COME FERMARE LE VIOLAZIONI DEI DATI ED EVITARE LE SANZIONI DEL GDPR

Un toolkit per prevenire la violazione dei dati
dedicato alle piccole e medie imprese

F-Secure

È ORA DI PREPARARSI AD AFFRONTARE LE VIOLAZIONI DEI DATI

Secondo te, la prevenzione della violazione dei dati è una priorità massima per la sicurezza?

Sono molte le aziende che la pensano in questo modo. Da uno studio globale che abbiamo realizzato verso le fine del 2018 è emerso che la stragrande maggioranza dei dirigenti IT e CISO ritiene che la prevenzione delle violazioni sia un'iniziativa chiave per la cyber security per le loro aziende nei prossimi anni, seguita immediatamente, come prevedibile, dalla conformità ai quadri normativi come il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea.

Questi due aspetti, ovviamente, vanno di pari passo. E oggi si iniziano a intravedere le ripercussioni di uno scenario di violazione in un mondo post-GDPR.

A luglio 2019, il garante britannico ICO (Information Commissioner's Office), ha annunciato l'intenzione di comminare a British Airways una sanzione da 183,39 milioni di sterline (229,45 milioni di dollari) per mancato rispetto del GDPR.[1] La sanzione deriva da una violazione messa in atto dal gruppo di hacker Magecart, che ha compromesso i dati personali di oltre 500.000 clienti nel 2018.

Subito dopo questo annuncio, l'ICO ha manifestato anche l'intenzione di multare Marriott International con una sanzione da 99 milioni di sterline (125 milioni di dollari) per una violazione che ha esposto i dati personali di circa 339 milioni di clienti.[2] L'attacco è iniziato nel 2014 nei confronti di Starwood Hotels & Resorts (una società acquisita da Marriott nel 2016) ed è proseguito per quattro anni prima di essere rilevato.[3]

GDPR IN BREVE

Il 25 maggio 2018 è entrato in vigore il Regolamento generale sulla protezione dei dati (GDPR). Esso prevede che tutte le società che controllano o trattano i dati personali dei cittadini dell'UE adottino misure sufficienti per garantire la privacy e la sicurezza dei dati che custodiscono.

Affiancandosi alle norme HIPAA e SOX, il GDPR è il primo standard di conformità per la protezione dei dati a comminare sanzioni pecuniarie alle aziende che perdono o non riescono a gestire adeguatamente le informazioni dei loro clienti.

Il GDPR prevede due livelli di sanzioni che si applicano a tutte le persone giuridiche che gestiscono dati dei cittadini UE. Il livello superiore si applica alle violazioni più gravi e può arrivare a 20 milioni di euro o al 4% del fatturato globale annuo. Quello inferiore si applica alle violazioni di entità minore e può arrivare fino a 10 milioni di euro o al 2% del fatturato globale annuo.

Si tratta di sanzioni più pesanti, e più probabili, rispetto a qualsiasi altro standard vigente. Vengono calcolate in base a tre fattori principali:

1. Quantità di dati personali dei cittadini UE gestiti in modo errato o perduti

2. Misure che erano in atto prima dell'incidente per evitare la perdita

3. Misure messe in atto dopo la perdita

Nel caso di British Airways, la sanzione da 183,39 milioni di sterline corrisponde all'1,5% del suo fatturato globale per l'anno 2017, quindi inferiore rispetto al massimo potenziale[4]. È comunque una cifra enorme, superiore a qualsiasi previsione della maggior parte degli esperti. Come era prevedibile, British Airways ha contestato la decisione del garante britannico e seguiranno azioni giudiziarie.

Per Marriott, la sanzione da 99 milioni di sterline equivale all'incirca allo 0,6% del suo fatturato globale per il 2017.[5] Anche la catena alberghiera ha annunciato l'intenzione di contestare la sanzione e "difendere strenuamente la propria posizione".

È bene ricordarlo ancora una volta: queste cifre rappresentano le intenzioni dell'ICO. Non possiamo prevedere il futuro e stimare con precisione quale sarà l'ammontare finale, ma c'è una cosa che possiamo affermare con certezza: è ora di dare la giusta attenzione alla cyber security. È evidente che le violazioni dei dati derivanti da cattive pratiche di sicurezza saranno sanzionate pesantemente dalle autorità. Elizabeth Denham, garante per la privacy dell'ICO, è stata piuttosto chiara nel suo commento rivolto in particolare a British Airways:

> "I dati personali delle persone sono, appunto, personali. Quando un'organizzazione non riesce a proteggerli da perdite, danni o furti, non si può parlare di un semplice disguido. Ecco perché la legge non lascia spazio a dubbi: quando ti vengono affidati dati personali, sei tenuto a tutelarli. **Chi non lo farà, sarà sottoposto al controllo del mio ufficio per verificare che abbia adottato misure adeguate per proteggere i diritti fondamentali di privacy."**[1]
> **Elizabeth Denham – Information Commissioner, ICO**

I cyber attacchi sono all'ordine del giorno e molto spesso causano violazioni di dati. È un dato di fatto nel moderno panorama delle minacce, con cui tutti noi dobbiamo fare i conti.

