Študija primera

Ko je bilo Londonsko letališče cilj zlonamernega napada, so tiskalniki HP zaznali grožnjo

Uradno zaključeno poročilo o varnostni kršitvi

Panoga
Letalski promet

Cilj
Prepoznavanje šibkih členov v praksah spletne zaščite in njihovo obravnavanje

Pristop
Razvoj celovitega varnostnega načrta v sodelovanju s HP-jevimi strokovnjaki za varnost

Zadeve na področju informacijske tehnologije
- Uveljavitev varnostnih ukrepov za končne točke interneta stvari
- Omogočanje vgrajenih varnostnih funkcij v tiskalnikih HP
- Izboljšanje nadzora nad zaščito v celotnem omrežju

Zadeve na področju poslovanja
Izboljšanje spletne varnosti za zaščito ključne mednarodne infrastrukture in vzdrževanje varnosti potnikov

Pregled

Londonsko letališče* vsak dan oskrbi več kot 300.000 potnikov na poti v 94 držav po vsem svetu. Na letališču dela skoraj 50.000 ljudi iz 300 podjetij, zato je dejansko mesto v malem.

Ko se je letališče širilo, je njegova infrastruktura postajala vse bolj povezana in avtomatizirana. Notranji sistemi, vse od HVAC do razsvetljave in tiskalnikov, so zdaj povezani v letališko omrežje. Tiskanje, skeniranje in kopiranje se zdaj izvaja na skupini več kot 60 večnamenskih naprav HP, ki so nameščene širom letališča.

23. aprila 2018 je spletni terorist, znan kot »The Wolf«, prek povezanih letaliških sistemov razsvetljave pridobil dostop do omrežja, v katerem je razširil svojo zlonamerno programsko opremo. Ker je poznan po izkoriščanju premalo zaščitenih končnih točk, so strokovnjaki za informacijsko tehnologijo kot del raziskave nemudoma pregledali dnevnike groženj na tiskalnikih HP Enterprise, da bi osamili in zaustavili napad. Presenetljivo so dnevniki vsebovali ključe, ki jih je pustil »The Wolf«, in so kazali na izvor vdora. Pozneje je Londonsko letališče zaprosilo HP še za nadaljnjo izboljšavo varnosti končnih točk.

Kaj se je zgodilo

Ko je »The Wolf« odkril ranljivost, najverjetneje prek sporočil z lažnim predstavljanjem, ki jih je pošiljal uporabnikom omrežja, je lahko sistem razsvetljave interneta stvari okužil z zlonamerno programsko opremo. Zlonamerno programsko opremo je lahko nato razširil po celotnem omrežju, s čimer je ustvaril oporo v drugih nenadzorovanih končnih napravah.

Ker je ekipa »The Wolfa« skrila svojo prisotnost v nenadzorovane naprave interneta stvari, je sistemi za nadzor omrežja niso mogli odkriti, medtem ko je razvijala več zagonskih točk za uničujoč napad velikih razsežnosti.

Vodstvo letališča si je obupno prizadevalo zaustaviti več sistemov, ne da bi to vplivalo na kritično infrastrukturo, na primer letala in potnike.

Odziv na napad

»The Wolf« je bil najet za napad na letališko omrežje. Letališko osebje za zaščito informacijske tehnologije *je bilo prepričano*, da je letališko omrežje dobro zaščiteno pred napadalci, toda spregledali so grožnje, skrite v naprave interneta stvari.

Na srečo so letališki tiskalniki HP Enterprise vključevali orodje HP Connection Inspector, ki je zaustavilo zlonamerno programsko opremo, ko je ta izvajala sumljive poskuse »klicanja domov« na ukaze in nadzorne strežnike napadalcev.

Dejanja so bila zajeta v sistemskih dnevnikih tiskalnikov. Ko je osebje, zadolženo za informacijsko tehnologijo, ugotovilo, da je nekaj narobe, so za odkrivanje podrobnosti o napadu pregledali sistemske dnevnike. Toda med razširjanjem zlonamerne programske opreme v omrežju je čas ključnega pomena. Če bi osebje, zadolženo za informacijsko tehnologijo, povezalo sistemske dnevnike odkrivanja groženj v tiskalnikih s sistemom za nadzorovanje varnostnih informacij in dogodkov (SIEM), bi bili o vdoru obveščeni takoj.

Zmogljivejša varnost kot kdaj koli prej

Po varnostni kršitvi je osebje, zadolženo za informacijsko tehnologijo, pregledalo varnostne prakse s svojim ponudnikom vodenih storitev tiskanja in HP-jevimi svetovalci za varnost.

Ko se je Londonsko letališče odločilo za namestitev tiskalnikov HP Enterprise, so naredili pravo potezo. Samo tiskalniki in večnamenske naprave HP Enterprise zagotavljajo funkcije zaznavanja vdorov med izvajanjem in orodje HP Connection Inspector, ki odkriva in zaustavlja zlonamerno programsko opremo med operacijami ter uveljavi vnovični zagon. Pri zagonu funkcija HP Sure Start preveri sistemski BIOS in v primeru spremenjene kode samodejno odpravi napake, funkcija Whitelisting pa preveri vdelano programsko opremo.

Ponudnik vodenih storitev tiskanja je namestil funkcijo HP JetAdvantage Security Manager, ki pri vsakem vnovičnem zagonu samodejno preveri varnostne nastavitve in ponastavi vse, ki so spremenjene.

Letališko osebje, zadolženo za varnost informacijske tehnologije, je tudi povezalo sistemske dnevnike tiskalnika s svojim orodjem SIEM. Za razliko od tiskalnikov drugih proizvajalcev lahko naprave HP zagotovijo dnevnike, specifične za grožnje, za številna orodja SIEM, da lahko osebje, zadolženo za informacijsko tehnologijo, sproti prejema obvestila o morebitnih varnostnih incidentih. Zato so tiskalniki HP neprecenljivi nadzorniki omrežja.

Sklep

Zaradi letaliških tiskalnikov HP Enterprise in ključev, ki jih je za seboj pustil »The Wolf«, je lahko varnostna ekipa dovolj hitro osamila napad, da je preprečila prekinitev delovanja, negativno publiciteto, kazni zaradi neizpolnjevanja zahtev in škodo, povezano z blagovno znamko.
Z uvedbo močnejših varnostnih praks in popolnim izkoriščanjem prednosti vgrajenih varnostnih funkcij tiskalnikov HP je letališče okrepilo varnost v celotnem omrežju.

**Londonsko letališče je izmišljena organizacija, ki je cilj spletnega napada v filmu HP Studio z naslovom »THE WOLF: PRAVI ALFA«.*

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

Prijavite se za posodobitve
hp.com/go/getupdated

Delite s sodelavci

4AA7-3560SLE, avgust 2018