IDC MARKET SPOTLIGHT

Den blinda fläcken för GDPR: Varför skrivare är en svaghet när det kommer till efterlevnad

juli 2017

Av Duncan Brown

Sponsrad av HP Inc.

IDC Market Spotlight lyfter fram sårbarheten hos skrivare i storföretagsnätverk och framför allt hur denna sårbarhet påverkar ett efterlevnadsprogram som är inriktat på Allmänna dataskyddsförordningen (General Data Protection Regulation, GDPR) och annan framtida lagstiftning. I artikeln finns även åtgärder för att minska risken med osäkra skrivare i verksamheten.

Inledning

Uppmärksamheten som ägnades åt säkerheten för Sakernas internet (IoT) ökade betydligt efter ett antal högprofilerade denial-of-service-attacker (DDoS) som fokuserade en stor mängd skadlig trafik från tusentals kompromitterande övervakningskameror, digitala videobandspelare och andra anslutna enheter för att sänka populära webbplatser. Vilken enhet är nästa mål?

När vi letar efter andra IoT-enheter som delar några egenskaper hos de enheter som används i i de senaste attackerna, riktas vår uppmärksamhet mot konsument-, småföretags- och storföretagsskrivare. Programvaruuppdateringar och åtkomstkontroll, som båda är prioriterade för traditionella IT-produkter, är ofta förbisedda för skrivare. Skrivare kan vara nästa vektor för en stor IoT-attack men kan också innebära
nya faror för affärsverksamheten eftersom de är placerade inuti företagsnätverket, vilket innebär risk för datastöld och DDoS på den interna delen av ett nätverk. Effekterna på affärer som intrång i personliga data innebär förvärras genom GDPR och andra nya regler, vilket innebär att nätverksskrivaren är den bortglömda slutpunkt som måste ses över snarast.

Er skrivare är en slutpunkt

Föreställ dig följande scenario: En okänd enhet placeras i ett storföretagsnätverk, bakom omgivande försvar som brandväggar, intrångsförebyggande system och annan IT-infrastruktur, så att enheten får otillbörlig tillgång till alla resurser i företagsnätverket. En webbserver är inbäddad i enheten för att maximera enhetens funktionalitet. Alla portar kommer att vara öppna som standard och aktiverar en anslutning med så mycket som en gigabit av Ethernet-anslutning för att göra enheten tillgänglig. Enheten kommer att ha ett avancerat OS, som Linux, för att maximera funktionaliteten. Den kommer inte att undersökas löpande av företagets sårbarhetsskanner eftersom den inbäddade webbservern troligtvis kommer att flaggas i företagets säkerhetsinformation och händelsehanteringsverktyg (SIEM) med falska positiva identifieringar. Sårbarhetsskannern konfigureras för att ignorera enheten, vilket leder till slutsatsen att enheten, beroende på varumärke, inte kommer att uppdateras, upprätthållas eller korrigeras under dess livslängd på 5–10 år. Enhetsskyddet kommer att bestå av ett standardlösenord och okontrollerade tredje parter kommer att upprätthålla enheten. Enheten kommer att vara kärnan i organisatorisk produktivitet, så det kommer att finnas en av dessa enheter för var tionde anställd. Dessa anställda kommer inte endast att använda enheten, utan kommer även att aktivt skicka känsliga personuppgifter till den, som sedan lagras. Ännu värre är att dessa data kan skickas till en utomstående person, utan autentisering eller åtkomstkontroll.

Vissa kanske kallar detta en mardröm; andra kallar det en skrivare.

En mycket viktig punkt måste klargöras. ”Skrivarsäkerhet” är en mogen säkerhetsdisciplin som för det mesta drivs av behovet för datasäkerhet. Som man kan anta så spelar efterlevnadsstandarder en stor roll i utvecklandet av skrivarsäkerhet. I EMEA innebär detta GDPR, men omfattar även säkerhetsdirektivet för nätverks- och informationssystem (NIS), samt uppdateringen av e-säkerhetsdirektivet och det reviderade betaltjänstdirektivet (PSD2). Dessa standarder utgör grunden för *säkerhetsresultat*, utan att specifikt ange de tekniska detaljerna för efterlevnad.

Grunderna i GDPR

GDPR är en välkommen och efterlängtad uppdatering av Europas dataskyddslagar. Den ersätter nuvarande lagstiftningen som är daterad från 1995, innan dot-com-boomen, Twitter, Facebook och molnet. GDPR uppdaterar lagen så att den innefattar dessa och framtida tekniker som skapar och använder personuppgifter.
En ytterligare fördel med GDPR är att den gäller för alla medlemsländer i Europeiska unionen (EU).

