IDC
Analyze the Future

I D C A N A L I S I D I M A R K E T I N G

La messa in sicurezza dell'infrastruttura di stampa è fondamentale per la trasformazione digitale

Dicembre 2016

Di Robert Palmer, Direttore della ricerca di IDC, imaging, stampa, e soluzioni documentali

Sponsorizzato da HP Inc.

Disporre di un piano di sicurezza informatica rappresenta un'elevata e scontata priorità per un'azienda al fine di garantire protezione adeguata e risposte a potenziali minacce e violazioni. Occorre che la sicurezza di stampa sia parte di questo piano, specialmente oggi, nell'era della 3ª piattaforma informatica (mobilità, cloud, big data e social). Parte di qualsiasi piano completo rivolto alla sicurezza dell'organizzazione dell'ambiente di stampa dovrebbe quindi includere soluzioni e servizi riguardanti la sicurezza dei dati e dei dispositivi. In questo documento si esamina l'importanza della messa in sicurezza dell'infrastruttura di stampa e documentale e il ruolo che i servizi di stampa gestiti possono avere nel raggiungimento di questo obiettivo.

Introduzione

Da oltre un decennio, i problemi connessi alla sicurezza e alla privacy dei dati sono diventati priorità per direttori informatici e responsabili IT. La ricerca di IDC dimostra che la sicurezza ha assunto importanza primaria per la maggior parte delle aziende, e si classifica appena al di sotto un'altra iniziativa chiave: la trasformazione digitale. Entrambe sono viste come discriminanti essenziali del business, è pertanto importante capire come la trasformazione digitale e la sicurezza siano fortemente legate.

Le aziende affrontano una vasta serie di minacce quando arriva il momento della messa in sicurezza del loro sistema informatico. Quasi tutte le aziende tecnologicamente avanzate hanno reso la sicurezza prioritaria, si sono focalizzate su problemi come la protezione della rete dagli attacchi esterni, la messa in sicurezza dei dispositivi in rete, la gestione dell'accesso ai dispositivi connessi, e impedito la divulgazione dei dati confidenziali.

Apparentemente è semplice vedere come tutti questi problemi ruotino intorno al bisogno di proteggere le risorse più importanti dell'azienda: informazioni commerciali e dati dei clienti. Le aziende spendono miliardi di dollari in software per la gestione documentale e per la gestione dei contenuti d'impresa (ECM: Enterprise Content Management), investono in modo significativo sui sistemi per ottenere un controllo sempre maggiore sui contenuti critici del business. La commistione delle sfide è l'impulso costante verso mobilità e cloud. Oggigiorno, il knowledge worker necessita di accesso ai dati 24 ore al giorno, 7 giorni alla settimana, e ciò significa che i contenuti devono muoversi liberamente sia dall'interno sia dall'esterno dell'azienda.

Stranamente, l'infrastruttura documentale e di stampa di un'azienda è posizionata unicamente sull'intersezione tra trasformazione digitale e sicurezza informatica. Tuttavia, la maggior parte delle aziende non riesce a riconoscere la corrispondenza esistente tra le vulnerabilità della sicurezza e i

loro attuali sistemi di stampa e documentali. Il cuore del problema consiste nel ruolo della stampante multifunzione, divenuta un nodo di elaborazione dati intelligente che serve da rampa di accesso e uscita per i dati aziendali, a prescindere dal fatto che si trovino sul dispositivo, sulla rete aziendale, su carta, o nel cloud.

Una minaccia invisibile e non gestita

La stampante multifunzione connessa è un potenziale rischio per la sicurezza in quanto dispositivo collegato non gestito. Tuttavia, la stampante multifunzione può anche essere impostata come risorsa di confine per la sicurezza dell'accesso alla rete, per gestire la sicurezza dei dati e per proteggere l'accesso ad essi.

Secondo la ricerca di IDC *User Perspectives on Print Security, 2015 (Prospettive dell'utente sulla sicurezza di stampa)* oltre il 30% delle aziende non dispone di policy di sicurezza impostate per gestire l'accesso e controllare i diritti d'utilizzo delle stampanti e delle multifunzione presenti sulla rete. Inoltre, più della metà degli intervistati esprime molta preoccupazione in merito all'utilizzo non autorizzato di copiatrici e stampanti multifunzione.

Si evidenziano simili incongruenze quando si chiede alle aziende di fare considerazioni sulle pratiche di sicurezza informatiche da loro attuate. Secondo il testo di IDC *MaturityScape Benchmark: Print Security in the United States, 2016 (MaturityScape Benchmark: la sicurezza di stampa negli Stati Uniti)* oltre il 70% degli intervistati afferma che la sicurezza di stampa ha un alto indice di influenza su stampanti e multifunzione che vengono comprate o noleggiate. Incredibilmente, tuttavia, la percentuale degli intervistati che affermava che la sicurezza di stampa fosse "molto importante" era 26%, inferiore rispetto a quella di chi risultava preoccupato per la sicurezza informatica in generale.

Molti responsabili IT e della sicurezza hanno ipotizzato che i sistemi creati per la protezione della rete dovrebbero essere estesi ad altri dispositivi connessi. Ma la sicurezza sul perimetro di rete è labile, e ogni dispositivo connesso è ora un punto di rischio estremo—stampanti e multifunzione comprese.

