



Sponsorizzato da: HP

Autori:

Angèle Boyd

Keith Kmetz
Matthew Marden

Novembre 2015

Il valore economico della stampa protetta

IDC OPINION

Secondo lo studio di IDC, l'80% delle imprese intervistate riconosce che la sicurezza IT è importante per i processi aziendali; ma solo il 59% considera altrettanto importante la sicurezza della stampa. Il 40% dei dirigenti di primo livello, peraltro, pensa che verrebbe più facilmente chiamato in causa per una decisione concernente la sicurezza dell'ambiente IT in generale, che non per problemi di sicurezza della stampa. A nostro avviso questi esiti rivelano una mancanza di attenzione per una questione che di fatto potrebbe creare vulnerabilità nel business. La ricerca di IDC mostra che le aziende hanno solidi motivi per prestare maggiore attenzione alla sicurezza della stampa, e che un ambiente di stampa protetto offre vantaggi sostanziali a livello sia di IT, sia di business; per esempio:

- » Lo studio di IDC mostra che oltre la metà delle aziende intervistate, negli scorsi 12 mesi, ha avuto un episodio di violazione della sicurezza con il coinvolgimento della stampa.
- » Tutti gli ambienti di stampa/gestione dei documenti aziendali sono pieni di vulnerabilità. Tali vulnerabilità possono essere create da attacchi ostili dall'interno o dall'esterno dell'organizzazione, o dall'uso disattento dei dispositivi e degli output di stampa. Le violazioni veicolate dalla stampa possono passare per le porte di rete del dispositivo, l'intercettazione di processi di stampa/copia/scansione, i dischi rigidi o la memoria RMA delle stampanti/stampanti multifunzione la presenza di documenti copiati o stampati abbandonati nei vassoi, o anche dall'uso illecito di materiali protetti (assegni, ricette), e così via.
- » Le interviste approfondite condotte da IDC con le organizzazioni che utilizzano workflow di stampa e documentali di vario livello hanno mostrato le aziende che utilizzano la protezione in area stampa/documenti rispondono a due grandi tipologie :
 - Aziende con esigenze di sicurezza e conformità che utilizzano una infrastruttura IT protetta a tutti i livelli
 - Aziende motivate dai benefici in termini di costo ed efficienza IT prodotti dalle iniziative di

sicurezza

- » Le interviste condotte da IDC mostrano che le organizzazioni che hanno avviato un programma di protezione della stampa hanno realizzato i benefici e il valore economico più significativi in tre aree: miglioramento della sicurezza delle stampanti, maggiore efficienza del personale IT e riduzione dei costi. Le organizzazioni intervistate hanno menzionato una quantità di risultati ottenuti negli ambienti di stampa e sicurezza, per esempio:
- Riduzione fino a sei volte, in media, delle violazioni della protezione legate alla stampa dopo l'implementazione delle soluzioni per la sicurezza della stampa
 - Dimezzamento in media dei tempi trascorsi dal personale nel supporto dell'ambiente di stampa dopo l'implementazione delle soluzioni per la sicurezza della stampa
 - Risparmio medio del 15% sui costi per carta, toner e inchiostro
- » Il modello di implementazione delle soluzioni determina non solo la loro efficacia, ma anche l'impatto sulla produttività dei collaboratori. Per ottenere il massimo dei benefici ci sono requisiti fondamentali da considerare, a livello di tecnologie, persone e processi.

In questo white paper

Il presente white paper si basa su uno studio primario e secondario condotto da IDC sul tema della sicurezza IT e la sicurezza legata ai processi di stampa. Dal luglio al settembre 2015, IDC ha realizzato interviste approfondite con persone responsabili dell'implementazione e gestione

TABELLA 1

Prospetto delle organizzazioni intervistate — Interviste approfondite			
	Media	Valore mediano	Intervallo
Numero di dipendenti	60.300	20.500	200 - 290.000
Numero di addetti IT	4.500	610	40 - 25.000
Numero di utenti IT	57.200	19.500	180 - 290.000
Numero totale di stampanti	8.800	1.200	4 - 100.000
Numero di utenti che usano la stampa	50.800	9.000	200 - 280.000
Numero di pagine stampate l'anno	51 milioni	10 milioni	10.000 - 300 milioni
Settori di attività	Telecomunicazioni, manifatturiero, servizi finanziari, editoria, aerospaziale, biotecnologie, istruzione e sanità		

n = 16 organizzazioni

Fonte: Interviste di IDC sulla stampa protetta, 2015

delle soluzioni per la sicurezza della stampa di 16 organizzazioni. Le interviste sono state predisposte in modo da permettere a IDC di comprendere l'impatto quantitativo e qualitativo ottenuto dalle organizzazioni utilizzando le rispettive soluzioni. Le interviste rispecchiano l'esperienza fatta da una varietà di organizzazioni diverse. La Tabella 1 offre una panoramica dell'ambiente di stampa delle 16 organizzazioni intervistate.

IDC ha integrato le interviste con l'analisi dal lavoro di rilevamento. I rispondenti, appartenenti a più di 440 organizzazioni di varie dimensioni, sono tutti qualificati e impiegati a tempo pieno. I rispondenti dovevano essere a conoscenza dell'attrezzatura di stampa usata nella propria organizzazione e delle policy di sicurezza IT dell'azienda.

