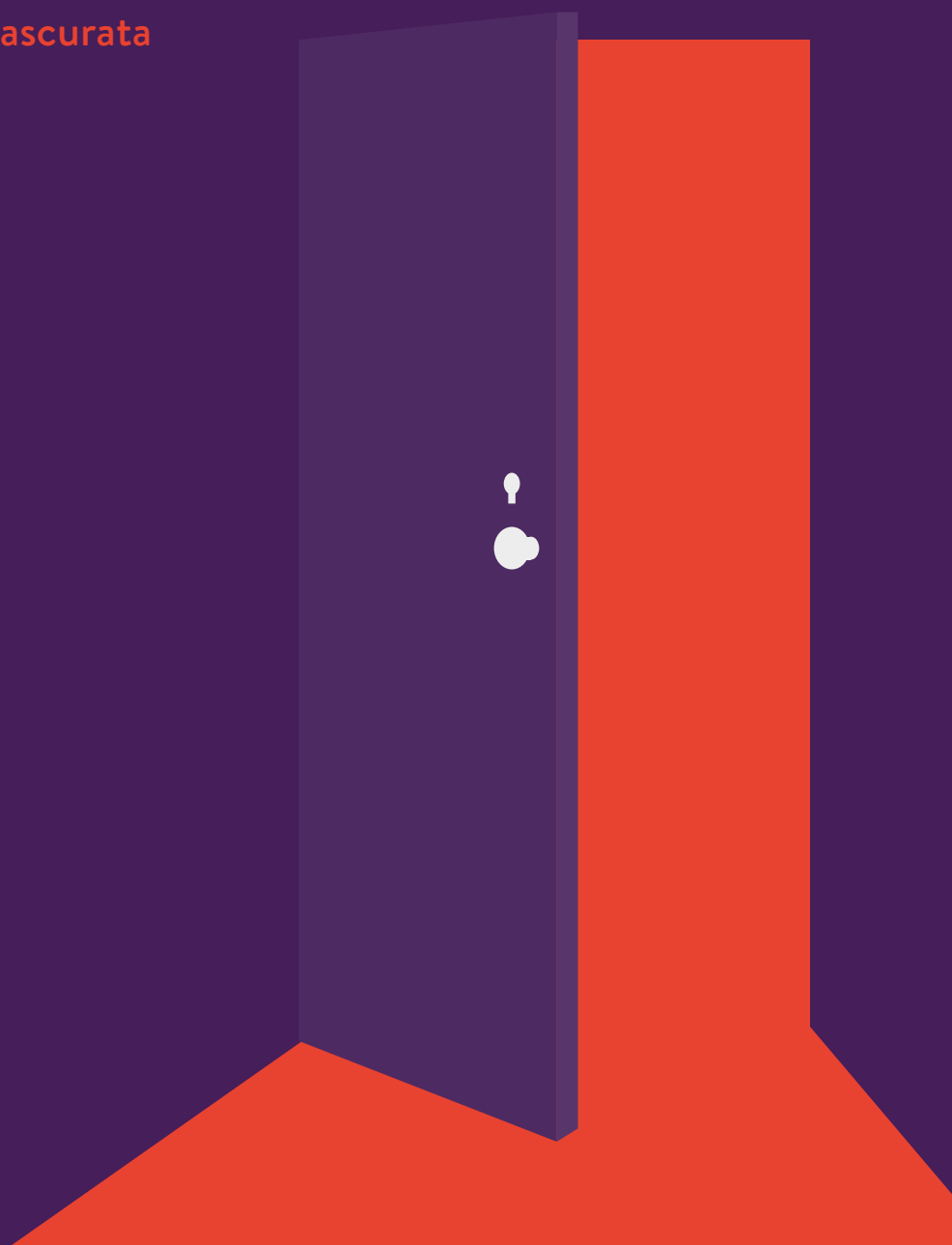
WHITE PAPER

PORTE SENZA PROTEZIONE

UNA RICERCA MOSTRA CHE LE STAMPANTI SONO VULNERABILI AGLI ATTACCHI INFORMATICI

Mentre il personale IT si concentra su altri endpoint, la sicurezza delle stampanti aziendali viene trascurata



Le stampanti sono un bersaglio facile: un numero troppo elevato di stampanti connesse in rete non presenta restrizioni agli accessi e non è messo in sicurezza.

La minaccia è reale e non deve essere ignorata. Le stampanti di classe enterprise si sono evolute in potenti dispositivi di rete presentando le stesse vulnerabilità che caratterizzano qualsiasi altro endpoint in rete. Si tratta di punti di ingresso non protetti, realmente esposti ad attacchi informatici; possono inoltre fornire l'accesso ai dati finanziari e privati dell'azienda, con conseguenze davvero preoccupanti.

