LA DURA REALTÀ DIETRO LA GESTIONE DEGLI ENDPOINT

Come colmare le lacune nella sicurezza multi-dispositivo

Central by LogMeIn

INDICE

Introduzione 3

Dinamiche di mercato: le minacce alla sicurezza sono reali e sempre più diffuse 4

Dinamiche aziendali: al mutare delle tendenze in ambito lavorativo, dovrebbe mutare anche il nostro approccio alla sicurezza 5

Problemi dell'approccio attuale: le aziende dovrebbero prepararsi a vincere la guerra anziché la singola battaglia 7

Impatto quantitativo: fallire a prepararsi significa prepararsi a fallire 9

Benefici dell'investimento: alla crescita dei rischi dovrebbe corrispondere una crescita degli investimenti 10

Come comportarsi 11

INTRODUZIONE

Una delle maggiori tendenze in materia di sicurezza ad aver acquisito rilievo nel corso del 2018 è la gestione degli endpoint. Gli strumenti di gestione degli endpoint semplificano il processo di gestione informatica delle imprese, consentendo loro di centralizzare la gestione, l'aggiornamento e la risoluzione dei problemi di tutti i dispositivi in uso, tra cui computer, portatili, smartphone, router e altro ancora.

Al fine di acquisire una comprensione più approfondita delle dinamiche di mercato e delle minacce alla sicurezza aziendale dei nostri giorni nonché degli approcci attualmente adottati dalle imprese per contrastare tali minacce, abbiamo condotto uno studio su un campione di 1.000 professionisti informatici. I professionisti informatici coinvolti erano rappresentativi del segmento PMI nelle regioni del Nord America e dell'Europa.

I risultati della nostra ricerca hanno dimostrato che una netta maggioranza di professionisti informatici considera la gestione degli endpoint una priorità per i propri team, per effetto della proliferazione di un ampio ventaglio di endpoint nei rispettivi ambienti aziendali. Tali professionisti sono consapevoli della natura pubblica ed estremamente onerosa delle violazioni di sicurezza verificatesi lo scorso anno a causa di sistemi privi di patch (come Equifax e l'attacco all'agenzia governativa statunitense NSA, per citarne solo alcune) e comprendono che la mancanza di un'adeguata preparazione al riguardo può avere un impatto significativo sul fatturato e sulla reputazione aziendale.

Tuttavia, l'adozione di strumenti di gestione degli endpoint sta diventando una priorità per la comunità informatica non soltanto a causa della necessità di affrontare e contrastare le minacce informatiche. Anche le tendenze in ambito lavorativo spingono in questa direzione:

1. Le politiche all'insegna del BYOD (Bring Your Own Device, in inglese) e del telelavoro, che prevedono l'uso di portatili e altri dispositivi mobili, stanno diventando una prassi sempre più diffusa tra le aziende di ogni dimensione e questa tendenza non accenna a diminuire nel prossimo futuro.
2. La pletora di dispositivi che ne consegue è accompagnata da un'esuberanza di app e software dalle caratteristiche eterogenee che necessitano di essere protetti dagli eventuali rischi e gestiti in maniera centralizzata.
3. Le imprese continuano a spostare i processi aziendali sul cloud, esponendo così i propri dati sensibili al rischio di accesso, visualizzazione o gestione non corretta.

Sebbene le tendenze in costante evoluzione che caratterizzano il mondo del lavoro comportino una maggiore comodità per gli utenti finali, implicano allo stesso tempo una crescita dei rischi di violazione della sicurezza. Se a ciò si aggiungono le minacce informatiche che le aziende devono affrontare quotidianamente, risulta evidente perché i professionisti informatici di tutto il mondo sono alla ricerca di metodi olistici e completi per la gestione centralizzata di tutti gli endpoint.