GDPR blev lag i april 2016 och träder i kraft den 25 maj 2018. Organisationer har mindre än ett år för att säkerställa efterlevnad, och påföljderna för bristande efterlevnad kan uppgå till 4 % av de globala årliga intäkterna eller 20 miljoner euro, beroende på vilket som är störst. GDPR inför även en obligatorisk anmälan om överträdelse, vars konsekvenser gäller styrelser som är oroade för ansvarsskador.

Observera att Storbritanniens framtida utträde ur EU (dvs. Brexit) inte väsentligt påverkar GDPR i stort.

- Företag i Storbritannien som behandlar EU-personuppgifter måste ändå följa GDPR, eftersom GDPR gäller utanför EU:s territorium för de personliga uppgifterna för personer inom EU.
- Storbritannien kommer troligtvis att genomföra lokala lagar som GDPR för att underlätta dataöverföringar från EU, som regleras genom lagar om ”tillräcklighet”.

GDPR är mer än en säkerhetsfråga. Förordningen innehåller en rad nya åtgärder, inklusive dataöverföring, samtycke och återkallande, åldersverifiering och rätten att bli bortglömd. En stor del av uppnåendet av efterlevnad handlar dock om god säkerhet. Vad säger GDPR om detta specifikt?

GDPR är anmärkningsvärt icke-föreskrivande när det gäller att definiera säkerhetsåtgärder. Av dess 99 artiklar är det endast artikel 32 som specifikt tar upp säkerhet. Kravet är att organisationer vidtar ”lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.” Med andra ord så är det upp till varje företag att bedöma risken som är kopplad till dess personuppgifter och genomföra de säkerhetsåtgärder som det anser vara nödvändiga.

En del i detta övervägande är vad GDPR kallar ”den senaste utvecklingen”. Företag är inte skyldiga att införa den nyaste tekniken. Men de måste vara medvetna om vad detta innebär och försvara sin position. En situation som företag måste undvika är att försöka motivera varför de *inte* införde en särskild säkerhetskontroll eller -teknik, vilket senare ledde direkt till ett dataintrång.

En av nyckeltesterna som sannolikt kommer att tillämpas av GDPR-regulatorer är vad IDC kallar ”Hur mycket försökte ni”-testet. Att inte känna till en sårbarhet är dåligt. Att känna till en sårbarhet och inte göra något åt den – det är värre. Att bortse från en säkerhetsrisk på en skrivarutrustning kan leda till dataintrång som berör personuppgifter. Om intrånget är tillräckligt allvarligt kan ditt företags organisatoriska och tekniska åtgärder för att skydda uppgifterna komma att ifrågasättas av reglerande myndighet.

Det är viktigt att GDPR:s materiella tillämpningsområde är ”behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.” Med andra ord, data måste inte vara i elektronisk form för att omfattas. Fysiska kopior av uppgifterna måste också förvaras säkert.

Säkerhetsdirektivet för nätverks- och informationssystem

EU förstår att, i en tid med allt fler cyberattacker, måste viktiga tjänster skyddas, framför allt de som är viktiga för att ekonomin eller samhället ska fungera. För att uppnå konsekvens i alla medlemsstater avseende skydd mot cyberattacker så har EU infört NIS-direktivet.

NIS innehåller överraskande lite information om säkerhetskrav. Det finns ett brett fokus på att skydda infrastrukturen, inklusive fysiska tillgångar och det finns en primär betoning på motståndskraft (incidenthantering, kontinuitetskontroll, etc.). Det inkluderar en obligatorisk anmälningsklausul för överträdelse (se artikel 16), men det finns inga föreskrivna böter för bristande efterlevnad.

Eftersom NIS är ett direktiv så måste det införlivas i lag av en medlemsstat och ratificeras av dess lagstiftare. NIS trädde i kraft i augusti 2016. Medlemsstaterna har till den 10 maj 2018 på sig att införliva direktivet i sina nationella lagar och ytterligare sex månader för att identifiera operatörer av väsentliga tjänster.

Fördelarna med skrivarsäkerhet

Skrivarsäkerhet, till skillnad från utskriftssäkerhet, är enbart inriktat på fysiska enheter som är förknippade med utskrifter och är en nätverkssäkerhetsdisciplin. I skrivarsäkerhet ses skrivaren som en slutpunkt och behandlas med samma omsorg som alla andra slutpunkter, som bärbara datorer, servrar och mobila enheter. Även om de har ett gemensamt språk och delar några relaterade problemområden så är utskriftssäkerhet och skrivarsäkerhet olika och unika discipliner.

Hur sårbara är nätverksskrivare?

Skrivare är mottagare av stora datamängder, varav några kommer att vara personuppgifter. Få användare, personal med ansvar för efterlevnad eller IT-administratörer överväger säkerheten hos sådana data när de skickas till, och lagras på, skrivare. Artikel 5.f i GDPR är krav på ”lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.” Men få organisationer tar hänsyn till datasäkerheten hos en skrivare.