Panoramica della situazione

Perché le imprese devono preoccuparsi della sicurezza dell'infrastruttura di stampa/gestione documenti

La maggior parte delle organizzazioni ha messo la sicurezza IT tra le sue prime priorità... e per ottime ragioni. La proliferazione di tecnologie di computing, mobile, cloud e di altro tipo sta conducendo a un tipo di ambiente IT in cui i lavoratori della conoscenza necessitano, e di fatto richiedono, di avere accesso "sempre e ovunque" alle informazioni di business. Tuttavia IDC nota che le risorse e le tecnologie collegate con la stampa vengono spesso trascurate nella strategia di sicurezza IT dell'organizzazione.

E allora, per quale motivo le aziende dovrebbero cambiare approccio e proteggere i dispositivi di stampa come fanno con le altre tecnologie (PC, server, dispositivi mobile, ecc.)? La risposta è che se l'infrastruttura di stampa non è sicura, non lo è neanche l'ambiente IT. Il rischio di violazioni della sicurezza collegate con la stampa è maggiore di quanto si potrebbe pensare, e lo stesso vale per i costi.

Lo studio di IDC ha rilevato che negli ultimi 12 mesi oltre la metà delle aziende ha avuto un episodio di violazione della sicurezza con il coinvolgimento della stampa. Questa vulnerabilità può dipendere da attacchi ostili dall'interno o dall'esterno dell'organizzazione, o dall'uso disattento dei dispositivi e degli output di stampa. Le violazioni veicolate dalla stampa possono passare per le porte di rete del dispositivo, l'intercettazione di processi di stampa/copia/scansione, i dischi rigidi o la memoria RMA delle stampanti/stampanti multifunzione, la presenza di documenti copiati o stampati abbandonati nei vassoi, o anche dall'uso illecito di materiali protetti (assegni, ricette), e così via. In particolare:

Lo studio di IDC ha rilevato che negli ultimi 12 mesi oltre la metà delle aziende ha avuto un episodio di violazione della sicurezza con il coinvolgimento della stampa.

Le preoccupazioni concernenti la sicurezza delle proprietà intellettuali (IP), le informazioni riservate o confidenziali, la conformità con le normative e l'esigenza di una infrastruttura IT aziendale coerente e sicura sono un fattore determinante nei programmi di protezione della stampa.

- » Le porte di rete non protette offrono un punto di ingresso alla rete e alle informazioni dell'azienda.
- » I documenti riservati (per es., informazioni su un paziente o le transazioni finanziarie di un cliente) stampati su un dispositivo condiviso, dove l'output di stampa resta per qualche tempo nel vassoio, espongono al rischio del furto di informazioni confidenziali e di violazione della conformità con le normative.
- » La trasmissione di dati stampati/scansionati non crittografati è praticamente un invito agli hacker.

Le violazioni della sicurezza costano. Potenzialmente, la responsabilità finanziaria può concretizzarsi a tre livelli:

- » **Necessità di usare risorse aziendali per fare fronte alla violazione.** Le imprese che subiscono una violazione della sicurezza dovranno impiegare tempo e risorse, quindi denaro, per risolvere l'incidente. Per gestire l'episodio verranno rimandate o annullate opportunità potenzialmente redditizie.
- » **Multe/penali.** In più, l'inadempienza può comportare sanzioni finanziarie per l'azienda (per es., HIPAA) o la citazione in giudizio da parte del cliente che ha visto leso il suo diritto alla riservatezza.
- » **Reputazione dell'azienda.** E all'indomani dell'incidente l'organizzazione potrebbe anche riportare danni finanziari per una cattiva pubblicità sui media.

Motivi determinanti per proteggere l'infrastruttura di stampa

Dalle interviste realizzate con le organizzazioni che hanno implementato, a vari livelli, la protezione della stampa, è emerso che l'iniziativa è stata dettata dai seguenti fattori determinanti:

- » Preoccupazioni in merito a sicurezza e conformità (anche in reazione a una violazione)
- » Standardizzazione della sicurezza proattiva su tutta l'infrastruttura IT
- » Risparmi sui costi ed efficienze IT

Preoccupazioni in merito a sicurezza e conformità

I risparmi sui costi sono uno dei benefici accessori, ma importanti, ricercati in un piano di protezione dei processi e dei documenti di stampa.

Le preoccupazioni concernenti la sicurezza delle proprietà intellettuali (IP), le informazioni riservate o confidenziali, la conformità con le normative e l'esigenza di una infrastruttura IT aziendale coerente e sicura sono un fattore determinante nei programmi di protezione della stampa. Alcune organizzazioni stanno implementando programmi di protezione della stampa più incisivi a seguito di incidenti o violazioni effettivamente avvenuti.

Spiega il senior systems director di un istituto di servizi finanziari: "Le preoccupazioni per la sicurezza sono ovunque, e la stampante è un dispositivo pubblicamente accessibile utilizzato per tutti i lavori - riservati, confidenziali e di pubblico dominio. I dispositivi di rete che gestiscono dati confidenziali/riservati sono soggetti a obblighi di sicurezza, conformità e auditing; così siamo dovuti intervenire."