Ciononostante, secondo un recente sondaggio, che Spiceworks ha condotto interpellando oltre 300 decision-maker IT aziendali, solo il 16% degli intervistati ritiene che le stampanti siano a rischio di violazione/minaccia della sicurezza in misura nettamente inferiore rispetto a desktop/notebook e dispositivi mobile.[1] Questa percezione ha alterato l'approccio del personale IT nei confronti della sicurezza di rete. Anche se quasi tre aziende su cinque hanno messo a punto procedure di sicurezza per le stampanti, questa percentuale è di gran lunga inferiore rispetto a quella relativa agli altri endpoint, lasciando così le stampanti vulnerabili, sebbene esistano soluzioni di facile implementazione per tutelare questo particolare punto di ingresso.

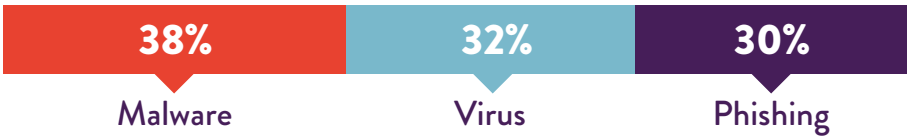
Il presente white paper mostra i dati sulla sicurezza delle stampanti in base a un sondaggio Spiceworks, l'impatto delle violazioni alla sicurezza e alcune moderne funzionalità di sicurezza integrate progettate per proteggere dagli attacchi informatici.

SOLO IL 16% DEGLI INTERVISTATI RITIENE CHE LE STAMPANTI SIANO A RISCHIO DI ATTACCHI INFORMATICI.[1]

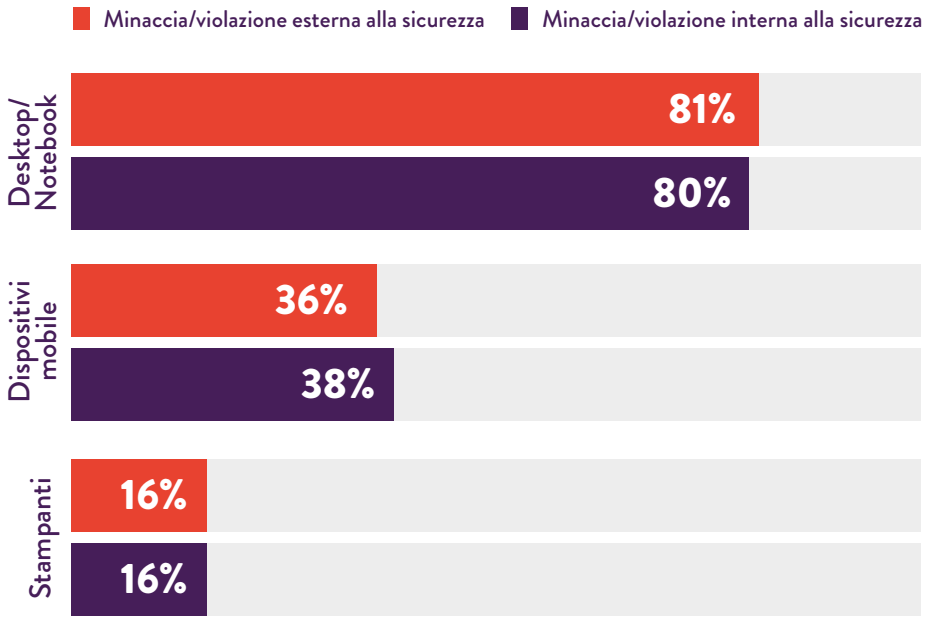
PUNTI DI ACCESSO PER GLI ATTACCHI

Nel sondaggio Spiceworks, il 74% degli intervistati (netto) ha dichiarato che la propria azienda ha riscontrato almeno qualche tipo di minaccia o violazione esterna alla sicurezza IT nel corso dell'ultimo anno. Il 70% (netto) ha riscontrato una minaccia o una violazione IT interna, generalmente in seguito a un errore dell'utente, all'uso di dispositivi personali a scopi lavorativi o a causa di dipendenti che utilizzano una rete domestica o pubblica nello svolgimento dell'attività lavorativa.[1]

PRINCIPALI MINACCE/VIOLAZIONI ESTERNE RISCONTRATE AI DANNI DELLA SICUREZZA IT



Le minacce principali si insinuano principalmente attraverso desktop e laptop, altre arrivano per mezzo di dispositivi mobile e stampanti.[1] (Il 16% che arriva tramite stampante è nettamente superiore rispetto al 4% rilevato in uno studio analogo Spiceworks del 2014). È inoltre possibile che il numero di attacchi che arriva tramite stampanti sia sottostimato, poiché le stampanti non sono monitorate minuziosamente come i PC e i dispositivi mobile.