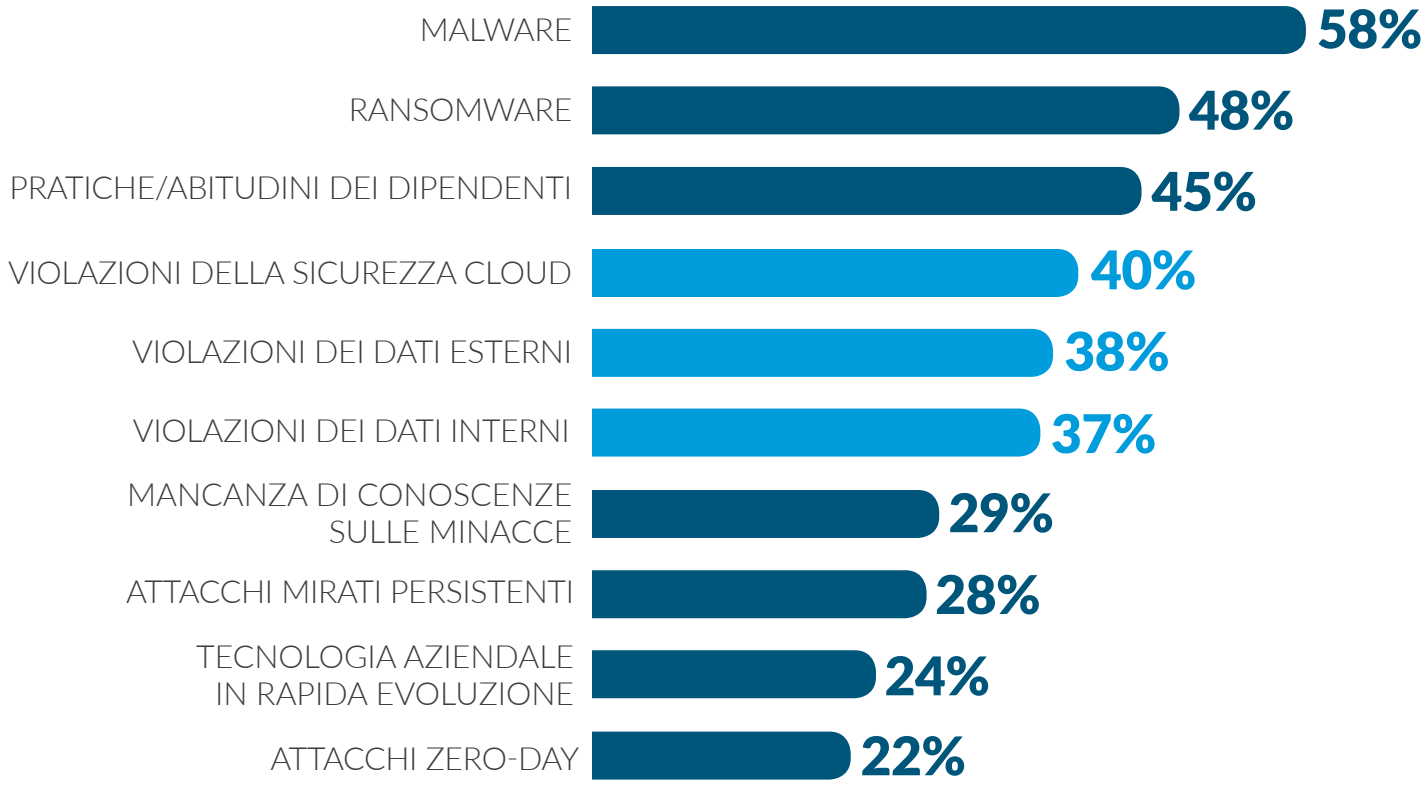
Benché la gestione degli endpoint sia considerata dai professionisti informatici una priorità e le tendenze in costante evoluzione in ambito lavorativo ne confermino la necessità, **SOLTANTO LA METÀ AFFRONTA PROATTIVAMENTE I PROBLEMI DI SICUREZZA** prima che si verifichi una violazione.

DINAMICHE DI MERCATO:
LE MINACCE ALLA SICUREZZA SONO REALI E SEMPRE PIÙ DIFFUSE

I professionisti informatici temevano che il 2018 sarebbe stato un anno segnato da numerosi problemi di sicurezza e le loro preoccupazioni al riguardo erano pienamente giustificate: secondo McAfee, gli attacchi ransomware sono cresciuti del 56%[5] e hanno rappresentato il 39% dei casi di natura malware nel 2017[5]. Di fatto, questo tipo di attacchi non è più rivolto esclusivamente ai computer, bensì coinvolge anche altri endpoint, come server e reti.[5]

Il nostro studio rivela che i professionisti informatici hanno del filo da torcere: affrontano una media di almeno 4 problemi di sicurezza, sia da fonti interne sia esterne. In cima alla classifica di questi problemi salgono i malware, seguiti dai ransomware e dalle pratiche/abitudini dei dipendenti. A breve distanza, troviamo una tripletta di violazioni: violazioni della sicurezza del cloud, violazioni dei dati esterni e violazioni dei dati interni. Si tratta di problemi concreti che non fanno altro che enfatizzare la necessità di adottare una metodologia di gestione degli endpoint completa a livello aziendale. La capacità di mettere in quarantena queste minacce alla sicurezza informatica rappresenta il primo passo per assicurare che l'intera rete aziendale non ne risulti compromessa.