La minaccia è reale, con potenziali criticità causate da attacchi infimi a stampanti di rete o stampanti multifunzione utilizzate come punti d'accesso, o da un utilizzo inconsapevole o poco attento dei dispositivi da parte dei dipendenti. L'ambiente di stampa è unico poiché viene impostato specificatamente per gestire dati, documenti e informazioni in formato digitale e cartaceo, quindi il contenuto critico viene allo scoperto e diventa vulnerabile in molti modi. L'assenza di sicurezza dell'ambiente di stampa nella strategia informatica generale rende l'azienda vulnerabile come se non avesse mai attuato azioni volte alla sicurezza.

Ciò che comporta una criticità nella sicurezza dell'infrastruttura di stampa e documentale è lo stesso di qualsiasi altro vuoto nella sicurezza: alti costi per la ricerca e l'identificazione della criticità, ammonizioni associate alla governance aziendale e alla conformità alle policy, perdita di clienti o altri gravi danni alla reputazione aziendale.

I Servizi di stampa di HP

Le sfide relative alla sicurezza di stampa e documentale sono facilmente identificabili, ma lo sviluppo di una strategia di stampa sicura risulta arduo per molte aziende. Uno dei problemi riguarda gli stakeholder presenti in azienda. La sicurezza dei dispositivi tende a essere una funzione informatica e solitamente coinvolge il dipartimento IT, il responsabile della sicurezza, il servizio clienti, la sicurezza generale e la sicurezza di rete. Inoltre, qualsiasi dibattito riguardante la sicurezza di stampanti e multifunzione spesso riguarda la gestione delle funzioni.

La sicurezza dei contenuti, d'altro canto, è spesso vista come collegata a problemi relativi alla conformità alle policy, e gli stakeholder tendono a rimanere entro il perimetro del rischio aziendale e della governance. Possono essere coinvolti anche rappresentanti di applicazioni ERP, cluster di

database, gestione dei contenuti, e altri settori di attività (LOB: line of business). Molto spesso, la sicurezza dei contenuti e delle stampanti viene gestita separatamente, cosa che comporta scarsità di integrazione e aumento delle vulnerabilità. Inoltre, le aziende spesso non sono a conoscenza delle varie soluzioni di sicurezza di stampa e dei servizi professionali disponibili sul mercato.

Questa è un'area in cui i servizi di stampa gestiti (MPS Managed Print Services) possono ricoprire un ruolo importante nel portare avanti la sicurezza di stampa e documentale. Mentre molte aziende hanno stipulato contratti con fornitori di MPS per ottimizzare la loro infrastruttura di stampa al fine di aumentarne l'efficienza e ridurne i costi, la sicurezza di stampa e di contenuto viene trascurata nella maggior parte dei contratti di servizio di stampa. Oggigiorno, alcuni fornitori di MPS dispongono di competenza, strumenti e risorse per supportare le aziende nell'identificare e dare priorità alle attuali minacce alla sicurezza. Parte di questo processo potrebbe includere a priori una valutazione della sicurezza, fondamentale per identificare carenze nei dispositivi installati e nell'infrastruttura di contenuto. Le aziende possono quindi lavorare con il fornitore di servizio per sviluppare e mettere in atto servizi di sicurezza di stampa gestiti per far fronte alle vulnerabilità, per rafforzare l'infrastruttura documentale e ridurre i futuri rischi per la sicurezza.

Il fornitore di MPS è anche l'unico in grado di convogliare i vari stakeholder che possono stipulare contratti di servizio di stampa ai dipartimenti e ai rami aziendali, cosa fondamentale per creare un approccio olistico verso i dispositivo e verso la sicurezza dei contenuti. Questo approccio è inoltre positivo ai fini dello sviluppo di un piano di sicurezza che si estende di pari passo con la strategia di trasformazione digitale dell'azienda stessa. I servizi per la sicurezza di stampa possono variare da un livello base per la protezione dei dispositivi e dei dati, fino a misure più avanzate che risultano considerevolmente più complesse da implementare e offrono un maggiore livello di sicurezza dei dispositivi e una maggiore protezione dei contenuti.

Conclusione: da reattivi a proattivi

La conclusione è che l'infrastruttura di sicurezza e documentale non ha ricevuto il livello di attenzione dato ad altre minacce della rete e alla cybersicurezza. Le violazioni creano paura e incertezza e l'impatto su costi operativi, prestazioni operative e reputazione aziendale può essere enorme.

Le aziende devono attuare azioni proattive per risolvere i problemi di sicurezza nell'infrastruttura documentale e di stampa, e il fornitore di MPS dovrebbe essere considerato un partner importante in questo lavoro. Quando cercate fornitori di servizi di stampa, considerate quelli che dimostrano di avere competenze di base nella valutazione del livello delle minacce e abilità nella loro risoluzione.

Inoltre, scegliete partner con hardware e soluzioni costruiti attorno a un ecosistema di sicurezza per risolvere le seguenti vulnerabilità nell'infrastruttura documentale:

- Autenticazione e autorizzazione dell'utente
- Gestione dei dispositivi
- Protezione dei dispositivi da malware
- Gestione dell'aggiornamento del firmware e gestione delle password
- Sicurezza dei contenuti, privacy e integrità dei dati
- Capacità di rivolgersi alle persone coinvolte nell'installazione, nella configurazione e nell'utilizzo dei dispositivi

Le soluzioni MPS dovrebbero anche essere progettate per integrarsi con la parte di gestione documentale di terzi e con i sistemi ECM per fornire ulteriore protezione e per dare sostegno alla governance e ai requisiti di conformità normativa.

Con questo approccio olistico, le aziende possono iniziare a eliminare i punti deboli e a rafforzare la protezione negli ambienti di stampa e documentali, che probabilmente rappresentano il collegamento meno sicuro della vostra azienda.

Sede: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com