White Paper

L'Impellente necessità di endpoint sicuri

Sponsorizzato da: Apple

Tom Mainelli Michael Suby
September 2023

L'OPINIONE DI IDC

La sicurezza è la principale preoccupazione dei responsabili delle decisioni IT (IT Decision Maker, ITDM). Anche le aziende gestite in modo ottimale e in grado di offrire prodotti o servizi di successo potrebbero subire gravi rischi in caso di una singola violazione della sicurezza. Gli ITDM più esperti e capaci sono al corrente di questo rischio.

A livello generale, la sicurezza è un problema sempre più scottante. Le spie aziendali, gli Stati canaglia, il crimine organizzato e i delinquenti comuni hanno tutti fatto un salto di livello nell'uso della tecnologia. Per contrastare i malintenzionati e mantenere al sicuro dipendenti, clienti e dati, i reparti IT delle aziende devono restare sempre concentrati e avvalersi di fornitori e tecnologie di tipo innovativo.

Il lungo elenco delle criticità di sicurezza che i reparti IT devono affrontare è lungo e coinvolge numerosi aspetti: dagli endpoint (computer) ai data center, alle reti che collegano tutto e al software gestionale che fa funzionare tutto. In questo articolo prenderemo in esame l'importanza della protezione degli endpoint, in quanto una singola macchina vulnerabile potrebbe mettere a rischio la sicurezza di un'intera azienda.

Una delle principali criticità legate alla sicurezza degli endpoint è che, tradizionalmente, un endpoint sicuro spesso comporta un compromesso per l'esperienza dell'utente finale con dispositivi bloccati difficili da utilizzare. In questi casi, per svolgere agevolmente il proprio lavoro, gli utenti cercavano metodi e configurazioni utili per aggirare le procedure di sicurezza, trasformando i propri sistemi in un punto debole dei sistemi di protezione aziendali. La sicurezza non deve causare difficoltà e contrasti tra gli utenti a livello operativo.

Grazie agli attuali progressi tecnologici è possibile offrire agli utenti un'esperienza di qualità senza rinunciare alla sicurezza. Gli sviluppi in termini di rilevamento delle minacce informatiche, protezione dei dati, autenticazione e integrazione tra hardware e software hanno eliminato qualsiasi compromesso in termini di sicurezza degli endpoint e produttività degli utenti.

METODOLOGIA

Nel luglio 2023 IDC ha condotto un'indagine online tra numerosi responsabili delle decisioni IT (ITDM) di una serie di aziende con sede negli Stati Uniti e in Canada (n=513). Il sondaggio verteva sulla sicurezza generica e degli endpoint, con un'attenzione particolare ai computer. Gli intervistati lavoravano in aziende dotate di almeno 500 dipendenti, attive in diversi settori e che utilizzavano diversi sistemi operativi, tra cui Microsoft Windows, Apple MacOS e Google ChromeOS. Queste

persone devono scegliere, acquistare o implementare il software di sicurezza della propria azienda o coordinare il personale dedicato a questo compito.

PANORAMICA DELLA SITUAZIONE

La sicurezza rimane un obbligo prioritario per i dirigenti di alto livello. Le aziende più attente hanno compreso l'importanza di una sicurezza efficace, che costituisce la base per il lavoro in un ambiente caratterizzato da numerose minacce in costante evoluzione perpetrate da malintenzionati coordinati e ben finanziati.

Secondo il sondaggio Future Enterprise Resiliency and Spending Survey (FERS) di IDC, condotto nel marzo 2023 tra gli ITDM delle aziende con almeno 500 dipendenti, negli ultimi 12 mesi oltre il 50% delle imprese intervistate a livello globale ha subito un attacco ransomware e una conseguente interruzione operativa. Secondo più di un terzo dei soggetti appartenenti a questo gruppo, l'attacco ha interrotto l'attività aziendale per almeno una settimana. Le grandi imprese, anche se dotate di efficaci protocolli di sicurezza, non sono immuni da questi attacchi. La percentuale più elevata delle interruzioni dovute al ransomware riguarda le aziende dotate di un numero di dipendenti compreso tra 1.000 e 2.499 (71%), seguite da quelle con 2.500 - 4.999 (72%) e 5.000 - 9.999 unità di personale (70%). In altre parole, le aziende di ogni dimensione possono subire questi attacchi.