I TEAM INFORMATICI DEVONO AFFRONTARE NUMEROSI RISCHI PER LA SICUREZZA: MALWARE E RANSOMWARE SI TROVANO IN CIMA ALLA CLASSIFICA DEI LORO PROBLEMI.



DINAMICHE AZIENDALI:
AL MUTARE DELLE TENDENZE IN AMBITO LAVORATIVO, DOVREBBE MUTARE ANCHE IL NOSTRO APPROCCIO ALLA SICUREZZA

IL BYOD CAUSA UNA PROLIFERAZIONE DI ENDPOINT. DI CONSEGUENZA, SE I TEAM INFORMATICI NON SVILUPPANO IL MODO IN CUI AFFRONTANO LA SICUREZZA, RISCHIANO DI RIMANERE ESPOSTI ALLE EVENTUALI MINACCE INFORMATICHE.

In tempi non lontani, gli endpoint che i professionisti informatici dovevano gestire e proteggere ammontavano a un numero preciso ed erano sotto il loro diretto controllo. Avevano così la possibilità di proteggere l'azienda da rischi e minacce informatiche rendendone sicuri il perimetro e i sistemi in esso contenuti. Nel corso degli ultimi anni, tuttavia, il BYOD e il telelavoro hanno trasformato le dinamiche lavorative, costringendo i team informatici a ripensare il modo in cui gestiscono e proteggono endpoint e reti aziendali.

Dal momento che le imprese mirano a dotare i propri dipendenti di maggiore flessibilità, raccogliendo i frutti economici del conseguente incremento in termini di produttività e risparmi, le politiche all'insegna del BYOD e del telelavoro continueranno a diffondersi. Di fatto, secondo un sondaggio condotto da MarketsandMarkets, il tasso di adozione del BYOD in Nord America era pari al 36% all'inizio del 2017, con un aumento previsto fino a quasi il 50% nel corso del 2018.[1]

La nostra ricerca dimostra che, nonostante i timori per le minacce agli endpoint, il 30% dei professionisti informatici non sa con esattezza a quanto ammontano i dispositivi endpoint della propria azienda.

QUAL È IL NUMERO TOTALE DI ENDPOINT REMOTI DI CUI DISPONE LA SUA AZIENDA?

