Teknisk vitbok

Lev upp till efterlevnadskrav för nätverks- och datasäkerhet

Rekommendationer för att applicera säkerhetskontroller i skrivarparken

Innehållsförteckning

Brister i efterlevnad kan skada ditt företag

Förutom dyra böter och stämningar, kan en säkerhetsöverträdelse resultera i förlorade intäkter och skadat rykte. När du skapar din säkerhetsplan, ska du komma ihåg att ditt nätverk bara är så säkert som den svagaste länken. Skrivare och MFP:er har till stor del samma säkerhetsproblem som finns i persondatorer. Det är viktigt att använda produkter och lösningar som hjälper dig att uppfylla efterlevnadskraven och skydda din företagsinformation mot säkerhetshot.

Vad är risken?

Brist på efterlevnad av regler och lagar resulterar i stora kostnader för globala organisationer. Böter, förlorade affärer, skadat rykte och grupptalan orsakar förluster på i genomsnitt 7 700 000 dollar per år.[1]

Oskyddade eller för dåligt skyddade klienter skapar större möjligheter för cyberbrott. Under 2015 rapporterade företagen 35 % ökning av cyberattacker jämfört med samma period föregående år.[2] Under 2015 skedde mer än 2 000 rapporterade brott som representerar över 2 miljarder kundregister - och cirka 71 % av dessa brott skedde genom ett nätverks klient.[3]

Även om många IT-avdelningar strikt tillämpar säkerhetsåtgärder för enskilda datorer och nätverket, är skrivare och MFP:er ofta förbisedda och blottade. Men skrivare kan innebära en öppning till ditt nätverk och att skydda dem är lika viktigt. Av alla betydande dataintrång som rapporterades av IT-chefer involverade 26 % deras skrivare.[4]

Utnyttja gemensamma säkerhetskontroller för att förbättra efterlevnaden

Det är utmanande att leva upp till branschens efterlevnadskrav och regler. Lyckligtvis har Center for Internet Security (CIS) skapat en uppsättning gemensamma säkerhetskontroller för att förenkla rekommendationerna för cybersäkerhet. CIS Critical Security Controls är 20 specifika åtgärder som kan hjälpa till att stoppa cyberattacker. (Mer information finns på https://www.cisecurity.org/critical-controls.cfm.) Kontrollerna är anpassade efter många andra branschregler som t. ex. PCI-DSS, ISO 27001, US CERT-rekommendationer, HIPAA, FFIEC och NIST. Kontrollerna ersätter inte dessa andra ramverk, men de används ofta av företag för att förstå andra ramverk.

CIS Critical Security Controls prioriterar ett mindre antal åtgärder som ger ett bra resultat. De behandlar de vanligaste attackmönstren från ledande hotrapporter. En bred grupp branschexperter – inklusive några av de bästa organisationerna för kriminalteknik och incidenthantering – hjälpte till att skapa dem. Dessutom uppdateras kontrollerna kontinuerligt baserat på nya hot och attacker.

Använd CIS Critical Security Controls för att få hjälp med att organisera din handlingsplan för säkerhet och följa efterlevnadskraven. Denna vitbok ger förslag på åtgärder för vart och ett av de 20 kontrollerna för att skydda dina skrivare, data och dokument som en del av större säkerhetsplan.

CIS Critical Security Controls och rekommenderade åtgärder

CSC 1: Inventering av auktoriserade och icke auktoriserade enheter

Kontroll – Hantera aktivt (inventera, spåra och korrigera) alla hårdvaruenheter i nätverket så att endast auktoriserade enheter ges tillgång, och hitta otillåtna och ohanterade enheter och förhindra dem att få tillgång.

Rekommendation – Se till att alla utskriftsenheter i nätverket redovisas och förvaltas aktivt för att uppfylla din säkerhetspolicy. Ett effektivt skrivarsäkerhetsverktyg kan upptäcka och leverera synlighet för alla nätverk och datoranslutna enheter.

CSC 2: Inventering av auktoriserade och icke auktoriserade enheter

Kontroll – Hantera aktivt (inventera, spåra och korrigera) all programvara i nätverket så att endast godkänd programvara är installerad och kan driftsättas, och hitta obehörig och oövervakad programvara och förhindra den från installation eller drift.

