid-19, per essere conformi alle regole imposte che impedivano di recarsi in azienda e, al contempo, consentire alle imprese di continuare la loro attività, si è fatto ampiamente ricorso allo smart working. Nella maggior parte dei casi, **si è trattato di una decisione presa rapidamente per far fronte a un'emergenza, senza, però, avere una dotazione IT adeguata.**

Questo ha portato i dipendenti a fare uso di dispositivi di proprietà, spesso con un livello di protezione molto basso o addirittura inesistente. Il risultato è stato **un repentino aumento del perimetro aziendale con un elevato numero di endpoint molto vulnerabili.** Un aspetto di cui i cybercriminali hanno presto approfittato.

Ora che l'attività lavorativa si sta regolarizzando, lo smart working, e più in generale il mobile working, non dovrebbero più essere pratiche emergenziali, ma ben gestite e regolamentate.
Spesso, però, uno stesso dispositivo viene usato sia per lavoro, sia per scopi personali, senza valutare i rischi che ne derivano.
Azioni come scaricare un'app, accedere a un servizio online o navigare su siti web trascurando le policy aziendali rappresentano tutte ottime opportunità per il cybercrime. In questi casi, **il rischio che può correre l'impresa di incorrere in danni, anche di grande entità, è molto elevato.**

Quanto costa al business un attacco cyber?

Supponiamo che un'azienda sia stata vittima di un attacco sferrato tramite ransomware: cosa succede dopo?

In un primo momento, potremmo pensare subito che **l'impresa sarà costretta a pagare una cifra importante per entrare nuovamente in possesso dei propri dati.** Pur essendo corretta, questa risposta purtroppo considera solo una minima parte delle conseguenze, seppure di per sé probabilmente importante in termini monetari. Infatti, oggi gli attacchi ransomware non si limitano più a una richiesta di riscatto, ma impongono anche il pagamento di un'ulteriore cifra per evitare che i dati vengano resi pubblici.

A riguardo, va precisato che **c'è stata un'evoluzione di questa tipologia di attacco.** Inizialmente, l'obiettivo puro e semplice di un ransomware era **cifrare il database di un'azienda e chiedere un riscatto.** Oggi, invece, questo cyber attack tende anche a **insediare il malware all'interno della rete aziendale, esfiltrare i dati e cancellare (o comunque rendere inutilizzabili) i backup.** Tutto questo rende l'attacco decisamente più articolato ed efficace.

Chi è vittima di un ransomware, se non ha predisposto un backup efficace "scollegato" dalla rete aziendale, **rischia di subire il blocco dell'attività.** Possono passare giorni - e in alcuni casi settimane - prima di ripristinare la regolare funzionalità dell'IT. In questo caso, i costi da sostenere vanno ben oltre quelli previsti dal riscatto.
Li quantifica IBM all'interno della ricerca **"Cost of a Data Breach Report 2021"**: secondo i dati raccolti, **il costo medio di un attacco ransomware per un'azienda è di 4,62 milioni di dollari.**

Questa cifra include i costi di:

- **escalation:** le investigazioni, gli assessment e la gestione della crisi;
- **notifica:** le attività per informare i soggetti interessati, le autorità di regolamentazione della protezione dei dati e altre terze parti;
- **perdite negli affari:** l'interruzione del business e perdite dovute ai tempi di inattività del sistema, costo dei clienti persi e della mancata acquisizione dei nuovi, perdita di reputazione;
- **risposta all'attacco:** help desk e comunicazioni con i clienti coinvolti nel data breach, monitoraggio del credito e servizi di protezione dell'identità, spese legali, eventuali multe per l'infrazione delle disposizioni di legge.

Per IBM, il ransomware è l'attacco più costoso per un'azienda.
Va rimarcato, inoltre, che **i 4,62 milioni di dollari non comprendono la cifra pagata per il riscatto.** Il dato riferito da IBM è una media a livello mondiale. A livello italiano, la stima del costo medio di un data breach per il 2021 è di 3,61 milioni di dollari (3,19 milioni di dollari nel 2020).