Secondo il sondaggio, gli endpoint sono il principale veicolo degli attacchi ransomware. I punti iniziali di compromesso includono la navigazione sul Web (21%), supporti removibili (18%), allegati alle e-mail (17%), aziende della filiera (17%), URL presenti nelle e-mail (14%) e attività condotte dal personale interno (8%).

La costante transizione verso un maggior numero di dipendenti che lavorano in situazioni ibride e remote ha reso solo più complicate le sfide legate al ransomware e ad altri rischi della sicurezza per l'IT. Secondo l'indagine Endpoint Security Survey, condotta da IDC nel dicembre 2022, oltre il 97% delle organizzazioni consente ai propri dipendenti di lavorare a distanza. Nonostante si preveda che tale numero diminuisca nei prossimi dodici mesi, rimarrà molto elevato nel prossimo futuro.

Nel tentativo di gestire le criticità legate a elementi quali l'ampia forza lavoro operativa a distanza, le aziende stanno adottando sempre di più le strategie zero-trust. Queste best practice si basano su controlli di sicurezza di base, difese avanzate per la protezione degli endpoint, verifica della legittimità dei dispositivi in grado di connettersi alla rete e autenticazione efficace degli utenti.

Tenendo conto di questi elementi, come si evince dalla figura 1, non sorprende che i partecipanti al nostro sondaggio abbiano indicato in modo schiacciante il miglioramento della sicurezza dei dati e dei computer come le principali priorità per il settore IT.

Inoltre, come indicato nella figura sottostante, il terzo argomento più importante per i reparti IT è il miglioramento della produttività dei dipendenti attraverso l'utilizzo di dispositivi di qualità. Alla richiesta di indicare i tre argomenti più importanti nel campo della sicurezza, gli intervistati hanno citato più volte i dispositivi di qualità. Si tratta di un concetto molto importante: per quanto sia fondamentale, la sicurezza non deve compromettere la produttività dei dipendenti. I dispositivi di qualità garantiscono la sicurezza e soddisfazione dell'utente finale senza imporre procedure di protezione.

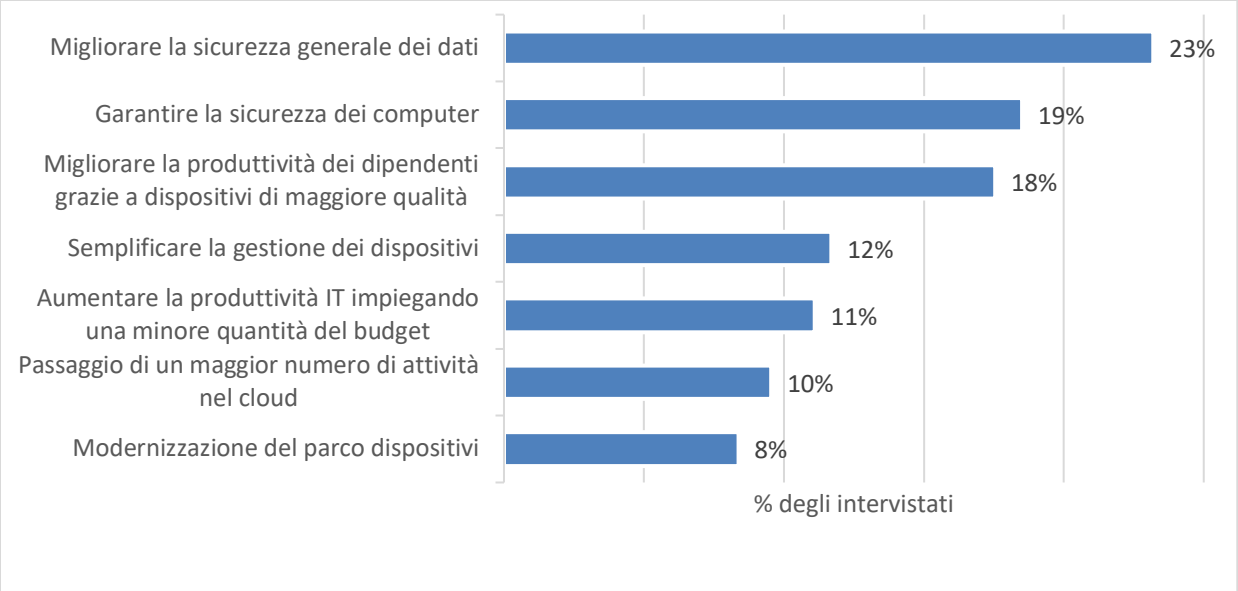
Secondo gli ITDM, la sicurezza è il fattore decisivo per la scelta di un nuovo fornitore di computer, seguita dalle prestazioni, dal supporto delle applicazioni esistenti e dall'integrazione con l'infrastruttura IT. Sorprendentemente, le specifiche tecniche sono state indicate con la minore frequenza in assoluto.

