Studija slučaja

Testiranje proboja pokazuje da je kršenje računalne sigurnosti tvrtke Torvik Industries koje je proveo Vuk moglo biti spriječeno da su bili korišteni HP-ovi pisači

Službeno konačno izvješće o kršenju sigurnosti podataka

Djelatnost
Isporuka

Cilj
Analiziranje i uklanjanje područja ranjivosti mreže

Pristup
Testiranje proboja radi pronalaska ranjivih točaka koje su dovele do napada

Rezultati i preporuke
- Educiranje korisnika da postanu oprezni pri otvaranju sumnjivih poruka e-pošte i privitaka za ispis
- Implementiranje otkrivanja prijetnji u HP-ove pisače
- Konfiguriranje svih krajnjih točaka tako da obuhvaćaju sigurnost, uključujući pri tome premještene infrastrukture i one na privremenim lokacijama

Poslovanje
Potrebno je primijeniti jače zaštitne mjere radi sprječavanja prekida u radu i poboljšanja pouzdanosti robne marke. Treba i poboljšati pravilnike za nadzor krajnjih točaka mreže na privremenim lokacijama.

Pregled

Tvrtka Torvik Industries* svake godine isporuči 8 milijuna kontejnera. Za 22 000 proizvođača i prodavača u veleprodaji Torvik je ključna veza između proizvoda i osoba diljem svijeta. Tvrtkina imovina obuhvaća luke za utovar, vozila, skladišta i svu tehnologiju koja podržava široku mrežu tvrtke Torvik.

Kako je tvrtka rasla, tako su se javljali problemi prilikom prilagođavanja tehnološke infrastrukture. Iako je osoblje zaduženo za sigurnost IT-ja konfiguriralo poslužitelje tvrtke, neki su pisači u udaljenim urfedima ili na privremenim lokacijama izostavljeni iz upravljanja sigurnošću.

Dana 23. travnja 2018. računalni terorist poznat samo pod imenom "Vuk" iskoristio je nezaštićeni pisač da bi sabotirao rad tvrtke Torvik Industries, obuhvaćajući PC-je i kranove, ali i brodove s kontejnerima. Savjetnik za sigurnost upotrijebio je testiranje proboja da bi analizirao trendove i pružio preporuke za povećanje sigurnosti i obuku zaposlenika.

Što se dogodilo?

Rukovodstvo tvrtke Torvik Industries naviklo je donositi odluke u situacijama u kojima pogreške nisu dozvoljene, pa nisu očekivali da će hakeri toliko duboko infiltrirati njihovu mrežu da će uspjeti isključiti tvrtkine kranove i preusmjeriti brodove na otvoreni ocean.

Sve što je Vuk trebao učiniti jest kompromitirati pisač za ispis velikog formata na gradilištu. Nakon toga se mogao kretati tvrtkinom mrežom sve do velikih igrača koji upravljaju operacijama. Vrhunska je tvrtka za isporuku u trenutku bila suočena s prekidima u radu, velikim brojem pitanja i provjera međunarodnih klijenata i tisućama bijesnih korisnika.

Kako se to dogodilo?

Tvrtkini zaposlenici koji su radili na zaštiti IT-ja mislili su da su zaštićeni. Njihovi su tehnički i logistički timovi neprestano nadzirali globalne operacije da bi spriječili potencijalne sigurnosne probleme. Čak su pripremili i sigurnosne procedure za krajnje točke kao što su pisači. No zaboravili su na nešto važno: sigurnosnu konfiguraciju pisača za ispis velikog formata koji je privremeno postavljen u ured na gradilištu.

Haker nije čak morao ni izravno pristupiti pisaču – jednostavno je zaposleniku tvrtke Torvik zaduženom za ispis dokumenata velikog formata poslao poruku e-pošte s privitkom u obliku PDF. Taj je PDF sadržavao skrivenu PostScript datoteku pretvorenu u oružje, koja se mogla sama otvoriti i pokrenuti kada se PDF pošalje na ispis. Kada zaposlenik pošalje zadatak na ispis, zlonamjerni se softver ugrađuje u pisač i zatim širi mrežom. Priključivanjem zlonamjernog softvera na bezopasni privitak e-pošte haker je zaobišao softver za zaštitu od zlonamjernog softvera na PC-jevima tvrtke.

To je kršenje sigurnosti bilo moguće jer pisač za ispis velikog formata nije imao snažnu ugrađenu zaštitu sigurnosti, kao što je otkrivanje prijetnji. Osim toga, tvrtka nije nadzirala konfiguraciju svih pisača (uključujući one koji se privremeno nalaze u udaljenim uredima) niti je njima upravljala.

Rješenje kršenja sigurnosti

Tvrtka Torvik Industries zatražila je usluge vrhunske tvrtke za testiranje proboja radi provođenja temeljite analize računalne sigurnosti organizacije.

Tim za testiranje proboja preporučio je korištenje HP-ovih pisača s ugrađenim sigurnosnim značajkama, uključujući seriju HP DesignJet sa sigurnim pokretanjem i odobravanjem firmvera. Te značajke pisaču pomažu da otkrije zlonamjerne kodove te da ih isključi, a zatim obavijesti IT odjel o potrebi ponovne instalacije legitimnog HP-ovog softvera.

Osim toga, preporučio je i korištenje sigurnosne značajke Instant-On u sklopu softvera HP JetAdvantage Security Manager, softverskog programa za upravljanje sigurnošću svih uređaja, koja će automatski primjenjivati sigurnosne pravilnike čim se uređaji dodaju na mrežu. HP Security Manager može stvarati i izvješća o usklađenosti koja pokazuju svaki HP-ov pisač, čak i one na udaljenim ili privremenim lokacijama. To pokazuje da su sigurnosne konfiguracije očuvane na razini svih uređaja.

Osim toga, sigurnosni je savjetnik predložio pokretanje edukacijskog programa koji će pomoći zaposlenicima da prepoznaju sumnjive poruke e-pošte te da ne ispisuju nepoznate privitke.

Zaključak

Tvrtka Torvik Industries još se uvijek oporavlja od posljedica koje je kršenje računalne sigurnosti imalo na njihove operacije, ali i od povećanog publiciteta koji su privukli nekonvencionalni stavovi i kriminalna djela njihova predsjednika. Dok organizacija radi na razvoju novog smjera upravljanja, smjer računalne sigurnosti zaista je jasan: odabir HP-ovih pisača i rješenja koja će spriječiti novog Vuka u napadu.

**Torvik Industries izmišljena je tvrtka koja je bila meta velikog računalnog napada u filmu koji je napravio HP Studio: "VUK: ISTINSKI ALFA".*

Dodatne informacije o HP-ovim rješenjima potražite na adresi:
HP DesignJet: hp.com/go/designjetsecurity
Sigurnost ispisa: hp.com/go/reinventsecurity
Da biste pogledali filmove o "Vuku", posjetite:
hp.com/thewolf

Registrirajte se za ažuriranja
hp.com/go/getupdated

Podijelite s kolegama

4AA7-3562HRE, kolovoz 2018.