Studiu de caz

Testul de penetrare arată că breşa de securitate de la Torvik Industries, produsă de „The Wolf”, ar fi putut fi oprită de imprimantele HP

Raportul oficial privind breşa de date

Industrie
Transporturi

Obiectiv
Analizarea şi rezolvarea zonelor de vulnerabilitate ale reţelei

Abordare
Teste de penetrare, pentru găsirea vulnerabilităţilor care au dus la atac

Constatări şi recomandări
- Instruiţi utilizatorii pentru a fi atenţi la deschiderea e-mailurilor şi a ataşărilor pentru imprimare care sunt suspecte
- Instalaţi imprimante HP cu funcţii de detectare a ameninţărilor
- Configuraţi toate punctele terminale pentru securitate, inclusiv infrastructura care este mutată sau aflată în locaţii temporare

Afacerea contează
Aplicaţi măsuri de securitate mai puternice, pentru a evita întreruperile în funcţionare şi a îmbunătăţi încrederea în brand. Îmbunătăţiţi politicile pentru monitorizarea punctelor terminale ale reţelei, aflate în locaţii temporare.

Prezentare generală

Torvik Industries* transportă anual 8 milioane de containere. Pentru 22.000 de producători şi vânzători angro, Torvik este conexiunea vitală între produse şi oameni din întreaga lume. Compania deţine docuri, vapoare, depozite şi toată tehnologia care susţine vasta reţea Torvik.

Pe măsură ce compania s-a dezvoltat, infrastructura tehnologică a acesteia a făcut eforturi să se adapteze. În timp ce personalul de securitate IT a configurat serverele companiei, unele imprimante din birouri satelit sau din locaţii temporare nu sunt gestionate din punct de vedere al securităţii.

Pe 23 aprilie 2018, teroristul cibernetic cunoscut sub numele „The Wolf” a utilizat o imprimantă neprotejată pentru a sabota operaţiile de la Torvik Industries, de la PC-uri până la macarale şi nave de transport ale containerelor. Consultantul companiei pe probleme de securitate a utilizat testarea la penetrare, pentru a analiza evenimentul şi a dat recomandări pentru creşterea securităţii şi instruirea personalului.

Ce s-a întâmplat

Conducerea companiei Torvik Industries era convinsă că deţine controlul în situaţii riscante, aşa încât nu se aştepta ca hackerii să se poată infiltra atât de adânc în reţeaua lor, încât să poată opri podurile rulante şi să redirecţioneze navele pe căi greşite în largul oceanului.

A fost suficient ca The Wolf să compromită o imprimantă de format mare dintr-un loc de construcţii. Apoi s-a putut mişca pe linie colaterală prin reţeaua companiei, către ţinte mai importante din cadrul operaţiilor companiei. Într-o clipă, această companie de transport de vârf s-a confruntat cu întreruperi operaţionale masive, cu verificări intense la nivel internaţional şi cu mii de clienţi furioşi.

Cum s-a întâmplat

Personalul de securitate IT al companiei credea că aceasta este protejată. Echipele lor tehnice şi logistice monitorizau în mod constant operaţiile globale, pentru a descoperi eventualele probleme de securitate. Aveau chiar şi proceduri de securitate stabilite pentru punctele terminale, precum imprimantele. Dar au scăpat din vedere un aspect: configuraţia de securitate a unei imprimante de format mare, amplasată temporar într-o remorcă de construcţii.

Nici nu era nevoie ca hackerul să acceseze imprimanta în mod direct – pur şi simplu a trimis un e-mail cu o ataşare PDF angajatului de la Torvik responsabil cu imprimarea documentelor de format mare. Acel PDF conţinea un fişier Postscript înarmat, care se putea deschide şi executa automat când fişierul PDF era trimis la imprimantă. Odată ce angajatul a trimis lucrarea de imprimare, malware-ul s-a încorporat singur în imprimantă, apoi s-a răspândit prin reţea. Prin integrarea malware-ului într-o ataşare de e-mail aparent inofensivă, hackerul a ocolit software-ul anti-malware de pe PC-urile companiei.

Breşa a fost posibilă deoarece imprimanta de format mare nu avea încorporată o securitate puternică, precum cea prevăzută cu detectarea ameninţărilor. De asemenea, compania nu a monitorizat şi nu a gestionat configuraţia fiecărei imprimante din flota de dispozitive, precum cele plasate temporar în birouri satelit.

Repararea breşei

Torvik Industries a apelat la o firmă de vârf în testarea penetrării, pentru a efectua o analiză minuţioasă a securităţii cibernetice a organizaţiei.

Echipa de testare a penetrării a recomandat instalarea imprimantelor HP cu caracteristici de securitate încorporate, inclusiv seria HP DesignJet cu Secure Boot şi liste de acces permis la firmware. Aceste caracteristici ajută imprimantele să detecteze codul rău intenţionat şi să se oprească, apoi să alerteze personalul IT privind nevoia de reinstalare autorizată Firmware HP.

De asemenea, au recomandat utilizarea caracteristicii de securitate Instant-On din HP JetAdvantage Security Manager, un program software de gestionare a securităţii la nivelul întregii flote de dispozitive, pentru aplicarea automată a politicilor de securitate pe măsură ce dispozitivele sunt adăugate la reţea. De asemenea, HP Security Manager poate să creeze rapoarte de conformitate, care prezintă fiecare imprimantă HP, situată chiar şi în locaţii de la distanţă sau temporare. Această capabilitate ajută la demonstrarea faptului că au fost menţinute configuraţiile de securitate a flotei de dispozitive.

În plus, consultantul pe probleme de securitate a sugerat un program de instruire, pentru a ajuta angajaţii să recunoască e-mailurile suspecte şi să evite imprimarea ataşărilor necunoscute.

Concluzie

Torvik Industries încă se clatină în urma impacturilor breşei de securitate cibernetică asupra operaţiilor, precum şi a publicităţii intense referitoare la punctele de vedere neconvenţionale şi infracţiunile comise de preşedintele companiei. În timp ce organizaţia caută să dezvolte o nouă direcţie în conducere, direcţia pentru securitate cibernetică este clară: trecerea la utilizarea imprimantelor şi soluţiilor de la HP va contribui la zădărnicirea planurilor următorului Wolf care va veni după vânat.

**Torvik Industries este o companie fictivă, supusă unui atac cibernetic amplu, în filmul realizat de Studiourile HP, „THE WOLF: TRUE ALPHA".*

Pentru mai multe informaţii despre soluţiile HP:
HP DesignJet: hp.com/go/designjetsecurity
Securitatea imprimării: hp.com/go/reinventsecurity

Pentru a vedea filmele „The Wolf", vizitaţi:
hp.com/thewolf

Înregistraţi-vă pentru actualizări
hp.com/go/getupdated

Partajaţi cu colegii

4AA7-3562ROE, august 2018