Questo, però, non ti esonera dal fare tutto il possibile per fermarli. Predisporre i processi, le soluzioni e le persone giuste non solo ti consentirà di gestire i cyber attacchi, ma sarà anche un elemento determinante nella gestione delle conseguenze, fino alla corte UE. Organizzare la difesa legale diventa molto più facile quando si può dimostrare di avere adottato misure basilari per proteggere i sistemi e i dati e, in sostanza, di avere preso sul serio la sicurezza.

Vediamo rapidamente come si sono svolti gli incidenti che hanno riguardato British Airways e Marriott International. Offriremo anche alcune raccomandazioni generali per evitare le violazioni dei dati e le sanzioni previste dal GDPR, rivolte espressamente alle PMI e alle aziende mid-market.

Anche se le violazioni e le sanzioni più importanti riguardano oggi le società di grandi dimensioni, non passerà molto tempo prima che tocchino anche le organizzazioni più piccole, che dopo tutto rappresentano uno dei target preferiti dagli attaccanti. In questi casi, le sanzioni possono avere effetti ancora più devastanti, dato che le imprese più piccole potrebbero non avere le risorse per riprendersi dopo un incidente.

Possiamo fornirti alcune raccomandazioni utili sulla creazione di un protocollo di cyber security che ti verrà in soccorso anche nelle situazioni di violazione più complesse.

Il **43%** delle violazioni coinvolge le piccole imprese

(Verizon – Data Breach Investigations Report 2019)

Le violazioni sono cresciute del **424%** tra il 2017 e il 2019, con uno spostamento dell'attenzione dei cyber criminali sulle piccole imprese.

(4iQ - Identity Breach Report 2019)

COME È AVVENUTA LA VIOLAZIONE DI BRITISH AIRWAYS?

Il 6 settembre 2018, British Airways ha dichiarato pubblicamente di avere subito una violazione. Il risultato finale è stato il furto di circa 500.000 dati personali dei clienti, comprese le informazioni sui pagamenti.
L'attacco, analizzato in dettaglio per la prima volta dalla società di gestione delle minacce digitali RiskIQ, ha utilizzato un modus operandi simile a quello di un altro famoso cyber incidente ai danni di Ticketmaster UK, condotto dal gruppo di hacker Magecart.[6] Magecart opera iniettando script malevoli in siti web commerciali, che estraggono i dati degli utenti inseriti nei moduli di pagamento digitali. Gli script vengono iniettati direttamente oppure tramite fornitori di terze parti compromessi utilizzati dal sito. In sostanza, crea una versione digitale di uno skimmer di carte, un dispositivo che spesso viene nascosto nei punti bancomat con l'intento di rubare le informazioni sulle carte di credito dei clienti.

Secondo RiskIQ, l'attacco contro British Airways ha seguito un approccio più semplice, ma più mirato, rispetto alle precedenti attività di Magecart. Lo skimmer è stato adattato specificamente in base all'impostazione della pagina di British Airways, il che indica che il gruppo ha studiato attentamente l'attacco a questo sito specifico, invece di limitarsi a iniettare i suoi script standard contro un bersaglio opportunistico.
Dato che Magecart ha configurato l'infrastruttura personalizzata in modo da restare nascosta nel sito web di British Airways, non è possibile sapere quanto tempo è durato l'accesso. È un esempio impressionante di cyber attacco mirato: un'operazione attentamente pianificata, messa in atto da cyber criminali professionisti.

COME È AVVENUTA LA VIOLAZIONE DI MARRIOTT INTERNATIONAL?

Il 30 novembre 2018, Marriott International ha annunciato di avere rilevato una violazione del proprio database di prenotazione degli ospiti di Starwood. L'attacco ha finito per compromettere i dati personali di circa 339 milioni di clienti, compresi nomi, numeri di telefono, indirizzi e-mail, numeri di passaporto e informazioni criptate sulle carte di pagamento.[3]
Marriott è venuta a conoscenza della violazione l'8 settembre 2018, quando la società IT che gestisce il suo database di prenotazione degli ospiti di Starwood ha segnalato un'anomalia. La società di sicurezza di terze parti incaricata di indagare sull'accaduto ha rapidamente individuato un malware nei sistemi IT di Starwood: un trojan di accesso remoto (RAT). I trojan RAT consentono agli attaccanti di accedere, ispezionare e assumere il controllo di un computer in segreto.