Standardizzazione generale dell'infrastruttura IT

La standardizzazione della sicurezza sull'intera infrastruttura IT di un'organizzazione incoraggia l'adozione di accorgimenti di protezione anche sulla stampa e i documenti, e di una strategia completa per la risoluzione dei problemi collegati con l'uso di queste attrezzature. Ecco il commento del vicepresidente dell'area information technology di un operatore dell'editoria: "Volevamo un ambiente con sicurezza basata su policy, capacità di autorisoluzione e la protezione basilare dei certificati di identità [delle stampanti], in linea con l'approccio che seguiamo negli altri servizi di infrastruttura."

Risparmi sui costi ed efficienze IT

Per il senior management, ogni iniziativa capace di abbattere i costi operativi dell'organizzazione è benvenuta. I risparmi sui costi sono uno dei benefici accessori, ma importanti, ricercati in un piano di protezione dei processi e dei documenti di stampa. Sebbene questo beneficio non sempre sia stato il primo obiettivo ricercato con l'adozione di un programma di sicurezza, un terzo dei rispondenti sostiene che, tuttavia, il suo impatto è stato quello più grande rilevato nei fatti.

Il senior IT director di un operatore dei servizi finanziari ha osservato: "L'esigenza di proteggere la proprietà intellettuale e i potenziali impatti finanziari legati alle violazioni della sicurezza sono stati i principali motivi per cui abbiamo implementato le soluzioni... siamo certi che i controlli che limitano le operazioni di stampa indiscriminate e non necessarie ci hanno fatto risparmiare sui costi sia della carta sia dei materiali."

In media dopo l'implementazione delle soluzioni di sicurezza queste organizzazioni hanno riferito riduzioni fino a sei volte nella frequenza delle violazioni associate alla stampa.

Naturalmente un'iniziativa di sicurezza della stampa porta anche risparmi su costi "meno diretti". Diverse organizzazioni hanno rilevato che le efficienze IT ottenute centralizzando e standardizzando la gestione della stampa e della sicurezza si traducono in risparmi sui costi. Gestendo e proteggendo la stampa in modo più proattivo, l'IT è più libero di dedicarsi ad altre esigenze tecnologiche prioritarie dell'organizzazione. Per esempio, il direttore IT di un'organizzazione ha spiegato: "Volevamo consolidare il controllo dei costi e la gestione centrale del nostro ambiente di stampa."

Il valore economico della stampa protetta

Le interviste approfondite di IDC con le 16 organizzazioni che usano soluzioni per la stampa sicura mostrano che questa implementazione sta offrendo un valore economico significativo. Le interviste in cui IDC ha chiesto di descrivere l'ambiente di stampa prima e dopo l'implementazione delle soluzioni, mostrano che le organizzazioni stanno raggiungendo l'obiettivo di creare un ambiente di stampa più sicuro realizzando, allo stesso tempo, efficienze in termini di costi e utilizzo del personale, .

- » **Sicurezza.** Gli ambienti di stampa sono divenuti più sicuri e i costi legati all'esigenza di riparare alle violazioni e garantire la conformità con normative e criteri di auditing si sono ridotti.
- » **Efficienze a livello di personale IT.** Il tempo totale impiegato dal personale per gestire e mantenere l'ambiente di stampa e creare, modificare e applicare le relative policy si è ridotto, lasciandolo più libero di dedicarsi ad altre iniziative.
- » **Risparmio sui costi.** Grazie alla maggiore visibilità dell'ambiente i costi associati alla stampa si sono ridotti e anche i comportamenti si sono modificati, portando risparmi anche a livello di stampanti e materiali di consumo.

Attenuazione dei rischi: miglioramento della protezione e della conformità della stampa

Le organizzazioni intervistate hanno riferito di aver sfruttato le capacità delle soluzioni per la sicurezza della stampa per mitigare gli impatti delle violazioni e migliorare l'efficienza e l'economia delle iniziative per la conformità.

IDC ha interrogato i rispondenti per sapere la frequenza con cui si verificano violazioni della sicurezza e dei dati associate alla stampa nella loro organizzazione, e se la stessa ha registrato violazioni che definirebbe sostanziali. In media dopo l'implementazione delle soluzioni di sicurezza queste organizzazioni hanno riferito riduzioni fino a sei volte nella frequenza delle violazioni associate alla stampa. L'utilizzo di processi criptati, autenticazione degli utenti e capacità di pull printing ha consentito di stabilire un livello rassicurante di tracciabilità e rendicontazione e di migliorare la prevenzione delle violazioni. In alcune organizzazioni la protezione della stampa ha consentito di completare le iniziative di sicurezza a protezione dell'infrastruttura IT, e quindi di chiudere le vulnerabilità rimaste. Le organizzazioni intervistate hanno fornito esempi delle violazioni associate da esse registrate; tra queste:

TABELLA 2

Impatto delle soluzioni per la sicurezza della stampa aziendale sulle violazioni della sicurezza: interviste approfondite

