Perché le aziende necessitano di una pianificazione intelligente dei servizi di stampa

Le soluzioni IoT sono strumenti preziosi nella fornitura di servizi gestiti. Viene illustrato il modo con cui fornitori di servizi utilizzano i dispositivi connessi all'IoT per offrire valore e informazioni alle aziende.

Per maggiori informazioni

"La maggior parte delle aziende non ritiene di aver bisogno di protezione per le proprie infrastrutture di stampa, per questo motivo la stampa occupa gli ultimi posti nel loro elenco di priorità in materia di sicurezza"

Jason O'Keefe, HP Print Security Advisor

Le stampanti collegate alla rete sono meno sicure di quanto pensi la gran parte della aziende. Con l'aumento delle minacce alla sicurezza, che assumono proporzioni sempre maggiori, le aziende di tutte le dimensioni necessitano di avvalersi di strategie dedicate ai servizi di stampa volte a proteggere l'azienda e a ridurre i rischi al minimo. Al centro della creazione di una strategia avanzata, per molte aziende esiste la collaborazione con un fornitore di servizi di stampa gestiti in grado di identificare e risolvere le vulnerabilità in tema di sicurezza, oltre a occuparsi di determinate attività (ad esempio la manutenzione delle apparecchiature), in modo che la stampa non costituisca un ostacolo alla produttività.

Affrontare la mancanza di protezione delle stampanti

In base a un'indagine, condotta a livello globale da Ponemon Institute su oltre 2.000 professionisti, il 60% degli intervistati ha riconosciuto di avere probabilmente subito una violazione di dati ai danni di stampanti connesse alla rete. La maggior parte degli intervistati ha previsto nei successivi 12 mesi il verificarsi di una violazione di dati generata da stampanti non protette connesse alla rete.

Soltanto il 34% degli intervistati ha riferito di avere adottato misure di sicurezza volte a limitare l'accesso a stampanti ad alto rischio e a documenti cartacei stampati. Queste evidenti criticità nella sicurezza possono esporre in particolare piccole e medie imprese al rischio di attacchi costosi nel migliore dei casi, e talvolta rovinosi.

Jason O'Keefe, HP Print Security Advisor, ha affermato che la maggior parte delle aziende sottostima la vulnerabilità a cui vengono sottoposte dalle proprie infrastrutture di stampa. "La maggior parte delle aziende non ritiene di aver bisogno di protezione per le proprie infrastrutture di stampa, per questo motivo la stampa occupa gli ultimi posti nel loro elenco di priorità in materia di sicurezza", ha dichiarato. "Quando presentiamo il nostro framework, che prevede fino a 200 controlli per individuare vulnerabilità all'interno dell'infrastruttura di stampa, improvvisamente nasce la consapevolezza e cambia l'atteggiamento. L'iniziale scetticismo diventa incredulità e profonda preoccupazione, dando luogo a una discussione sincera e vivace".

Una buona strategia relativa ai servizi di stampa dovrebbe iniziare da una valutazione delle vulnerabilità. Secondo Michael Howard, HP Chief Security Advisor, la maggior parte delle vulnerabilità della sicurezza causate dalla stampa si riduce a quattro fattori: tecnologia obsoleta; mancata implementazione dei corretti controlli di sicurezza; ambienti di fornitori eterogenei; ambienti di stampa non gestiti.

Sapevate che un'azienda media si avvale all'incirca di una stampante ogni sei utenti? Mentre computer e notebook possono essere bloccati quando non utilizzati, le stampanti non seguono un simile protocollo, generando una vulnerabilità ogni sei utenti. "Molti team addetti alla sicurezza non sono a conoscenza del numero di dispositivi di stampa presenti nei propri ambienti. Potrebbero essere 5.000 dispositivi, tutti accessibili", ha affermato Howard. "Quando si pensa all'imponente presenza delle attività di stampa nella gran parte delle aziende, la mancanza di sicurezza proattiva è molto allarmante e genera apprensione".

Perché le strategie relative ai servizi di stampa sono importanti

Una strategia di stampa intelligente blocca le stampanti (proprio come i computer), limita i privilegi amministrativi, implementa linee guida su nomi utente e password e offre funzionalità di monitoraggio. Si tratta di elementi fondamentali per ottenere visibilità, tracciabilità e responsabilità.

