VITBOK

OLÅSTA DÖRRAR

FORSKNINGEN VISAR ATT SKRIVARE OFTA ÄR SÅRBARA FÖR CYBERATTACKER

Under tiden som IT-avdelningarna fokuserar på säker heten för andra slutpunkter, hamnar skrivarna på efterkälken

Skrivarna är enkla måltavlor: Alltför många nätverksanslutna skrivare saknar restriktioner och är inte låsta på ett säkert sätt.

Hoten är verkliga och bör inte ignoreras. Företagsklassade skrivare har utvecklats till kraftfulla nätverksenheter med samma sårbarhet som alla andra slutpunkter i nätverket. Dessa vanligtvis icke-prioriterade ingångspunkter öppnar dörren för cyberattacker. De kan även ge obehörig åtkomst till företagets ekonomiska och privata data, som kan leda till allvarliga konsekvenser för företaget.

Trots detta visar en ny Spiceworks-undersökning, som inkluderar IT-beslutsfattare från fler än 300 företag, att endast 16 % av de tillfrågade anser att skrivare löper hög risk för säkerhetshot och säkerhetsöverträdelser. Ett betydligt lägre antal än för stationära/bärbara datorer och mobila enheter.[1] Denna uppfattning har påverkat hur IT-personalen ser på nätverkssäkerhet. Medan nästan tre av fem organisationer har säkerhetsrutiner på plats för sina skrivare, är denna andel avsevärt lägre än för andra slutpunkter. Detta gör skrivarna sårbara, trots att det finns enkla lösningar för att skydda denna ingångspunkt.

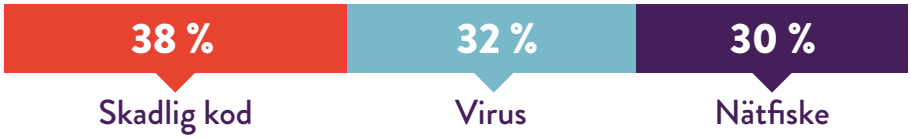
I det här informationsdokumentet presenteras skrivarsäkerhetsdata som bygger på Spiceworks-undersökningen, effekterna av säkerhetsöverträdelser och en del av de moderna inbyggda skrivarsäkerhetsfunktioner som utformats för att skydda mot cyberattacker.

ENDAST 16 % AV DE TILLFRÅGADE TROR ATT SKRIVARE LÖPER HÖG RISK FÖR SÄKERHETSHOT OCH SÄKERHETSÖVERTRÄDELSER.[1]