In seguito, gli investigatori hanno trovato anche uno strumento di penetrazione chiamato Mimikatz, che permette agli attaccanti di setacciare la memoria dei dispositivi alla ricerca di nomi utente e password. Mimikatz potrebbe essere stato usato anche per passare dai sistemi di Starwood ad altre posizioni nella rete di Marriott.

Il **56%** delle violazioni è stato scoperto dopo mesi o più

(Verizon – Data Breach Investigations Report 2019)

A novembre 2018 Marriot ha finalmente scoperto che la presenza degli attaccanti nei suoi sistemi durava da luglio 2014. Più avanti nello stesso mese, ha scoperto anche che era stata acquisita una quantità enorme di dati dei clienti attraverso due file compressi e crittografati.

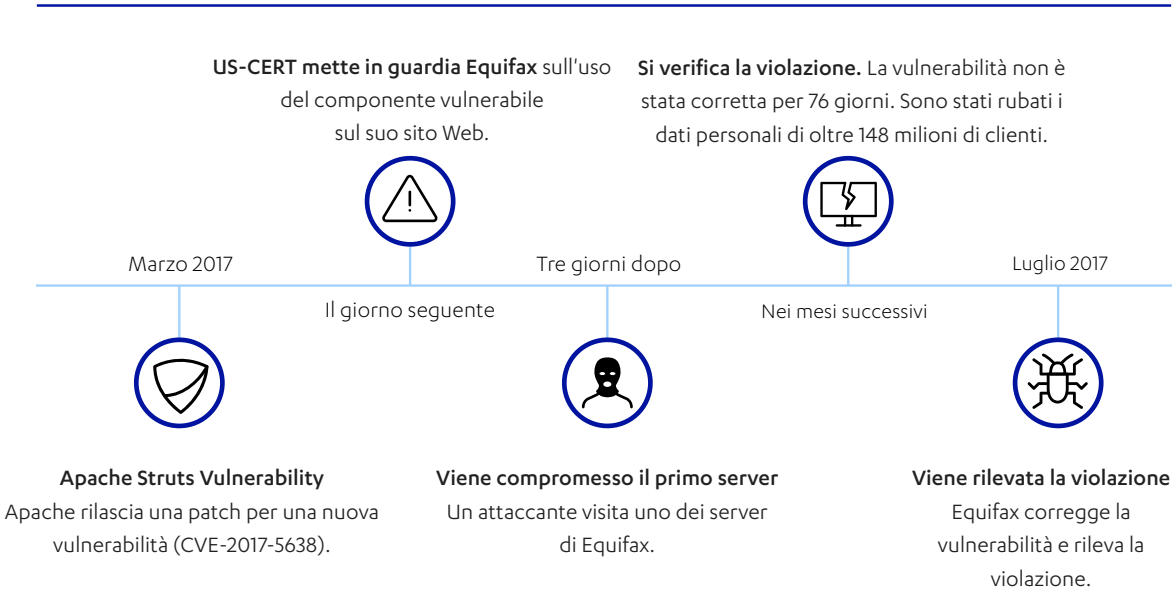
L'identità degli attaccanti è tuttora ignota e non si sa ancora esattamente in che modo è stato condotto l'attacco. In termini generali, la violazione subita da Marriott è una dimostrazione eloquente di quale sia uno dei maggiori punti deboli della cyber security: il ritardo tra l'intrusione e il rilevamento.

LAVORO IN UNA PICCOLA AZIENDA. MI DEVO PREOCCUPARE DELLE VIOLAZIONI?

Sì. Anche se gli attacchi mirati in genere si rivolgono a società del calibro di British Airways e Marriott International, gli stessi metodi finiscono per essere applicati su scala ridotta anche contro target più piccoli. Inoltre, nella maggior parte dei casi, le violazioni sono ancora di tipo opportunistico e si rivolgono a piccole imprese impreparate ad affrontare il livello di competenza e automazione su cui contano gli attaccanti. Ecco uno scenario tipico di cyber attacco andato a buon fine:

