HVIDBOG

ULÅSTE DØRE

FORSKNING VISER, AT PRINTERE EFTER-LADES SÅRBARE OVER FOR CYBERANGREB

Mens IT-teams fokuserer på andre slutpunkter, halter sikkerheden for virksomhedernes printere bagefter

Printere er lette mål: Alt for mange netværkstilsluttede printere har ingen begrænsninger og er ikke forsvarligt låst.

Men truslen er reel, og bør ikke ignoreres. Virksomhedsprintere har udviklet sig til stærke, netværksbaserede enheder med de samme sårbarheder som andre slutpunkter på dit netværk. Disse typisk usikrede indgange giver en meget reel mulighed for cyberangreb. De kan også tilbyde adgang til din virksomheds finansielle og private data, hvilket fører til meget reelle forretningsmæssige konsekvenser.

Alligevel viser en nylig Spiceworks-undersøgelse blandt mere end 300 IT-beslutningstagere fra virksomheder, at kun 16 % af de adspurgte tror, at printere er i høj risiko for en sikkerhedstrussel/brud, altså betydeligt mindre end stationære og bærbare computere samt mobilenheder.[1] Denne opfattelse har ændret IT-folks tilgang til netværkssikkerhed. Mens næsten tre ud af fem organisationer har en sikkerhedspraksis til printere på plads, er denne procentdel langt under procentdelen for andre slutpunkter og efterlader printere sårbare, selvom der er nemme løsninger til at beskytte denne særlige indgang.

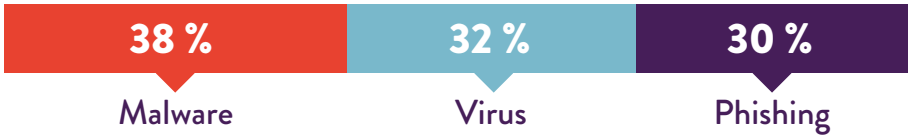
Denne hvidbog præsenterer data om printersikkerhed baseret på Spiceworks-undersøgelsen, virkningen af brud på sikkerheden samt nogle af de moderne indbyggede printersikkerhedsfunktioner, som er designet til at beskytte mod cyberangreb.

KUN 16 % AF DE ADSPURGTE TROR, AT PRINTERE ER I HØJ RISIKO FOR EN SIKKERHEDSTRUSSEL/BRUD.[1]