Vidare så är det vanligt att se bortglömda utskrivna dokument i skrivarens pappersfack. Med hänsyn till GDPR kan lösningar för utskriftsbegäran bidra till att skydda oavsiktlig förlust av personuppgifter, särskilt inom organisationer vars behandling av personuppgifter innebär att uppgifterna skrivs ut

Skrivare är en lockande måltavla för cyberbrottslingar, delvis eftersom de inte anses vara en del av IT och därmed inte uppmärksammas särskilt mycket av säkerhetspersonal. Skrivarhantering anses ofta vara en del av anläggningsfunktionen. När skrivare blev nätverksanslutna enheter betraktades de i stor utsträckning som en ”låg risk”, så länge som enheterna fanns bakom företagets brandvägg. Sårbarheten för skrivarslutpunkterna identifierades i väldigt liten utsträckning.

Kombinationsskrivare/skannrar/faxmaskiner blir dessutom alltmer sofistikerade och de har inbyggda datorer installerade för att kontrollera alla åtgärder. Windows- och Linux-system är ofta inbyggda i många moderna skrivare. Eftersom dessa datorkontroller får lite uppmärksamhet i fråga om uppdateringar så är de ofta sårbara. Dessutom kräver funktionalitet anslutning, vilket resulterar i att många skrivare skickas med en mängd öppna portar för att stödja användbarheten.

Bristande uppmärksamhet i kombination med kraftfull datorkraft och en mängd olika anslutningsmöjligheter innebär att angripare kan komma åt skrivare på flera sätt, såsom genom ett modem, en trådlös åtkomstpunkt eller stationära datorer smittade med spionprogram. Efter att ha fått åtkomst till systemet kan angripare använda denna kraft för att slå till på andra maskiner i det interna nätverket eller delta i en distribuerad DDoS-attack. De flesta skrivare har obegränsad åtkomst till ett internt nätverk. En angripare som komprometterar en skrivare kan skanna hela nätverket efter exploaterbara system.

Som med andra slutpunktsenheter som kräver skydd så är skrivare inte bara en väg in utan också ett mål för cyberbrottslingar. Skrivare lagrar ofta känsliga dokument i sin utskriftshanterare. De kombineras också ofta med en dokumentskanner och dokument är ofta lagrade i skanningsarkivet längre än de flesta tror.

Överväganden

Om skrivarsäkerhet inte har varit ett fokus för er organisation så har IDC några rekommendationer för var ni ska börja.

Allt börjar med synlighet

Som med alla slutpunkter som kräver säkerhet så ska man börja med grunderna: Steg ett är ständig synlighet. Skapa en fullständig inventering av alla skrivare, inklusive varumärke, modell, funktioner och konfigurationer. Att skapa en sådan lista kan vara problematiskt eftersom enskilda initiativ ofta placerar skrivare på oidentifierade platser (skugg-IT) Labb, chefskontor eller fältkontor har ofta en skrivare i nätverket av bekvämlighetsskäl, eller har den ansluten direkt till en dator, oavsett vilka säkerhetsimplikationer det innebär.

Det är önskvärt att en slutpunktsinventering som innehåller skrivare baseras på ett NAC-verktyg eller tillgångshanteringsverktyg, som har enhetsupptäckt som kärnfunktionalitet. Att uppnå en heltäckande synlighet för skrivare är extremt svårt utan en NAC. Vissa skrivarmodeller kan dock tillhandahålla automatisk upptäckt när de är anslutna till nätverket. Om ert nätverk inte har en homogen installationsbas av sådana skrivare är NAC lösningen.

Skydda era skrivarslutpunkter

Skrivare inom organisationen måste hanteras precis som andra anslutna slutpunkter. Stäng av alla onödiga tjänster som skrivaren erbjuder, såsom FTP. De flesta organisationer behöver inte FTP-åtkomst till sina skrivare och det kan ofta orsaka mer skada än vara till nytta. Vissa skrivare gör till exempel att en angripare kan göra FTP-förfrågningar och ta bort jobb från en utskriftshanterare anonymt. Många FTP-tjänster på moderna skrivare är dessutom föremål för FTP-studsattacker. Med ett verktyg som Nmap (Network Mapper) kan en angripare dölja källan till en portsökning och övertyga en kompatibel FTP-server att tillåta
proxy FTP-anslutningar. Sådana FTP-studsskanningar har funnits med länge, men ett förvånansvärt stort antal nya skrivarservrar är mottagliga för sådana attacker.

