HVITEBOK

ULÅSTE DØRER

FORSKNING VISER AT SKRIVERE ER SÅR-BARE FOR ANGREP OVER INTERNETT

Mens IT-team fokuserer på andre endepunkter, sakker sikkerhet for bedriftsskrivere akterut

Skrivere er enkle mål: For mange nettverkstilkoblede skrivere har ingen begrensninger og er ikke sikkert avstengt.

Men trusselen er reell, og bør ikke ignoreres. Skrivere i bedriftsklassen har utviklet seg til kraftig nettverksutstyr med samme sårbarheter som ethvert annet endepunkt i nettverket ditt. Disse typisk usikrede inngangspunktene gir en svært reell mulighet for angrep via Internett; de kan også gi tilgang til selskapets finansielle og private data, og føre til svært reelle forretningskonsekvenser.

En nylig Spiceworks-undersøkelse med mer enn 300 IT-beslutningstakere viser at bare 16 % av respondentene ser på skrivere som en høy risiko for sikkerhetstrusler/sikkerhetsbrudd, betydelig mindre enn stasjonære/bærbare PC-er og mobileenheter.[1] Denne oppfatningen har påvirket hvordan IT-personell tilnærmer seg nettverkssikkerhet. Selv om nesten tre av fem organisasjoner har sikkerhetsrutiner på plass for skrivere, er denne prosentdelen godt under tilsvarende for endepunkter – og gjør skrivere sårbare, når det er enkle løsninger for å verne dette spesifikke inngangspunktet.

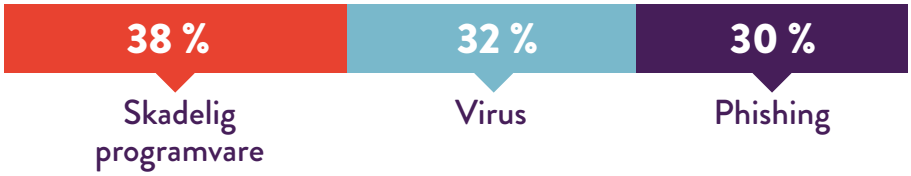
Denne hvitboken presenterer data om skriversikkerhet basert på Spiceworks-undersøkelsen, virkningen av sikkerhetsbrudd og noen av de moderne, innebygde skriversikkerhetsfunksjonene utviklet for å beskytte mot Internett-trusler.

KUN 16 % AV RESPONDENTENE MENER AT SKRIVERE ER I STOR FARE FOR SIKKERHETSTRUSLER/SIKKERHETSBRUDD.[1]

