IDC
Analyze the Future

I D C M A R K E T S P O T L I G H T

Il punto cieco del GDPR: perché le stampanti rappresentano un punto debole in materia di conformità

Luglio 2017

di Duncan Brown

Sponsorizzato da HP

Questa analisi di mercato IDC mette in evidenza la vulnerabilità delle stampanti nelle reti aziendali e, in particolare, in che modo questa vulnerabilità influenzi un programma di conformità incentrato sul regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) e altre normative in fase di attuazione. L'analisi fornisce inoltre suggerimenti su come ridurre i rischi in cui incorrono le aziende a causa delle stampanti non protette.

Introduzione

L'attenzione dedicata alla sicurezza dell'Internet-of-Things (IoT) è cresciuta in modo significativo dopo una serie di
attacchi di tipo denial-of-service (DDoS) ad alto profilo che hanno concentrato un enorme volume di traffico dannoso proveniente da migliaia di videocamere di sorveglianza, videoregistratori digitali e altri dispositivi connessi compromessi allo scopo di violare noti siti Web. Quale sarà il prossimo obiettivo?

Nel domandarci quali altri dispositivi IoT condividono alcune delle caratteristiche dei dispositivi utilizzati nei più
recenti attacchi, abbiamo rivolto la nostra attenzione alle stampanti per uso domestico e per piccole e grandi imprese. Gli aggiornamenti del software e il controllo degli accessi, due priorità relative ai tradizionali prodotti IT, vengono spesso trascurati sulle stampanti. Le stampanti possono essere il prossimo vettore di un grande attacco IoT, ma potrebbero anche rappresentare
nuovi pericoli per il business perché risiedono all'interno della rete aziendale, mostrandosi vulnerabili al potenziale furto di dati e DDoS sulla porzione interna di una rete. Con le conseguenze a carico delle aziende di violazioni dei dati personali, ipotizzate dal GDPR e da altre normative in via di formazione, la stampante di rete rappresenta l'endpoint trascurato che richiede immediata attenzione.

La stampante è un endpoint

Consideriamo il seguente scenario: Un dispositivo sconosciuto viene inserito in una rete aziendale, nell'ambito della protezione perimetrale come firewall, sistemi di prevenzione delle intrusioni e altre infrastrutture IT, in modo che abbia accesso libero a tutte le risorse di rete. Nel dispositivo è integrato un server Web per ottimizzare le diverse funzionalità. Tutte le porte sono "aperte" per impostazione predefinita per consentire la connettività Ethernet e il massimo di gigabit possibile al fine di rendere accessibile il dispositivo. Il dispositivo possiede inoltre un sistema operativo complesso come Linux per ottimizzare le funzionalità. Questo dispositivo non verrà esaminato in modo continuo dagli strumenti di ricerca delle vulnerabilità dell'impresa in quanto il server Web integrato probabilmente restituirà un gran numero di falsi positivi agli strumenti di gestione degli eventi e informazioni di protezione (SIEM) aziendali. Gli strumenti di ricerca delle vulnerabilità pertanto saranno configurati

per ignorare il dispositivo, con la conseguenza, a seconda del marchio, che il dispositivo non verrà mai aggiornato o non seguirà criteri di manutenzione o applicazione di patch durante la sua vita utile di 5-10 anni. La protezione del dispositivo sarà costituita da una password predefinita e il dispositivo potrà essere sottoposto a manutenzione da parte di terzi non monitorati. Il dispositivo sarà fondamentale per la produttività aziendale, quindi ve ne sarà a disposizione uno ogni 10 dipendenti. Questi dipendenti non solo utilizzeranno il dispositivo, ma vi inoltreranno attivamente dati personali sensibili, in cui rimarranno memorizzati. Peggio ancora, i dati potranno essere trasmessi a chiunque, senza alcun controllo di autenticazione o accesso.

Questa situazione potrebbe essere paragonata a un incubo; altri, la chiamano semplicemente "gestione della stampante".