Viene rilevata una nuova vulnerabilità: qualcuno rileva una nuova vulnerabilità in un sistema operativo diffuso o in una nota applicazione di terze parti. Nel giro di due settimane gli attaccanti codificano un exploit per la vulnerabilità, che viene poi fatto circolare sul dark web.
Entra in gioco l'automazione: gli attaccanti utilizzano strumenti automatizzati per eseguire una scansione sulla rete Internet pubblica alla ricerca di sistemi che siano ancora vulnerabili per l'exploit. Nella maggior parte dei casi, trovano migliaia di dispositivi che non sono stati aggiornati con le patch: le aziende impiegano un tempo sconcertante (mediamente tre mesi) per correggere le vulnerabilità. L'automazione non distingue tra aziende con 1 o 10.000 dipendenti. Minori sono le difese e le risorse di personale IT a disposizione, meglio è.
I criminali scelgono le azioni di follow-up: gli attaccanti osservano le aziende che hanno compromesso e decidono come agire, ad esempio se distribuire ransomware, sottrarre dati o installare software di cryptomining. Dal tuo punto di vista, sono tutte cattive notizie: i tuoi sistemi e tuoi dati corrono un grave rischio. A peggiorare la situazione, gli attaccanti possono rimanere nascosti per mesi o anni prima di essere scoperti.

Anche se le piccole e medie imprese sono spesso un target privilegiato, gli esempi più eclatanti riguardano comunque le aziende più grandi. Per illustrare meccanismi descritti, osserviamo la violazione subita da Equifax nel 2017.



Questa è la fotografia dell'attuale panorama delle minacce e gli stessi identici principi si applicano sia alle PMI che alle grandi imprese. Con scarse capacità di previsione, correzione e prevenzione degli attacchi e l'incapacità di rilevare e rispondere concretamente a questi attacchi, non hai speranza di batterti ad armi pari con i cyber criminali.

COME EVITARE LE VIOLAZIONI DI DATI E LE SANZIONI DEL GDPR?

Il modo migliore per evitare le violazioni consiste nel risolvere le carenze strutturali nella protezione dei sistemi e dei dati dell'azienda. Le azioni di base che si possono intraprendere per ridurre al minimo la possibilità di un attacco e mantenersi conformi al GDPR sono molte, ma purtroppo la maggior parte delle aziende stenta ancora a metterle in atto in misura sufficiente. Ecco alcuni esempi importanti, suddivisi nelle quattro aree principali della cyber security: previsione, prevenzione, rilevamento e risposta:

LISTA DI CONTROLLO PER LA PREVENZIONE DELLA VIOLAZIONE DI DATI

PREVEDI	• Ricerca le vulnerabilità più comuni e pericolose nei sistemi, nel software e negli asset orientati al web • Applica tempestivamente le patch correttive su tutti i tuoi sistemi • Crea report per dimostrare di avere predisposto misure idonee a proteggere i dati personali dei tuoi clienti
PREVIENI	• Usa una piattaforma di protezione degli endpoint con tassi di rilevamento malware testati da terze parti e applica soluzioni di filtro antispam ai tuoi gateway e-mail • Configura (rafforza) i dispositivi endpoint in funzione delle più comuni strategie di attacco • Usa il controllo delle applicazioni o una soluzione di white-listing analoga per evitare l'esecuzione di applicazioni sospette • Offri ai tuoi dipendenti una formazione specifica sul rilevamento dello spam e delle e-mail di phishing e crea un protocollo aziendale per il reporting dei cyber incidenti
RILEVA E RISPONDI	• Acquisisci strumenti per il monitoraggio dell'ambiente IT e raccogli gli eventi relativi ai dati per individuare le attività inconsuete • Sviluppa competenze interne per rispondere ai cyber incidenti oppure affidati a un provider di servizi competente

Anche se queste attività potrebbero comportare un costo maggiore per la sicurezza in un primo momento, l'investimento sarà più che ripagato in futuro. John Pescatore di SANS ha condiviso questo commento significativo sulla sanzione di British Airways (BA = British Airways)[7]:

> Parlando di numeri, quella sanzione da 229,45 milioni di dollari corrisponde all'incirca al 6% del fatturato 2018 di BA. Rappresenta circa 40 dollari per ogni record esposto, mentre i costi maggiori (gestione del problema, comunicazione con i clienti interessati, fornitura di servizi di controllo del credito, gestione delle cause legali, ecc.) ammontano tipicamente a 50-75 dollari per record, ovvero altri 250 milioni di dollari. **Quindi, il costo totale di questo singolo incidente è di circa 500 milioni, pari a più del 10% del fatturato 2018 di BA. Il costo per fare in modo che il software web non contenesse vulnerabilità facilmente sfruttabili prima di consentirne l'accesso al sito web sarebbe stato inferiore all'1% del costo effettivo finale.**
>
> **John Pescatore - Director of Emerging Security Trends, SANS**

In fin dei conti, è una questione di gestione del rischio. Nella maggior parte dei casi è molto più sensato fare un investimento iniziale relativamente contenuto ed evitare costi molto più elevati in seguito, data l'altissima probabilità di subire un attacco. Secondo il nostro studio del 2018, il 72% delle aziende ha segnalato uno o più tentativi di cyber attacco. Analogamente, il 451 Group stima che circa il 60% delle aziende globali sia stato oggetto di violazione.