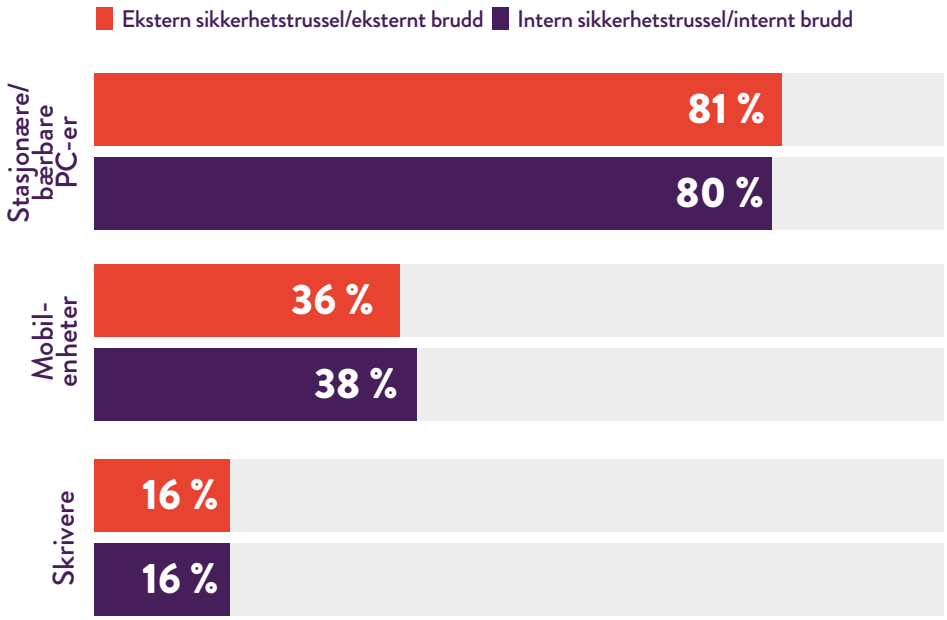
INNGANGSPUNKTER FOR ANGREP

I Spiceworks-undersøkelsen svarte 74 % av respondentene (netto) at organisasjonen deres har opplevd minst én form for ekstern IT-sikkerhetstrussel eller -brudd det siste året. Og 70 % (netto) har opplevd en intern IT-sikkerhetstrussel eller et brudd, oftest som følge av brukerfeil, bruk av personlig utstyr til arbeidsformål eller at ansatte bruker et privat eller offentlig nettverk til arbeidsformål.[1]

VANLIGSTE EKSTERNE IT-SIKKERHETSTRUSLER/-BRUDD OPPLEVD



De største truslene snek seg inn primært gjennom stasjonære og bærbare PC-er, mens andre kom gjennom mobile enheter og skrivere.[1] (16 % inn via skrivere er merkbart høyere enn de 4 % man finner i en lignende Spiceworks-studie fra 2014.) Det er også mulig at antallet angrep som trenger gjennom skrivere, er for lavt, siden skrivere ikke overvåkes like nøye som PC-er og mobilenheter.



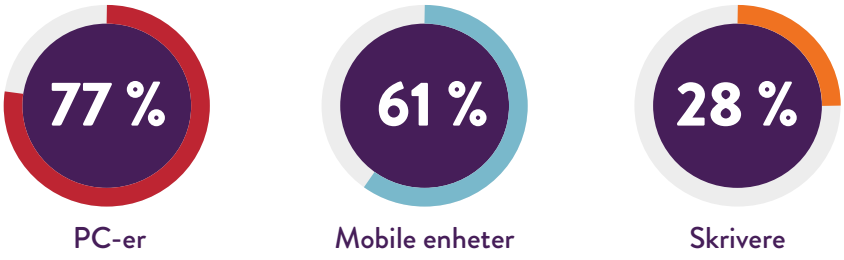
VI IGNORERER SKRIVERNE VÅRE

Uansett årsak gjør Spiceworks-undersøkelsen det klart at skriversikkerhet ofte er en ettertanke.

Organisasjoner er svært oppmerksomme på viktigheten av nettverks-, endepunkts- og datasikkerhet. Faktisk bruker mer enn tre fjerdedeler av respondentene enten nettverkssikkerhet, tilgangskontroll/-styring, databeskyttelse eller endepunktssikkerhet – eller en kombinasjon av disse.[1]

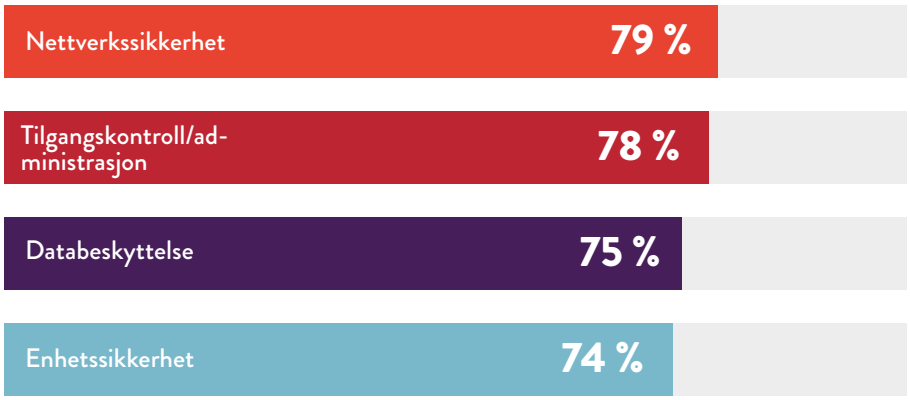
Men disse løsningene distribueres langt sjeldnere på skrivere. Selv om 83 % av respondentene bruker nettverkssikkerhet på stasjonære/bærbare PC-er og 55 % på mobile enheter, bruker kun 41 % det på skrivere.[1]