La cyber security come strumento utile al business

I danni causati da un attacco di stampo criminale alla sicurezza informatica di un'azienda possono essere tali da mettere in serie difficoltà l'impresa, che rischia addirittura di chiudere.
Infatti, anche se si riescono a fronteggiare i costi per ripristinare l'attività, il danno d'immagine può essere tale da far venire meno la fiducia dei clienti, con conseguenze catastrofiche.
Per questo si dovrebbe fare il possibile per evitare di essere vittima di un attacco. Nell'ecosistema attuale, però, in cui gli attacchi informatici non sono più eventualità ma certezze, è necessario farsi trovare **preparati per assicurare la continuità al business.**

Si dovrebbe, perciò, **sempre prevedere a budget una cifra da destinare alla cyber security.** In un primo momento, si potrebbe commettere l'errore di limitarsi a considerarlo un investimento che non porta guadagni concreti.
In realtà, il guadagno è da valutarsi nel lungo termine: è in quello che non si perde quando si viene attaccati, ovvero nel business che non si ferma e che continua a macinare risultati, nonostante tutto. In sostanza, solitamente l'importanza di un investimento in cyber security lo si comprende e lo si apprezza davvero al momento di un attacco.

Sarebbe, quindi, necessario **attuare un'adeguata protezione del perimetro aziendale,** o superficie di attacco, come si è sempre più soliti dire. Erigere un elevato livello di difesa degli endpoint è il primo passo, ma è importante anche evitare che eventuali vulnerabilità - di cui non si conosce ancora l'esistenza - spianino la strada ai cybercriminali. Quindi, sarebbe una buona pratica **eseguire dei vulnerability assessment** per avere la certezza di non lasciare aperti dei varchi alla mercè di azioni di advanced persistent threat (ATP).

Nel caso di un attacco in corso, invece, è consigliabile adottare tecniche di risposta efficaci che, sfruttando l'intelligenza artificiale (AI), siano in grado di segnalare anomalie nel sistema IT, aiutando a limitare i danni.

C'è, poi, un altro aspetto da considerare: solitamente, quando si è stati vittima di un attacco si tende a eccedere nella protezione, salvo poi, dopo qualche tempo, iniziare a limitare le pratiche in atto sino a ridurle al minimo. È necessario, in questi casi, stabilire una precisa linea di condotta, adeguata all'attività dell'azienda, che deve essere mantenuta nel tempo ed eventualmente adattata di continuo alle nuove tipologie e metodologie di attacco.

L’errore fatale del business

Sono ancora troppe le aziende che pensano di essere immuni agli attacchi per dimensioni, tipo di attività o altre caratteristiche distintive. Tuttavia, oggi nessuno può ritenersi al sicuro.

Sottovalutare le minacce informatiche è il primo passo per cadere nella trappola del cyber crimine ed è l’errore che può essere fatale al business.

Le notizie che sentiamo ogni giorno in televisione e che leggiamo quasi quotidianamente su magazine e social media raccontano di attacchi particolarmente eclatanti: le vittime, solitamente, sono grandi strutture, che subiscono danni ingenti, tanto da fare clamore. Questo, però, rischia di portare anche le piccole e medie imprese a credere che l’obiettivo dei cybercriminali siano solo le enterprise. Qui parte il primo passo falso: si inizia a pensare di essere poco interessanti agli occhi dei criminali informatici.

In realtà, però, è proprio l’opposto, nel senso che la grande realtà è, si, il traguardo da raggiungere, ma prima si devono affrontare delle tappe intermedie. Questi step consistono “nell’infettare” piccole e medie imprese che, in qualche modo, intrattengono relazioni commerciali con large enterprise. Questa strategia si fonda sull’assunto che una grande azienda abbia sicuramente un sistema di difesa evoluto, difficile da scardinare, mentre è molto più facile che una realtà contenuta abbia una protezione

limitata e sia facilmente accessibile. Una volta entrati nel sistema della piccola impresa, che solitamente non si accorge dell'attacco in corso, i cybercriminali attendono il momento giusto (a volte settimane o addirittura mesi) per raggiungere l'obiettivo finale. Ecco perché, per esempio, sono sempre più frequenti gli attacchi alle supply chain: l'obiettivo non è la catena in quanto tale, ma invece l'azienda a cui fa capo.