Il **72%** delle società globali ha rilevato tentativi di cyber attacco nel 2018

(F-Secure - B2B Market Survey 2018)

Il **60%** delle società globali ha subito una violazione

(451 Group - Thales Data Threat Report 2019)

Le violazioni e le sanzioni conseguenti a carico di British Airways e Marriott International dovrebbero essere gli esempi perfetti da presentare alla prossima riunione del Consiglio di Amministrazione per richiedere un incremento del budget. La probabilità di essere attaccati deve essere presa in seria considerazione e per mitigare questo rischio è importante iniziare a seguire le raccomandazioni citate sopra.

PREVEDERE GLI ATTACCHI

Come sottolineato negli esempi precedenti, la ricerca delle vulnerabilità e l'applicazione di apposite patch è un modo efficace per aumentare le possibilità di evitare una violazione. È anche importante cercare semplicemente di restare al passo con il crescente numero di falle di sicurezza che vengono scoperte ogni anno; solo nel 2018 sono state rese note oltre 16.000 nuove vulnerabilità.[13]

Per illustrare l'efficacia della gestione della vulnerabilità nella prevenzione delle violazioni, lo studio 2018 Cost of a Data Breach di Ponemon ha identificato due capacità chiave nelle aziende che sono riuscite a evitare gli attacchi. Le loro performance medie sono risultate superiori per quanto riguarda[8]:

- La capacità di individuare rapidamente le vulnerabilità (superiore del 19%)
- La capacità di correggere tempestivamente le vulnerabilità (superiore del 41%)

Il **57%** delle società che ha segnalato una violazione ha affermato che è stata la conseguenza di una vulnerabilità nota che avrebbe potuto essere corretta.

(Ponemon – Cost of a Data Breach 2018)

In poche parole, queste società hanno ridotto drasticamente il rischio di subire violazioni dei dati, e le violazioni del GDPR che ne derivano, adottando procedure efficaci per la gestione delle vulnerabilità. A supporto di questa strategia, consigliamo una soluzione software come F-Secure Radar.
F-Secure Radar è una piattaforma chiavi in mano per la gestione e la scansione delle vulnerabilità. Consente di analizzare i sistemi, identificare e gestire le minacce interne ed esterne, segnalare i rischi e restare conformi alle normative attuali e future, quali PCI e GDPR. Inoltre, offre maggiore visibilità sullo shadow IT, permettendo di mappare la superficie di attacco completa e rispondere anche alle vulnerabilità nascoste prima che vengano sfruttate, ad esempio quelle presenti su server e sistemi "dimenticati".
Grazie alla sua funzionalità di reporting, F-Secure Radar ti consente anche di presentare alle autorità UE tutta la documentazione necessaria, la quale dimostra che hai:

- la capacità di misurare il rischio per i sistemi che contengono, trattano o trasferiscono dati personali
- predisposto un processo per testare le misure adottate per proteggere i dati personali
- messo in atto misure di sicurezza tecniche e organizzative per proteggere i tuoi sistemi
- la capacità di creare un piano d'azione per correggere o attenuare i rischi per i sistemi

Report accurati e chiari non solo sono utili per monitorare lo stato delle patch e per istruire la leadership dell'organizzazione, ma sono anche una parte importante della conformità al GDPR. Questi report dimostreranno che hai minimizzato la superficie di attacco, proteggendo così i dati sensibili dei tuoi clienti.
Una soluzione per la gestione delle vulnerabilità consentirà anche di ridurre le operazioni manuali e le ore-uomo solitamente necessarie per la scansione dei sistemi e l'applicazione di patch. Ecco perché è un'ottima aggiunta al tuo portfolio di cyber security: ti semplifica il lavoro e al contempo ti assicura un risparmio economico. F-Secure Radar, inoltre, può essere utilizzato facilmente anche dagli specialisti IT junior ed è quindi una soluzione adatta alle aziende più piccole.

GDPR ARTICOLO 32

Predisporre un processo di valutazione regolare
Richiede l'esecuzione di valutazioni delle misure di sicurezza correlate al trattamento dei dati.