La figura 1 contiene un elenco delle principali priorità dei reparti IT, mentre la figura 2 indica le principali valutazioni per la scelta di un fornitore di computer.

FIGURA 1

Principali priorità dell'IT: sicurezza dei dati e degli endpoint

D. Quali tra i seguenti argomenti IT, rappresentano oggi una priorità per la sua azienda?



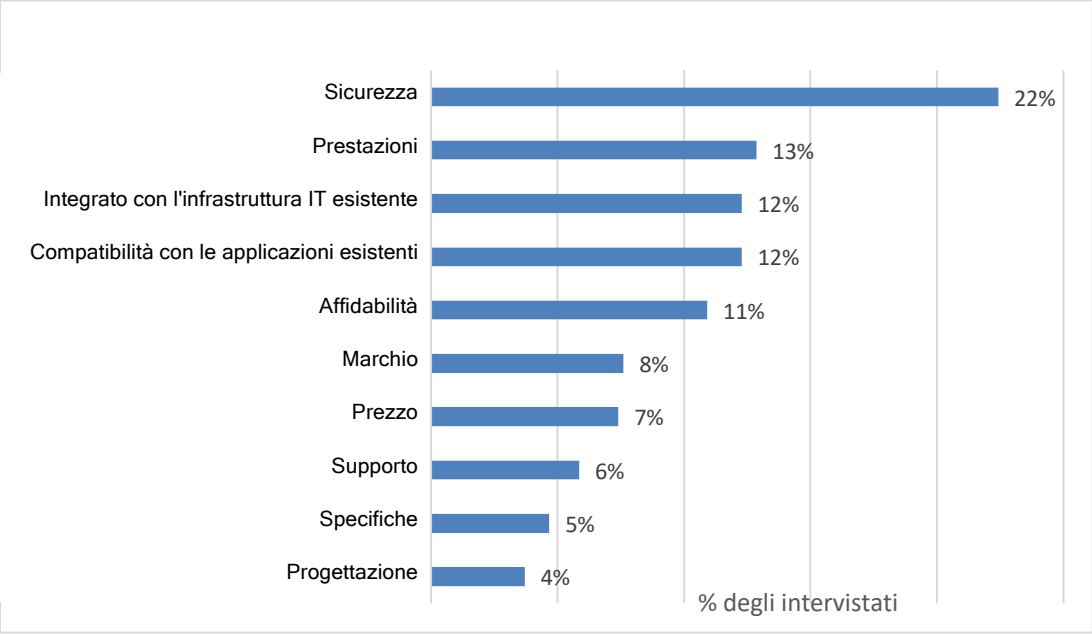
Fonte. Sondaggio Secure Endpoint di IDC, n=513

Nota. I dati includono gli elementi classificati come più importanti (indicati al primo posto)

