

**Come
mantenere in
sicurezza i tuoi
documenti e tutti
i dati aziendali**



Gli ostacoli ai mancati investimenti nella sicurezza di stampa

Con la crescente minaccia di attacchi e violazioni di riservatezza sempre più pericolosi, la maggior parte delle piccole e medie imprese (PMI) è estremamente consapevole della necessità di proteggere i propri sistemi IT.

Per evitare violazioni di privacy e attacchi informatici bisogna scegliere tecnologie sicure e affidabili.

La gestione della sicurezza dell'ambiente IT costituisce una problematica che deve essere affrontata su larga scala. Stampanti, multifunzione e scanner devono essere protetti tanto quanto altre apparecchiature IT. Se trascurati, questi dispositivi rischiano di offrire agli hacker un facile accesso non autorizzato (backdoor) all'interno dell'organizzazione. Le PMI sono sempre più consapevoli dell'importanza di questo problema, con il **72%** delle aziende che afferma che la sicurezza delle proprie stampanti, multifunzione e scanner è di importanza critica. Questo aspetto è ancora più cruciale tra quelle organizzazioni che gestiscono dati sensibili in settori come i servizi professionali (**82%**) e l'assistenza sanitaria (**81%**).

Tuttavia, rimane ancora quasi un terzo delle organizzazioni che non ne riconoscono l'importanza. Allo stesso tempo, quasi la metà ritiene che la propria organizzazione non abbia investito a sufficienza nella sicurezza dei dispositivi di stampa.

Perché le aziende non investono nella sicurezza di stampa, nonostante ne riconoscano l'importanza?

La nostra ricerca evidenzia due specifici motivi:



Insufficiente responsabilizzazione per la sicurezza di stampa



Mancanza di comprensione e conoscenza delle norme e delle minacce relative alla sicurezza

Questo report è stato ideato per consentire ai decision maker delle PMI di comprendere l'importanza della sicurezza sia a livello di stampa che di soluzioni. Fa parte di una serie di report che aiutano i decision maker a capire come utilizzare al meglio le tecnologie digitali all'interno delle organizzazioni di piccole e medie dimensioni.

I report si basano su un solido programma di ricerca intrapreso tra i decision maker delle PMI nel perimetro EMEA. La serie è suddivisa in quattro report, ognuno dei quali affronta uno dei seguenti temi:

- Flussi di lavoro digitali
- Implementazione della corretta soluzione per la propria azienda
- Sicurezza
- Sostenibilità



Chi è responsabile della sicurezza delle stampanti?

Troppo spesso vi è una mancanza di chiarezza e di identificazione riguardo alla responsabilità individuale per la sicurezza di stampa. Quasi la metà delle PMI in tutta l'Europa occidentale (**44%**) dichiara che non è chiaro chi sia responsabile della sicurezza delle stampanti all'interno della propria organizzazione. Laddove la responsabilizzazione è insufficiente, è quindi probabile che il processo decisionale e l'implementazione della sicurezza di stampa ne risentano e che le aziende si trovino in una condizione di vulnerabilità.

E' probabile che nella maggior parte dei casi non esista un vero e proprio responsabile della sicurezza di stampa poiché solitamente la configurazione dei dispositivi di stampa non viene considerata un "punto debole" alla pari di altri dispositivi, come ad esempio i computer portatili.

Sebbene la nostra ricerca indichi come i decision maker si stiano iniziando a rendere conto che la sicurezza di stampa sia fondamentale, gli impiegati delle PMI sembra non si siano ancora posti il problema.




Le PMI sono particolarmente vulnerabili rispetto alla mancanza di responsabilità poiché spesso un numero molto ridotto di dipendenti si occupa dell'intera struttura di hardware e software dell'organizzazione. Se i professionisti IT non sono consapevoli dei rischi relativi alla sicurezza di stampa, questa può diventare una problematica con una priorità bassa.

Tuttavia, tutti i dipendenti all'interno di un'organizzazione hanno una certa responsabilità nel garantire la sicurezza delle informazioni sensibili.



