IDC
Analyze the Future

I D C - M A R K E D S S P O T L I G H T

Den blinde vinkel ved GDPR: Derfor repræsenterer printere svagheder i compliance

Juli 2017

Af Duncan Brown

Sponsoreret af HP

Dette IDC-markedsspotlight fremhæver sårbarheden ved printere i virksomhedsnetværk, og især hvordan denne sårbarhed påvirker et complianceprogram, der er fokuseret på GDPR (General Data Protection Regulation) og anden kommende lovgivning. Artiklen indeholder også foranstaltninger til at reducere den risiko, som usikrede printere udgør for forretningen.

Indledning

Opmærksomheden på IoT-sikkerheden (Internet-of-Things) steg betydeligt efter en række højt profilerede DDoS-angreb (Distributed Denial-of-Service), der samlede et enormt omfang af ondsindet trafik fra tusindvis af kompromitterede overvågningskameraer, digitale videooptagere og andre tilsluttede enheder med henblik på at lukke populære websteder ned. Hvilken enhed bliver det næste mål?

Når vi leder efter andre IoT-enheder, der deler nogle af de egenskaber, som de enheder, der blev anvendt i de seneste angreb, bliver vores opmærksomhed rettet mod printere til almindelige forbrugere, små virksomheder og større virksomheder. Softwareopdateringer og adgangskontrol, som er højt prioriteret på traditionelle it-produkter, overses ofte på printere. Printere kan blive det næste mål for et stort IoT-angreb, men de kan også udgøre
nye farer for erhvervslivet, fordi de befinder sig i virksomhedens netværk, hvilket skaber et potentiale for datatyveri og DDoS på den indre del af et netværk. Med de mere alvorlige forretningsmæssige konsekvenser af brud på persondatasikkerheden, der følger med GDPR og andre kommende regler, er netværksprinteren det glemte slutpunkt, der kræver opmærksomhed med det samme.

Din printer er et slutpunkt

Overvej følgende scenarie: En ukendt enhed placeres i et virksomhedsnetværk bag forsvarsværker som firewalls, systemer til forebyggelse af cyberangreb og anden it-infrastruktur, så enheden har uhindret adgang til alle virksomhedens netværksressourcer. En webserver er integreret i enheden for at maksimere enhedens funktionalitet. Alle portene vil som standard blive indstillet som "åbne" og muliggøre forbindelse med en Ethernet-tilslutning på op til en gigabit for at gøre enheden tilgængelig. Enheden vil have et omfattende operativsystem som Linux for at maksimere funktionaliteten. Den vil ikke blive undersøgt løbende ved hjælp af virksomhedens sårbarhedsscanner, da den integrerede webserver sandsynligvis vil give organisationens SIEM-værktøjer (Security Information and Event Management) falske positiver. Sårbarhedsscanneren vil blive konfigureret til at ignorere enheden, hvilket fører til den konklusion, afhængigt af mærket, at enheden ikke skal opdateres, vedligeholdes eller sikres i løbet af dens 5 til 10 års brugstid. Enhedsbeskyttelse består af en standardadgangskode, og tredjeparter vedligeholder enheden. Enheden vil være kernen i den organisatoriske produktivitet, så der vil være en af disse enheder for hver 10 medarbejdere. Disse medarbejdere vil ikke kun bruge denne enhed, men vil også aktivt sende følsomme

personoplysninger til den, hvor de bliver gemt. Hvad værre er, så kan dataene ses af en hvilken som helst person, som står ved siden af enheden, uden godkendelse eller adgangskontrol.

Nogen vil måske kalde det et mareridt; andre kalder det en printer.

En meget vigtig pointe skal præciseres. "Udskrivningssikkerhed" er en moden sikkerhedsdisciplin, der hovedsageligt drives af behovet for datasikkerhed. Som man måske kan regne ud, spiller compliance-standarderne en stor rolle i forhold til opretholdelse af udskrivningssikkerheden. I EMEA betyder dette GDPR (eller Persondataforordningen), men det drejer sig også om NIS (Network and Information Systems Security Directive) samt ePrivacy Directive og PSD2 (Revised Payment Services Directive). Disse standarder udgør grundlaget for sikkerhedsresultaterne uden at specificere de tekniske detaljer for compliance.