"La visibilità è essenziale," afferma O'Keefe. "Vorrei anche evidenziare la collaborazione come cardine per ottenere un'efficace sicurezza di stampa. Per acquisire informazioni e competenza necessarie per l'ottenimento di una solida sicurezza, le aziende devono eliminare le barriere tra gli amministratori delle stampanti, i professionisti della sicurezza e il personale addetto ai controlli interni. Questi soggetti devono essere in grado di collaborare in sinergia per proteggere un componente fondamentale della rete sottovalutato per anni".

Inoltre, le aziende possono porre rimedio alla proprie vulnerabilità legate alla stampa:

- Aggiornando regolarmente il firmware
- Riducendo i diritti di amministratore all'interno dell'infrastruttura di stampa
- Aggiornando i database di stampa da edizioni express a enterprise
- Implementando processi e introducendo norme volti a mantenere una sicurezza uniforme e misurabile
- Offrendo agli amministratori dei dispositivi di stampa formazione mirata alla consapevolezza sulla sicurezza.

"Il mantenimento della sicurezza di stampa, al pari della sicurezza aziendale, rappresenta un processo in costante evoluzione" afferma Howard. "Per questo motivo è fondamentale perseguire il miglioramento continuo attraverso una valutazione approfondita e i consigli degli esperti".

Una valutazione più approfondita e costante è legata all'importanza attribuita alla governance. In materia di stampa, la governance dovrebbe includere la gestione degli account utenti (chi accede all'infrastruttura di stampa), la conformità alle politiche aziendali, la gestione del rischio, la documentazione sulla sicurezza e la registrazione degli eventi.

Gestito o non gestito, questo è il problema

Una strategia valida richiede un'ampia gamma di componenti. Per la maggior parte delle aziende, in particolare piccole e medie imprese, realizzare e mettere in atto questo tipo di strategia non è ipotizzabile a livello interno. Preferiscono dedicare tempo ed energie alla gestione aziendale. Collaborare con fornitori di servizi di stampa gestiti, in grado di occuparsi degli aspetti essenziali e di offrire il livello di sicurezza che le aziende necessitano per lavorare senza rallentamenti, rappresenta una soluzione di qualità.

Il primo passo per creare una strategia di stampa intelligente è porsi alcune domande. Per iniziare, quali stampanti sono più adatte alla propria azienda? Si dovranno scegliere stampanti laser o a getto d'inchiostro? Quali funzionalità di stampa sono necessarie? Per rispondere a queste domande è indispensabile bilanciare esigenze di affidabilità, costo e prestazioni. Le aziende, poi, dovranno provvedere a sicurezza, manutenzione e assistenza. Si renderà necessario gestire le stampanti internamente o collaborare con un fornitore di servizi? Questa domanda ne nasconde altre come: il team IT aziendale è in grado di affrontare i problemi legati alle stampanti? Sarà più costoso gestire i servizi di stampa internamente nel lungo periodo? Per le imprese più piccole, la risposta è spesso sì.

Le aziende che scelgono servizi di stampa gestiti dovrebbero riflettere su quando prendere in considerazione un contratto e su quale fornitore scegliere. A questo scopo, è necessario porsi domande come: quali servizi si rendono necessari? Cosa bisogna inserire nell'accordo sul livello di servizio? Quale costo verrà sostenuto? Per quando si prevede la crescita della rete di stampanti? Ipotizzando una crescita, come dovrà cambiare la strategia di stampa all'interno dell'azienda?

I pericoli legati all'utilizzo di stampanti non protette connesse alla rete sono evidenti; le aziende di ogni dimensione devono fare in modo che i servizi di stampa costituiscano parte del loro approccio complessivo alla sicurezza e alla produttività. Fortunatamente, esistono fornitori di soluzioni in grado di fare fronte alle criticità in tema di protezione.

"La sicurezza di stampa, proprio come la sicurezza dell'azienda, è un processo costante"

Michael Howard, HP Chief Security Advisor

Per maggiori informazioni
hp.com

4AA7-1720ITE, novembre 2017