Violazioni complessive della sicurezza

Numero medio di violazioni l'anno, prima dell'implementazione della stampa sicura	9,9
Numero medio di violazioni l'anno, con l'implementazione della stampa sicura	1,5
Variazione nel numero di violazioni della sicurezza	Fino a 6 volte di meno

Violazioni significative della sicurezza

Numero di organizzazioni intervistate che hanno avuto	5
Numero medio di dipendenti interessati dagli impatti	54
Tempo medio dedicato dai dipendenti a risolvere l'evento (ore)	277
Costo medio totale di riparazione per singola violazione (sanzioni incluse) n = 16 organizzazioni	521.400 dollari

Fonte: Interviste di IDC sulla stampa protetta, 2015

Le organizzazioni intervistate sostengono che dopo l'implementazione delle soluzioni il personale ha dimezzato, in media, i tempi per il supporto dell'ambiente di stampa.

- » **Stampa di informazioni confidenziali mirata all'utilizzo improprio.** Il direttore IT di uno stabilimento manifatturiero ha spiegato che la sua organizzazione ha perso proprietà intellettuali per varie cause, e tra queste la stampa da parte di dipendenti di informazioni altamente riservate e segrete che gli stessi hanno poi fornito alla concorrenza.
- » **Stampa e gestione impropria di dati protetti.** Il direttore IT di un'azienda di servizi finanziari ha spiegato che i collaboratori dell'organizzazione mettevano a rischio design e altre proprietà intellettuali con operazioni di stampa indiscriminate, o lasciando sostare i lavori nella stampante.

Le organizzazioni intervistate hanno fornito diversi esempi di come le soluzioni per la sicurezza della stampa aziendale le hanno aiutate a minimizzare l'impatto delle violazioni perpetrate tramite le stampanti:

- » **Protezione delle informazioni lungo l'intero processo di stampa.** Ecco il commento del vicepresidente dell'area information technology di un operatore dell'editoria: "La soluzione ci ha fornito uno strumento vitale per proteggere il flusso di dati e contenuti da e verso le nostre stampanti sulla rete, garantendo un'affidabilità effettiva e la riduzione delle opportunità che si verificano violazioni."
- » **Prevenire operazioni di stampa non necessarie o improprie.** Il direttore IT di un operatore dei servizi finanziari ha osservato: "Spesso la documentazione sensibile che diffondiamo internamente non può tassativamente essere stampata. Queste soluzioni ci aiutano a minimizzare le violazioni, che si verificano sempre più a livello interno per atti deliberati o avventati."

Come si vede nella Tabella 2, per quanto ogni violazione nella stampa possa avere un suo costo, quelle più significative sono le più importanti da evitare, perché comportano notevoli costi di riparazione. Stando alle cinque organizzazioni che in anni recenti hanno avuto una violazione definita sostanziale della sicurezza associata alla stampa, il costo medio di una violazione del genere si traduce in perdita di produttività per 54 dipendenti, 277 ore di tempo per la riparazione e un costo secco di oltre 500.000 dollari a violazione, sanzioni comprese.

Oltre a ridurre la frequenza delle violazioni, 10 organizzazioni sulle 16 intervistate ritengono che le soluzioni per la sicurezza della stampa adottate abbiano reso più efficaci ed efficienti le iniziative rivolte alla conformità normativa e all'auditing. Il miglioramento della protezione e della tracciabilità comportano una serie di benefici:

- » **Maggiore sicurezza:** come ha notato il direttore IT di un operatore dei servizi finanziari:

“Il motivo fondamentale per implementare questo modello di sicurezza è il beneficio di ottenere un ambiente molto robusto e sicuro che protegge dati e documenti, migliora la riservatezza del design e dell’architettura e protegge le stampanti, e che ci ha concretamente aiutato a raggiungere i nostri standard di sicurezza.”

- » **Tracciabilità e visibilità:** il vicepresidente del reparto information technology di un operatore dell’editoria ha spiegato: “Siamo riusciti a creare un tracciato di verifica, a prevenire l’intercettazione dei dati e a mostrare che abbiamo limitato l’accesso ai dati riservati dei clienti. E ora le nostre procedure di verifica e auditing comprendono l’identificazione dei rischi e l’analisi delle minacce, con la procedura di risoluzione consigliata dei problemi. La panoramica ci offre una visione approfondita dello stato del sistema, permettendo il monitoraggio in tempo reale di tutti i parametri di conformità.”

Questi miglioramenti hanno anche generato risparmi sui costi e sui tempi spesi per gli obblighi di conformità e di verifica delle organizzazioni. In media i soggetti intervistati hanno riferito che utilizzando le soluzioni di sicurezza della stampa sono riusciti a risparmiare fino a più di 200 ore di lavoro e 250.000 dollari circa sui costi l’anno, anche in termini di supporto esterno per gli obblighi di auditing e conformità.