Deve essere chiarito un punto molto importante. La "sicurezza di stampa" è una disciplina di sicurezza matura, guidata in gran parte dalla necessità di garantire la sicurezza dei dati. Come si può supporre, gli standard di conformità svolgono un ruolo di guida nella sicurezza di stampa dei documenti. Nell'area EMEA questa disciplina si identifica con il GDPR, ma si estende anche alla direttiva sulla sicurezza delle reti e delle informazioni (NIS), all'aggiornamento della direttiva ePrivacy e alla direttiva di revisione dei servizi di pagamento (PSD2). Questi standard costituiscono la base per i *risultati* di sicurezza senza specificare minuziosamente i dettagli tecnici di conformità.

I fondamenti del GDPR

Il GDPR rappresenta un aggiornamento gradito e atteso da troppo tempo delle leggi europee sulla protezione dei dati. Sostituisce la legislazione attuale che risale al 1995, precedente il boom di dot-com, Twitter, Facebook e cloud. Il GDPR aggiorna la legge per tenere conto di questi e futuri sviluppi che creano e utilizzano i dati personali.
Un ulteriore vantaggio del GDPR è che si applica a tutti gli stati membri dell'Unione Europea (UE).

Il GDPR è stato firmato nell'aprile 2016 ed entrerà in vigore il 25 maggio 2018. Le imprese hanno meno di un anno per garantire la conformità; le sanzioni per chi non sarà conforme potrebbero raggiungere il 4% del fatturato globale annuo o 20 milioni di euro, a seconda di quale cifra sia maggiore. Il GDPR introduce anche una notifica obbligatoria di violazione, le cui conseguenze riguardano i consigli di amministrazione che abbiano a cuore i danni all'immagine.

Si noti che la prospettiva di uscita del Regno Unito dall'Unione Europea (Brexit) non influisce in misura rilevante sul vasto panorama del GDPR:

- Le imprese britanniche che elaborano i dati personali di utenti nell'UE dovranno rispettare il GDPR in ogni caso perché si applica in modo extra-territoriale nel caso di qualsiasi dato personale di cittadini UE.
- Il Regno Unito implementerà con tutta probabilità leggi locali come il GDPR per facilitare i trasferimenti di dati dall'UE, disciplinati dalle regole di "adeguatezza".

Il GDPR non riguarda solo l'ambito della protezione. Contiene anche una serie di nuove misure, tra cui la portabilità dei dati, il consenso e la revoca, la verifica dell'età e il diritto all'oblio. Tuttavia, l'ottenimento della conformità deriva in gran parte da una buona protezione. Cosa dice il GDPR in proposito?

Il GDPR è notevolmente carente in materia di normative sulla definizione delle misure di sicurezza. Dei suoi 99 articoli, solo l'articolo 32 tratta in modo specifico di sicurezza e protezione. Il requisito è che le organizzazioni adottino "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". In altre parole, ciascuna azienda deve valutare il rischio associato ai propri dati personali e implementare i controlli di sicurezza che ritiene necessari.

Un aspetto di questa considerazione è rappresentato da ciò che il GDPR definisce "stato dell'arte". Le aziende non sono obbligate a implementare una tecnologia all'avanguardia. Tuttavia, devono sapere che cosa significa ciò e difendere la propria posizione. Una situazione da evitare per le aziende è cercare di giustificare il motivo per cui *non* abbiano implementato un particolare controllo o tecnica di sicurezza, generando direttamente una violazione dei dati.

Uno dei test fondamentali che probabilmente verrà applicato dalle autorità di regolamentazione del GDPR è quello che IDC identifica come test sull'entità dell'impegno da parte delle aziende di implementare adeguate procedure di sicurezza ("How hard did you you try"). Non essere a conoscenza di una vulnerabilità è del tutto negativo. Essere a conoscenza di una vulnerabilità e non intraprendere azioni è peggio. Ignorare una vulnerabilità di una flotta di stampanti in materia di sicurezza potrebbe sfociare in una violazione dei dati personali che, nei casi più gravi, potrebbe indurre un'autorità regolatrice a dubitare dell'implementazione di adeguate misure organizzative e tecniche volte alla protezione dei dati.