Vigtigheden af GDPR

GDPR er en velkommen og længe ventet opdatering af Europas databeskyttelseslovgivning. Den erstatter gældende lovgivning, der stammer fra 1995, dvs. før dot-com-boomet, Twitter, Facebook og skyen. GDPR opdaterer loven for at tage højde for disse og fremtidige tjenester og teknologier, der opretter og bruger personoplysninger.
En yderligere fordel ved GDPR er, at den gælder for alle EU-medlemsstater.

GDPR blev underskrevet som lov i april 2016 og træder i kraft den 25. maj 2018. Organisationer har mindre end et år til at sikre overholdelse. Straffen for manglende overholdelse kan være op til 4 % af den globale årlige omsætning eller 20 mio. euro, alt efter hvad der er størst. GDPR indfører også en obligatorisk meddelelse om overtrædelser, hvis konsekvenser har betydning for bestyrelser, der bekymrer sig om skader på virksomheders omdømme.

Bemærk, at Storbritanniens forestående udmeldelse af EU (også kaldet Brexit) ikke har væsentlig indflydelse på GDPR-landskabet:

- Virksomheder i Storbritannien, der behandler EU-personoplysninger, skal alligevel overholde GDPR, fordi GDPR gælder eksterritorialt for personoplysninger fra enhver person i EU.
- Storbritannien vil sandsynligvis indføre lokale love som GDPR for at lette dataoverførsler fra EU som reguleret af "tilstrækkelighedsregler".

GDPR handler om mere end sikkerhedsproblemer. Den indeholder en række nye foranstaltninger, herunder dataportabilitet, samtykke og tilbagekaldelse, aldersbekræftelse og retten til at blive glemt. Overholdelse handler imidlertid i høj grad om god sikkerhed. Hvad siger GDPR specifikt om dette?

GDPR er bemærkelsesværdigt ikke-normativ i forhold til at definere sikkerhedsforanstaltninger. Ud af sine 99 artikler handler kun artikel 32 specifikt om sikkerhed. Kravet er, at organisationer etablerer "passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici". Med andre ord er det op til hver enkelt virksomhed at vurdere risikoen i forbindelse med personoplysninger og gennemføre den sikkerhedskontrol, som den finder nødvendig.

Et aspekt af denne overvejelse er, hvad GDPR kalder "state of the art". Virksomheder er ikke forpligtet til at implementere state-of-the-art-teknologi. De skal dog vide, hvad det betyder, og forsvare deres holdning. Én situation skal virksomheder undgå, og det er at forsøge at retfærdiggøre, hvorfor de ikke har implementeret en bestemt sikkerhedskontrol eller -teknik, hvilket har ført direkte til et brud på persondatasikkerheden.

En af de nøgletest, som sandsynligvis vil blive anvendt af GDPR-tilsynsmyndigheder, er, hvad IDC kalder "Hvor stor en indsats har du gjort"-testen. Ikke at kende til en sårbarhed er skidt. At kende til en sårbarhed og ikke gøre noget ved det er endnu værre.

Hvis du ignorerer sikkerhedssårbarheder på en printer, kan det resultere i brud på personoplysninger, som, hvis det er alvorligt, kunne forårsage, at kontrolmyndigheder vil være i tvivl om, hvorvidt passende organisatoriske og tekniske tiltag er blevet implementeret til at beskytte dataene.

Det vigtigste område for GDPR er "behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register". Med andre ord behøver data ikke at være i elektronisk format for at være omfattet. Det er også vigtigt at beskytte fysiske kopier af data.