STIAMO IGNORANDO LE STAMPANTI

Il sondaggio Spiceworks mette in rilievo come la sicurezza delle stampanti rappresenti spesso una questione secondaria.

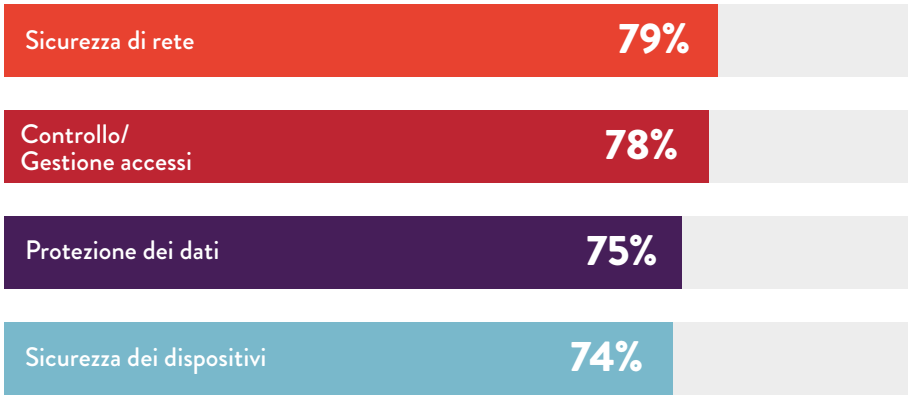
Le aziende sono ben consapevoli dell'importanza della sicurezza di rete, endpoint e dati. Infatti, oltre tre quarti degli intervistati utilizza la sicurezza di rete, la gestione/il controllo degli accessi, la protezione dei dati o la sicurezza endpoint, oppure una combinazione delle tre.[1]

Queste soluzioni sono tuttavia implementate con minor frequenza sulle stampanti. Mentre se l'83% degli intervistati utilizza la sicurezza di rete su desktop/notebook e il 55% su dispositivi mobile, solo il 41% ne fa uso sulle stampanti.[1]

La disparità è ancora più evidente per la sicurezza degli endpoint:

Non arrivano a un terzo (28%) gli intervistati che dichiarano di implementare certificati di sicurezza sulle proprie stampanti, rispetto al 79% per quel che concerne i PC e al 54% riferito ai dispositivi mobile[1] (apex).

PRINCIPALI PROCEDURE DI SICUREZZA PER ENDPOINT



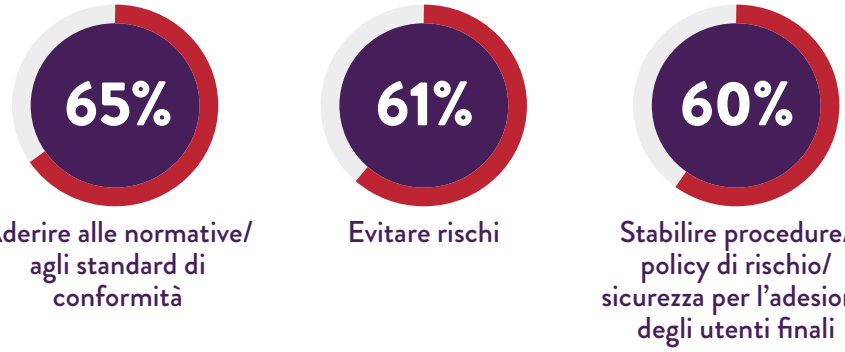
Tra le protezioni applicate sui dispositivi endpoint in genere, è stato rilevato che le misure di sicurezza più utilizzate per le stampanti erano la sicurezza dei documenti, la sicurezza di rete e controllo dell'accesso. Una percentuale inferiore alla metà degli intervistati ha tuttavia dichiarato che la propria azienda utilizza questo tipo di misura sulle stampanti.[1]

Alcune aziende si avvalgono di procedure di sicurezza specifiche per le stampanti, ma anche in questo caso, si tratta di procedure molto eterogenee. Poco più del 40% delle aziende ha implementato l'autenticazione utente, e meno del 40% ha utilizzato password amministratore per l'interfaccia della configurazione web.[1] Per una difesa efficace, ogni azienda dovrebbe utilizzare una combinazione di tutti questi approcci, e molti altri.

PRINCIPALI RPOCEDURE DI SICUREZZA SPECIFICHE DELLE STAMPANTI

Quando si parla di conformità di endpoint e procedure di controllo, i controlli di sicurezza delle stampanti si collocano sempre dietro a quasi tutti gli altri endpoint. Quasi il 90% delle aziende ha implementato policy di sicurezza delle informazioni, ma che non si estendono in genere alle stampanti. Ad esempio, mentre il 57% degli intervistati ha dichiarato di aver implementato protezioni antimalware sui propri PC, solo il 17% le ha implementate sulle stampanti.[1]

QUASI 9 PROFESSIONISTI IT SU 10 DICHIARANO CHE LA PROPRIA AZIENDA HA IMPLEMENTATO UNA POLICY DI SICUREZZA DELLE INFORMAZIONI PER LE RAGIONI SEGUENTI:



È chiaro che le aziende non stanno attribuendo la giusta importanza alla sicurezza delle stampanti, ma dovranno sicuramente farlo.

