Študija primera

Simulacijski vdori kažejo, da bi tiskalniki HP lahko ustavili napad na spletno varnost, ki ga je v podjetju Torvik Industries izvedel »The Wolf«

Uradno zaključeno poročilo o varnostni kršitvi

Panoga
Transport

Cilj
Analiza in odpravljanje omrežnih ranljivosti

Pristop
Simulacijski vdori, da se poiščejo ranljivosti, zaradi katerih je bil mogoč napad

Ugotovitve in priporočila
- Priprava uporabnikov, da so pozorni pri odpiranju sumljivih e-poštnih sporočil in tiskanju prilog
- Uvedba tiskalnikov HP s funkcijami odkrivanja groženj
- Konfiguriranje vseh končnih točk za varnost, vključno s premično infrastrukturo ali infrastrukturo na začasnih lokacijah

Zadeve na področju poslovanja
Uvedba strožjih varnostnih ukrepov, da se prepreči zastoj delovanja in izboljša zaupanje v blagovno znamko Izboljšanje pravilnikov za nadzor omrežnih končnih točk na začasnih lokacijah

Pregled

Podjetje Torvik Industries* vsako leto transportira 8 milijonov zabojnikov. Za 22.000 proizvajalcev in veleprodajalcev je Torvik vitalna povezava med izdelki in ljudmi po vsem svetu. Lastnina podjetja vključuje pristanišča, plovila, skladišča in vso tehnologijo, ki podpira Torvikovo omrežje tudi v najbolj oddaljenih krajih.

S širitvijo podjetja so se pojavile težave s prilagajanjem tehnološke infrastrukture. Čeprav je osebje, zadolženo za varnost informacijske tehnologije, konfiguriralo strežnike podjetja, se na nekaterih tiskalnikih v satelitskih pisarnah ali na začasnih lokacijah ne izvaja upravljanje varnosti.

23. aprila 2018 je spletni terorist, znan kot »The Wolf«, prek nezaščitenega tiskalnika sabotiral delovanje podjetja Torvik Industries, vključno z računalniki, žerjavi in kontejnerskimi ladjami. Njihov svetovalec za zaščito je na podlagi simulacijskega vdora analiziral dogodek in podal priporočila za povečanje zaščite in usposabljanje osebja.

Kaj se je zgodilo

Podjetje Torvik Industries imelo zaradi svoje vodilne vloge glavno besedo v poslih z visokimi tveganji, zato niso pričakovali, da bi se lahko napadalci v njihovo omrežje infiltrirali tako globoko, da bi zaustavili prekladne žerjave podjetja in preusmerili ladje na odprto morje.

Vse, kar je moral narediti »The Wolf«, je bilo vdreti v tiskalnik velikega formata na gradbišču. Nato se je lahko prek omrežja podjetja dokopal do velikih tarč v poslovanju podjetja. V trenutku se je ta vrhunska ladjarska družba soočila z obsežnimi prekinitvami poslovanja, strogim mednarodnim nadzorom in več tisoč besnimi strankami.

Kako se je to lahko zgodilo

Osebje, zadolženo za varnost informacijske tehnologije v podjetju, je menilo, da so zaščiteni. Njihove tehnične in logistične ekipe so ves čas izvajale nadzor nad morebitnimi varnostnimi težavami v globalnem poslovanju. Izvajali so tudi ukrepe za končne točke, na primer za tiskalnike. Nekaj pa so vseeno spregledali: varnostno konfiguracijo tiskalnika velikega formata, ki je bil začasno postavljen v prikolico na gradbišču.

Napadalcu sploh ni bilo treba neposredno dostopiti do tiskalnika; uslužbencu v podjetju Torvik, odgovornemu za tiskanje dokumentov velikega formata, je preprosto poslal e-poštno sporočilo s prilogo PDF. V tej datoteki PDF je bila skrita zlonamerna datoteka Postscript, ki se je lahko odprla in zagnala, ko je bila datoteka PDF poslana na tiskalnik. Ko je uslužbenec poslal tiskalni posel, se je zlonamerna programska oprema vgradila v tiskalnik, nato pa razširila po celotnem omrežju. S prikritjem zlonamerne programske opreme v navidez neškodljivi e-poštni prilogi je napadalec zaobšel protivirusno programsko opremo na računalnikih podjetja.

Do kršitve je lahko prišlo, ker tiskalnik velikega formata ni uporabljal močnih varnostnih funkcij, na primer odkrivanja groženj. V podjetju prav tako niso nadzirali in upravljali konfiguracije vseh tiskalnikov v skupini naprav, na primer tistih na začasnih lokacijah v satelitskih pisarnah.

Popravilo kršitve

V podjetju Torvik Industries so s pomočjo najboljše ekipe za simulacijske vdore izvedli natančno analizo spletne varnosti organizacije.

Ekipa za simulacijske vdore je priporočila namestitev tiskalnikov HP z vdelanimi varnostnimi funkcijami, vključno s HP DesignJet series s funkcijama Secure Boot in Whitelisting za vdelano programsko opremo. Te funkcije pomagajo tiskalniku pri odkrivanju zlonamerne kode in zaustavitvi, nato pa obvestijo informacijsko tehnologijo, da je treba znova namestiti overjeno vdelano programsko opremo HP.

Priporočili so tudi uporabo varnostne funkcije Instant-On, ki je del orodja HP JetAdvantage Security Manager, programa za upravljanje varnosti programske opreme v celotni skupini naprav, ki samodejno uveljavi varnostne pravilnike takoj, ko so naprave dodane v omrežje. HP Security Manager lahko tudi ustvari poročila o skladnosti, ki prikazujejo vse tiskalnike HP, tudi tiste na oddaljenih ali začasnih lokacijah. Ta poročila pomagajo pri pregledu vzdrževanja varnostnih konfiguracij v celotni skupini naprav.

Svetovalec za zaščito je predlagal tudi izobraževalni program, ki bi bil uslužbencem v pomoč pri prepoznavanju sumljivih e-poštnih sporočil in preprečevanju tiskanja neznanih prilog.

Sklep

Podjetje Torvik Industries si še vedno ni opomoglo od vplivov, ki jih je imel spletni vdor na poslovanje, kot tudi od povečane publicitete zaradi nenavadnih pogledov in kaznivih dejanj svojega predsednika. Medtem ko si organizacija prizadeva razviti nove smeri, ki bi jim zagotovile vodilno vlogo, je smer na področju spletne varnosti jasna: uporaba tiskalnikov in rešitev HP bo pomagala odgnati naslednjega »Wolfa« pri iskanju plena.

**Torvik Industries je izmišljeno podjetje, ki je cilj spletnega napada v filmu HP Studio z naslovom »THE WOLF: PRAVI ALFA«.*

Več informacij o HP-jevih rešitvah:
HP DesignJet: hp.com/go/designjetsecurity
Varnost tiskanja: hp.com/go/reinventsecurity
Za ogled filmov »The Wolf« obiščite spletno mesto
hp.com/thewolf

Prijavite se za posodobitve
hp.com/go/getupdated

Delite s sodelavci

4AA7-3562SLE, avgust 2018