Benefici in termini di produttività del personale IT

I soggetti intervistati da IDC riferiscono che in seguito all’implementazione delle soluzioni per la sicurezza della stampa i tempi richiesti per gestire e supportare l’ambiente si sono abbreviati. Queste efficienze sono determinate da una serie di fattori, come l’uso di capacità avanzate di gestione centralizzata e automazione che consentono anche di risolvere più velocemente i problemi operativi. Il senior IT director di un operatore dei servizi finanziari ha osservato: “L’impatto [delle soluzioni di sicurezza della stampa] sul nostro staff è stato profondo, sia in termini di ore spese in attività laboriose, sia per la maggiore libertà del personale di dedicarsi ad attività più strategiche. Ora la risposta, in caso di problemi nell’ambiente, non è più isolata, ma olistica e ripetibile.” Le organizzazioni intervistate sostengono che dopo l’implementazione delle soluzioni il personale ha dimezzato, in media, i tempi per il supporto dell’ambiente di stampa.

I soggetti riferiscono che le soluzioni hanno consentito delle efficienze tra il personale addetto all’ambiente di stampa. Il risparmio sui tempi di lavoro è consentito dall’introduzione di determinati cambiamenti, come l’automazione del supporto e della manutenzione, con l’automazione anche dei certificati, e l’applicazione di altri processi ripetibili. Per esempio, il vicepresidente di un’azienda di servizi finanziari che utilizza certificati unici e criteri di

autenticazione dei collaboratori, ha spiegato che la sua organizzazione ha ottenuto una riduzione del 60% del tempo utilizzato dal personale per monitorare i dispositivi: “Risparmiamo tempo del personale, perché possiamo creare e lanciare facilmente i profili verso molti dispositivi simultaneamente, e possiamo automatizzare la gestione dei certificati.”

Frattanto le organizzazioni intervistate registrano risparmi di tempo anche nella creazione, applicazione e modifica delle policy associate all’ambiente di stampa. In media il personale in queste organizzazioni impiega il 59% di tempo in meno sulle policy associate alle stampanti. Al di là dei risparmi sul personale, l’implementazione più efficace delle policy ha prodotto benefici anche a valle, come la definizione di linee guida più efficaci sull’uso dei dispositivi e la riduzione delle probabilità di una violazione.

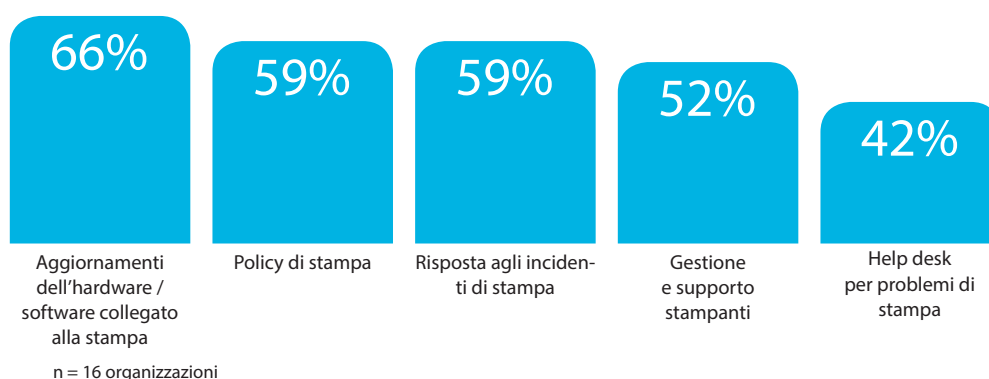
Quando son sorti problemi nell’ambiente, le organizzazioni intervistate dicono che il personale ha beneficiato delle funzionalità delle soluzioni di sicurezza della stampa, per esempio della disponibilità di una console centralizzata (più efficace) e dell’accesso remoto alle stampanti. Questi fattori, uniti al miglioramento delle policy legate alle stampanti, hanno consentito ai soggetti intervistati di ridurre, rispettivamente, del 59% e del 42%, il tempo medio di risposta agli incidenti e il tempo medio di risposta alle chiamate di assistenza degli utenti collegate all’ambiente di stampa (vedi Figura 1). Il vicepresidente IT di un operatore dell’editoria che utilizza varie soluzioni, tra cui autoriparazione e gestione di certificati univoci, ha spiegato come queste abbiano impattato la capacità di supporto dell’ambiente di stampa del suo team: “Ora abbiamo meno problemi, e quelli che si verificano vengono risolti in tempi complessivamente più brevi. L’impatto, che è stato favorevole, si è tradotto in una maggior quantità di tempo libero per altre attività di supporto e pianificazione.” Osserva il direttore IT di un’azienda del ramo servizi finanziari, che utilizza un prodotto per gestire la protezione delle stampanti: “Ora il nostro help desk ha una visione più chiara delle impostazioni, delle autorizzazioni e dei problemi del nostro ambiente di stampa, e può intervenire autonomamente oppure, per il supporto di 2° livello, può contattare un piccolo team dedicato alla stampa aziendale.”

FIGURA 1

Risparmio di tempo medio del personale addetto all’ambiente di stampa —

Interviste approfondite

Le iniziative per la sicurezza della stampa hanno sensibilizzato i collaboratori rispetto al modo di usare le stampanti, contribuendo anche a far risparmiare sui costi.