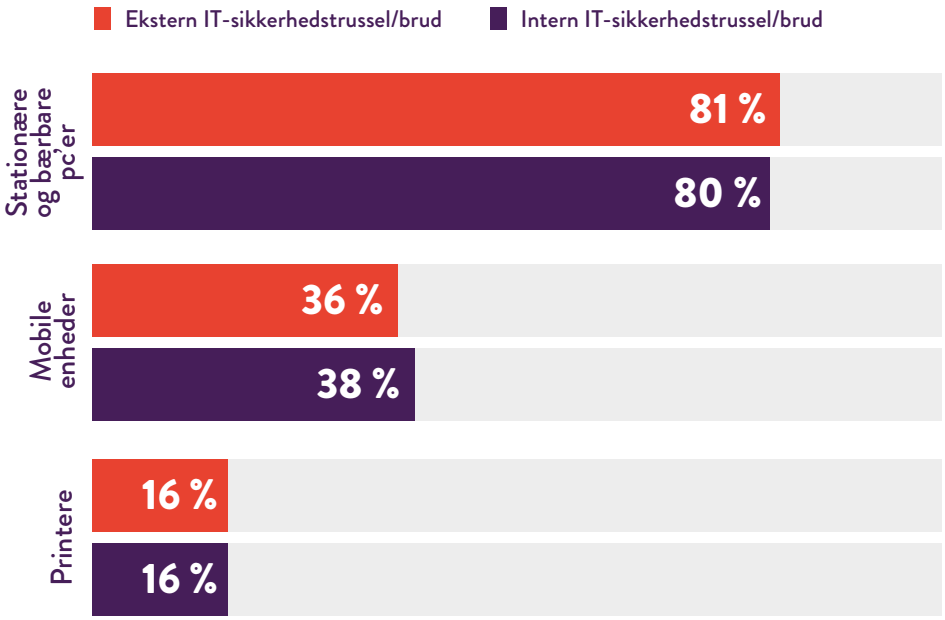
DØRÅBNINGER TIL ANGREB

I Spiceworks-undersøgelsen sagde 74 % af de adspurgte (netto), at deres organisation har oplevet mindst én form for ekstern IT-sikkerhedstrussel eller -brud i det forløbne år. Og 70 % (netto) oplevede en intern IT-sikkerhedstrussel eller -brud, hyppigst på grund af brugerfejl, brug af personlige enheder i arbejdsøjemed eller medarbejdere, der bruger et hjemmenetværk eller offentligt netværk i arbejdsøjemed.[1]

OFTEST OPLEVEDE EKSTERNE IT-SIKKERHEDSTRUSLER/BRUD



De største trusler sneg sig primært ind igennem stationære og bærbare computere, mens andre kom fra mobilenheder og printere.[1] (De 16 % , som kom fra printere, er markant højere end de 4 %, som blev fundet i en lignende Spiceworks-undersøgelse fra 2014). Det er også muligt, at antallet af angreb igennem printere er undervurderet, da printere ikke bliver overvåget så nøje som computere og mobilenheder.



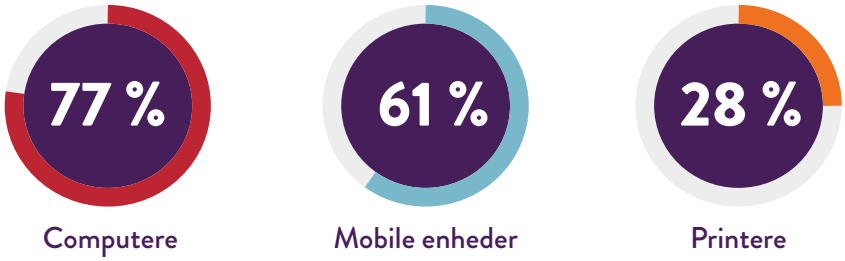
VI IGNORERER VORES PRINTERE

Hvorom alting er, gør Spiceworks-undersøgelsen det klart, at printersikkerhed ofte er en eftertanke.

Organisationerne er fuldstændig klar over vigtigheden af netværks-, slutpunkt- og datasikkerhed. Faktisk bruger mere end tre fjerdedele af respondenterne enten netværkssikkerhed, adgangskontrol/-styring, databeskyttelse eller slutpunktsikkerhed - eller en kombination af disse.[1]

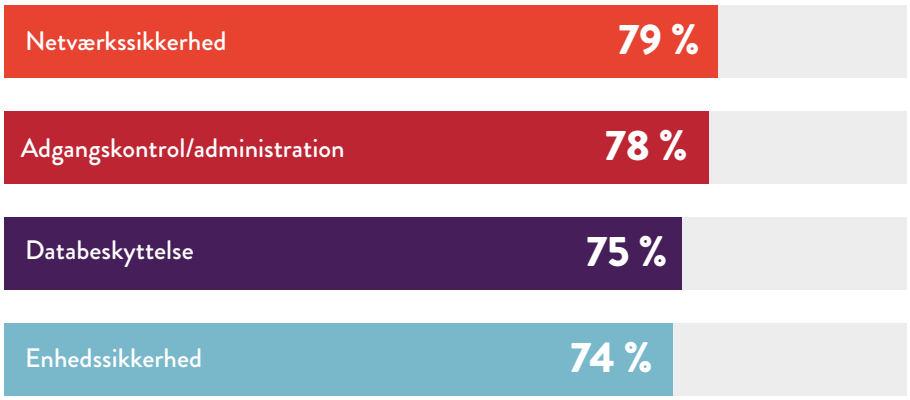
Disse løsninger bliver bare implementeret langt sjældnere på printere. Mens 83 % af de adspurgte bruger netværkssikkerhed på stationære og bærbare computere og 55 % på mobilenheder, bruger kun 41 % det på printere.[1]

Forskellen er endnu større for slutpunktsikkerhed:



