IDC
Analyze the Future

IDC MARKET SPOTLIGHT

Att skydda utskriftsinfrastrukturen är avgörande för digital omvandling

December 2016

Av Robert Palmer, IDC:s forskningschef för bildbehandlings-, utskrifts- och dokumentlösningar

Sponsrad av HP Inc.

En organisations IT-säkerhetsplan är en viktig prioritet för att säkerställa lämpligt skydd mot och respons på potentiella hot och intrång. Skrivarsäkerhet behöver vara del av den planen, framför allt i våra tider med databehandling på den tredje plattformen (mobilitet, molnet, Big Data och sociala medier). Som del av en utförlig säkerhetsplan för organisationens skrivarmiljö bör alltså ingå lösningar för att hantera säkerheten för både enheter och data. Den här avhandlingen undersöker vikten av att skydda skrivar- och dokumentinfrastrukturen, och den roll som hanterade utskriftstjänster kan ha i att uppnå det målet.

Inledning

Frågor som rör säkerhet och dataintegritet har genomgående rankats högst på listan för CIO:er och IT-chefer i över ett årtionde. IDC:s egen forskning visar att säkerhet nu har blivit en hög prioritet för en majoritet av företag. Det rankas endast en aning lägre än ett annat viktigt företagsinitiativ: digital omvandling. Båda ses som viktiga företagsaspekter, och det är viktigt att förstå hur digital omvandling och säkerhet är sammankopplade.

Organisationer möter många olika hot när det gäller att säkra IT-infrastrukturen. De flesta tekniksmarta organisationer har gjort säkerhet till en av sina främsta prioriteter genom att fokusera på frågor som att skydda nätverket från yttre attacker, säkra nätverksenheter, administrera åtkomsten till anslutna enheter och förhindra att konfidentiella data avslöjas.

Det är lätt att se att alla dessa frågor kretsar kring behovet av att skydda organisationens värdefullaste tillgångar: företagsinformation och kunddata. Företag lägger miljarder dollar på dokumenthantering och ECM-programvara (Enterprise Content Management), stora investeringar i system för att få kontroll över affärskritiskt innehåll. Något som gör utmaningen än svårare är den fortsatta rörelsen mot mobilitet och molnanvändning. Dagens kunskapsarbetare kräver åtkomst till information vid dygnets alla timmar, vilket innebär att innehåll måste flyttas fritt både inom och utom företagets brandvägg.

Det är intressant att notera att en organisations utskrifts- och dokumentinfrastruktur har en unik position just där digital omvandling och IT-säkerhet möts. Ändå inser inte de flesta företag de sårbarheter i säkerheten som är förknippade med deras befintliga utskrifts- och dokumentmiljö. Frågans kärna handlar om rollen för den smarta multifunktionsskrivaren (MFP:en), en enhet som har blivit ett intelligent nav för att behandla företagsinformation. MFP:en leder information både in i och ut från företaget, vare sig den informationen sparas i enheten, på företagsnätverket, på papper eller i molnet.

Ett osett och ohanterat hot

Den anslutna MFP:en är en potentiell säkerhetsrisk om den är en ohanterad ansluten enhet. Men MFP:en kan också användas som en tillgång på frontlinjen, för att säkra nätverksåtkomst, hantera datasäkerhet och skydda åtkomsten till information.

Enligt forskning i IDC:s *User Perspectives on Print Security, 2015*, har fler än 30 % av alla organisationer inte några säkerhetspolicyer för att hantera åtkomst till och kontrollera användarrättigheter för skrivare och MFP:er anslutna till sitt nätverk. Samtidigt uppgav över hälften av de tillfrågade i undersökningen att de i hög grad var bekymrade över obehörig användning av kopiatorer eller MFP:er.

Det finns liknande motsägelser när det gäller hur företag ser på sina befintliga IT-rutiner. IDC:s undersökning *MaturityScape Benchmark: Print Security in the United States, 2016,* visar att fler än 70 % av de tillfrågade uppger att utskriftssäkerhet i hög grad påverkar vilka skrivare eller MFP:er som de köper eller leasar. Men överraskande nog var antalet tillfrågade som bedömde utskriftssäkerhet som ”mycket viktigt” endast 26 % eller färre av de som var bekymrade om den övergripande IT-säkerheten.

Många säkerhets- och IT-chefer har antagit att system som används för att skydda nätverket även omfattar ansluten kringutrustning. Men säkerheten kring nätverkets gränser faller samman, och alla enheter som är anslutna till nätverket utgör nu en risk för ändpunktssäkerhet – inklusive skrivare och MFP:er.

Hotet är äkta, och potentiella säkerhetsöverträdelser kan ske antingen på grund av illasinnade attacker med en nätverksskrivare eller MFP som ingångspunkt, eller omedvetet vårdslös användning av enheter från medarbetare. Utskriftsmiljön är unik, eftersom den är inriktad specifikt på att hantera information och dokument både i digitalt format och i papperskopior, så affärskritiskt innehåll är utsatt och sårbart på flera olika sätt. Att underlåta att skydda utskriftsmiljön som en del av den övergripande IT-strategin lämnar en organisation lika sårbar som att inte vidta några åtgärder alls för IT-säkerheten.

Resultatet av en säkerhetsöverträdelse för utskrifts- och dokumentinfrastrukturen är samma som för alla andra säkerhetsöverträdelser: Stora kostnader på grund av stilleståndstid för att identifiera och åtgärda säkerhetsöverträdelsen, böter förknippade med företagsstyrning och regelefterlevnad samt förlorade kunder eller annan skada för företagets rykte.