Cosa importante è l'ambito materiale del GDPR è "la trasformazione dei dati personali in tutto o in parte mediante mezzi automatizzati e il trattamento tramite mezzi non automatizzati dei dati personali che fanno parte di un sistema di archiviazione o sono destinati a far parte di un sistema di archiviazione". In altre parole, i dati non devono essere necessariamente in formato elettronico. Anche le copie fisiche dei dati dovrebbero essere messe in sicurezza.

La direttiva sulla sicurezza delle reti e delle informazioni

L'UE è consapevole che, in un'epoca di crescenti attacchi informatici, i servizi importanti devono essere protetti, in particolare quelli ritenuti critici per il funzionamento economico o sociale. Per raggiungere l'uniformità in tutti gli stati membri in materia di protezione contro gli attacchi informatici, l'UE ha approvato la direttiva NIS.

La NIS è sorprendentemente scarna nei dettagli in materia di requisiti di sicurezza. Dedica ampia attenzione alla protezione dell'infrastruttura, inclusi i beni fisici, e la maggiore enfasi è sulla resilienza (gestione degli incidenti, gestione della continuità aziendale, ecc.). Comprende una clausola relativa a notifiche di violazione obbligatorie (articolo 16), ma non prevede ammende in caso di mancata conformità.

Poiché la NIS è una direttiva, deve essere trasposta in legge da uno stato membro e ratificata dalla relativa legislazione. La NIS è entrata in vigore nell'agosto 2016. Gli stati membri avranno tempo fino al 10 maggio 2018 per la trasposizione della direttiva nelle rispettive legislazioni nazionali e altri sei mesi per identificare gli operatori dei servizi essenziali.

I vantaggi della protezione della stampante

La protezione della stampante, in contrapposizione alla protezione dei documenti stampati, è incentrata esclusivamente sui dispositivi fisici associati alla stampa e rappresenta una disciplina di sicurezza di rete. La protezione della stampante vede la stampante come endpoint, trattandola con la stessa cura di qualsiasi altro endpoint, ad esempio notebook, server e dispositivi mobili. Anche se condividono una lingua comune e alcune aree di interesse, la protezione dei documenti stampati e la protezione della stampante sono discipline differenti.

Quanto sono vulnerabili le stampanti di rete?

Le stampanti sono destinatarie di notevoli volumi di dati, alcuni dei quali personali.
Pochi utenti, professionisti della conformità o amministratori IT, prendono in considerazione la sicurezza di tali dati trasmessi e memorizzati sulle stampanti. Articolo 5.f

prevede “un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali". Ma poche organizzazioni prendono in considerazione la sicurezza dei dati presenti in una stampante.

Inoltre, è comune vedere i documenti stampati dimenticati nei vari vassoi delle stampanti. Alla luce del GDPR, le soluzioni di stampa pull potrebbero diventare parte integrante della prevenzione della perdita accidentale dei dati personali, in particolar modo per quelle organizzazioni per cui la stampa rappresenta il primo strumento per il trattamento dei dati.

Le stampanti sono un obiettivo appetibile per gli hacker, in parte perché non vengono considerate vero IT e non suscitano particolare attenzione da parte del personale addetto alla sicurezza IT. La gestione della stampante è spesso demandata a chi si occupa della gestione delle facility aziendali. Quando le stampanti sono diventate dispositivi di rete, fintantoché rimanevano dietro il firewall aziendale sono state considerate prevalentemente "a basso rischio". La vulnerabilità degli endpoint di stampa ha sempre ricoperto un ruolo secondario.

Le multifunzione, ad esempio stampanti/scanner/fax, sono inoltre sempre più sofisticate e dispongono di computer di uso generico installati all'interno per controllarne le azioni. I sistemi Windows e Linux sono spesso integrati in molte stampanti moderne. Poiché questi elementi informatici ottengono scarsa attenzione e manutenzione, risultano spesso vulnerabili. Inoltre, la funzionalità richiede connettività, con la risultante proliferazione di porte di rete aperte per supportare la fruibilità.