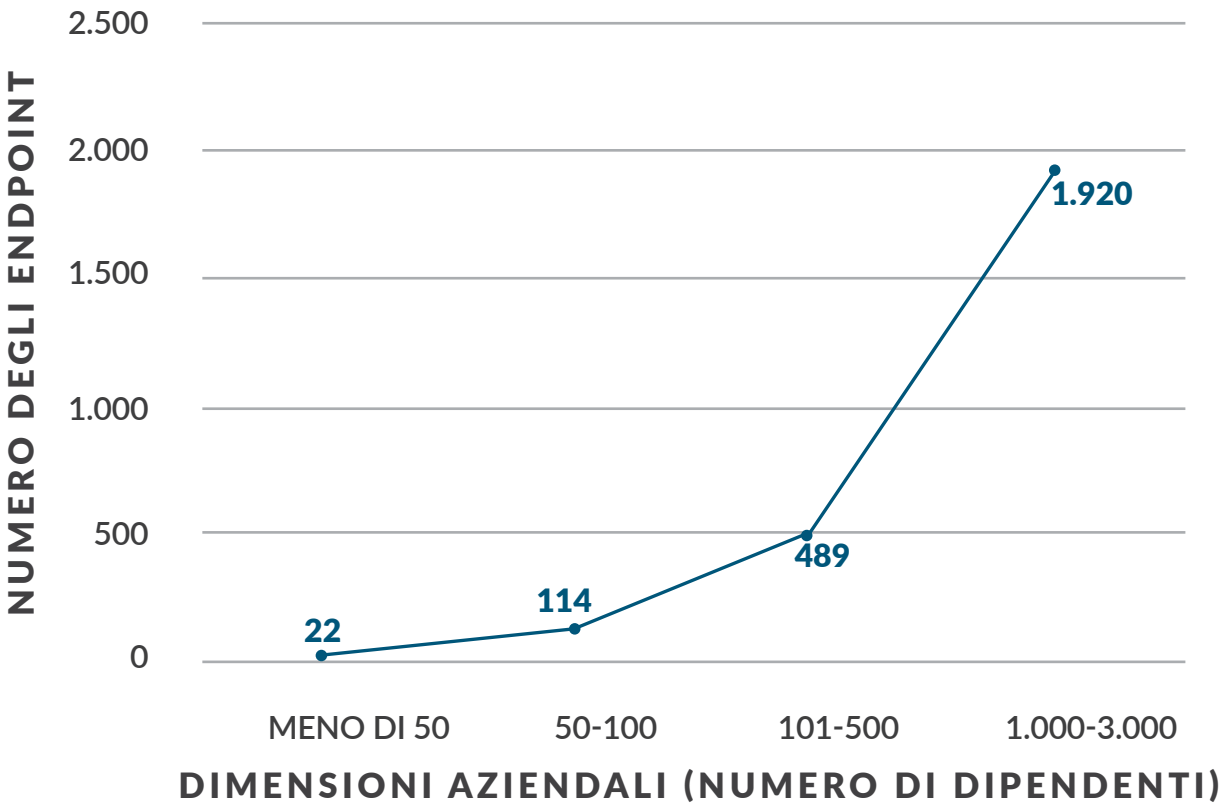
IL 70%
CONOSCE IL NUMERO DEGLI ENDPOINT

IL 30%
NON NE È SICURO

Per tali aziende, trovare un modo per adattarsi alla crescente tendenza al BYOD con una soluzione completa che gestisca in maniera sicura un'ampia gamma di dispositivi si rivelerà cruciale per una prevenzione efficace dei ciberattacchi.

Da quei professionisti informatici che sono stati in grado di riferire il numero di endpoint aziendali, si ricava una media di 750 endpoint, tra server, dispositivi mobili e computer dei dipendenti. Questo numero considerevole aggiunge un ulteriore livello di complessità alla sfida rappresentata dal bisogno di gestire tali endpoint efficacemente, garantendo al contempo la protezione delle aziende dalle minacce alla sicurezza interna ed esterna.

NUMERO MEDIO DI ENDPOINT PER DIMENSIONI AZIENDALI



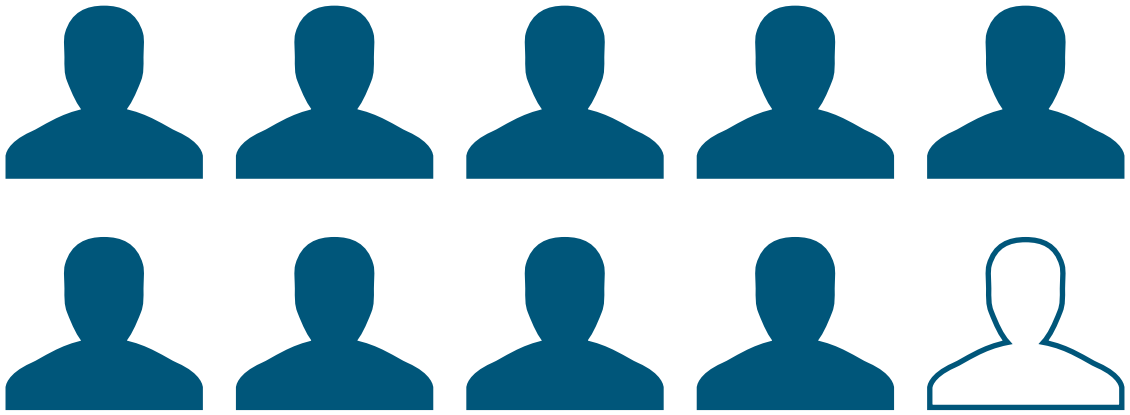
PROBLEMI DELL'APPROCCIO ATTUALE:
LE AZIENDE DOVREBBERO PREPARARSI A VINCERE LA GUERRA ANZICHÉ LA SINGOLA BATTAGLIA

Considerata la pletora di endpoint nonché di problemi di sicurezza interna ed esterna, non sorprende che quasi 9 professionisti informatici su 10 (l'88%) considerino la gestione degli endpoint una priorità per i propri team. Difatti, la protezione antimalware sugli endpoint è al secondo posto tra le misure di sicurezza più adottate dai professionisti informatici per affrontare i problemi di sicurezza.

Tra le altre misure più diffuse per contrastare le minacce alla sicurezza troviamo i firewall, l'autenticazione degli utenti e la crittografia.

Per effetto di tali misure di sicurezza, gran parte dei professionisti informatici (l'82%) si sente preparata ad affrontare i problemi di sicurezza, anche se soltanto il 26% è molto convinto che queste misure siano efficaci per gli utenti finali.

SEBBENE LA GESTIONE DEGLI ENDPOINT RAPPRESENTI GIÀ UNA PRIORITÀ, SAREBBE NECESSARIO UN IMPEGNO MAGGIORE PER TENERE LE IMPRESE AL SICURO NEL LUNGO PERIODO.



