Prípadová štúdia

# Testy ukázali, že narušenie kybernetickej bezpečnosti spoločnosti Torvik Industries hackerom s prezývkou The Wolf by tlačiarne HP dokázali zastaviť

## Oficiálna záverečná správa o narušení dát

**Odvetvie**
Nákladná lodná doprava

**Cieľ**
Analýza a vyriešenie oblastí zraniteľnosti siete

**Prístup**
Penetračné testovanie na odhalenie rizikových miest, ktoré viedli k útoku

**Zistenia a odporúčania**
- Upozornite používateľov, aby boli opatrní pri otváraní podozrivých e-mailov a pri tlačení príloh
- Nasaďte tlačiarne HP, ktoré dokážu zisťovať hrozby
- Nakonfigurujte všetky koncové body s ohľadom na zabezpečenie vrátane pracovísk, ktoré sa menia alebo sú na dočasných miestach

**Obchodné záležitosti**
Aplikujte prísnejšie opatrenia zabezpečenia, aby ste predišli prevádzkovým prestojom a zvýšili dôveru značky. Zlepšite politiky monitorovania koncových bodov siete na dočasných pracoviskách.

## Prehľad

Spoločnosť Torvik Industries* každoročne prepraví 8 miliónov kontajnerov. Pre 22 000 výrobcov a veľkoobchodníkov je Torvik životne dôležitým spojením medzi výrobkami a ľuďmi po celom svete. Spoločnosť vlastní prekladiská, plavidlá, sklady a všetky technológie, ktoré podporujú veľkú sieť spoločnosti Torvik.

S rozvojom spoločnosti rástla aj snaha prispôsobiť jej veľkosti technologickú infraštruktúru Zatiaľ čo personál zabezpečujúci IT nakonfiguroval servery spoločnosti, o zabezpečenie tlačiarní vo vysunutých či dočasných pracoviskách nebolo postarané.

23. apríla 2018 kyberterorista známy len ako „The Wolf“ použil nezabezpečenú tlačiareň, aby sabotoval operácie spoločnosti Torvik Industries, od počítačov až po žeriavy a kontajnerové lode. Bezpečnostný poradca spoločnosti použil penetračný test na analýzu udalosti a poskytol odporúčania týkajúce sa zvýšenia zabezpečenia a školení zamestnancov.

## Čo sa stalo

Vedenie spoločnosti Torvik Industries pohybujúce sa vo vysokých sférach ochodu neočakávalo, že by hackeri prenikli do jej siete tak hlboko, aby dokázali zastaviť jej portálové žeriavy a presmerovať lode na otvorenom oceáne.

Všetko, čo Wolf musel urobiť, bolo preniknúť do veľkoformátovej tlačiarne na stavenisku. Cez sieť už potom mohol pristupovať k veľkým cieľom v prevádzke firmy. V priebehu pár okamihov táto špičková lodná spoločnosť čelila masívnym prerušeniam prevádzky, intenzívnej medzinárodnej kritike a tisícom nahnevaných zákazníkov.

## Ako sa to stalo

Pracovníci zabezpečenia IT si mysleli, že firma je chránená. Technické a logistické tímy neustále monitorovali globálne operácie a pracovali na odhaľovaní potenciálnych problémov so zabezpečením. Mali dokonca zavedené bezpečnostné postupy pre koncové body, ako sú tlačiarne. Niečo však prehliadli: konfiguráciu zabezpečenia veľkoformátovej tlačiarne dočasne umiestnenej v prívese na stavbe.

Hacker dokonca ani nemal priamy prístup k tlačiarni – poslal len e-mail s prílohou vo formáte PDF zamestnancovi, ktorý mal na starosti tlač veľkoformátových dokumentov. Dokument PDF obsahoval skrytý útočný súbor PostScript, ktorý sa mohol sám otvoriť a spustiť pri odoslaní súboru PDF do tlačiarne. Keď pracovník Torvik Industries odoslal tlačovú úlohu, malvér sa vložil do tlačiarne a rozšíril sa po celej firemnej sieti. Vďaka tomu, že sa malvér tváril ako nevinne vyzerajúca e-mailová príloha, hacker obišiel softvér na ochranu proti malvéru vo firemných počítačoch.

Prienik teda umožnila veľkoformátová tlačiareň, ktorá nemala silné vstavané zabezpečenie, teda napríklad detekciu hrozieb. Spoločnosť tiež nedokázala monitorovať a spravovať konfiguráciu každej jednej tlačiarne vo flotile, napríklad ani tých, ktoré boli dočasne umiestnené v dočasných kanceláriách.

## Náprava po útoku

Spoločnosť Torvik Industries si najala špičkovú firmu na penetračné testovanie, aby získala dôkladnú analýzu kybernetickej bezpečnosti organizácie.

Tím vykonávajúci penetračné testy odporučil inštaláciu tlačiarní HP so vstavanými funkciami zabezpečenia vrátane radu HP DesignJet s funkciou Secure Boot a povoľovaním firmvéru. Tieto funkcie pomáhajú tlačiarni rozpoznať škodlivý kód, vypnúť sa a následne upozorniť IT oddelenie na potrebu preinštalovať legitímny firmvér spoločnosti HP.

Odporučili tiež použiť bezpečnostnú funkciu Instant-On softvéru HP JetAdvantage Security Manager, softvéru na správu zabezpečenia v rámci celej flotily, aby sa pravidlá zabezpečenia uplatnili automaticky na nové zariadenie pridané do siete. Program HP Security Manager dokáže tiež vytvárať správy o zhode, ktoré zobrazujú každú
tlačiareň HP, a to aj na vzdialenom alebo dočasnom pracovisku. To pomáha preukázať, že konfigurácie zabezpečenia flotily zariadení boli zachované.

Okrem toho poradca pre bezpečnosť navrhol vzdelávací program, ktorý pomôže zamestnancom rozpoznať podozrivé e-maily a netlačiť neznáme prílohy.

## Záver

Spoločnosť Torvik Industries sa stále vzpamätáva z narušenia kybernetickej bezpečnosti svojich operácií a rovnako aj z rastu publicity, ktorú vzbudili nekonvenčné názory a trestné činy jej prezidenta. Zatiaľ čo sa organizácia usiluje nájsť nový smer v jej vedení, smerovanie kybernetickej bezpečnosti je jasné: prechod na tlačiarne a riešenia HP jej pomôže zbaviť sa ďalšieho hackera, ktorý sa k nej prikradne na lov.

** Torvik Industries je fiktívna spoločnosť čeliaca veľkému kyberútoku vo filme THE WOLF: TRUE ALPHA od spoločnosti HP Studio.*

**Ďalšie informácie o riešeniach od HP:**
HP DesignJet: hp.com/go/designjetsecurity
Zabezpečenie tlače: hp.com/go/reinventsecurity

**Ak si chcete pozrieť film The Wolf, navštívte stránku:** hp.com/thewolf

Registrácia na príjem noviniek
hp.com/go/getupdated

Zdieľať s kolegami



4AA7-3562SKE, august 2018