Una mancanza di attenzione combinata alle potenti capacità di elaborazione e un mix di opzioni di connettività consentono agli hacker numerose vie di accesso alle stampanti, ad esempio tramite modem, punto di accesso wireless o computer desktop infetti da spyware. Dopo aver ottenuto l'accesso, gli hacker possono utilizzare questo potere per colpire altre macchine sulla rete interna o partecipare a un denial-of-service distribuito. La maggior parte delle stampanti ha libero accesso a una rete interna. Un attacco che comprometta una stampante potrebbe trovare la via sgombra per individuare tutti i sistemi utilizzabili.

Come per altri dispositivi endpoint che richiedono protezione, le stampanti non sono solo un "punto di accesso", ma anche un vero e proprio obiettivo di attacchi informatici. Le stampanti spesso memorizzano documenti sensibili nel loro interno. Spesso sono combinate a uno scanner di documenti, e spesso i documenti sono memorizzati nell'archivio di scansione per molto più tempo di quanto creda la maggior parte degli utenti.

Considerazioni

Se la protezione della stampante non è mai stata al centro dell’attenzione della vostra aziendale, IDC ha alcune raccomandazioni su dove iniziare.

Tutto comincia con la visibilità

Come per qualsiasi endpoint che richieda sicurezza, iniziare dalle basi: il primo passo è sempre la visibilità. Compilate un inventario completo di tutte le stampanti, includendo marca, modello, funzionalità e configurazioni. La creazione di un tale elenco può essere problematica perché l'iniziativa individuale spesso colloca stampanti in luoghi non identificati (IT ombra). Nei laboratori, come negli uffici del top management o dei dipendenti, vengono spesso installate stampanti in rete o collegate direttamente a un PC per comodità, indipendentemente dalle implicazioni sulla sicurezza.

Idealmente, un inventario degli endpoint che includa le stampanti sarà derivato da un controller di accesso di rete (NAC) o uno strumento di gestione degli asset che ha come funzionalità di base la

scoperta dei dispositivi. Ottenere una visibilità veramente completa delle stampanti è estremamente difficile senza un NAC. Certo, alcuni modelli di stampanti offrono il rilevamento automatico quando sono connessi alla rete. Se l'ambiente di rete non ha la fortuna di includere una base omogenea di tali stampanti, un NAC rimane la soluzione migliore.

Potenziare le stampanti come endpoint

Le stampanti all'interno dell'azienda devono essere gestite come qualsiasi altro endpoint connesso. Chiudete tutti i servizi non necessari che la stampante offre, ad esempio FTP. La maggior parte delle organizzazioni non necessita di accesso FTP, il quale è più spesso motivo di danni che di vantaggi. Ad esempio, alcune stampanti potrebbero consentire a un utente malintenzionato di eseguire richieste FTP e di disattivare in modo anonimo i processi di stampa. Inoltre, molti servizi FTP sulle stampanti moderne sono soggetti ad attacchi di rimbalzo FTP. Con uno strumento come Nmap (Network Mapper), un utente malintenzionato può oscurare l'origine di una scansione di porte, convincendo un server FTP compatibile a consentire
connessioni FTP proxy. Sebbene tali scansioni di rimbalzo FTP siano tecniche vecchie, un notevole numero di server di stampa attualissimi è oggi suscettibile a tali attacchi.

La singola attività più importante nel potenziamento delle stampanti come endpoint rimane tuttavia la gestione delle password.
L'errore più eclatante delle imprese è non modificare le password predefinite. Secondo il *2016 Data Breach Investigations Report* di Verizon, il 63% delle violazioni di dati confermate ha coinvolto l'utilizzo di password deboli, predefinite o rubate. Se le stampanti sono gestite da strutture o fornitori di terze parti, la convenienza è fondamentale (per loro). Quando un dispositivo necessita di manutenzione, la ricerca di una password può rappresentare un problema. Quando è disponibile una stampante per 10 dipendenti, un'organizzazione con 10.000 dipendenti può avere 1.000 password da gestire. La sicurezza, dunque, cede il passo alla comodità. La gestione delle password non è semplicemente una manchevolezza da parte del personale non tecnico. Il secondo errore più grave è avere il nome utente e la password liberamente accessibili in testo non crittografato, disponibili a chiunque abbia una connessione http.