QUASI

9 professionisti informatici **su** 10

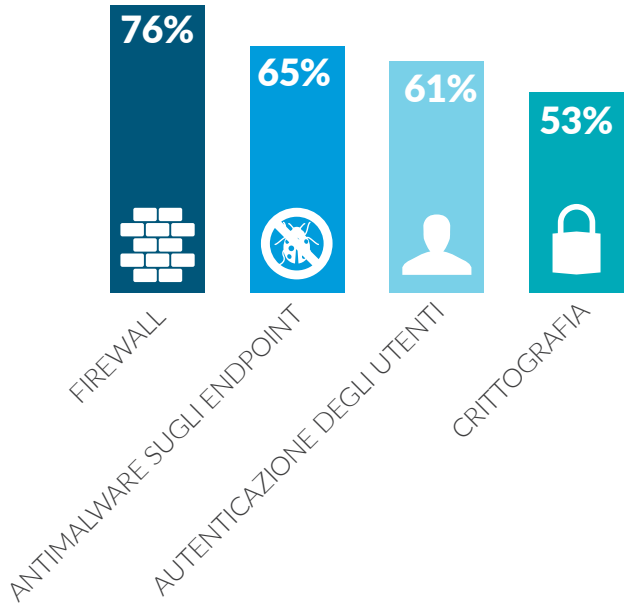
considerano la gestione degli endpoint una priorità.

QUESTI DATI DIMOSTRANO CHE SONO DAVVERO MOLTI I PROGRESSI ANCORA DA COMPIERE IN TERMINI DI PROTEZIONE DEGLI ENDPOINT A LUNGO TERMINE IN UN'OTTICA OLISTICA E ONNICOMPRENSIVA:

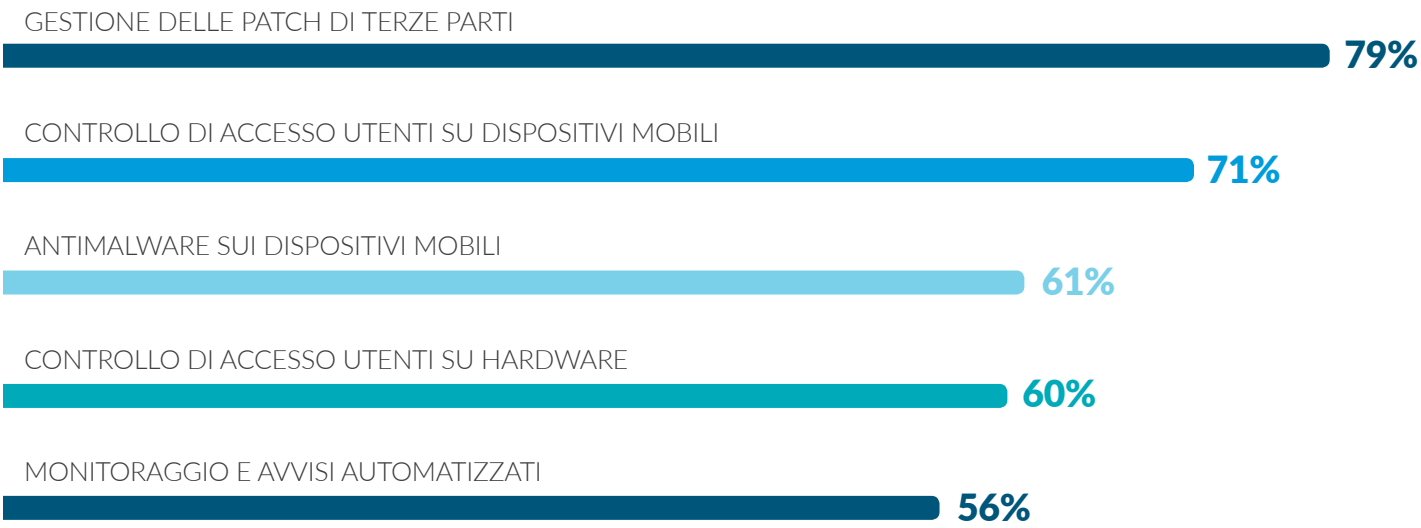
1. Malgrado il 71% dei professionisti informatici sostenga di occuparsi attivamente della sicurezza hardware, soltanto il 56% si occupa attivamente di quella software, mentre solo il 48% si occupa attivamente della sicurezza sui dispositivi mobili. Questa copertura incompleta lascia notevoli falle nella loro strategia di sicurezza. Poiché un numero crescente di dipendenti ricorre a smartphone e tablet personali per motivi di lavoro (tra cui scaricare documenti, applicare modifiche e inviare e-mail), accertarsi che tali dispositivi risultino sicuri quanto i PC e gli altri endpoint sta acquisendo sempre maggiore rilevanza.