Desuden implementerer ikke engang en tredjedel (28 %) af de adspurgte sikkerhedscertifikater til printere, i modsætning til 79 % for computere og 54 % til mobilenheder.[1]

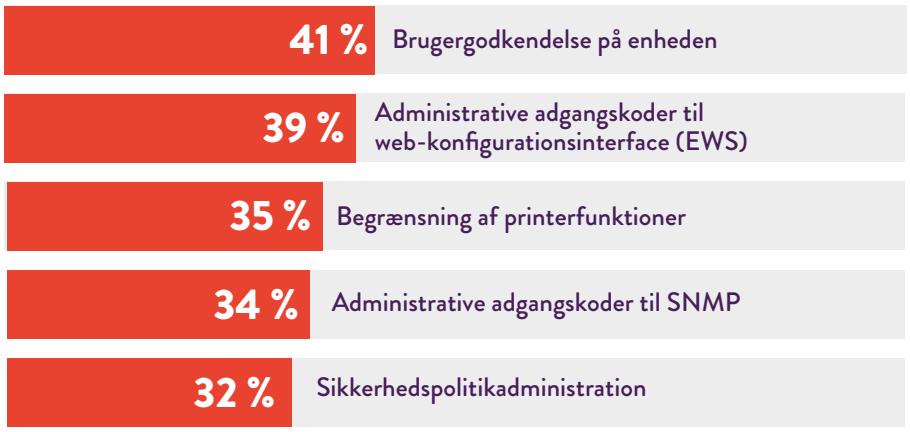
BEDSTE SIKKERHEDSMETODER TIL SLUTPUNKTER



Blandt beskyttelsesmetoder, som anvendes på generelle slutpunktsenheder, var de mest anvendte sikkerhedsforanstaltninger til printere dokumentsikkerhed, netværkssikkerhed og adgangskontrol. Men mindre end halvdelen af de adspurgte sagde, at deres organisationer bruger en eller flere af dem på deres printere.[1]

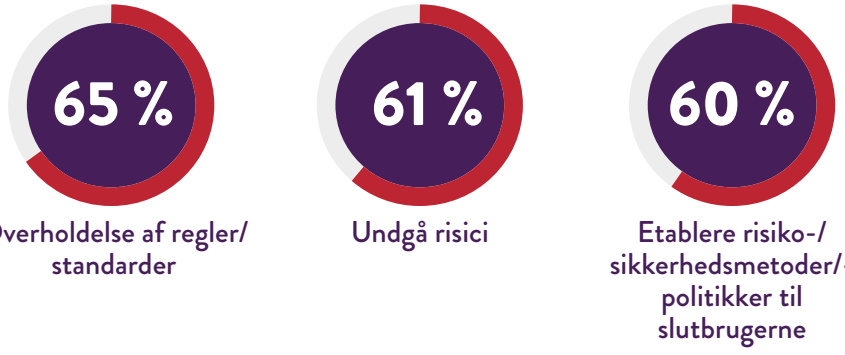
Nogle virksomheder har printerspecifikke sikkerhedsforanstaltninger, men selv der er metoderne meget uensartede. Lidt over 40 % af organisationerne implementerede brugergodkendelse, og mindre end 40 % anvendte administratoradgangskoder til deres webkonfigurationsgrænseflade.[1] For et stærkt forsvar bør alle organisationer benytte en blanding af alle disse tilgange og mere til.

BEDSTE PRINTERSPECIFIKKE SIKKERHEDSMETODER



Når det kommer til slutpunkternes overholdelse af standarder og revisionspraksis, halter printersikkerhedskontrol bagefter næsten alle andre slutpunkter. Næsten 90 % af organisationerne har en informationssikkerhedspolitik, men disse politikker er typisk ikke udvidet til printere. Mens 57 % af de adspurgte sagde, at de har malware-forsvar på deres computere, havde kun 17 % det på deres printere.[1]

NÆSTEN 9 UD AF 10 IT-PROFESSIONELLE OPLYSER, AT DERES ORGANISATION HAR EN INFORMATIONSIKKERHEDSPOLITIK AF FØLGENDE ÅRSAGER:



Det er klart, er organisationerne ikke tager printersikkerhed alvorligt nok - men det burde de gøre.

