KONICA MINOLTA

SIKKERHETSVURDERING AV NTT DATA

KAN STÅ IMOT 80 TIMER MED "WHITE HAT HACKING"

UAVHENGIG TESTING AV EN RESPEKTERT GLOBAL SIKKERHETSEKSPERT

Alle enheter med en CPU og et operativsystem som er koblet til et nettverk representerer en sikkerhetsrisiko. For å beskytte data og overholde sikkerhetskrav som PCI, HIPAA, FERPA og GDPR, overvåker internasjonale selskaper fremvoksende trusler hos alle enheter, inkludert skrivere. I det siste har flere medier publisert historier hvor skrivere er blitt benyttet som en inngangsport til bedriftens nettverk, for å påføre skade og stjele informasjon. Konica Minoltas kunder er naturligvis opptatt av sikkerhetsutfordringer som kan være til stede i eget selskap.

Selv om Konica Minolta kan tilby kundene sine designspesifikasjoner og interne testdata som viser hvordan Konica Minoltas multifunksjonsprintere er sikre mot angrep, besluttet vi å leie inn en uavhengig ekspert for å forsøke å bryte seg inn på en av våre skrivere. Testen ble utført av NTT DATA og NTT Security på en av våre bestselgende bizhub-enheter med gjennomtrengnings-tester, inkludert script-angrep og avanserte hackingstaktikker.

Som internasjonalt anerkjente sikkerhetseksperter var NTT DATA og NTT Security det åpenbare valget for å gjennomføre testingen. Konica Minolta stilte en multifunksjonsprinter med tilhørende kildekode til rådighet for ingeniørene, slik at "white hat-hackingen" kunne utføres på den bredeste og mest aggressive måten. Testene foregikk over flere uker, med totalt 80 timer aktiv forsøk på hacking av enheten. Ingen alvorlige sårbarheter ble funnet, hvilket underbygger og dokumenterer at Konica Minoltas printere er godt sikret mot angrep, inkludert såkalt "brute force".

KONICA MINOLTA
MFP SIKKERHETSFUNKSJONER

Oppdatert og sertifisert
Konica Minolta utvikler og leverer de nyeste sikkerhetsfunksjonene for å beskytte kundens data. De fleste Konica Minolta-maskinene er sertifisert etter ISO 15408 og FIPS140-2.

Et sikkert nettverk
Maskiner utstyrt med brukerautentisering sikrer at kun personer med tilgang kan bruke dem. Autentisering som administrator er nødvendig for å få tilgang til hele adresseboken, en funksjon som forhindrer at hele adresseboken kan komme på avveie. Ubrukte MFP-porter og protokoller kan slås AV for å forhindre innbrudd. Fakslinjen støtter bare faksprotokoller, og hvis andre kommunikasjonsprotokoller forsøker å bruke linjen, er det ikke støtte for dette. Kryptering, toveis sertifikat-verifisering og mulighet for å sette nettverk i karantene, er også tilgjengelig.

Forbli virusfri
Konica Minoltas multifunksjonsprintere bruker et operativsystem med en Linux-kjerne, som blir holdt oppdatert med alle nødvendige sikkerhetsoppdateringer, slik at den kan kjøre sikkert med Windows OS-enheter, som eksempelvis servere. Hvis en infisert USB-pinne kobles til enheten, finnes det ingen mekanismer som autokjører filer, dette betyr at "run file"-virus ikke har noen effekt.

Dine data er i trygge hender
Data lagret på de interne harddiskene er kryptert og kan låses med passord. Dette betyr at i tilfelle harddisken skulle bli stjålet, forblir dataene beskyttet (dette er et tillegg på enkelte maskiner). Midlertidige data blir overskrevet side for side, slik at det blir umulig å skrive ut dataene igjen. For å forhindre at utskriftene blir tatt fra utskuffen av en tredjepart, kan du bruke sikker utskrift-funksjonen. Utskriften starter etter at passordet er oppgitt på panelet på printeren.

LENKE TIL ORIGINAL ARTIKKEL FRA NTT DATA

10/2018

Konica Minolta Business Solutions Norway AS · Maridalsveien 323 · 0872 Oslo Norge · www.konicaminolta.no