Direktivet for netværks- og informationssystemsikkerhed

EU forstår, at vigtige tjenester i en tid med flere og flere cyberangreb skal beskyttes, især dem, der anses for kritiske for, at økonomien eller samfundet kan fungere. For at opnå konsistens på tværs af alle medlemsstater med hensyn til beskyttelse mod cyberangreb vedtog EU NIS-direktivet.

NIS er overraskende udetaljeret, hvad angår sikkerhedskrav. Der er bred fokus på beskyttelse af infrastrukturen, herunder fysiske aktiver, og der lægges primært vægt på hændelsesstyring, forretningskontinuitetskontrol mv. Det indeholder en klausul om en obligatorisk meddelelse om overtrædelser (se artikel 16), men der er ingen foreskrevne bøder for manglende overholdelse.

Da NIS er et direktiv, skal det gennemføres som lov af medlemsstater og ratificeres af lovgiverne. NIS trådte i kraft i august 2016. Medlemsstaterne har indtil den 10. maj 2018 til at gennemføre direktivet i deres nationale love og yderligere seks måneder til at identificere operatører af væsentlige tjenester.

Fordelene ved printersikkerhed

Printersikkerhed er i modsætning til udskrivningssikkerhed udelukkende fokuseret på fysiske enheder forbundet med udskrivning, og det er en netværkssikkerhedsdisciplin. Printersikkerhed omfatter printeren som et slutpunkt og behandler den med samme omhu som ethvert andet slutpunkt, som f.eks. bærbare computere, servere og mobilenheder. Selv om de har en vis lighed med hinanden og har nogle problemområder, der minder om hinanden, er udskrivningssikkerhed og printersikkerhed forskellige discipliner.

Hvor sårbare er netværksprintere egentlig?

Printere modtager betydelige datamængder, hvoraf nogle vil være personoplysninger.
Få brugere, compliance-medarbejdere eller it-administratorer overvejer sikkerheden for disse data, når de overføres til og gemmes på printere. Paragraf 5.f i GDPR kræver "tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger". Men få organisationer tager hensyn til sikkerheden for data på en printer.

Desuden er det almindeligt, at udskrevne dokumenter glemmes i printerens papirbakker. I lyset af GDPR, kan pull-udskrivningsløsninger blive en vigtig faktor i beskyttelsen af utilsigtet tab af personoplysninger, specielt for organisationer hvis primære behandling af personoplysninger involverer udskrivning

Printere er et tiltrækkende mål for it-kriminelle, og det skyldes til dels, at de ikke betragtes som en del af it-systemet og dermed ikke får meget opmærksomhed af sikkerhedspersonalet. Printerstyring betragtes ofte som en del af facilitetsdriften. Da printere blev til netværksenheder, blev de stort set betragtet som enheder med "lav risiko", så længe enhederne befandt sig bag virksomhedens firewall, Sårbarheden af printerslutpunkter bliver stadig undervurderet.

Kombinerede printere/scannere/faxmaskiner bliver også mere avancerede med tiden, og de har almindelige computere installeret indeni til at styre alle handlinger. Windows- og Linux-systemer er ofte indbygget i mange moderne printere. Eftersom disse computere får meget lidt beskyttelse og opmærksomhed vedrørende sikring, er de ofte sårbare. Desuden kræver funktionaliteten tilslutningsmuligheder, så mange printere leveres med en lang række åbne porte for at understøtte brugervenligheden.

Manglende opmærksomhed kombineret med kraftig computerkraft og mange tilslutningsmuligheder betyder, at angriberne kan få adgang til printerne på flere måder, f.eks. via et modem, et trådløst adgangspunkt eller fra spyware-inficerede computere. Efter at have fået adgang kan angriberne bruge denne styrke til at ramme andre maskiner på det interne netværk eller deltage i en DDoS. De fleste printere har uhindret adgang til et internt netværk. En angriber, som kompromitterer en printer, kan scanne netværket for systemer, der kan udnyttes.