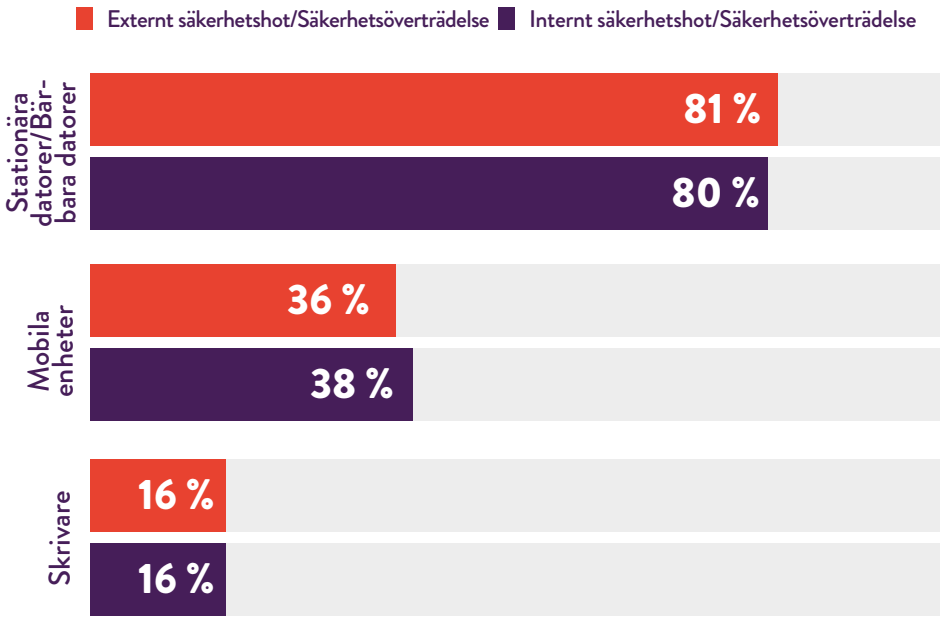
MÖJLIGHETER FÖR ATTACKER

I Spiceworks-undersökningen sade 74 % av de tillfrågade (netto) att deras organisation upplevt åtminstone någon typ av externa IT-säkerhetshot eller säkerhetsöverträdelser under det senaste året. 70 % (netto) hade upplevt interna IT-säkerhetshot eller säkerhetsöverträdelser, oftast p.g.a. felanvändning, användning av personliga enheter för arbetsändamål eller anställda som använt ett hemnätverk eller offentligt nätverk för sitt arbete.[1]

DE VANLIGASTE EXTERNA IT-SÄKERHETSHOTEN/SÄKERHETSÖVERTRÄDELSERNA



De vanligaste angreppen skedde huvudsakligen mot de stationära och bärbara datorerna, medan andra tog sig in via mobila enheter och skrivare.[1] (De 16 % som tog sig in via skrivare är ett betydligt högre antal än 4 %, vilket rapporterades i en liknande Spiceworks-undersökning från 2014. Antalet attacker som inträffar i skrivare kan vara ännu högre, eftersom skrivare inte övervakas lika noga som datorer och mobila enheter.



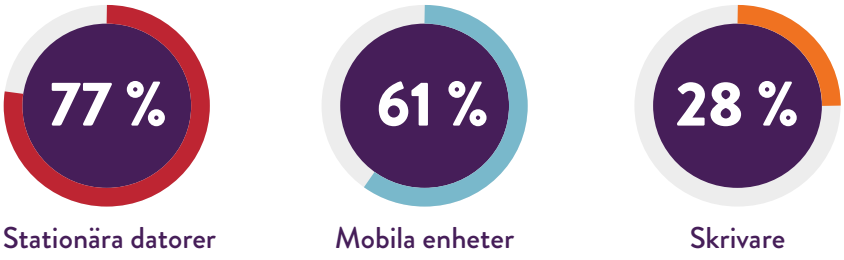
SKRIVARNA IGNORERAS

Hur som helst så tydliggör Spiceworks undersökning att skrivarsäkerheten ofta tas på allvar först när skadan redan skett.

Organisationerna är väl medvetna om vikten av nätverk, slutpunkter och datasäkerhet. Faktum är att mer än tre fjärdedelar av de tillfrågade använder antingen nätverkssäkerhet, åtkomstkontroll/-hantering, dataskydd eller slutpunktssäkerhet – eller en kombination av dessa.[3]

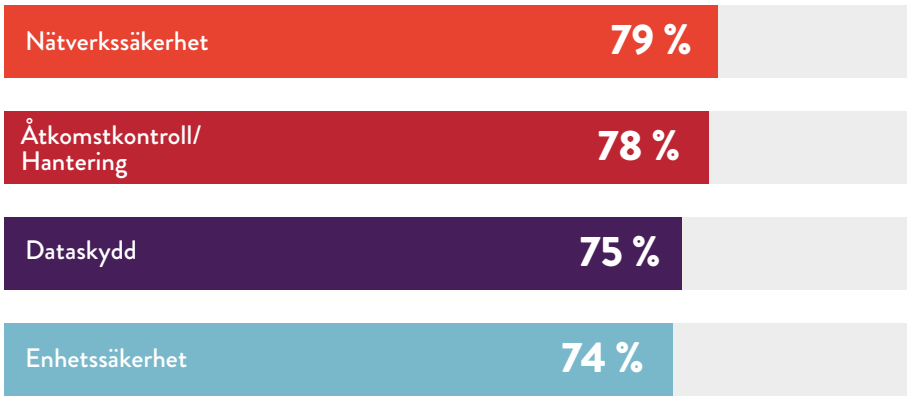
Men dessa lösningar implementeras sällan på skrivarna. 83 % av de tillfrågade använder nätverkssäkerhet för stationära/bärbara datorer och 55 % på mobila enheter, men endast 41 % tillämpar detta för skrivarna.[1]