Fonte: Interviste di IDC sulla stampa protetta, 2015

Riduzione dei costi legati all'ambiente di stampa

Ogni iniziativa IT concreta risulta più attraente se consente anche di ridurre i costi. Di conseguenza, per i soggetti intervistati la capacità di generare risparmi con l'implementazione delle soluzioni per la sicurezza della stampa ha rappresentato un valore aggiunto fondamentale. Procedure quali l'autenticazione dei collaboratori e la stampa "pull" (ossia sospesa fino al rilascio sul dispositivo da parte dell'utente autorizzato) risultano tra le più adottate da quanti hanno risposto alle interviste approfondite (più di due terzi degli intervistati). Queste soluzioni preservano la riservatezza dei documenti e generano risparmi sui costi perché costringono gli utenti a seguire delle procedure specifiche per stampare i loro lavori e riducono il numero di stampe non ritirate o erroneamente indirizzate. Questa capacità delle soluzioni di fornire un veicolo per la riduzione dei costi dell'ambiente di stampa risulta piuttosto chiara, se consideriamo che diversi intervistati hanno citato l'ottimizzazione dei costi come il volano primario della loro iniziativa.

Le organizzazioni intervistate hanno spiegato che le soluzioni di protezione della stampa le hanno aiutate a ridurre i costi attraverso:

- » **Un minor uso della stampa, a seguito del cambiamento dei comportamenti:** il tesoriere di un'azienda del settore alimenti ha osservato: "La funzione di pull printing che usiamo permette l'invio in stampa, ma perché la stampante effettivamente esegua il processo l'utente deve prima recarsi personalmente al dispositivo e autenticarsi con il suo badge. In base alle ultime cifre che ho visto, credo che abbiamo avuto una riduzione tra il 21 e il 24% delle stampe rispetto a prima."
- » **Maggiore visibilità sull'utilizzo dei dispositivi:** il direttore del reparto IT di una università spiega: "Ora possiamo tracciare i costi di stampa delle pagine effettivamente rilasciate ai fini del charge-back ai singoli dipartimenti". La capacità di allocare i costi di stampa ai singoli dipartimenti consente all'università di ripartire gli oneri in base

all'utilizzo effettivo, e questo incoraggia gli utenti a usare le stampanti nel modo più responsabile possibile.

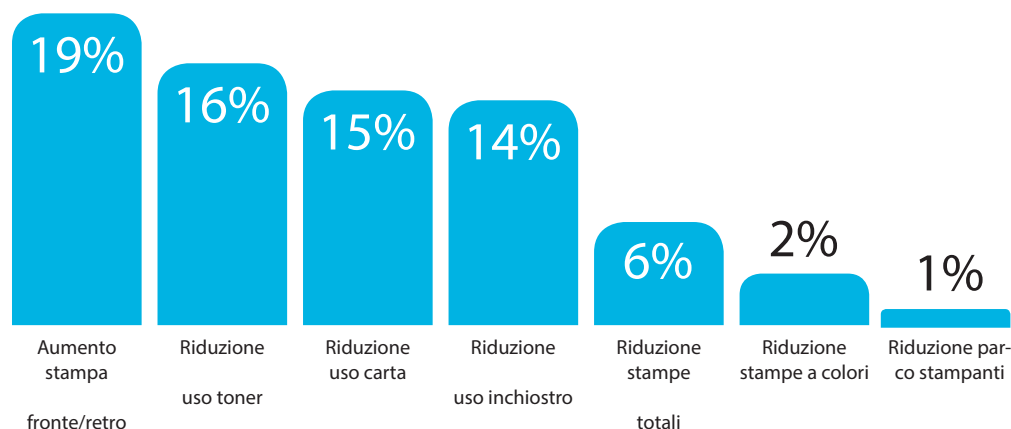
- » **Eliminazione delle stampanti non necessarie o obsolete:** il vicepresidente di un istituto di servizi finanziari racconta: "Stiamo gradualmente riducendo il numero di processi di stampa non necessari, perché la gente sa che l'attività di stampa è monitorata; e poi stiamo dismettendo e sostituendo il vecchio hardware di stampa che non supporta i criteri di sicurezza di base".

Le iniziative per la sicurezza della stampa hanno sensibilizzato i collaboratori rispetto al modo di usare le stampanti, contribuendo anche a far risparmiare sui costi. In media i rispondenti alle interviste approfondite hanno detto che adesso l'invio di processi al dispositivo sbagliato da parte dei dipendenti si è ridotto del 43%. E quindi è diminuito anche il numero di lavori abbandonati o ripetuti. Come si vede nella Figura 2, questo genere di miglioramenti ha contribuito a rendere complessivamente più efficiente l'uso della stampa, con la riduzione del totale di stampe eseguite (-6% in media), l'aumento della stampa fronte/retro (+19%) e una lieve riduzione della stampa a colori (-2%). Questi elementi, insieme alla migliore visibilità sull'ambiente di stampa, hanno permesso alle organizzazioni di ottenere notevoli risparmi sui costi, anche grazie alla riduzione del numero di dispositivi implementati e gestiti (-1%, pari a 115 stampanti in media per organizzazione) e dei costi associati a carta, inchiostro e toner (rispettivamente, -15%, -14% e -16%).