Som med andre slutpunktsenheder, der kræver beskyttelse, er printere ikke kun en "gateway", men også et mål for it-kriminelle. Printere gemmer ofte følsomme dokumenter i deres udskriftsspooler. De kombineres ofte med en dokumentscanner, og dokumenterne gemmes ofte i scanningsarkivet i langt længere tid, end de fleste regner med.

Overvejelser

Hvis der ikke har været fokus på printersikkerheden i din organisation, har IDC nogle anbefalinger til, hvor du skal starte.

Det hele starter med synlighed

Som med alle slutpunkter, der kræver sikkerhed, skal du starte med det grundlæggende: Trin 1 er altid synlighed. Lav en komplet oversigt over alle printere, herunder mærke, model, funktioner og konfigurationer. Oprettelsen af en sådan liste kan være problematisk, fordi printere ofte placeres på uidentificerede steder (skjult it). I laboratorier, mødelokaler eller kontorer vil der ofte være en printer, som for nemheds skyld er tilsluttet netværket, eller også er den forbundet direkte med en computer, uanset de sikkerhedsmæssige konsekvenser.

Ideelt set vil en slutpunktsopgørelse, der indeholder printere, kunne udtrækkes af en NAC (Network Access Controller) eller et aktivstyringsværktøj, der har enhedsregistrering som kernefunktionalitet. Det er ekstremt vanskeligt at opnå komplet synlighed i forbindelse med printere uden en NAC. Nogle printermodeller kan dog sørge for automatisk enhedsregistrering, når de er forbundet til netværket. Hvis du ikke er så heldig, at dit netværksmiljø inkluderer en homogen base af sådanne printere, er en NAC den rette løsning.

Forstærk dine printerslutpunkter

Printerne i organisationen skal forvaltes ligesom alle andre tilsluttede slutpunkter. Luk alle unødvendige tjenester, som printeren tilbyder, såsom FTP. De fleste organisationer behøver ikke FTP-adgang til deres printere, og det kan ofte gøre mere skade end gavn. Nogle printere giver for eksempel en angriber mulighed for at foretage FTP-anmodninger og anonymt hente jobs ud af en udskriftsspooler. Derudover udsættes mange FTP-tjenester på moderne printere for FTP-bounce-angreb. Med et værktøj som Nmap (Network Mapper) kan en angriber skjule kilden til en portscanning, hvilket overbeviser en kompatibel FTP-server om, at den kan give tilladelse til FTP-proxyforbindelser. Disse FTP-bounce-scanninger er gamle teknikker, men der er et bemærkelsesværdigt antal helt nye printerservere, som er modtagelige for sådanne angreb.

Den vigtigste aktivitet til styrkelse af printerslutpunkter er dog adgangskodeadministration. Den alvorligste fejl, der sker i organisationer, er, at man undlader at ændre standardadgangskoderne.

Ifølge Verizons *2016 Data Breach Investigations Report* omfattede 63 % af de bekræftede brud på persondatasikkerheden udnyttelse af svage og stjålne adgangskoder eller standardadgangskoder. Hvis printerne styres af tredjepartsleverandører af facilitetstjenester, er bekvemmeligheden af afgørende betydning (for dem). Når en enhed skal vedligeholdes, kan det være et problem at finde en adgangskode. Når der er en printer for hver 10 medarbejdere, kan en organisation med 10.000 medarbejdere have 1.000 adgangskoder at vedligeholde. Sikkerheden må derfor vige for bekvemmeligheden. Adgangskodeadministration er ikke kun en mangel hos ikke-tekniske medarbejdere. Den næststørste fejl er, at der er fri adgang til brugernavnet og adgangskoden i ukrypteret tekst for alle med en http://-forbindelse.

Vedligeholdelse og sikring

De fleste brud opstår på grund af manglende hygiejne. Ifølge Verizons *2016 Data Breach Investigations Report* udgjorde de 10 mest udnyttede sårbarheder i 2015 85 % af de gennemførte udnyttelser. De mest udnyttede sårbarheder er kendte og offentliggjorte. It-kriminelle bruger det, der virker, og maksimerer den investering, de har lavet i deres malware-værktøjer.