Skillnaden är ännu större för slutpunktssäkerhet:



Dessutom distribuerar inte ens en tredjedel (28 %) av de tillfrågade säkerhetscertifikat för sina skrivare, jämfört med 79 % för stationära datorer och 54 % för mobila enheter.[1]

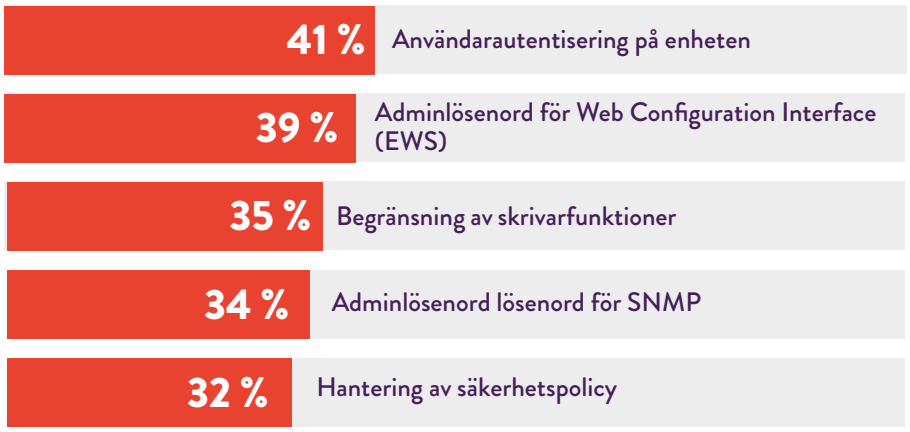
VANLIGA SÄKERHETSRUTINER FÖR SLUTPUNKTER



Bland de skydd som används för allmänna slutpunktsenheter var de mest använda säkerhetsåtgärderna för skrivare dokumentsäkerhet, nätverkssäkerhet och åtkomstkontroll, men mindre än hälften av de tillfrågade sade att deras organisationer använder någon av dem på sina skrivare.[1]

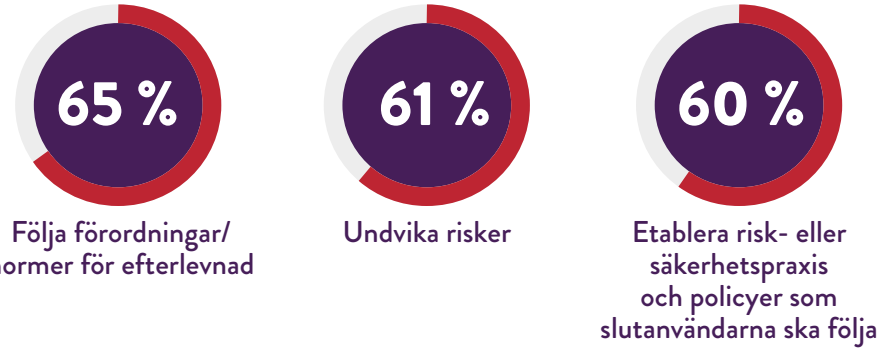
Vissa företag har skrivarspecifika säkerhetsrutiner, men även där skiljer sig praxis mycket åt. Drygt 40 % av organisationerna tillämpar användarautentisering och mindre än 40 % använder administratörslösenord för webbkonfigurationsgränssnitt.[1] Alla organisationer bör använda en kombination av dessa metoder, och även andra, för att få ett ordentligt skydd.

VANLIGA SKRIVARSPECIFIKA SÄKERHETSRUTINER



När det gäller slutpunktsefterlevnad och revisionsmetoder, hamnar kontrollen av skrivarsäkerheten på efterkälken. Nästan 90 % av organisationerna tillämpar en implementerad informationssäkerhetspolicy, men denna policy omfattar sällan skrivarna. 57 % av de tillfrågade berättade att de använde skydd mot skadlig kod på sina datorer, medan endast 17 % använde ett liknande i sina skrivare.[1]

NÄSTAN 9 AV 10 IT-PROFFS SÄGER ATT DERAS ORGANISATION HAR EN INFORMATIONSSÄKERHETSPOLICY PÅ PLATS AV FÖLJANDE ANLEDNINGAR:



Det är tydligt att organisationerna inte tar skrivarsäkerheten på allvar, men de borde verkligen göra det.