Mentre gli specialisti IT sono responsabili della sicurezza dei dispositivi, i dipendenti hanno la responsabilità di garantire la sicurezza dei dati. La sicurezza dei dati costituisce forse l'area di maggior rischio per le informazioni sensibili dell'azienda.

La sicurezza dei dati riguarda molteplici rischi, tra cui:

-  accesso non autorizzato alle stampe
-  mancato logout (disconnessione utenza), dopo la stampa di documenti riservati
-  mancanza di tracciabilità di chi ha avuto accesso a determinati documenti sulla stampante

In quasi 9 aziende su 10 si è verificato un problema di sicurezza di stampa...



... e sette su dieci (**72%**) sostengono che la sicurezza dei dati costituisce una minaccia più grande della sicurezza dei dispositivi. Tuttavia, attualmente, meno di un'azienda su tre afferma di essere pienamente convinta che la propria infrastruttura di stampa adotti misure di sicurezza sufficienti. Questo in confronto al **53%** di aziende che ritiene di avere implementato il corretto livello di sicurezza dei propri dispositivi.

La maggior parte delle PMI (**64%**) afferma che garantire la sicurezza dei propri dati costituisce una priorità assoluta. Questa è considerata una problematica chiave e può costituire un vero ostacolo all'efficienza delle prestazioni.

Attualmente, quasi la metà delle PMI (**48%**) afferma di avere adottato poche soluzioni o nessuna per tracciare i processi di stampa. Non c'è da stupirsi che quasi nove imprese su dieci (**86%**) dichiarino di aver avuto un problema di sicurezza relativo alla stampa.

Questi problemi di sicurezza riguardano nella maggior parte dei casi: documenti riservati lasciati incustoditi sulla stampante, stampe non prelevate o dipendenti che ritirano documenti riservati che non gli appartengono.

Di conseguenza, la maggior parte delle PMI (**64%**) sta iniziando ad adottare delle misure per affrontare i problemi di sicurezza relativi alla stampa, limitando l'accesso a certe stampanti o prevedendo l'utilizzo di schede di identificazione/ codici PIN per rilasciare le stampe solo alle persone autorizzate.

Nei prossimi anni, sarà importante per tutte le aziende introdurre processi più sicuri e per quelle che hanno già intrapreso il nuovo percorso mantenere e migliorare la trasparenza e il controllo delle attività di stampa.

I tre obiettivi principali per la sicurezza delle informazioni formano l'acronimo CIA (dal'inglese: Confidentiality, Integrity, Availability ovvero Riservatezza, Integrità e Disponibilità).

Questi riguardano sia la sicurezza dei dispositivi che quella dei dati:

Riservatezza

Proteggere i dati aziendali riservati per garantire che vengano condivisi solo con il destinatario previsto. La chiave di tutto questo è costituita dall'autenticazione e dalle misure di autorizzazione che richiedono agli utenti di verificare la propria identità e di ottenere l'autorizzazione per utilizzare la funzionalità desiderata, prima che venga rilasciata qualsiasi stampa.

Integrità

Garantire che il firmware del dispositivo sia sicuro e resiliente agli attacchi di hacking e ad altre minacce esterne.

Disponibilità

Garantire che il dispositivo sia perfettamente funzionante e accessibile agli utenti autorizzati per eseguire attività fondamentali.

La mancanza di conoscenze specifiche in materia favorisce procedure di sicurezza inefficienti

Meno di un terzo (**32%**) dei principali decision maker IT che lavorano all'interno di PMI afferma di avere una conoscenza avanzata della sicurezza tecnologica e delle potenziali minacce.

Se i decision maker in materia di IT non dispongono di conoscenze sufficienti sulle minacce, le aziende continueranno ad avere difficoltà a mettere in atto le misure adeguate per proteggersi. Nelle PMI, il decision maker in materia di IT svolge tipicamente un ruolo che comprende un gran numero di piattaforme tecnologiche differenti. È comprensibile che non sia un esperto di sicurezza specifica per le stampanti.