FIGURA 2

Fattori principali per la scelta di un fornitore di computer

D. Quali sono i fattori decisivi per la scelta di un computer per la sua azienda?



Fonte. Sondaggio Secure Endpoint di IDC, n=513

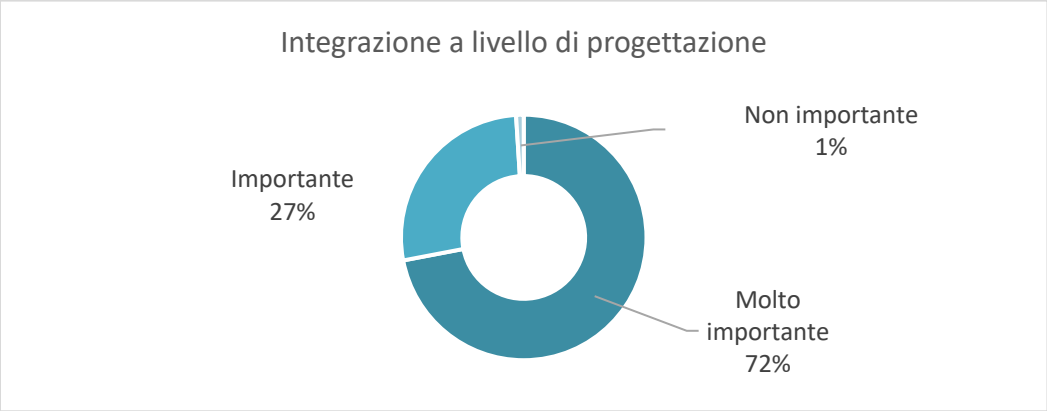
Nota. I dati includono gli elementi classificati come più importanti (indicati al primo posto)

I due elementi indicati con maggiore frequenza dagli intervistati erano la sicurezza e protezione integrata dei dati. L'integrazione della sicurezza a livello hardware, firmware e sistema operativo per la protezione dalle minacce attuali e future è un aspetto di importanza essenziale per il 72% dei soggetti interpellati, di una certa importanza per il 27% e scarsamente rilevante solo per l'1% del campione. Approfondendo l'analisi dei dati, rispettivamente l'84% e il 75% degli ITDM delle aziende sanitarie e finanziarie considera la sicurezza come un elemento essenziale, così come il concetto di protezione integrata dei dati. Il 71% degli intervistati ritiene la crittografia dei dati integrata a livello hardware un elemento essenziale, il 29% considera questa funzione importante e nessun soggetto interpellato ripone una scarsa fiducia in questo tipo di caratteristica. Consultare la figura 3 per maggiori dettagli sulla sicurezza e crittografia integrata dei dati.

FIGURA 3

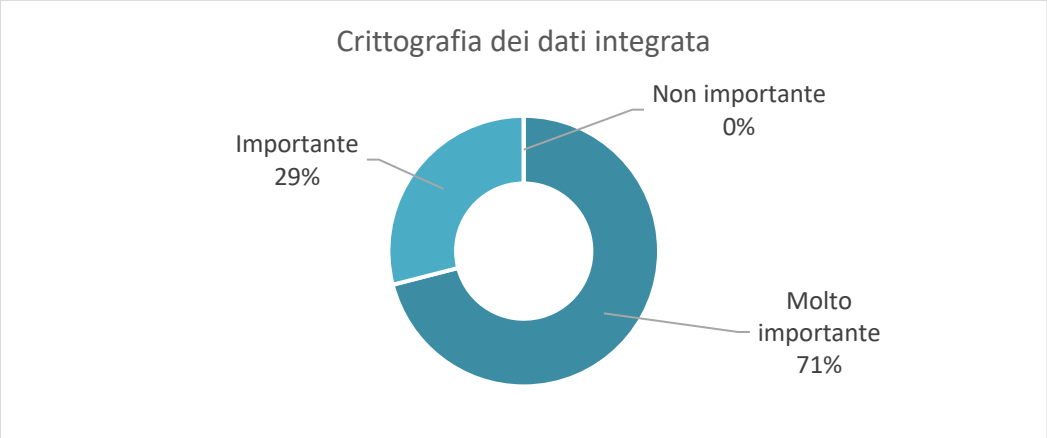
Importanza della sicurezza e crittografia integrata dei dati

D. Qual è l'importanza dell'integrazione, a livello hardware, firmware e sistema operativo, della sicurezza per la protezione dalle minacce attuali e future?