2. In aggiunta, sono tante le misure di sicurezza importanti che attualmente non vengono adottate da un'elevata percentuale di team informatici, come la gestione delle patch di terze parti e il controllo di accesso utenti sui dispositivi mobili. Di conseguenza, le aziende per cui lavorano rimangono esposte ai ciberattacchi.

MISURE ADOTTATE PER AFFRONTARE I PROBLEMI DI SICUREZZA



PERCENTUALE DI PROFESSIONISTI INFORMATICI CHE NON ATTUANO LE SEGUENTI MISURE



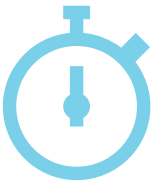
IMPATTO QUANTITATIVO:
FALLIRE A PREPARARSI SIGNIFICA PREPARARSI A FALLIRE

Nonostante la recente copertura mediatica degli attacchi informatici e dei problemi di sicurezza, soltanto poco più della metà dei professionisti informatici (il 52%) dedica del tempo ad affrontare proattivamente i problemi di sicurezza prima che si verifichi una violazione o un attacco.

I rischi che queste minacce alla sicurezza comportano per le imprese non sono soltanto operativi, in quanto possono anche avere un impatto concreto sul fatturato, ripercussioni a lungo termine sulla reputazione aziendale e perfino causare un arresto forzato delle attività.

LE CIFRE SONO SCONCERTANTI

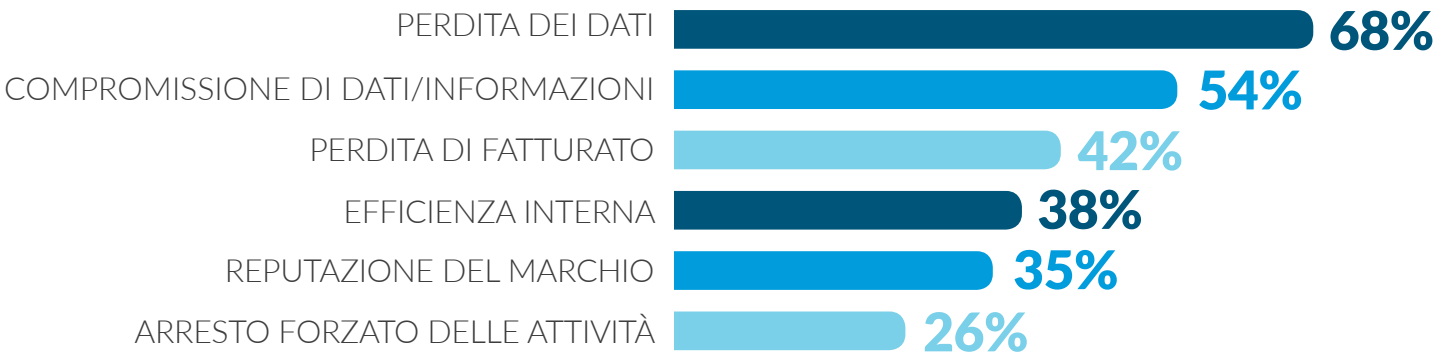
Secondo alcune stime, i danni complessivi causati esclusivamente da WannaCry a livello globale oscillano tra centinaia di milioni e miliardi di dollari. L'attacco ransomware ExPetr è costato a FedEx/TNT un mancato guadagno di circa $ 300 milioni.[5]



Inoltre, secondo un sondaggio globale condotto da Osterman Research per conto di Malwarebytes, circa il 16% delle aziende colpite da un attacco ransomware ha registrato almeno 25 ore di inattività, un tempo di fermo che per alcune ha superato anche le 100 ore.

Il nostro studio dimostra che i rischi derivanti da una violazione della sicurezza che vengono percepiti come più elevati tra i professionisti informatici sono la perdita dei dati, la compromissione dei dati e la perdita di fatturato.

RISCHI DERIVANTI DAI PROBLEMI DI SICUREZZA



BENEFICI DELL'INVESTIMENTO: ALLA CRESCITA DEI RISCHI DOVREBBE CORRISPONDERE UNA CRESCITA DEGLI INVESTIMENTI

LA SICUREZZA INFORMATICA DEVE ANDARE OLTRE I METODI DI PROTEZIONE CONVENZIONALI PER AFFRONTARE LE EMERGENTI MINACCE ALLA SICUREZZA NELLA LORO GLOBALITÀ.