Ad eccezione dei responsabili IT, non tutti all'interno di una azienda conoscono correttamente il linguaggio della sicurezza di stampa. Oltre la metà delle PMI (**51%**) afferma che ci sono troppi termini specialistici riguardo alla sicurezza di stampa - soprattutto in Francia e in Italia.

E quasi il 60% delle PMI afferma di avere una buona comprensione degli standard di sicurezza pertinenti.

A questo proposito, è anche improbabile che i decision maker abbiano una conoscenza approfondita rispetto ai partner tecnologici di stampa che potrebbero soddisfare meglio le loro esigenze di sicurezza. Di conseguenza, non sorprende che le aziende si rivolgano a marchi che "conoscono" per la fornitura di stampanti sicure, senza comprendere veramente quali misure di sicurezza adottino o meno.

I partner tecnologici devono fare di più per consentirvi di decodificare gli standard di sicurezza pertinenti e per garantirvi di scegliere la soluzione migliore per la vostra azienda.



Approfondimenti Brother

Data la natura complessa del panorama relativo alla sicurezza di stampa, Brother offre sette approfondimenti e raccomandazioni fondamentali per consentire alle PMI di proteggersi dalle profonde implicazioni finanziarie, legali e a livello di reputazione per la perdita di dati.



Integrare la sicurezza nelle scelte strategiche aziendali a livello direttivo

L'entità della devastazione causata dagli attacchi informatici e dalle violazioni dei dati, combinata con i requisiti previsti dalla normativa del regolamento generale sulla protezione dei dati (GDPR), implica che la sicurezza di stampa deve andare oltre la responsabilità dei reparti IT. Deve essere presa in considerazione strategicamente a livello direttivo con il coinvolgimento del direttore informatico (Chief Information Officer, CIO) e del direttore della sicurezza informatica (Chief Information Security Officer, CISO).



Effettuare un controllo approfondito

È fondamentale per le aziende scoprire qualsiasi potenziale vulnerabilità della sicurezza di stampa, provvedendo a includere il proprio ambiente di stampa nei regolari controlli di sicurezza. Questo è particolarmente importante se l'azienda dispone di una combinazione di dispositivi nuovi e di vecchia generazione. Per quanto riguarda i servizi di stampa gestita (MPS), occorre considerare che non solo la maggior parte dei fornitori offre valutazioni complete ma che una valutazione approfondita consente di organizzare il monitoraggio continuo dei dispositivi una volta che il parco installato viene ottimizzato e messo in sicurezza.



Cambiare le password amministrative preimpostate

Le password amministrative predefinite o preimpostate costituiscono un punto debole per i dispositivi di stampa: la buona notizia è che questo problema è facilmente risolvibile. Una volta installato il dispositivo, basta cambiare le password, optando per password complesse e sicure.



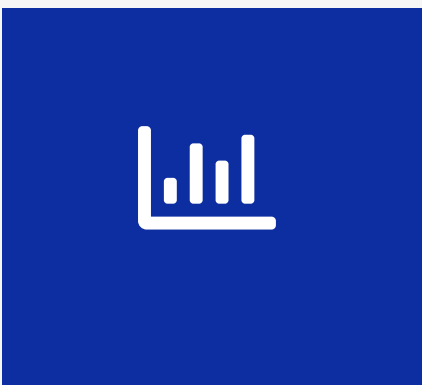
Aggiornare il firmware e applicare le patch di sicurezza

Le potenziali vulnerabilità di sicurezza dei dispositivi di stampa possono essere notevolmente ridotte aggiornando il firmware e configurando il dispositivo per gli aggiornamenti automatici. Se si hanno domande in merito, contattare il fornitore del proprio dispositivo di stampa per una consulenza.



Proteggere i processi di stampa

La protezione è necessaria non solo per i dispositivi di stampa, ma anche per i documenti da stampare. La crittografia end-to-end del traffico di rete garantisce il trasferimento sicuro dei processi di stampa alle stampanti. Poiché la maggior parte delle stampanti memorizza temporaneamente i lavori di stampa, è necessario assicurarsi che i dati siano criptati.