PREVENIRE GLI ATTACCHI

La maggior parte delle aziende utilizza una piattaforma di protezione degli endpoint (EPP) per proteggere i propri dispositivi, quali laptop, server e dispositivi mobili. E lo fa per una buona ragione: la piattaforma EPP è un'ottima soluzione per proteggere dalle minacce tradizionali che sono ancora comuni nel panorama delle minacce, quali malware, ransomware, spam e truffe online. Questi tipi di minacce sono anche direttamente correlate alla conformità alle normative. L'articolo 5 del GDPR prevede infatti che i dati personali vengano trattati in maniera tale da garantirne la protezione da perdita, distruzione o danni accidentali. Le minacce come il malware e il ransomware rappresentano un rischio evidente in questo senso. Anche l'utilizzo sempre crescente di dispositivi mobili e servizi cloud ha un effetto sulla riservatezza e sulla perdita dei dati.

GDPR ARTICOLO 5

Garantire la sicurezza dei dati personali
Richiede che i dati personali vengano trattati in maniera tale da garantirne la protezione da perdite, distruzione o danni accidentali.

La sicurezza degli endpoint può anche proteggerti da attacchi più avanzati. Obbliga gli avversari a utilizzare metodi di intrusione innovativi, che tendenzialmente aumentano i loro costi. Tutto questo, unitamente a dispositivi dotati di adeguate patch e misure di rafforzamento, con tutta probabilità farà desistere gli hacker opportunisti che si orienteranno verso prede più facili. Una soluzione EPP può anche snellire i tuoi processi di rilevamento e risposta, riducendo il numero di avvisi associati alle minacce più comuni. Questo permette al tuo team di sicurezza IT di rilevare le violazioni effettive in modo più rapido ed efficace. Tuttavia, non tutte le piattaforme di protezione degli endpoint sono uguali. La soluzione che sceglierai dovrà offrire prestazioni all'altezza degli standard moderni, almeno per quanto riguarda le funzionalità di base: rilevamento del malware (anche le nuove varianti), applicazione di regole firewall aggiornate e controllo di dispositivi e porte. La tua piattaforma EPP dovrà anche coprire tutti i tipi di dispositivi utilizzati in azienda: macchine Windows, Mac, dispositivi mobili e server. Il nostro prodotto per la sicurezza degli endpoint basato su cloud, F-Secure Protection Service for Business, riunisce tutti gli strumenti necessari per migliorare la sicurezza preventiva e soddisfare i requisiti del GDPR. Gestito tramite un unico portale, include:

- Protezione per Windows, Mac, iOS, Android e un'ampia gamma di piattaforme server
- Gestione delle patch automatica e pienamente integrata (che, insieme a F-Secure Radar, ti aiuterà a fronteggiare l'afflusso costante di nuove vulnerabilità di sicurezza)
- I migliori tassi di rilevamento malware al mondo, comprovati da organizzazioni di terze parti indipendenti come AV-TEST
- Firewall con regole programmate da esperti, controllo di connessioni e dispositivi, controllo delle applicazioni e protezione mirata contro il ransomware
- Integrazione completa con la nostra soluzione EDR, F-Secure Rapid Detection & Response, per una protezione avanzata dalle minacce

Il **67%** dei professionisti della sicurezza IT afferma che la propria organizzazione ha subito un attacco a livello di endpoint nel 2018

(Ponemon – State of Endpoint Security Risk 2018[12])

Un prodotto per la sicurezza degli endpoint che sia robusto e multilivello è uno dei modi più semplici per migliorare il profilo di sicurezza. Analogamente alla gestione delle vulnerabilità, una soluzione EPP è una componente fondamentale della cyber security che ti farà risparmiare tempo, denaro e preoccupazioni. Un unico pacchetto che include così tante funzioni essenziali (come la gestione delle patch) accelera e semplifica notevolmente il lavoro del team IT.

RILEVARE E RISPONDERE AGLI ATTACCHI

Per quanto tu possa impegnarti per gestire le vulnerabilità e proteggere gli endpoint, gli attaccanti esperti e motivati troveranno comunque un modo per superare le tue difese.
Ci rendiamo conto che questo suoni strano, detto proprio da una società di sicurezza che fornisce queste soluzioni. Torniamo esattamente al punto da cui siamo partiti: violazioni di dati in piena regola, come quelle di British Airways e Marriott International.
Oltre alla crescente motivazione degli avversari (il cyber crime è relativamente a basso rischio/alto rendimento rispetto ai crimini tradizionali), entrano in gioco altri trend. Eccone alcuni esempi:

- Molti avversari utilizzano tecniche di attacco avanzate che sono molto difficili da bloccare, come malware fileless, spear-phishing e exploit zero-day
- L'ambiente IT aziendale include più servizi cloud e centinaia di applicazioni diverse, che estendono la superficie di attacco
- È difficile trovare esperti di sicurezza IT che conoscono le moderne metodologie di attacco come gli hacker criminali