Il nostro studio rivela che, al momento, gli antimalware sugli endpoint rappresentano una delle prime 3 priorità per cui viene utilizzato gran parte del bilancio aziendale stanziato per la sicurezza informatica. I firewall e la formazione informatica completano la triade in cima alla classifica delle priorità che ricevono gran parte del bilancio.

Eppure, in materia di sicurezza, esistono anche altre aree che aiutano a prevenire le minacce ma che non ricevono la stessa considerazione in termini di investimenti, tra cui il monitoraggio e gli avvisi automatizzati (il 26%), gli antimalware sui dispositivi mobili (il 17%) e la gestione delle patch di terze parti (il 14%).

Di fatto, le aree indicate dai professionisti informatici come quelle che riceveranno meno investimenti sono:

gestione delle patch di terze parti e controllo di accesso utenti a dispositivi mobili e hardware.

Nonostante gli investimenti inferiori, tuttavia, si tratta di misure la cui implementazione apporta grandi vantaggi, tra cui:

- la possibilità di risparmiare tempo e denaro nonché di aumentare la produttività, monitorando le minacce e riconoscendo quelle reali da quelle false;
- la possibilità di rafforzare la protezione, concentrandosi sugli incidenti di sicurezza reali;
- la possibilità di garantire la conformità alle migliori pratiche in materia di sicurezza;
- la possibilità di garantire che la sicurezza della propria azienda sia aggiornata, grazie a ogni nuova caratteristica o funzionalità;
- la possibilità di assicurare che i dispositivi mobili dei dipendenti non diventino un punto di ingresso alle informazioni e ai dati aziendali privati.

BILANCIO STANZIATO PER L'INFORMATICA: 2018 VS 2017

La **grande maggioranza (il 70%) dei professionisti informatici** dedica **meno del 25%** del proprio bilancio alla sicurezza informatica.

COME COMPORTARSI

Se, da una parte, i ciberattacchi diventano più frequenti e sofisticati e le tendenze in costante evoluzione in ambito lavorativo comportano una proliferazione di endpoint, dall'altra i team informatici si preparano adottando svariate misure di sicurezza e attribuendo importanza prioritaria alla gestione degli endpoint. Ciononostante, sarebbe necessario un impegno maggiore per evitare di restare vittima di tali attacchi:

ESSERE PROATTIVI

Per migliorare la sicurezza, non è necessario attendere che si verifichi un attacco o una violazione. Misure di sicurezza preventive quali il monitoraggio e gli avvisi automatizzati o l'applicazione di patch aggiornate possono contribuire a difendere le aziende da numerosi attacchi.

INSTALLARE LE PATCH NEI SISTEMI

La gestione delle patch è un'attività essenziale per rendere sicura un'infrastruttura informatica. Tenere sotto controllo tale attività è cruciale, sia che si dedichi un giorno della settimana alla distribuzione delle patch ai propri sistemi sia che si impostino avvisi proattivi per sapere quando è necessario farlo.

IMPLEMENTARE UN APPROCCIO PIÙ OLISTICO ALLA SICUREZZA

Gli attacchi non sono più indirizzati unicamente ai PC. Anche altri endpoint, come i dispositivi mobili e i server, stanno diventando sempre più vulnerabili ai ciberattacchi.

EDUCARE LA FORZA LAVORO ALLA SICUREZZA

La preparazione e il supporto dei propri dipendenti in merito alle abitudini e alle pratiche più adeguate in materia di sicurezza dei dati e cibersicurezza sono aspetti fondamentali della protezione di ogni infrastruttura informatica.