Avviket er enda større for endepunktssikkerhet:



Og ikke engang en tredjedel (28 %) av respondentene distribuerer sikkerhetssertifikater for skrivere, i motsetning til 79 % for PC-er og 54 % for mobile enheter.[1]

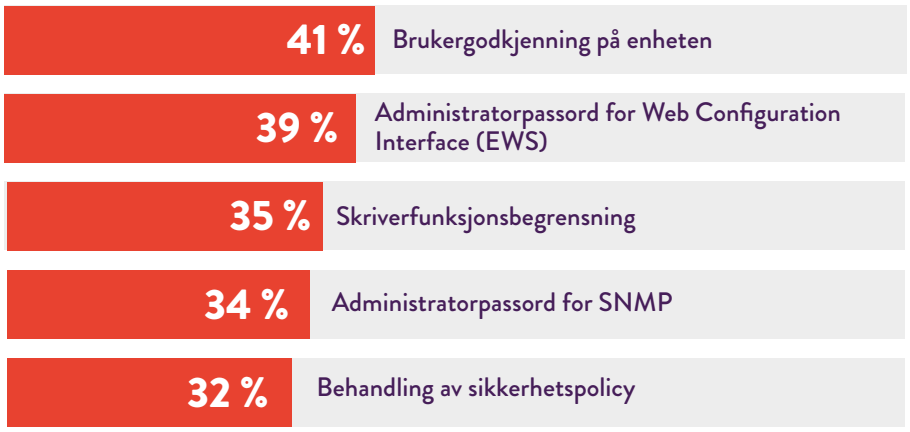
VANLIGSTE SIKKERHETSPRAKSISER FOR ENDEPUNKTER



Blant beskyttelse som brukes på generelle endepunktsenheter, var de mest brukte sikkerhetstiltakene for skrivere dokumentsikkerhet, nettverkssikkerhet og tilgangskontroll, men mindre enn halvparten av respondentene svarte at organisasjonen deres bruker noen av disse på skriverne sine.[1]

Noen selskaper har skriverspesifikke sikkerhetspraksiser, men selv der er praksisene svært forskjellige. Like over 40 % av organisasjonene distribuerte brukergodkjenning, og mindre enn 40 % brukte administratorpassord for nettkonfigurasjonsgrensesnitt.[1] For et sterkt forsvar bør alle organisasjoner bruke en blanding av alle disse tilnærmingene – og mer.

VANLIGSTE SKRIVERSPESIFIKKE SIKKERHETSPRAKSISER



Når det gjelder endepunktssamsvar og revisjonspraksiser, ligger skriversikkerhetskontroller bak nesten alle andre endepunkter. Nesten 90 % av organisasjonene har distribuert en informasjonssikkerhetspolicy, men disse retningslinjene gjelder vanligvis ikke skrivere. For eksempel: mens 57 % av respondentene svarte at de hadde skadeprogramforsvar distribuert på PC-er, hadde kun 17 % av dem distribuert det på skrivere.[1]

NESTEN 9 AV 10 IT-ARBEIDERE OPPGIR AT DERES ORGANISASJON HAR EN INFORMASJONSSIKKERHETSPOLICY PÅ PLASS, AV FØLGENDE ÅRSAKER:

Åpenbart tar ikke organisasjoner skriversikkerhet tilstrekkelig på alvor – men det burde de definitivt gjøre.