Monitorare i dispositivi

Conoscere lo stato attuale dei propri dispositivi di stampa offre una visione globale dell'intero ambiente di stampa. Le aziende dovrebbero prendere in considerazione l'utilizzo di strumenti software per monitorare i dispositivi e fare in modo che i problemi vengano risolti non appena si verificano. I dispositivi generano una grande quantità di dati che spesso è possibile utilizzare per identificare potenziali eventi relativi alla sicurezza e consentire una reazione tempestiva agli attacchi. Gli utenti dei servizi MPS possono anche ottenere regolari report di conformità, che dovrebbero includere il monitoraggio e la segnalazione delle violazioni dei dati.



Formare i dipendenti

Poiché molti episodi relativi alla perdita di dati sono provocati involontariamente, è fondamentale che le aziende informino adeguatamente i dipendenti sull'importanza di proteggere le informazioni sensibili affinché vengano sensibilizzati sui pericoli derivanti dalle minacce relative alla sicurezza. Spesso i fornitori di servizi MPS offrono assistenza per le esigenze di formazione.



Considerazioni finali

I sistemi di stampa possono aver rappresentato un aspetto trascurato della sicurezza organizzativa in passato, ma le PMI si stanno sempre più rendendo conto della loro importanza. Ciononostante, permangono notevoli problematiche da risolvere per l'implementazione della sicurezza di stampa.

Le PMI dovranno definire chiaramente le responsabilità in materia di sicurezza di stampa, per garantire che i dispositivi siano adeguatamente protetti e sempre aggiornati rispetto alle minacce.

Oltre alla sicurezza dei dispositivi, anche le violazioni della sicurezza dei dati costituiscono un aspetto fondamentale da prendere in considerazione e, per ridurre al minimo i rischi, sarà necessaria la collaborazione dei dipendenti dell'azienda.

Anche se esistono definizioni chiare delle responsabilità all'interno delle PMI, avere conoscenze sufficienti per gestire efficacemente la sicurezza di stampa costituisce comunque una problematica di primaria importanza. La tecnologia di stampa è sempre più complessa e nell'ambiente si utilizza in modo massiccio un linguaggio estremamente specialistico. Le aziende dovrebbero cercare di affidarsi a fornitori di fiducia per prendere decisioni efficaci.

Una configurazione di stampa efficace deve essere più che sicura. Gli altri report sulla Trasformazione digitale contengono maggiori informazioni sull'implementazione dei flussi di lavoro digitali, sulla massimizzazione della produttività e sulla sostenibilità delle soluzioni.