”I många skrivare används fortfarande standardlösenord, elleringaalls. Eller så använder tio personer samma lösenord”, berättade Michael Howard, chefssäkerhetsrådgivare för Computerworld i juni. ”En skrivare utan lösenordsskydd är en guldgruva för en hacker. En vanlig överträdelse är en s.k. man-i-mitten-attack, där de tar över en skrivare och avleder [inkommande dokument] till en bärbar dator innan de skrivs ut. De får åtkomst till allt som VD:n skriver ut.”[2]

DEN POTENTIELLA EFFEKTEN AV SKRIVARINTRÅNG

Enligt en högt uppsatt e-hotsanalytiker på Bitdefender, Bogdan Botezatu utgör skrivare en potentiellt allvarlig säkerhetslucka. ”Vi får in mycket telemetridata på våra sårbarhetsanalyslaboratorier. Routern är inte längre den mest sårbara enheten på webben. Det är skrivaren.”[3]

Denna sårbarhet kan få långtgående effekter för ett företag. Med en enda oskyddad skrivare, kan hela nätverk av anslutna enheter bli sårbart för attacker, vilket ger hackare möjlighet att spionera på dina nätverksanslutna enheter och äventyra säkerheten i hela nätverket.

Vi har alla sett följderna av säkerhetsöverträdelser. Enligt Spiceworks-undersökningen är de fem vanligaste följderna av en säkerhetsöverträdelse:[1]

1. Ökat antal samtal till helpdesk och mer support

2. Minskad produktivitet och effektivitet

3. Fler driftsavbrott

4. Ökad tidsåtgång för supportsamtal

5. Ökad förstärkning av policyer för slutanvändare

Säkerhetsöverträdelser på skrivare kan vara allvarligare än så, särskilt om du använder en multifunktionsskrivare som lagrar tryckta data elektroniskt.

Utskriftsjobb som lagras i skrivarens cacheminne gör det möjligt för hackare att få tillgång till känslig personlig information eller företagsinformation.

Ännu mer oroväckande är att hackare kan komma åt bredare företagsnätverk via oskyddade skrivare och stjäla personnummer, finansiell information eller interna PM och dokument. Stölden påverkar inte bara enskilda anställda, utan kan även utnyttjas av konkurrenter eller skada företagets rykte allvarligt.

DEN ENKLA LÖSNINGEN: INBYGGDA SÄKERHETSFUNKTIONER

Det är uppenbart att företagen måste ta itu med säkerheten även för deras skrivare. Vissa av dagens moderna företagsklassade skrivare har lättanvänd, inbyggd säkerhet som skyddar mot skrivarangrepp. De innefattar:

- Automatisk upptäckt av attacker, skydd och reparation
- Spårning för att förhindra obehörig användning
- Enkla inloggningsalternativ såsom PIN-kod eller smartkort
- Kontaktlös kortläsare där du snabbt och säkert kan verifiera och skriva ut med din identifieringsbricka
- Säkra, krypterade utskrifter för känsliga dokument

När du köper din nästa skrivare, vare sig det är en stationär skrivare eller multifunktionsskrivare, bör du kontrollera de integrerade säkerhetsåtgärderna och se till att aktivera dem. När det finns enkla skrivarspecifika funktioner finns det ingen anledning att utsätta sig för onödiga skrivarangrepp. Det finns tillräckligt med andra sårbara åtkomstpunkter på webben, **se till att skrivaren inte är en av dem.**

LETAR DU EFTER SÄKRARE SKRIVARE?

LÄS MER ›

Källor:

[1] Spiceworks-undersökning som besvarades av 309 IT-proffs i Nordamerika, EMEA och APAC för 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/