Fonte. Sondaggio Secure Endpoint di IDC, n=513

Qual è l'importanza delle funzionalità di crittografia dei dati integrate a livello hardware?



Fonte. Sondaggio Secure Endpoint di IDC, n=513

Anche se l'hardware dotato di sicurezza e crittografia dei dati integrata è un elemento molto importante, gli esperti di sicurezza considerano gli utenti finali come l'anello debole di qualsiasi catena di protezione. Questo scenario giustifica l'introduzione di una serie di procedure di autenticazione avanzata, che vengono ottimizzate in modo continuativo dai fornitori di prodotti tecnologici al fine di migliorarne l'efficacia. Secondo la nostra indagine, numerose organizzazioni sono ancora in ritardo in questo campo, ma il 68% degli intervistati utilizza le password complesse e il 63% l'autenticazione a due fattori.

Esistono anche aspetti meno positivi. Ad esempio, solo il 23% delle aziende interpellate utilizza le tecnologie di single sign-on (SSO) e appena il 20% la sicurezza biometrica (ad es. identificazione tramite impronte digitali o volto). Inoltre, il 56% dei soggetti intervistati considera l'autenticazione biometrica come una tecnologia più sicura delle password, il 35% abbastanza più sicura, il 9% la considera altrettanto sicura e nessuno (0%) ritiene tale tecnologia meno sicura rispetto alle password.

Le passkey sono una nuova tecnologia di autenticazione che consiste in una credenziale digitale basata su una coppia di chiavi. Si tratta di una soluzione molto più sicura di una semplice password. Trattandosi di una tecnologia di recente introduzione, al momento viene utilizzata solo dal 14% degli intervistati. Gli ITDM più previdenti dovrebbero valutare con attenzione questa tecnologia. Per maggiori dettagli sull'uso dell'autenticazione degli utenti, consultare la figura 4.

FIGURA 4

Metodi di autenticazione degli utenti

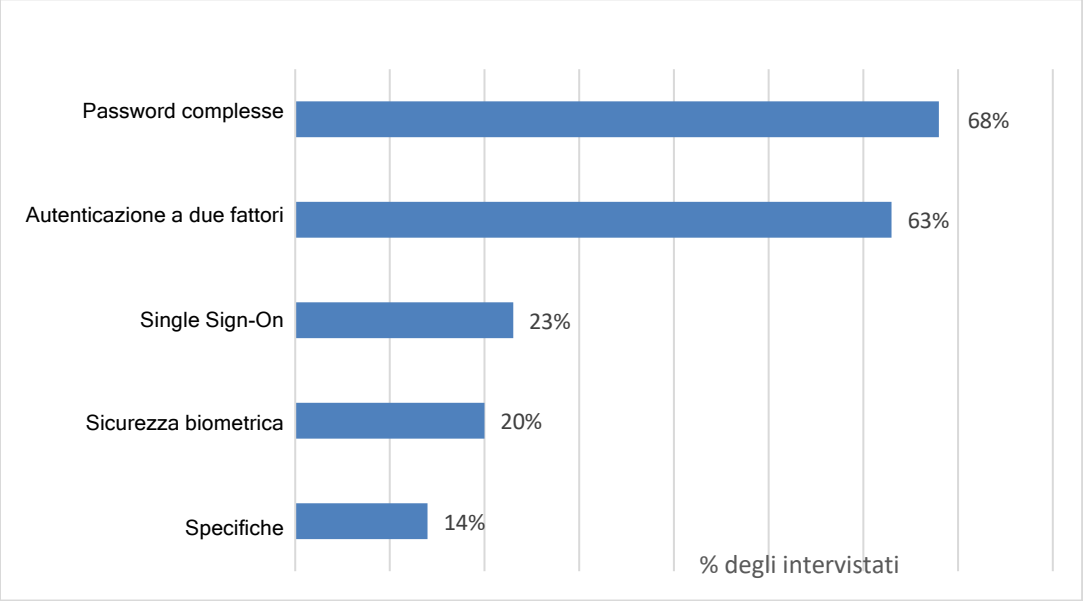
D1. La sua azienda impone ai dipendenti l'utilizzo di password complesse per l'accesso ai computer di lavoro?