Men den enskilt viktigaste åtgärden när det gäller att skydda era skrivarslutpunkter är lösenordshantering.
Det mest allvarliga misstag som görs av organisationer är att inte ändra standardlösenorden. Enligt Verizons *2016 Data Breach Investigations Report* inbegrep 63 % av de bekräftade dataintrången att man utnyttjade svaga, standardmässiga eller stulna lösenord. Om skrivarna hanteras av tredjepartsanläggningar eller -leverantörer så är bekvämlighet det som är viktigast (för dem). När en enhet behöver upprätthållas kan det vara ett problem att hitta ett lösenord. När det finns en skrivare för var tionde anställd kan en organisation med 10 000 anställda ha 1 000 lösenord som måste upprätthållas. Bekvämligheten prioriteras därmed framför säkerheten. Lösenordshantering är inte

bara ett problem som beror på den icke-tekniska personalen. Det näst vanligaste misstaget är att ha användarnamnet och lösenordet fritt tillgängligt i okrypterad text, tillgänglig för alla med en http://-anslutning.

Upprätthåll och uppdatera

De flesta intrång uppstår på grund av brist på uppdatering. Enligt Verizons *2016 Data Breach Investigations Report* utgjorde de 10 oftast utnyttjade sårbarheterna under 2015 85 % av lyckade säkerhetsintrång. De mest utnyttjade sårbarheterna är kända och offentliggjorda. Cyberbrottslingar kommer att använda det som fungerar och maximera investeringen som de har gjort i sina verktyg för skadlig programvara.

Om man upprätthåller och uppdaterar skrivarslutpunkter blir man en svårare måltavla, och gör att cyberbrottslingarna kommer att använda sina verktyg på organisationer som inte upprätthåller sina system.

När det gäller uppdateringar är inte alla skrivare likvärdiga. Vissa tillverkare erbjuder hanteringsverktyg som gör att man kan övervaka, hantera och uppdatera vissa skrivarmodeller. Sådana verktyg är extremt värdefulla eftersom ett storföretags sårbarhetsskanner förmodligen kommer att ha problem med skrivare på grund av den inbäddade webbservern. Om ni råkar ha sådana skrivare med robusta hanteringsverktyg så har ni tur. Om inte kan ni vara tvungna att uppdatera varje skrivare manuellt eftersom det kan vara svårt att skapa en automatiserad lösning.

För att förhindra att ”brus” importeras till SIEM-verktygen konfigurerar organisationer ofta sårbarhetskanners så att de ignorerar skrivare. Det här problemet beror lika mycket på SIEM- och sårbarhetshanteringsverktyg som på skrivare. Det kan vara komplicerat att konfigurera sådana verktyg så att de endast accepterar vissa meddelanden från skrivare, men på kort sikt kan den här åtgärden hjälpa till att skydda nätverket från virusinfektioner som är knutna till skrivare.

Skydda anslutningen

Stärk hanteringsprotokollen som används för skrivaren. De flesta moderna skrivare stöder någon typ av hantering via HTTP och/eller HTTPS och vissa stöder även Telnet eller Secure Shell (SSH). Välj omsorgsfullt ett hanteringsprotokoll som tillhandahåller kryptering, såsom HTTPS eller SSH, och inaktivera svaga eller brutna koder som SSLv3.

Slutligen ska ni se till att era skrivare inte har öppen åtkomst till resten av ert interna nätverk. Att segmentera storföretagsnätverk är bästa praxis för nätverkssäkerhet och skrivare måste ingå i åtgärden. Certifikat kan användas för att logiskt segmentera åtkomst till nätverksresurser och att kryptera trafik. Var dock medvetna om att dessa ytterligare säkerhetsåtgärder kan försämra skrivarens funktionalitet, så som begränsning av åtkomst till katalogtjänster (t.ex. Active Directory) och molnbaserad hantering och övervakning. Att få balans mellan säkra skrivare och bevarandet av affärsfunktionen är alltid en fråga om omdöme och bedömning av affärsrisk.

Sammanfattning

Skrivare har inte fått den uppmärksamhet som ges till andra delar av säkerheten på Internet. Sårbarheten och de motsvarande hoten är mycket verkliga. Organisationer av alla storlekar måste vidta åtgärder för att ta itu med problemet och ta itu med det snabbt. Cyberbrottslingar är effektiva efterapare. När en hotvektor har utnyttjats för vinst av en illasinnad aktör kommer andra att följa.

De finansiella konsekvenserna och konsekvenserna för ryktet av att ignorera skrivarsäkerheten kommer att eskalera ända upp till styrelsenivå i och med GDPR. Det vore olyckligt att se en

organisation som i alla andra fall uppfyller kraven, som arbetat hårt med sina processer och tekniker för informationssäkerhet, bli lidande på grund av oskyddade skrivare.