"Mange printere har stadig standard-adgangskoder eller ingen adgangskoder overhovedet, eller også bruger 10 mennesker den samme adgangskode", udtalte Michael Howard, chefsikkerhedsrådgiver for HP, til Computerworld i juni. "En printer uden adgangskodebeskyttelse er en guldgrube for en hacker. Et af de brud, vi ofte ser, er et mellemmandsangreb, hvor de overtager en printer og videresender [indgående dokumenter] til en bærbar computer, før de udskrives. De kan se alt, hvad den administrerende direktør udskriver."[2]

DE POTENTIELLE VIRKNINGER AF PRINTERHACKING

Ifølge en højtstående analytiker i onlinetrusler hos Bitdefender, Bogdan Botezatu, udgør printere et anseligt potentielt sikkerhedshul. "Vi modtager en masse telemetri i vores laboratorier med vurderinger af sårbarheder. Routeren er ikke længere den værste enhed på internettet. Det er printeren."[3]

Denne sårbarhed kan have dybtgående virkninger på en virksomhed. Med en enkelt usikret printer, kan du efterlade hele dit netværk af tilsluttede enheder sårbare over for angreb, hvilket giver hackere mulighed for at spionere på dine netværksenheder - og kompromittere sikkerheden i hele netværket.

Vi har alle set virkningerne af brud på sikkerheden. I Spiceworks-undersøgelsen sagde de adspurgte, at de fem største konsekvenser ved et brud er:[1]

1. Øget opkalds- og supporttid i helpdesk

2. Reduceret produktivitet/ effektivitet

3. Højere systemnedetid

4. Øget tid i supportopkald

5. Øget håndhævelse af slutbrugerpolitikker

Men et brud på printersikkerhedenkan være endnu mere alvorligt end det, især hvis du bruger en multifunktionsprinter, som kan lagre trykte data elektronisk.

Udskriftsjobs, som bliver gemt i printerens cache, gør det muligt for hackere at få adgang til følsomme personlige eller forretningsmæssige oplysninger.

Endnu mere bekymrende er det, at hackere kan få adgang til bredere virksomhedsnetværk via en usikret printer og stjæle ting som CPR-numre, finansielle oplysninger eller interne notater og dokumenter. Disse stjålne oplysninger kan ikke kun påvirke den enkelte medarbejder, men anvendes af konkurrenten eller forårsage alvorlig skade på en virksomheds omdømme.

DEN NEMME LØSNING: INDBYGGEDE SIKKERHEDS-FUNKTIONER

Det er klart, at virksomheder er nødt til at tage sikkerheden alvorligt, selv med deres printere. Nogle af nutidens moderne virksomhedsprintere har indbygget sikkerhed, der bekæmper printertrusler, og som er nem at bruge. Disse omfatter:

- Automatisk registrering af angreb, beskyttelse og udbedring
- Registrering af brug for at forhindre uautoriseret anvendelse
- Enkle login-muligheder, såsom pinkode eller chipkort
- En kortlæser, der lader brugerne hurtigt godkende og udskrive sikkert på en printer ved hjælp af deres identifikationskort
- Sikker og krypteret udskrivning til følsomme dokumenter.

Når du overvejer din næste printer, uanset om det er en standard- eller multifunktionsprinter, skal du undersøge de integrerede sikkerhedsforanstaltninger - og sørge for at aktivere dem. Med enkle, printerspecifikke funktioner som dem er der ingen grund til at forblive sårbar på grund af dine printere; med tingenes internet er der trods alt masser af andre adgangspunkter at bekymre dig om - **dine printere behøver ikke at være et af dem.**

LEDER DU EFTER FLERE SIKRE PRINTERE?

YDERLIGERE OPLYSNINGER ›

Kilder:

[1] Spiceworks-undersøgelse med 309 It-beslutningstagere i Nordamerika, EMEA og APAC på vegne af HP, november 2016

[2] "Printersikkerhed: Er din virksomheds data virkelig sikre?" Computerworld, 1. juni 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printere er nu det mindst sikre på internettet", The Register, 8. september 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/