Case study

I test dimostrano che la violazione della sicurezza informatica alle Torvik Industries da parte di "The Wolf" avrebbe potuto essere bloccata dalle stampanti HP

Rapporto ufficiale sulla violazione dei dati

Settore
Spedizioni

Obiettivo
Analizzare e risolvere le aree di vulnerabilità della rete

Approccio
Test di penetrazione per trovare le vulnerabilità che hanno portato all'attacco

Risultati e raccomandazioni
- Educare gli utenti a non aprire e-mail sospette e stamparne gli allegati
- Implementare stampanti HP con funzionalità di rilevamento delle minacce
- Configurare tutti gli endpoint per garantire la sicurezza, includendo le infrastrutture collocate in altre sedi o installate temporaneamente

Vantaggi per il business
Applicare maggiori misure di sicurezza per evitare tempi di inattività e fidelizzare i clienti. Migliorare le policy per il monitoraggio degli endpoint di rete installati temporaneamente.

Panoramica

Torvik Industries* spedisce 8 milioni di container ogni anno. Per 22.000 produttori e grossisti, Torvik è il collegamento vitale tra prodotti e persone in tutto il mondo. Il gruppo comprende cantieri navali, navi, magazzini e tutta la tecnologia a supporto della vasta rete di Torvik.

La sua infrastruttura tecnologica ha faticato a stare al passo con l'espansione dell'azienda. Anche se il personale addetto alla sicurezza IT ha configurato i server aziendali, alcune stampanti collocate in uffici distaccati o sedi temporanee non vengono gestite per quanto riguarda la sicurezza.

Il 23 aprile 2018, il cyber-terrorista noto come "The Wolf" ha usato una stampante non protetta per sabotare le operazioni di Torvik Industries, coinvolgendo PC, gru e navi portacontainer. L'esperto della sicurezza ha utilizzato i test di penetrazione per analizzare l'evento e ha fornito consigli per aumentare la sicurezza e la formazione del personale.

Cos'è accaduto

Il management di Torvik Industries ha sempre detenuto il comando delle attività, ma non era stato previsto che gli hacker si infiltrassero nella rete aziendale così profondamente da poter disattivare i carriponte e dirigere le navi in mare aperto.

Tutto ciò che The Wolf ha dovuto fare è stato compromettere una stampante per grandi formati di un cantiere. Successivamente, è riuscito a insinuarsi nella rete aziendale per avere il controllo su obiettivi più importanti. In un attimo, questa importante compagnia di spedizioni ha dovuto affrontare interruzioni operative, attenzione internazionale e migliaia di clienti furiosi.

Come è accaduto

Lo staff della sicurezza IT dell'azienda pensava che i sistemi fossero protetti. I team tecnici e logistici monitoravano costantemente le operazioni globali in vista di potenziali problemi legati alla sicurezza. Si avvalevano persino di procedure di sicurezza per endpoint come le stampanti. Ma qualcosa è stato trascurato: la configurazione di sicurezza di una stampante per grandi formati posizionata temporaneamente in una struttura in cantiere.

L'hacker non ha nemmeno avuto bisogno di accedere direttamente alla stampante: si è limitato a inviare un'e-mail con un allegato PDF al dipendente di Torvik responsabile della stampa di documenti di grande formato. Il PDF conteneva un file Postscript nascosto e "armato", in grado di aprirsi ed eseguirsi autonomamente al momento dell'invio del PDF alla stampante. Una volta che il dipendente ha inviato il lavoro di stampa, il malware si è annidato nella stampante e da lì si è diffuso in tutta la rete. Veicolando il malware con un allegato e-mail apparentemente innocuo, l'hacker ha aggirato il software anti-malware dei PC aziendali.

La violazione è stata possibile perché la stampante per grandi formati non disponeva di efficienti funzionalità di sicurezza integrate, come il rilevamento delle minacce. Inoltre, l'azienda non è riuscita a monitorare e gestire la configurazione di ogni singola stampante del parco dispositivi, come quelle posizionate temporaneamente in uffici distaccati.

Risoluzione del problema

Torvik Industries si è rivolta a un'importante società esperta in test di penetrazione per eseguire un'analisi approfondita della sicurezza informatica aziendale.

Il team che ha eseguito i test ha raccomandato l'installazione di stampanti HP con funzionalità di sicurezza integrate, tra cui la serie HP DesignJet dotata di avvio sicuro e whitelisting del firmware. Queste funzionalità aiutano la stampante a rilevare eventuali codici dannosi e ad arrestarsi, inviando notifiche all'IT per richiedere la reinstallazione del firmware originale HP.

Il team ha inoltre consigliato l'uso della funzionalità di sicurezza Instant-On di HP JetAdvantage Security Manager, un software per la gestione della sicurezza a livello di parco dispositivi, per applicare automaticamente le policy di sicurezza durante l'aggiunta dei dispositivi in rete. HP Security Manager è inoltre in grado di creare report di conformità che mostrano tutte le stampanti HP presenti, anche quelle posizionate temporaneamente o in sedi distaccate. Questo contribuisce a dimostrare la corretta gestione delle configurazioni di sicurezza del parco dispositivi.

Il team ha anche suggerito di attuare un programma di formazione per aiutare i dipendenti a riconoscere le e-mail sospette e ad evitare di stampare allegati sconosciuti.

Conclusione

Torvik Industries è ancora in fase di ripresa dalle conseguenze sofferte a causa della violazione della sicurezza informatica, che ha interessato l'area operativa dell'azienda, nonché dall'accresciuta pubblicità negativa in merito alle opinioni e alle azioni non convenzionali del suo presidente. Mentre l'azienda cerca di dare vita a una nuova impostazione della leadership, l'orientamento della sicurezza informatica è chiaro: avvalersi di stampanti e soluzioni HP aiuterà a sventare il prossimo attacco da parte di individui come The Wolf.

**Torvik Industries è un nome di fantasia, citato solo ai fini della realizzazione del film, per rappresentare l'oggetto di un grande attacco informatico nella produzione di HP Studios dal titolo "THE WOLF: TRUE ALPHA."*

Per maggiori informazioni sulle soluzioni HP:
HP DesignJet: hp.com/go/designjetsecurity
Sicurezza di stampa: hp.com/go/reinventsecurity
Guardate "The Wolf" su
hp.com/thewolf

4AA7-3562ITE, agosto 2018