FIGURA 2

Risparmi medi su costi ed efficienze nell'ambiente di stampa — Interviste approfondite

(Efficienza o miglioramento espresso in percentuale)



IDC consiglia alle organizzazioni di massimizzare l'efficacia delle tecnologie di protezione della stampa/documenti.

n = 16 organizzazioni

Fonte: Interviste di IDC sulla stampa protetta, 2015

Sfide

In quasi tutte le nuove iniziative lanciate in un'organizzazione, la pianificazione preliminare permette di evitare alcune difficoltà. Le difficoltà segnalate dal gruppo di studio riguardano tutte e tre le fasi dell'implementazione di una iniziativa di sicurezza della stampa: pianificazione, implementazione e postimplementazione.

Le aziende studiate hanno riferito di essersi sentite in lotta contro il tempo per sviluppare la strategia e il piano d'azione. Per raggiungere la riduzione del carico di lavoro sull'IT in fase di postimplementazione occorre un notevole lavoro preliminare. Peraltro la forzatura dei criteri di conformità sugli utenti dovrebbe avvenire con un processo automatico, comprendente strumenti di monitoraggio, un processo di escalation e le procedure di remediation volte a ridurre le chiamate all'help desk.

Per quanto riguarda gli utenti della stampa all'interno dell'organizzazione, segnaliamo in particolare che andrebbero pianificate due precauzioni:

- » **Bilanciare il rigore della protezione con l'esigenza di minimizzare gli impatti sulla produttività degli utenti:** la protezione del business deve sempre avere la più alta importanza: ciò nondimeno, l'organizzazione deve poter disporre di un sistema utilizzabile con il minimo delle perdite di produttività. Alcune organizzazioni, per esempio, che implementano la stampa "pull" per esigenze di sicurezza, possono incontrare resistenze dagli utenti per la necessità di doversi autenticare (cioè, di inserire una password) e aspettare il termine del processo di stampa. La scelta, in questo scenario, è tra proteggere le informazioni contenute nel documento (per es., nessuno può vedere i documenti stampati lasciati nel vassoio) e attendere i tempi di stampa del documento (la stampa si avvia solo dopo che l'utente si autentica sulla stampante).
- » **Formazione dei dipendenti:** sempre in relazione all'aspetto della produttività, il piano di sicurezza della stampa deve includere anche il processo e i tempi necessari per istruire il personale rispetto alle nuove politiche e procedure. Le aziende devono prepararsi all'eventualità di ripetere la formazione e di utilizzare diversi modelli di erogazione, per accogliere i diversi stili di apprendimento e generazionali dei collaboratori.

Sede globale di IDC

5 Speen Street

Framingham, MA 01701

USA

508.872.8200

Twitter: @IDC

idc-insights-community.com

www.idc.com

Avviso di copyright:

Per la pubblicazione esterna di informazioni e dati di IDC. Ogni informazione di proprietà di IDC da utilizzarsi a mezzo pubblicità, stampa o materiale promozionale si richiede la previa autorizzazione scritta del vicepresidente o del country manager, a seconda dei casi. La richiesta dovrà essere corredata da una redazione del documento proposto per la pubblicazione. IDC si riserva il diritto di rifiutare a sua discrezione l'approvazione dell'utilizzo esterno proposto.

Copyright 2015 IDC. Ogni riproduzione senza autorizzazione scritta è rigorosamente vietata.

Orientamento essenziale

IDC ha individuato varie importanti ragioni per integrare nel quadro complessivo della sicurezza IT aziendale anche i workflow di stampa e gestione documenti. Naturalmente uno dei benefici essenziali è che in questo modo si dispone di un programma completo di sicurezza IT che abbraccia anche la stampa: ma questo tipo di piano ha anche una serie di altri benefici, al di là della sicurezza. I due benefici più importanti sono una significativa riduzione dei costi e una maggiore efficienza IT.

IDC consiglia alle organizzazioni di massimizzare l'efficacia delle tecnologie di protezione della stampa/documenti. Per farlo devono riconoscere che un simile obiettivo è effettivamente raggiungibile solo coinvolgendo anche le persone e i processi nell'esecuzione dei piani.

Tecnologia

Quando si tratta di implementare soluzioni di sicurezza, non c'è tanto da sottiglie: o l'organizzazione è sicura, o non lo è.

IDC: chi siamo

International Data Corporation (IDC) è il primo fornitore globale di servizi di consulenza, market intelligence ed eventi nel mercato delle tecnologie dell'informazione, delle telecomunicazioni e di consumo. IDC offre a professionisti IT, dirigenti d'azienda e investitori dati concreti che supportano i processi decisionali legati all'acquisto delle tecnologie e alla strategia di business. Con oltre 1.100 analisti, IDC fornisce competenze sulle opportunità tecnologiche e settoriali a livello globale, regionale e locale in più di 110 paesi del mondo. Da 50 anni IDC aiuta i suoi clienti con insight strategici che facilitano il raggiungimento dei loro obiettivi più importanti. IDC è una consociata di IDG, la società leader mondiale in area media, ricerca ed eventi nel mercato delle tecnologie.