Fonti

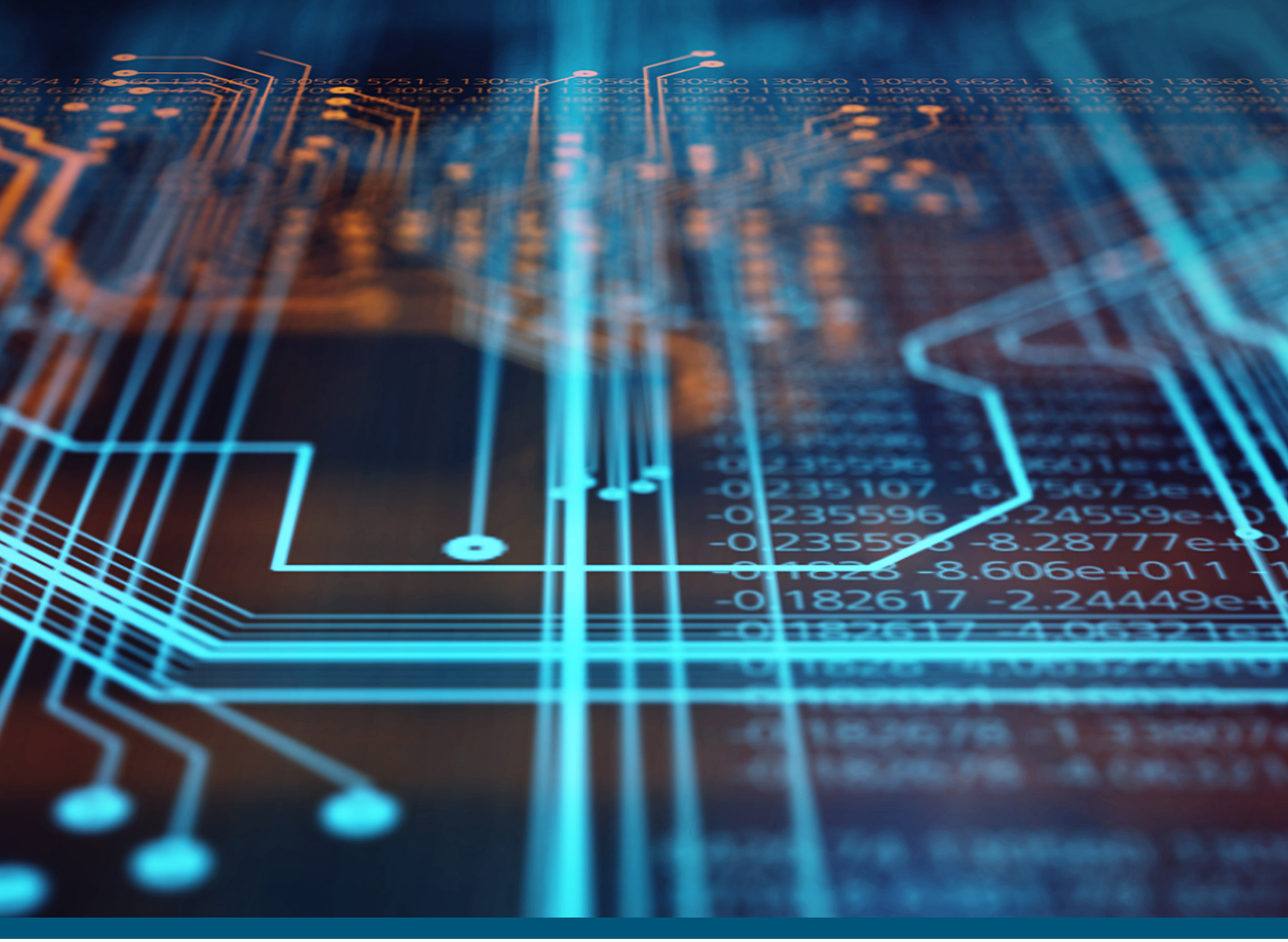
[1] The latest BYOD trends and predictions, from mobile focus to endpoint management, di Jonathan Crowl, Mobile Business Insights, 14 agosto 2017

[2] Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware, di Jorge Rey, Entrepreneur, 30 novembre 2016

[3] Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud, di Amy Talbott, ZDNet.com, 2 ottobre 2017

[4] 2016-2017 Ransomware statistics and facts, di Sam Cook, Comparitech, 17 gennaio 2018

[5] Verizon 2018 Data Breach Investigations Report, di Maria Korolov, autrice esterna, CSO, 10 aprile 2018



Central by LogMeIn

LA SEMPLICITÀ E LA SICUREZZA DELL'AUTOMAZIONE INFORMATICA E DELLA GESTIONE DEGLI ENDPOINT

In quanto membro della famiglia di prodotti per la gestione delle identità e degli accessi di LogMeIn Inc., Central è una soluzione dedicata per la gestione degli endpoint basata sul cloud che consente ai professionisti informatici di monitorare, gestire e proteggere la propria infrastruttura di endpoint in modo efficace. Grazie a LogMeIn Central, le imprese con telelavoratori o endpoint sparsi per il globo possono avere la velocità, la flessibilità e le informazioni necessarie ad aumentare la produttività, ridurre la spesa informatica e limitare i rischi. Classificato come lo strumento di accesso remoto n° 1 rivolto alle piccole imprese per la gestione di più computer, LogMeIn Central dota ciascun endpoint della rete aziendale di un accesso remoto avanzato per risolvere qualsiasi problema, in qualunque momento e in qualsivoglia luogo.

https://www.logmein.com/it/central