Esettanulmány

A behatolási vizsgálatok szerint a Torvik Industries megállíthatta volna The Wolf kiberbiztonsági támadását HP nyomtatókkal

Hivatalos jelentés a támadásról

Iparág
Szállítás

Cél
A hálózati sebezhető területeinek elemzése és megoldása

Megközelítés
A behatolási vizsgálatok segítenek azon sebezhető területek megtalálásához, amelyek a támadáshoz vezettek

Eredmények és ajánlások
- A felhasználók oktatása azzal kapcsolatban, hogy legyenek óvatosak a gyanús e-mailek megnyitásakor és mellékletek nyomtatásakor
- Fenyegetésészleléssel rendelkező HP nyomtatók használata
- Az összes végpont konfigurálása a biztonság érdekében, beleértve az áthelyezett vagy ideiglenes helyeken lévő infrastruktúrát

Üzleti pontok
Hatékonyabb biztonsági intézkedések alkalmazása a működési állásidő elkerülése és a márka iránti bizalom javítása érdekében.
Az ideiglenes helyeken lévő hálózati végpontok felügyeletére vonatkozó irányelvek javítása.

Áttekintés

A Torvik Industries* évente 8 millió konténert szállít. A 22 000 gyártó és nagykereskedő számára a Torvik a létfontosságú kapcsolat a termékek és emberek között a világ minden táján. A vállalat holdingjai közé tartoznak a kikötők, a hajók, a raktárak és a Torvik távoli hálózatát támogató technológia is.

Ahogy a vállalat növekedett, technológiai infrastruktúrája nehezen alkalmazkodott. Míg az IT biztonsági személyzet konfigurálta a vállalat szervereit, egyes nyomtatókat a kihelyezett irodákban vagy ideiglenes telephelyeken nem kezelnek a biztonság tekintetében.

2018. április 23-án a „The Wolf” néven ismert kiberterrorista egy nem biztonságos nyomtatót használ a Torvik Industries műveleteinek szabotálására, a számítógépektől a darukon át a konténerszállító hajókig. Biztonsági tanácsadójuk behatolási vizsgálatot használt az esemény elemzésére, és ajánlásokat adott a biztonság növelésére és a személyzet képzésére.

Mi történt?

A Torvik Industries vezetése nagyban játszott – így nem számítottak arra, hogy a hekkerek olyan mélyen beszivároghatnak a hálózatukba, hogy le tudják kapcsolni a cég daruit, és eltereljék a hajókat a nyílt óceánon.

Csak annyit kellett The Wolfnak tennie, hogy behatoljon egy nagy formátumú nyomtatóba egy építkezési területen. Ezután a vállalat hálózatán keresztül oldalirányban támadhatja meg nagy célpontjait a vállalat működési területei között. Egy pillanat alatt ez a vezető hajózási társaság masszív működési zavarokkal, intenzív nemzetközi ellenőrzéssel és több ezer dühös ügyféllel szembesült.

Hogyan történt?

A vállalat IT biztonsági személyzete úgy gondolta, hogy megfelelő védelemmel rendelkeznek. A technológiai és logisztikai csapatok folyamatosan felügyelték a globális műveleteket a potenciális biztonsági problémák végett. Még a végpontok, mint például a nyomtatók esetében is voltak biztonsági eljárások. Azonban figyelmen kívül hagytak valamit: egy nagy formátumú nyomtató biztonsági konfigurációját, amely ideiglenesen egy építési konténerben állt.

A hekkernek nem is kellett közvetlenül hozzáférnie a nyomtatóhoz – egyszerűen küldött egy e-mailt egy PDF melléklettel a Torvik egyik alkalmazottjának, aki a nagy formátumú dokumentumok nyomtatásáért felelős. Ez a PDF egy rejtett, fegyverezett Postscript-fájlt tartalmazott, amely megnyitható és futtatható, amikor a PDF-et elküldik a nyomtatóra. Miután a munkatárs elküldte a nyomtatási feladatot, a kártevő program beágyazódott a nyomtatóba, majd elterjedt a hálózaton. Az ártatlannak tűnő e-mail mellékletek kártevő programmal való ellátásával a hekker megkerülte az vírusirtó szoftvereket a vállalati számítógépeken.

A behatolás azért volt lehetséges, mert a nagy formátumú nyomtatónak nem volt erős beépített biztonsági rendszere, például a fenyegetések észlelésére. Továbbá a vállalat nem felügyelte és kezelte a flotta összes nyomtatójának konfigurációját – hasonlóan a műholdas irodákban ideiglenesen elhelyezettek esetében sem.

A behatolás javítása

A Torvik Industries felkért egy piacvezető, behatolásokat vizsgáló céget, hogy végezzen alapos elemzést a szervezet internetes biztonságáról.

A behatolásvizsgáló csapat javasolta a beágyazott biztonsági funkciókkal ellátott HP nyomtatók telepítését, beleértve a HP DesignJet sorozatát biztonságos rendszerindítással és a firmware engedélyezési listával. Ezek a funkciók segítik a nyomtatót a kártevő kód észlelésében és leállításában, majd figyelmeztetik az IT-t arról, hogy újra kell telepítenie a megfelelő HP firmware-t.

Emellett a HP JetAdvantage Security Manager azonnali aktiválás biztonsági funkcióját is ajánlották, amely a flotta egészére kiterjedő biztonsági felügyeleti szoftver, hogy automatikusan alkalmazzák a biztonsági irányelveket, amint eszközöket adnak hozzá a hálózathoz. A HP Security Manager megfelelőségi jelentéseket is létre tud hozni, amelyek tartalmazzák az összes HP nyomtatót, még a távoli vagy ideiglenes helyeken is. Ez segít demonstrálni, hogy a flotta biztonsági konfigurációi folyamatosan érvényben vannak.

Ezenkívül a biztonsági tanácsadó egy olyan oktatási programot javasolt, amely segítséget nyújt az alkalmazottaknak a gyanús e-mailek felismerésében és az ismeretlen mellékletek nyomtatásának elkerülésében.

Összegzés

A Torvik Industries még mindig a kiberbiztonsági feltörésének hatása alatt áll, valamint az elnökök nem mindennapi nézeteinek és bűncselekményeinek fokozott nyilvánosságától zajos. Miközben a szervezet új vezetési irányra törekszik, a kiberbiztonság iránya világos: a HP nyomtatókra és megoldásokra való áttérés segíteni fog a következő portyázó farkas megállításában.

**A Torvik Industries egy fiktív vállalat, amelyet egy hatalmas kibertámadás ért a HP Studio filmjében, amelynek címe: „THE WOLF: IGAZI ALFA".*

További tudnivalók a HP megoldásokról:
HP DesignJet: hp.com/go/designjetsecurity
Nyomtatási biztonság: hp.com/go/reinventsecurity

A „The Wolf" filmek megtekintéséhez:
hp.com/thewolf

Iratkozzon fel a friss hírekre
hp.com/go/getupdated

Megosztás a kollégákkal

4AA7-3562HUE, 2018. augusztus