D2. La sua azienda utilizza computer dotati di misure di sicurezza biometriche, come ad esempio gli scanner per impronte digitali?

D3. La sua azienda sta prendendo in considerazione i vantaggi offerti dall'utilizzo delle passkey?

D4. La sua azienda impone l'utilizzo dell'autenticazione a due fattori?

D5. La sua azienda utilizza le funzionalità di Single Sign-on (SSO)? (S/N)



Fonte. Sondaggio Secure Endpoint di IDC, n=513

I dati indicano la percentuale delle risposte affermative.

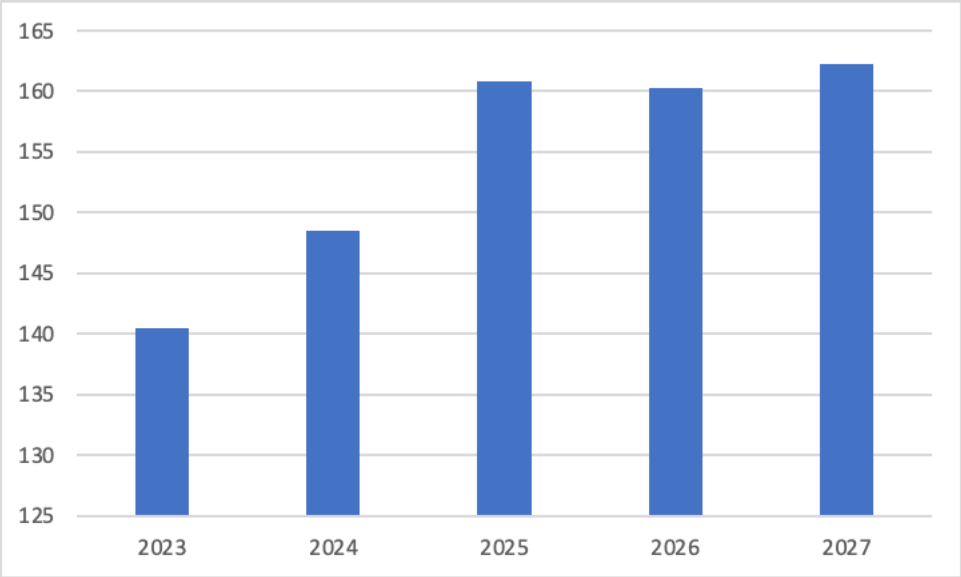
Un'elevata percentuale delle aziende intervistate non utilizza nemmeno i protocolli di autenticazione di base, vale a dire le password complesse (32%) o l'autenticazione a due fattori (37%). **In tal senso, consigliamo di valutare l'implementazione** di un tipo di autenticazione coerente in tutta

l'organizzazione. Una volta completata questa analisi, occorre prendere in considerazione la sinergia tra le funzionalità di SSO e un efficace protocollo di autenticazione principale. Infine, in corrispondenza del prossimo aggiornamento hardware, consigliamo di prendere in considerazione solo computer in grado di offrire i massimi livelli di autenticazione, vale a dire sicurezza biometrica e passkey, che consentono ai dipendenti di accedere in modo rapido e sicuro a computer, applicazioni e siti Web.

Concludiamo questa sezione prendendo in esame il problema dell'aggiornamento dell'hardware. Numerose aziende utilizzano computer ormai prossimi alla sostituzione. Un'azienda dotata di endpoint acquistati nel 2020 possiede computer risalenti quasi a quattro anni fa, un periodo in cui la sicurezza hardware si è evoluta per rispondere alle nuove minacce. Inoltre, gran parte di questi prodotti è stata commercializzata prima dell'adozione di massa del lavoro a distanza e ibrido, risultando priva di funzionalità come fotocamere, microfoni e altoparlanti di alta qualità. Questi elementi consentono ai dipendenti di utilizzare in modo ottimale le app di collaborazione e conferenza Web, divenute ormai indispensabili per ogni azienda. Secondo il Personal Computing Device Tracker di IDC, nei prossimi tempi, dopo diversi anni di stagnazione, è prevista una crescita delle vendite in questa categoria di prodotti. Nota: le unità commerciali indicano i dispositivi acquistati dai soggetti aziendali (non privati). La figura 5 indica le previsioni di IDC sulle vendite dei computer per privati e aziende.