Vedligeholdelse og sikring af printerslutpunkter vil gøre dig til et sværere mål, der presser it-kriminelle til at bruge deres værktøjer på organisationer, som ikke har vedligeholdt deres systemer.

Med hensyn til sikring er det ikke alle printere, der er skabt ens. Nogle producenter tilbyder styringsværktøjer, der giver dig mulighed for at overvåge, administrere og sikre nogle printermærker og -modeller. Disse værktøjssæt er yderst værdifulde, fordi en virksomheds sårbarhedsscanner sandsynligvis vil have problemer med printere på grund af den integrerede webserver. Hvis du tilfældigvis har sådanne printere med robuste styringsværktøjer, er du heldig. Hvis det ikke er tilfældet, skal du muligvis sikre hver eneste printer manuelt, fordi det kan være svært at flikke en automatiseret løsning sammen.

For at forhindre at "støj" bliver importeret til SIEM-værktøjerne, konfigurerer organisationer ofte deres sårbarhedsscannere til at ignorere printere. Det er et lige så stort problem i forbindelse med SIEM- og sårbarhedsstyringsværktøjer som i forbindelse med printere. Det kan være kompliceret at konfigurere sådanne værktøjer til kun at acceptere visse meddelelser fra printere, men på kort sigt vil denne indsats hjælpe med at beskytte netværket mod printerinfektioner.

Gør forbindelsen sikker

Forstærk de administrationsprotokoller, der bruges til printeren. De fleste moderne printere understøtter en form for administration via HTTP og/eller HTTPS, og nogle få understøtter endda Telnet eller Secure Shell (SSH). Vælg omhyggeligt en administrationsprotokol, der leverer kryptering, såsom HTTPS eller SSH, og deaktivér svage eller ødelagte cifre, f.eks. SSLv3.

Sørg til sidst for, at printerne ikke giver åben adgang til resten af det interne netværk. Segmentering af virksomhedsnetværk er god praksis for netværkssikkerhed, og printere skal medtages i indsatsen. Certifikater kan bruges til logisk segmentering af adgangen til netværksressourcer og kryptering af trafik. Vær dog opmærksom på, at disse ekstra sikkerhedsforanstaltninger kan forringe printerfunktionaliteten, såsom begrænse adgangen til katalogtjenester (f.eks. Active Directory) og skybaseret styring og overvågning. At opnå balance mellem sikrede printere og bevarelsen af forretningsfunktionaliteten er altid et spørgsmål om vurdering af forretningsrisiciene.

Konklusion

Printere har ikke fået den samme opmærksomhed som andre trusselsfaktorer inden for it-sikkerhed. Sårbarheden og den relaterede trussel er meget reel. Organisationer af alle størrelser skal gøre noget for at håndtere problemet og løse det hurtigt. It-kriminelle er grådige efterlignere. Når en

trusselsfaktor er blevet udnyttet af en it-kriminel til en ondsindet handling, følger de andre hurtigt efter.

Konsekvenserne (både for økonomien og omdømmet) af at ignorere printersikkerheden er ved at stige til bestyrelsesniveaustatus med GDPR. Det ville være uheldigt at se en organisation, der ellers overholder reglerne og har arbejdet hårdt på sine informationssikkerhedsprocesser og -teknologier, blive slået ned af en overset printer.

OM DENNE PUBLIKATION

Denne publikation blev produceret af IDC Custom Solutions. De holdninger, analyser og forskningsresultater, der præsenteres her,
stammer fra mere detaljeret forskning og analyse, der udføres uafhængigt og offentliggøres af IDC, medmindre specifik sponsorering nævnes. IDC Custom Solutions gør IDC-indhold tilgængeligt i en bred vifte af formater til distribution via forskellige virksomheder. En licens til distribution af IDC-indhold er ikke udtryk for nogen form for godkendelse af eller holdning til licenshaveren.