Tutti questi problemi si combinano tra loro, rendendo molto difficile per i team IT monitorare lo stato della sicurezza e tenere a bada gli attaccanti. Se in questo momento chiedessi al tuo team "Siamo al sicuro?", come risponderebbe?
La risposta sincera più probabile è "No". Le ricerche condotte da Verizon, Ponemon e da noi suggeriscono che la frequenza delle minacce non tradizionali cresce con un ritmo allarmante, anche per le piccole imprese. Per affrontare questo problema, occorre sviluppare nuove capacità di rilevare e rispondere ai cyber incidenti in modo flessibile. Non si tratta di una diretta **riduzione del rischio** mediante la previsione o la prevenzione, ma di **resilienza al rischio**, mirante a preparare l'azienda a tutta una serie di minacce IT che accomunano qualsiasi ambiente aziendale.

Il modo più facile per raggiungere questo obiettivo è scegliere un prodotto pronto all'uso o affidarsi a un provider di servizi competente. **Una soluzione EDR (Endpoint Detection and Response)** è ottima per la maggior parte delle aziende, soprattutto quelle che operano nel comparto PMI. Estende le capacità di protezione degli endpoint con funzionalità aggiuntive di rilevamento, indagine e risposta, aumentando la sicurezza per affrontare i problemi indicati nei punti precedenti.

Dal punto di vista del GDPR, EDR consente anche di determinare rapidamente la portata di un attacco, stabilire se sono coinvolti dati personali e soddisfare i requisiti normativi di notifica della violazione dei dati entro 72 ore.

Alcune soluzioni, come F-Secure Rapid Detection & Response, possono persino offrirti l'assistenza di esperti per le indagini e la risoluzione dell'attacco.

Nel **52%** dei casi, gli attacchi agli endpoint non possono essere realisticamente bloccati

(Ponemon – State of Endpoint Security Risk 2018[12])

GDPR ARTICOLI 33 E 34

Notifica entro 72 ore dal rilevamento di una violazione
Prevede che una violazione venga segnalata alle autorità e agli interessati entro 72 ore dal momento in cui viene scoperta. La notifica deve includere una quantità considerevole di informazioni.

Grazie alla nostra funzionalità "Segnalare a F-Secure", i rilevamenti di minacce gravi o complesse possono essere inoltrati direttamente agli esperti di cyber security specializzati di F-Secure. Questi eseguiranno un'analisi professionale sui metodi, le metodologie, i percorsi di rete, le origini del traffico e le tempistiche associati all'attacco sospetto. Quando invii una richiesta di intervento in F-Secure Rapid Detection & Response, puoi scegliere tra queste due opzioni:

CONVALIDA DELLA MINACCIA - F-Secure fornirà ulteriori informazioni su un rilevamento effettuato negli ultimi 7 giorni. Include un riepilogo scritto da un esperto, la descrizione dell'evento rilevato e tutti gli altri dati utili per stabilire se è necessario mettere in atto risposte specifiche.

INDAGINE SULLA MINACCIA - F-Secure condurrà un'indagine estremamente dettagliata su un determinato rilevamento, utilizzando tutti i dati recenti e storici. Questa opzione include anche una guida pratica per la risposta agli incidenti elaborata dai nostri esperti di cyber security, nonché un report completo sul tipo di attacco rilevato.

Sapere di poter sempre contare su un aiuto in situazioni difficili non solo è un ottimo modo per gestire lo stress, ma potenzia significativamente le capacità del reparto IT senza costi significativi. In sostanza, avrai accesso all'aiuto di esperti in ogni momento, ma pagherai solo quando ne usufruirai. Nessun costo continuativo del provider di servizi, né risorse inattive.

Tieni presente che una soluzione EDR non elimina la necessità di gestire le vulnerabilità e proteggere gli endpoint. Nonostante la proliferazione degli attacchi avanzati, resta comunque importante, e anche economicamente vantaggioso, limitare il più possibile la superficie di attacco e individuare la maggior parte delle minacce a livello di gateway o endpoint.

È anche importante predisporre uno strumento che ti consenta di intervenire quando qualcosa sfugge ai controlli. La nostra esperienza nella gestione di centinaia di casi di cyber crime ci suggerisce che poter indagare sul modo in cui un attaccante è entrato nel sistema, cosa ha fatto dopo essere entrato e quali dati è riuscito a sottrarre è di importanza fondamentale.

CHE COS'È EDR?