FIGURA 5

Previsioni sui computer commerciali a livello globale



Fonte. IDC PCD Tracker, agosto 2023

Per restare competitive sul mercato e attrarre (e mantenere) i talenti più capaci, le aziende devono rivedere continuamente le esigenze informatiche dei dipendenti. Se un tempo i reparti IT erano costretti a scendere a compromessi tra la sicurezza e soddisfazione dei dipendenti, adesso esistono prodotti in grado di evitare questo tipo di vie di mezzo. Infine, un'**altra best practice da considerare è** l'applicazione dei principi di accesso "zero trust" alla prossima implementazione hardware. Si tratta di una strategia basata su un semplice presupposto: qualsiasi dispositivo non verificato che richieda l'accesso a una risorsa aziendale verrà considerato non attendibile. Il concetto di "zero trust" si basa su tecnologie e processi in grado di verificare lo stato della sicurezza di un dispositivo (se possibile, a

livello di hardware, applicazioni IT, sicurezza e via dicendo), di una rete di connessione (ad es. Wi-Fi pubblico o rete privata) e dell'identità dell'utente.

Valutare l'acquisto dei Mac per le aziende

Sempre più reparti IT aziendali stanno adottando i Mac, una scelta evidenziata dai risultati del nostro sondaggio. Il 76% dei soggetti intervistati, che lavorano in aziende dotate di una vasta gamma di sistemi operativi, considera i Mac i computer più sicuri sul mercato. Nei prossimi 12 mesi, il motivo principale dell'adozione dei Mac da parte di queste aziende sarà la sicurezza (47%), funzionalità seguita a ruota dalla facilità di implementazione e gestione (36%).

I prodotti Apple offrono un'esperienza e sicurezza eccellente a livello hardware e software. Un esempio di questo concetto è Touch ID, una funzione di sicurezza biometrica integrata nei prodotti della casa di Cupertino. I processori Apple sono dotati di Secure Enclave, una funzione che consente di crittografare e proteggere il passcode utilizzato per la protezione dei dati di Touch ID.

L'opinione dei clienti Apple

"Una delle funzionalità più importanti dei prodotti Apple è l'integrazione della privacy e sicurezza. Non si tratta di un elemento aggiunto in un secondo momento, ma integrato a livello di progettazione, una caratteristica da noi molto apprezzata", Linda Jojo, vicepresidente esecutivo e responsabile delle relazioni con i clienti della United Airlines

Per prevenire il rischio di compromissione del sistema operativo e della sequenza di boot, i Mac sono dotati delle funzioni Secure Boot, che consente di avviare il sistema solo in presenza di una versione crittograficamente certificata di macOS, e Signed System Volume, che protegge l'integrità del sistema operativo durante l'utilizzo. Anche i software non aggiornati rappresentano un rischio. Apple contrasta questo fenomeno attraverso l'automazione e protezione della distribuzione e installazione degli aggiornamenti software.

Il software di terze parti, un elemento essenziale per la produttività delle aziende, deve essere privo di malware. In tal senso, Apple utilizza un approccio a più livelli per la prevenzione delle minacce informatiche. Ad esempio, il Mac App Store analizza la presenza del malware in tutte le applicazioni disponibili. Inoltre, Apple sottopone le applicazioni scaricabili dal Web a un servizio di controllo che esegue una scansione malware. Gatekeeper è una funzione di macOS che impedisce l'esecuzione delle app non firmate, mentre XProtect è uno strumento anti-malware che arresta e rimuove il software dannoso.

I dati sono tra le risorse più preziose di un'organizzazione. Occorre proteggere le informazioni aziendali a ogni costo. La combinazione tra la crittografia hardware di FileVault, i protocolli VPN supportati da Apple e la crittografia end-to-end dei servizi della casa di Cupertino (ad es. iMessage e iCloud) garantisce la protezione dei dati, siano essi inattivi, in transito e in uso.