Manutenzione e patch

La maggior parte delle violazioni si verifica a causa della mancanza di buone pratiche. Secondo il *2016 Data Breach Investigations Report* di Verizon, le prime 10 vulnerabilità sfruttate nel 2015 hanno rappresentato l'85% del traffico di sfruttamento riuscito. Le vulnerabilità più sfruttate sono conosciute e divulgate pubblicamente. Gli hacker utilizzano tutto quel che funziona e sanno ottimizzare gli investimenti nei loro strumenti malware.

Patch e manutenzione di stampanti renderanno questi endpoint un obiettivo più difficile, spingendo gli hacker a prendere di mira le organizzazioni che non si dedicano alla manutenzione dei propri sistemi.

Quando si tratta di patch, non tutte le stampanti sono uguali. Alcuni produttori offrono set di strumenti gestionali che consentono di monitorare, gestire e applicare patch per alcune marche e modelli di stampanti. Questi set di strumenti sono estremamente utili perché l'analizzatore delle vulnerabilità dell'impresa probabilmente avrà problemi con le stampanti a causa del loro server Web integrato. Se le vostre stampanti hanno un set di strumenti gestionali robusto, siete fortunati. In caso contrario, potrebbe essere necessario eseguire patch manualmente su ciascuna stampante, poiché raccogliere tutto in un'unica soluzione automatizzata potrebbe risultare ostico.

Inoltre, per impedire l'importazione di "interferenze" negli strumenti SIEM, le organizzazioni spesso configurano gli analizzatori delle vulnerabilità per ignorare le stampanti. Questo rappresenta sia un problema con gli strumenti di gestione di vulnerabilità e SIEM sia con le stampanti. Può essere complicato configurare tali strumenti per accettare solo alcuni messaggi dalle stampanti, ma a breve

termine questo sforzo contribuirà a proteggere la rete da attacchi che utilizzano le stampanti come veicolo.

Proteggere le connessioni

Sostenete i protocolli di gestione utilizzati per la stampante. La maggior parte delle stampanti moderne supporta una sorta di gestione tramite HTTP e/o HTTPS e alcune supportano persino Telnet o Secure Shell (SSH). Scegliete con attenzione un protocollo di gestione che fornisca crittografia, ad esempio HTTPS o SSH, e disabilitate crittografie deboli o violate come SSLv3.

Infine, assicuratevi che le stampanti non dispongano di un accesso esteso a tutto il resto della rete interna. La segmentazione delle reti aziendali è una buona pratica di sicurezza di rete e le stampanti devono essere incluse in questo sforzo. I certificati possono essere utilizzati per segmentare logicamente l'accesso alle risorse di rete e per crittografare il traffico. Tuttavia, bisogna tenere presente che queste misure di sicurezza aggiuntive possono compromettere alcune funzionalità della stampante, come la limitazione dell'accesso ai servizi di directory (ad esempio Active Directory) e la gestione e il monitoraggio basati su cloud. Ottenere l'equilibrio tra la mera sicurezza delle stampanti e la conservazione delle funzionalità aziendali è sempre una questione di giudizio e valutazione del rischio aziendale.

Conclusione

Le stampanti non ricevono l'attenzione riservata ad altri vettori di minacce informatiche. La vulnerabilità e le minacce che ne derivano sono invece realtà tangibili. Le imprese di tutte le dimensioni devono adottare misure per affrontare il problema e risolverlo rapidamente. Gli hacker sono copioni incalliti. Una volta che un vettore di minaccia è stato sfruttato da un utente malintenzionato, altri hacker seguiranno a ruota.

Le conseguenze economiche e di immagine risultanti dall’aver ignorato la sicurezza delle proprie stampanti stanno per ottenere l'attenzione dei consigli di amministrazione grazie al GDPR. Sarebbe un peccato vedere un’impresa altrimenti conforme, che ha lavorato duramente sui propri processi di governance delle informazioni e sulle proprie tecnologie, cadere nella trappola di un punto cieco rappresentato da una stampante.