IDC consiglia di implementare su tutta l'estensione dell'ambiente aziendale le seguenti capacità al più presto possibile. Il personale IT e i fornitori dell'infrastruttura di stampa dovranno accertarsi che su tutti i dispositivi di stampa usati nell'organizzazione vengano configurate le seguenti funzionalità e caratteristiche:

- » Accertarsi che tutti i dispositivi di stampa di rete abbiano le seguenti funzionalità o, quantomeno, che il loro firmware venga aggiornato in modo da renderle fruibili.
- » Accertarsi che i dispositivi usino solo protocolli di comunicazione criptati, e gli altri vengano disabilitati.
- » Introdurre un sistema che, in occasione della dismissione del dispositivo, esegua l'eliminazione o la distruzione dei dati contenuti nel relativo disco rigido.
- » Supportare come minimo una modalità di autenticazione dell'utente (meglio due o tre), e considerare l'implementazione della stampa "pull" negli ambienti con elevati volumi di informazioni riservate o requisiti di conformità.
- » Accertarsi che solo firmware lecito venga caricato e che questo sia sempre aggiornato.
- » Accertarsi che tutte le unità disco rigido delle stampanti siano protette (crittografia e eliminazione periodica dei dati).
- » Implementare funzionalità di stampa anticontraffazione o usare stampanti con cassette a serratura per i supporti speciali, se usati per l'output dell'organizzazione. Ciò consente di proteggere i prodotti di stampa potenzialmente presi di mira dai falsari, quali assegni, prescrizioni mediche/farmacologiche e altro.
- » Usare uno strumento centrale per gestire, monitorare e riparare i dispositivi al fine di garantire la conformità con le policy di sicurezza. In questo modo l'organizzazione potrà evitare di dover configurare e mantenere manualmente i singoli dispositivi. Il tool dovrà consentire di creare e amministrare in modo facile/semplice le policy di sicurezza, rilevare l'aggiunta di dispositivi in rete, consentire la gestione di certificati univoci per i dispositivi, registrare i casi di difformità e risolvere gli incidenti con un processo di escalation e remediation. Il tool dovrà interagire con i sistemi di gestione della protezione IT di livello aziendale che monitorano gli endpoint rilevando incidenti di non conformità e anomalie, per consentire la rapida identificazione delle potenziali violazioni della sicurezza.
- » Accertarsi che i processi di stampa e scansione da desktop e dispositivo mobile (sia in movimento che at rest) siano criptati, per garantire la totale protezione dei dati. Ciò significa che per un maggior livello di protezione, anche gli allegati da stampare

dovranno essere aperti e sottoposti a imaging . Un altro elemento per la massima sicurezza e conformità con le politiche aziendali e gli standard di settore è disporre di un tool capace di monitorare i contenuti di stampa e scansione.

Persone

Per porsi seriamente nei riguardi della sicurezza l'organizzazione dovrà assicurare che il team di sicurezza includa persone con competenze di protezione dei dispositivi di stampa e i flussi di lavoro documentali collegati. Questo team potrà essere costituito in seno all'azienda, con il suo personale, e/o da risorse esterne competenti. Il team interverrà come consulente nei futuri problemi di sicurezza della stampa e dei workflow collegati, e contribuirà all'integrazione del piano di sicurezza IT di livello aziendale.

Per garantire che i sistemi di protezione dei dispositivi di stampa e dei workflow documentali non impattino negativamente la produttività dei dipendenti, l'organizzazione si incaricherà, nell'ambito del processo di pianificazione, di raccogliere l'input di una selezione di dipendenti. Altrettanto consigliabile è prevedere l'intervento di un esperto di gestione del cambiamento, soprattutto se si richiedono cambiamenti di significativa entità o natura. Questo esperto potrà fornire consulenza anche sul rollout dell'iniziativa e gli approcci di formazione da adottare.

La maggior parte delle organizzazioni non dispongono internamente delle conoscenze e dello skill set necessari per proteggere da sé l'infrastruttura di stampa e gestione documenti. In questo caso dovrà considerare la possibilità di chiedere al fornitore dei dispositivi di stampa quali risorse ha a disposizione l'IT. Le risorse spaziano dalle funzioni di sicurezza disponibili nell'hardware delle stampanti/stampanti multifunzione interne ai tool di sicurezza software, fino ai servizi di sicurezza (quali servizi professionali di sicurezza, valutazioni della protezione, gestione del cambiamento e competenze in materia di conformità normativa in settori specifici).

Procedura

È importante che l'organizzazione dia inizio all'iniziativa di sicurezza procedendo a valutare la situazione attuale dell'ambiente di stampa e a sviluppare un piano che assicuri livelli di protezione coerenti con quelli del rimanente ambiente IT. L'iniziativa dovrà comprendere una fase di studio dei requisiti di sicurezza essenziali specifici del settore di attività, e un piano per il monitoraggio, l'escalation, la correzione e la forzatura di questi criteri su base permanente.

Il piano dovrà essere periodicamente rivisto a fronte dei dati raccolti nel periodo di riferimento, per vedere se servono ritocchi e apprendere dalla casistica delle violazioni

registrate al di fuori dell'azienda. Ogni eventuale aggiustamento rispecchierà i dati raccolti nonché il livello di rischio e di spesa di protezione accettabile per l'organizzazione.