Säkra utskriftstjänster

Utmaningarna kring utskrifts- och dokumentsäkerhet går lätt att identifiera, men att utveckla en säker utskriftsstrategi har visat sig vara svårt för många företag. Ett problem har att göra med de olika parterna inom organisationen. Enhetssäkerhet ligger ofta hos IT-funktionen, och innefattar vanligtvis IT-avdelningen, säkerhetschefen och supportavdelningen, samt ändpunktssäkerhet och nätverkssäkerhet. Utöver det inbegriper diskussioner om säkerheten för skrivare och MFP:er också ofta fastighetsförvaltning.

Innehållssäkerhet ses däremot ofta i samband med frågor kring regelefterlevnad, och de som är inblandade finns oftast inom riskhantering och i ledningen. Representanter för ERP-program, databaskluster, innehållshantering och chefer för andra verksamhetsområden kan också vara inblandade. Oftast hanteras säkerheten för innehåll och skrivare separat, vilket leder till bristande integrering och en ökning av sårbarhetsluckor. Samtidigt känner företag ofta inte till de olika lösningarna för säker utskrift och de professionella tjänster som finns tillgängliga på marknaden.

Det här är ett område där hanterade utskriftstjänster (MPS) kan spela en stor roll för att öka utskrifts- och dokumentsäkerheten. Många företag har avtal med en MPS-leverantör för att optimera sin

utskriftsinfrastruktur, så att man kan öka effektiviteten och minska utskriftskostnaderna, men utskrifts- och innehållssäkerhet är till stor del förbisett i de flesta avtal för utskriftstjänster. Idag har en del MPS-leverantörer kapaciteten, verktygen och resurserna för att hjälpa företag att identifiera och prioritera befintliga säkerhetshot. En del av den här processen kan innehålla en inledande säkerhetsbedömning, vilket är viktigt för att identifiera luckor i den befintliga enhets- och innehållsinfrastrukturen. Företagen kan sedan arbeta tillsammans med tjänsteleverantören för att utveckla och driftsätta säkra hanterade utskriftstjänster för att hantera befintliga sårbarheter, stärka dokumentinfrastrukturen och mildra framtida säkerhetsrisker.

MPS-leverantören har också en unik förmåga att samla de olika inblandade parterna för att ge avtalade utskriftstjänster som spänner över olika avdelningar och verksamhetsområden, något som är av stor vikt för att driftsätta en helhetsstrategi för enhets- och innehållssäkerhet. Ett sådant tillvägagångssätt gynnar också utvecklingen av en säkerhetsplan som löper jämsides med företagets egen strategi för digital omvandling. Säkra utskriftstjänster kan gå från grundläggande säkerhet för att skydda utrustningen och informationen, till mer avancerade åtgärder som är betydligt mer komplicerade i implementeringen och erbjuder en högre nivå av enhetssäkerhet och innehållsskydd.

Sammanfattning: Från reaktiv till proaktiv

Summan av det hela är att utskrifts- och dokumentinfrastruktur inte har fått lika mycket uppmärksamhet som andra hot mot nätverks- och cybersäkerheten. Säkerhetsöverträdelser skapar rädsla och osäkerhet, och effekten på driftskostnader, arbetsprestationer och företagets rykte kan bli avsevärd.

Organisationer måste ta proaktiva steg för att möta säkerhetsproblemen i utskrifts- och dokumentinfrastrukturen, och MPS-leverantören bör ses som en viktig partner i det arbetet. När man söker leverantörer för skrivartjänster bör man se till dem som uppvisar kärnkompetens i att bedöma hotnivåer och avhjälpa problem.

Välj också partner som har hårdvara och lösningar uppbyggda kring ett säkerhetsekosystem för att hantera följande sårbarheter i dokumentinfrastrukturen:

- Användarautentisering och verifiering
- Enhetshantering
- Enhetsskydd för sabotageprogram (malware)
- Uppdateringar för inbyggd programvara och lösenordshantering
- Innehållssäkerhet, sekretess och dataintegritet
- Kapacitet att hantera den mänskliga faktorn i installationen, konfigureringen och användningen av utrustningen

MPS-lösningar bör också utformas för att integrera med dokumenthantering och ECM-system från tredje part för att ge ytterligare skydd och för att bistå arbetet med styrning och krav på regelefterlevnad.

Genom att utgå från ett helhetstänkande kan företag börja täppa till sårbarhetsluckor och förstärka skyddet i skrivar- och dokumentmiljön, vilket sannolikt är organisationens svagaste säkerhetslänk.

OM DEN HÄR PUBLIKATIONEN

Den här publikationen är producerad av IDC Custom Solutions. De åsikter, analyser och forskningsresultat som presenteras häri är grundade på mer detaljerad forskning och analys som utförts och publicerats oberoende av IDC, om inte en specifik leverantörssponsring noterats. IDC Custom Solutions gör IDC-innehåll tillgängligt i en mängd olika format för att distribueras av olika företag. En licens för att distribuera IDC-innehåll antyder inte stöd av eller åsikter om licenstagaren.

COPYRIGHT OCH RESTRIKTIONER

Mer information om IDC finns på www.idc.com. Mer information om IDC Custom Solutions finns på http://www.idc.com/prodserv/custom_solutions/index.jsp.

Globalt huvudkontor: 5 Speen Street Framingham, MA 01701 USA P.508,872.8200 F.508,935.4015 www.idc.com