L'ingegneria sociale è una delle abilità più pericolose utilizzate dai criminali informatici. Apple aiuta gli utenti a prevenire questo tipo di trappole attraverso Safari Fraudulent Website Warning, una funzione che indica i siti Web dannosi visitati con Safari. A causa del frequente furto delle credenziali di autenticazione, Apple supporta le passkey per aiutare le organizzazioni a modernizzare i propri metodi di autenticazione senza compromettere l'esperienza degli utenti finali.

Una sicurezza efficace richiede una gestione dei dispositivi altrettanto valida. A tal fine, Apple offre funzionalità come un framework di gestione integrato con Mobile Device Management (MDM), Apple Business Manager, che offre l'implementazione zero-touch e il collegamento alle soluzioni MDM, e le

API di Endpoint Security per Mac, che consentono agli sviluppatori di creare soluzioni in grado di monitorare, analizzare e contrastare le minacce alla sicurezza. Apple offre anche le integrazioni dell'identità con un framework SSO integrato e compatibile con i moderni fornitori di soluzioni di identità (Identity Provider, IdP).

Infine, le funzioni di sicurezza aggiuntive di macOS, tra cui gli aggiornamenti software principali e secondari, vengono offerte in via del tutto gratuita ai clienti aziendali o privati.

SFIDE E OPPORTUNITÀ

Nonostante la continua evoluzione delle minacce informatiche, i reparti IT delle aziende devono offrire una maggiore produttività usando una minore quantità di risorse finanziarie, operative e di personale. Oltre a gestire i continui rischi di sicurezza che interessano ogni azienda, i reparti IT devono anche ottimizzare la produttività e soddisfazione dei dipendenti attraverso la distribuzione di hardware, software e servizi di qualità. È difficile lavorare in modo ottimale e migliorare allo stesso tempo la sicurezza, produttività e soddisfazione dei dipendenti. Tuttavia, questo percorso consente ai reparti IT di rivalutare l'hardware, il software e i servizi acquistati, i fornitori e le modalità di supporto di una forza lavoro sempre più ibrida. Inoltre, consigliamo anche di rivedere i modelli relativi al costo totale di proprietà (TCO) e allinearli con le modalità d'acquisto della tecnologia da parte delle aziende.

CONCLUSIONI

La sicurezza resterà ancora per molto tempo una delle principali preoccupazioni dei reparti IT. In un periodo come quello attuale, caratterizzato da budget IT limitati e frequenti aggiornamenti dell'hardware, consigliamo di valutare con attenzione i fornitori e prendere in esame l'implementazione delle buone prassi di autenticazione, le soluzioni "zero-touch" e l'acquisto di un hardware in grado di attuare questi cambiamenti. Come regola generale, consigliamo di non assegnare alla sicurezza una maggiore priorità rispetto alla produttività e soddisfazione dei dipendenti e di scegliere prodotti informatici dotati di funzionalità di sicurezza e crittografia dei dati integrate. In questo modo sarà possibile offrire una protezione massima e un'esperienza piacevole agli utenti finali.

Informazioni su IDC

International Data Corporation (IDC) è il principale fornitore al mondo di informazioni di mercato, servizi di consulenza e organizzazione di eventi per il settore IT, delle telecomunicazioni e tecnologie consumer. IDC aiuta professionisti, dirigenti e investitori IT a prendere decisioni informate in materia di acquisti tecnologici e strategie di business. Gli oltre 1.100 analisti di IDC mettono a disposizione la propria esperienza a livello globale e locale per individuare opportunità e andamenti tecnologici di settore in oltre 110 Paesi. Per 50 anni, IDC ha fornito approfondimenti strategici utili ai clienti per raggiungere i propri obiettivi aziendali più importanti. IDC è una consociata di IDG, azienda leader globale nel campo di media, ricerca ed eventi del settore tecnologico.

Sede centrale

140 Kendrick Street
Building B
Needham, MA 02494
USA
+1 508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com