“Molte stampanti sono ancora dotate di password predefinite, talvolta non dispongono di password, oppure in dieci utilizzano la stessa password”, come ha affermato Michael Howard, responsabile della consulenza sulla sicurezza per HP, a Computerworld a giugno. “Una stampante senza protezione con password è una miniera d’oro per un hacker. Una delle violazioni a cui spesso assistiamo è un attacco man-in-the-middle, che consiste nel prendere il controllo di una stampante e deviare i documenti in arrivo a un notebook, prima che vengano stampati. In questo modo sono visibili tutti i documenti che un amministratore invia in stampa”.[2]

L’IMPATTO POTENZIALE DELLE INTRUSIONI NELLE STAMPANTI

Secondo un analista esperto di minacce informatiche presso Bitdefender, Bogdan Botezatu, le stampanti presentano un’importante criticità potenziale della sicurezza. “Ci avvaliamo della telemetria nei nostri laboratori adibiti alla valutazione delle vulnerabilità. Il router non è più il dispositivo più esposto su Internet, la stampante ha preso il suo posto”.[3]

Questa vulnerabilità può avere effetti gravi su un’azienda. È sufficiente una singola stampante non protetta per esporre l’intera rete di dispositivi connessi al rischio di attacchi, permettendo così agli hacker di spiare nei dispositivi in rete e compromettendo la sicurezza dell’intera rete.

1. Aumento delle chiamate all’help desk e dei tempi dedicati al supporto

2. Riduzione di produttività/ efficienza

3. Aumento del tempo di inattività del sistema

4. Aumento del tempo dedicato alle chiamate per la richiesta di assistenza

5. Aumento dell’imposizione di policy agli utenti finali

Tutti abbiamo assistito agli effetti delle violazioni della sicurezza. Nel sondaggio Spiceworks, gli intervistati hanno dichiarato quali sono le prime cinque conseguenze di una violazione.[1]

Ma la violazione di una stampante può avere conseguenze persino più gravi, in particolare se si utilizza un dispositivo multifunzione in grado di memorizzare elettronicamente i dati stampati. I processi di stampa memorizzati nella cache della stampante permettono agli hacker di ottenere l’accesso a informazioni aziendali e personali riservate.

Un fatto ancora più preoccupante è che gli hacker possono accedere alla rete più ampia dell'azienda attraverso una stampante non protetta, impossessandosi di dati importanti come dati fiscali e numeri di previdenza sociale, informazioni finanziarie o promemoria interni e documenti. Queste informazioni sottratte non solo possono influire sui singoli dipendenti ma possono essere utilizzate dalla concorrenza o provocare danni gravi alla reputazione di un'azienda.

LA SOLUZIONE FACILE: OPZIONI DI SICUREZZA INTEGRATE

È evidente che le aziende devono affrontare la questione della sicurezza anche per quanto concerne le stampanti. Alcune stampanti moderne di livello enterprise sono caratterizzate da funzionalità di sicurezza integrate di facile utilizzo che ne contrastano le minacce. Esse includono:

- Rilevamento, automatico degli attacchi, protezione e auto-riparazione
- Monitoraggio dell'utilizzo per impedire accessi non autorizzati
- Opzioni di accesso semplici come PIN o smartcard
- Implementazione di un lettore di badge di prossimità che consenta agli utenti di autenticarsi rapidamente e stampare con sicurezza da una stampante utilizzando un badge di identificazione
- Stampa protetta crittografata per documenti sensibili

In fase di scelta della prossima stampante, sia essa desktop o multifunzione, analizzate le protezioni di sicurezza integrate e assicuratevi di attivarle. Avvalendovi di semplici funzionalità specifiche per stampanti come quelle elencate, il rischio di vulnerabilità per le stampanti è praticamente nullo. Dopo tutto, con l'Internet delle cose, esistono tanti altri punti di accesso di cui preoccuparsi: **le stampanti non devono rientrare in questa categoria.**

SIETE IN CERCA DI STAMPANTI PIÙ SICURE?

MAGGIORI INFORMAZIONI ›

Fonti:

[1] Sondaggio Spiceworks su 309 decision-maker IT in Nord America, EMEA e APAC per conto di HP, novembre 2016.

[2] "Printer Security: Is your company's data really safe?" *Computerworld,* 1 giugno 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet," *The Register*, 8 settembre 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/