Quanto pesa una buona strategia di cybersecurity sul raggiungimento degli obiettivi aziendali

Avere una buona strategia di sicurezza informatica favorisce il business. La conferma arriva dallo studio di Forrester **"Better Security And Business Outcomes With Security Performance Management".** Del campione esaminato (207 responsabili della sicurezza IT inglesi e statunitensi), **il 38% sostiene di aver perso occasioni commerciali proprio a causa della percezione data all'esterno della mancanza di un adeguato livello di sicurezza.**

Siccome l'80% delle aziende intervistate ha subito un incidente informatico o di sicurezza nell'ultimo anno, le organizzazioni si rendono conto **che una solida posizione di cybersecurity è fondamentale per guadagnare la fiducia dei clienti, proteggere la proprietà intellettuale e la brand identity.**

I clienti vogliono fare business con aziende sicure e, dato che possono facilmente spostare la loro attività altrove se si sentono vulnerabili, i responsabili della sicurezza devono cercare di capire e quantificare l'efficacia del loro programma di cyber security e misurarne l'impatto sugli obiettivi di business aziendali.

Devono essere attenti alle indicazioni di fallimento che danneggiano maggiormente l'azienda. I partecipanti al sondaggio lo hanno confermato, sostenendo che sono più propensi a fare affari con aziende "sicure", perché sanno che i loro dati e la loro proprietà intellettuale sono protetti.limitata e sia facilmente accessibile.

Una volta entrati nel sistema della piccola impresa, che solitamente non si accorge dell'attacco in corso, i cybercriminali attendono il momento giusto (a volte settimane o addirittura mesi) per raggiungere l'obiettivo finale. Ecco perché, per esempio, sono sempre più frequenti gli attacchi alle supply chain: l'obiettivo non è la catena in quanto tale, ma invece l'azienda a cui fa capo.

In che modo la sicurezza gestita garantisce la continuità?

Oggi una linea di difesa non può – e non deve – mancare in nessuna azienda, il rischio che si corre è troppo alto. Tuttavia, impostare una strategia di protezione efficace significa **disporre di persone, competenze e strumenti adeguati.** Per molte aziende questo comporta costi e impegni difficili da sostenere o, quantomeno, le risorse interne non permettono di ottenere un livello tale da assicurare la continuità operativa.

In questo caso, **la soluzione è avvalersi dei servizi di cyber security che può offrire un provider esterno**. In questo modo, è possibile usufruire sia di una gestione completa della sicurezza, sia del potenziamento degli strumenti e delle attività già presenti in azienda attraverso funzioni atte a rafforzarla.
Questo permette al business di avere a disposizione **personale qualificato h24** (importantissimo se si considera che il 76% dei ransomware ha luogo nella notte o nel weekend) costantemente aggiornato su minacce e tecniche emergenti.
Si ha anche l'opportunità di attivare un **servizio di managed detect and response,** che consente di prevedere un **continuous scanning dell'infrastruttura** e avere, quindi, la certezza di un controllo costante

e di un intervento tempestivo. Altro vantaggio riguarda l'esfiltrazione dei dati, che solitamente vengono sottratti e messi in vendita sul dark web. Un service provider può, attraverso un servizio di threat intelligence, scandagliare l'Internet che non si vede per verificare se si è stati vittime di un data breach e se le informazioni sottratte sono già nelle mani di qualcun altro. Questo consente di avere una protezione interna ed esterna, ed evita tentativi di frode.

Il service provider può anche arrivare a **vestire i panni di un ethical hacker** per verificare la solidità della dell'infrastruttura IT, lanciando una serie di attacchi che emulano le modalità che utilizzerebbe un cyber criminale.

In conclusione, la cyber security oggi non è più un'opzione e il cyber crimine non fa "sconti". Per questo bisogna sempre essere preparati contro un eventuale attacco. Perciò, se non si dispone di una struttura interna in grado di garantire un'adeguata protezione, scegliere di puntare su un service provider affidabile è un modo efficace per assicurare la continuità – e la solidità – del business.

Contatti

Cyberoo S.p.A.
via Brigata Reggio, 37
42124 (RE)

tel. 0522 385011

www.cyberoo.com

CYBEROO