«Mange skrivere har fortsatt standard passord, eller ikke noe passord i det hele tatt, eller ti stykker bruker det samme passordet», fortalte Michael Howard, øverste sikkerhetsrådgiver for HP, til Computerworld i juni. «En skriver uten passordbeskyttelse er en gullgruve for hackere. Et av bruddene vi ofte ser, er et mellommann-angrep, der de tar over en skriver og avleder [innkommende dokumenter] til en bærbar PC før de skrives ut. Dermed kan de se alt direktøren skriver ut.»[2]

POTENSIELLE VIRKNINGER AV SKRIVERINNTRENGNINGER

Ifølge senior e-trusselanalytiker hos Bitdefender, Bogdan Botezatu, utgjør skrivere et betydelig potensielt sikkerhetshull. «Vi har mye tele-metri i våre sårbarhetsvurderingslaboratorier. Ruteren er ikke lenger den verste enheten på Internett. Det er nå skriveren.»[3]

Denne sårbarheten kan ha sterk innvirkning på en virksomhet. Med en usikret skriver kan det være at du gjør hele nettverket av tilkoblede enheter sårbart for angrep, gir hackere muligheten til å spionere på nettverksenhetene dine – og setter sikkerheten til hele nettverket i fare.

1. Økte henvendelser om støtte og støttetid

2. Redusert produktivitet/ effektivitet

3. Økt systemnedetid

4. Økt tid på kundestøtteanrop

5. Økt håndhevelse av retningslinjer for sluttbrukere

Vi har alle sett virkningene av sikkerhetsbrudd. I Spiceworks-undersøkelsen svarte respondentene at de fem største innvirkningene fra et brudd er:[1]

Men et skriverbrudd kan være enda mer alvorlig enn det, særlig hvis du bruker en flerfunksjonsskriver som kan lagre data som er skrevet ut,

elektronisk. Utskriftsjobber lagret i skriverens hurtigbuffer, gjør det mulig for hackere å få tilgang til sensitiv person- eller forretningsinformasjon.

Enda mer bekymringsfullt er det at hackere kan få tilgang til det bredere bedriftsnettverket gjennom en usikret skriver, og stjele ting som personnumre,finansiell informasjon eller interne notater og dokumenter. Denne stjålne informasjonen berører ikke kun enkeltpersoner, men kan også brukes av konkurrenter eller føre til alvorlig skade på et selskaps rykte.

DEN ENKLE LØSNINGEN: INNEBYGDE SIKKERHETSFUNKSJONER

Selskaper må åpenbart håndheve sikkerheten, selv med skriverne sine. Enkelte av dagens moderne bedriftsskrivere inneholder brukervennlig innebygd sikkerhet som bekjemper trusler fra Internett. Disse omfatter:

- Automatisk angrepsoppdagelse, beskyttelse og utbedring
- Sporing av bruk for å forhindre uautorisert bruk
- Enkle alternativer for pålogging, f.eks. PIN-koder eller smartkort
- En nærhetskortleser som raskt lar brukere autentisere og skrive ut trygt på en skriver som bruker deres identifikasjonsmerke
- Sikker kryptert utskrift for sensitive dokumenter

Når du vurderer din neste skriver, enten det er en vanlig eller en med flere funksjoner, bør du undersøke integrerte funksjoner for sikkerhetsbeskyttelse – og sørge for å aktivere dem. Med enkle skriverspesifikke funksjoner som disse, er det ingen grunn til å forbli sårbar gjennom skriverne dine; med Internett-verden er det tross alt mange andre tilgangspunkter å bekymre seg for – **skriverne dine behøver ikke å være blant dem.**

UTE ETTER SIKRERE SKRIVERE?

LES MER ›

Kilder:

[1] Spiceworks-undersøkelse blant 309 IT-beslutningstakere i Nord-Amerika, EMEA og APAC, på vegne av HP, november 2016.

[2] «Printer Security: Is your company's data really safe?» *Computerworld*, 1. juni 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] «Printers Now the Least-secure Things on the Internet», *The Register*, 8. september 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/