Oltre a chiudere a chiave le porte di notte, molti palazzi di uffici hanno misure di sicurezza aggiuntive, quali telecamere e rilevatori di movimento. La soluzione Endpoint Detection & Response (EDR) svolge una funzione analoga per l'infrastruttura IT: ti permette di scovare un attaccante non appena sfugge ai tuoi controlli di cyber security standard.

EDR raccoglie, archivia e analizza un numero enorme di eventi relativi ai dati (come esecuzioni di processi, connessioni di rete e operazioni sui file) dalle workstation e dai server dell'organizzazione. Sulla base di questi dati, identifica le attività sospette e pericolose sulla rete, tra cui:

- Attacchi malware fileless distribuiti da siti web che contengono codice malevolo, documenti PDF caricati in browser o macro incorporate in file di MS Office
- Altri processi insoliti avviati dalle workstation aziendali
- Uso di software pericoloso, quali applicazioni e servizi cloud noti per essere vulnerabili ad exploit comuni
- Connessioni di rete remote non autorizzate tra l'azienda e parti esterne

La possibilità di rilevare rapidamente questi tipi di attacchi è un elemento cruciale nell'odierno panorama delle minacce. I prodotti EDR includono anche funzionalità per isolare i dispositivi compromessi dalla rete, impedendo di fatto l'espansione di un attacco. Si tratta di due capacità essenziali per impedire che gli attacchi si trasformino in vere e proprie violazioni dei dati.

CONCLUSIONE

Questi tre tipi di soluzioni ti consentiranno di gestire le violazioni dei dati e la conformità al GDPR. Con il supporto di adeguati processi interni e formazione, sarai in grado di:

- Prevedere la maggior parte dei percorsi di attacco e correggere proattivamente le vulnerabilità di sicurezza
- Prevenire l'infezione degli endpoint da parte di minacce tradizionali e tenere l'organizzazione al riparo da ransomware che compromettono i dati
- Rilevare e rispondere alle minacce avanzate che eludono le misure di sicurezza preventive

I prodotti non sono tutto, ma possono aiutarti a ridurre al minimo molti problemi comuni alle aziende più piccole. La tua azienda dispone di un numero sufficiente di professionisti dedicati alla sicurezza IT? Sono formati per gestire le minacce avanzate? Hanno tempo per applicare manualmente le patch? Con soluzioni olistiche e automatizzate, queste attività diventano parti gestibili di una normale giornata lavorativa, anziché ostacoli insormontabili.

Quindi, anche se non abbiamo la bacchetta magica, siamo consapevoli delle complessità insite nella prevenzione delle violazioni dei dati e nella conformità alle normative. E soprattutto, possiamo aiutarti ad affrontare questi problemi in modo efficace con prodotti e processi testati sul campo da centinaia di migliaia di clienti soddisfatti.

Se vuoi parlare con uno dei nostri esperti della tua situazione attuale per quanto riguarda la sicurezza IT o il GDPR, contattaci.
f-secure.com/contact-us

Nessuno può vantare una visibilità sui cyber attacchi reali maggiore di F-Secure. Stiamo colmando il divario tra rilevamento e risposta, impiegando l'impareggiabile threat intelligence di centinaia dei migliori consulenti tecnici del settore, milioni di dispositivi che eseguono il nostro pluripremiato software e innovazioni incessanti nell'intelligenza artificiale. Le maggiori banche, compagnie aeree e imprese si affidano a noi per il nostro impegno volto a sconfiggere le minacce più potenti del mondo.

Insieme alla nostra rete costituita dai più importanti partner di canale e da oltre 200 service provider, il nostro obiettivo è fare in modo che ognuno disponga della cyber security di livello enterprise di cui tutti noi abbiamo bisogno. Fondata nel 1988, F-Secure è quotata sul listino NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure_it | linkedin.com/f-secure

1 - ICO. (2019). Intention to fine British Airways £183.39m under GDPR for data breach.
2 – ICO. (2019). Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach.
3 – Forbes. (2019). Marriott CEO Reveals New Details About Mega Breach.
4 - BBC. (2019). British Airways faces record £183m fine for data breach.
5 – Bank Info Security. (2019). Marriott Faces $125 Million GDPR Fine Over Mega-Breach.
6 – RiskIQ. (2018). Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims.
7 – SANS. (2019). Newsletters: Newsbites. (newsletter on 8th of July)
8 – Ponemon. (2018). Cost of a Data Breach.
9 – Verizon. (2019). Data Breach Investigations Report.
10 - 451 Group. (2019). Thales Data Threat Report.
11 - AV-TEST. (2019). Malware Statistics.
12 – Ponemon. (2018). State of Endpoint Security Risk.
13 - CVE Details (2019). Number of New CVEs Published Each Year.

F-Secure