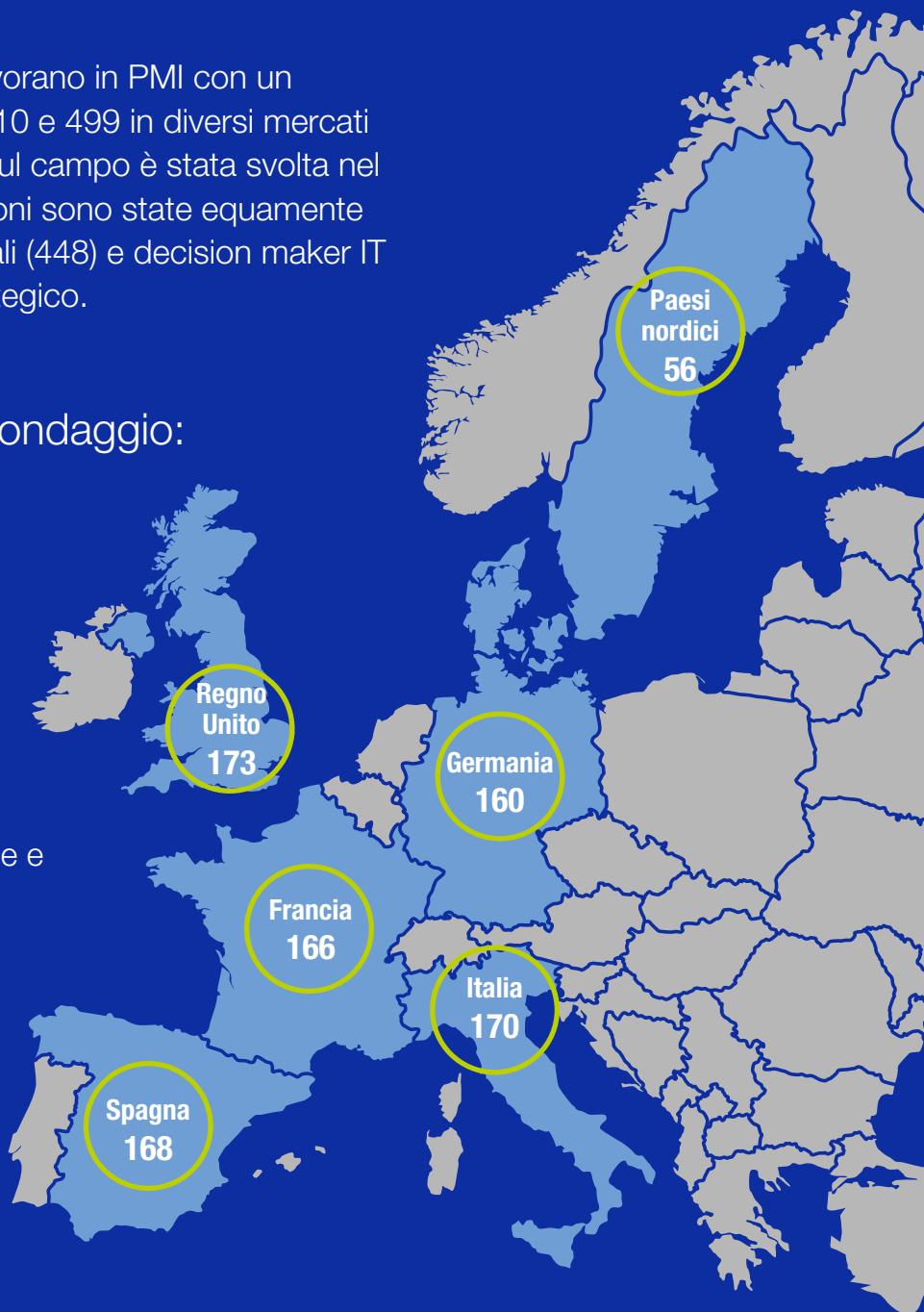
La nostra metodologia

Il presente report si basa su 893 sondaggi online con decision maker aziendali e IT.

Decision maker aziendali e IT che lavorano in PMI con un numero di dipendenti compreso tra 10 e 499 in diversi mercati dell'Europa occidentale. La ricerca sul campo è stata svolta nel 2019 e all'inizio del 2020. Le rilevazioni sono state equamente suddivise tra decision maker aziendali (448) e decision maker IT aziendali (445) entrambi a livello strategico.

Settori chiave sottoposti al sondaggio:

-  Assistenza sanitaria - 152
-  Vendite al dettaglio - 117
-  Logistica - 113
-  Settore alberghiero, ristorazione e imprese ricettive - 81
-  Trasporto e stoccaggio - 62
-  Servizi professionali - 65
-  Produzione - 54
-  Servizi finanziari - 53
-  Istruzione - 51
-  Edilizia - 39



Ulteriori rilevazioni sono state effettuate in altri settori, tra cui energia, prodotti farmaceutici, agricoltura, difesa, proprietà e immobili, sport e intrattenimento.

Per maggiori approfondimenti,

non perdere i prossimi report sulla trasformazione digitale secondo Brother.

Disponibili a breve



brother

at your side

www.brother.it

Brother Italia S.p.A.

Segreen Business Park - Via San Bovio, 3

20090 San Felice - Segrate (MI) - Italy

Tel: +39 02 950019.1

Fax: +39 02 95301484