Rekommendation – Se till att all förinstallerad programvara och alla lösningar som är nedladdade på skrivare och MFP:er är aktuella, signerade och bevisat giltiga. Välj utskriftsenheter med inbyggt skydd för BIOS och inbyggd programvara för att säkerställa att endast giltig kod är nedladdad. Proaktiva uppdateringar av inbyggd programvara kan göras i hela skrivarparken med lösningar för hantering av skrivarparken. Programvara (serverbaserad och klientbaserad) bör undertecknas och valideras som giltig.

CSC 3: Säkra konfigurationer för hårdvara och programvara på mobiltelefoner, bärbara datorer, arbetsstationer och servrar

Kontroll – Upprätta, inför och hantera aktivt (spåra, rapportera och korrigera) konfigurationssäkerheten för bärbara datorer, servrar och arbetsstationer med hjälp av en rigorös konfigurationsstyrning och ändra styrprocessen för att förhindra angripare att utnyttja sårbara tjänster och inställningar.

Rekommendation – Precis som med andra klienter i nätverket, bör skrivare konfigureras på ett säkert sätt. Du bör skapa och installera en säkerhetspolicy i alla skrivare och aktivt åtgärda alla avvikelser från den policyn. Säkerhetschecklistor (som NIST) eller rådgivningstjänster för säkerhet kan hjälpa dig designa och installera en övergripande skrivarsäkerhetspolicy. Ett effektivt hanteringsverktyg för skrivarsäkerhet kan automatisera din policys framtagande, installation, bedömning och åtgärdande av skrivarinställningar för hela skrivarparken. Multifunktionsskrivare på Enterprise-nivå (MFP:er) har mer än 250 säkerhetsinställningar, så automatisering av den här processen kan spara avsevärt med tid.

CSC 4: Kontinuerlig sårbarhetsanalys och åtgärder

Kontroll – Se till att kontinuerligt skaffa, utvärdera och vidta åtgärder om ny information för att identifiera sårbarheter och för att sanera och minimera möjliga fönster för angripare.

Rekommendation – Security Information and Event Management (SIEM)-lösningar som ArcSight, Splunk eller SIEMonster kan övervaka aktivitet i ditt nätverk i realtid och meddela administratörer när incidenter sker. Det är lika viktigt att övervaka skrivare som datorer – se till att dina skrivare kan skicka syslog-meddelanden vid händelser till ditt SIEM-verktyg.

Välj skrivare med funktioner som kan upptäcka attacker i realtid och automatiskt återställas, för att maximera upptiden och samtidigt minimera insatserna för IT-avdelningen.

För att minska sårbarheter, ska du använda ett säkerhetshanteringsverktyg för skrivarparken som kan identifiera nya skrivare och automatiskt tillämpa ditt företags säkerhetspolicyinställningar så snart nya enheter ansluts till nätverket. Schemalägg regelbundna bedömningar/åtgärder för att hålla hela skrivarparken i enlighet med företagets policy.

CSC 5: Kontrollerad användning av administrativa privilegier

Kontroll – Spåra, kontrollera, förhindra och korrigera användning, tilldelning och konfiguration av administratörsbehörigheter för datorer, nätverk och applikationer.

Rekommendation – Välj skrivare och lösningar med förmåga att autentisera användare och kontrollera åtkomst till funktionalitet baserat på en persons roll, så att bara IT-personal eller annan behörig personal kan installera och konfigurera enhetens inställningar. Använd säkerhetshanteringsprogram för skrivarparken för att distribuera administratörslösenord för hela skrivarparken.

CSC 6: Underhåll, övervakning och analys av granskningsloggar

Kontroll – Samla in, hantera och analysera granskningsloggar av händelser för att hjälpa till att upptäcka, förstå eller återställa efter en attack.

Rekommendation – Skrivare bör ha förmåga att generera syslog-meddelanden vid incidenter, så att säkerhetsteamet regelbundet kan undersöka granskningsloggar för att upptäcka och lösa problem. Välj enheter som kan skicka sådana meddelanden till skrivarparkens säkerhetshanteringslösningar och SIEM-verktyg för både realtidsövervakning och förmåga att generera rapporter för granskning eller andra efterlevnadskrav.

CSC 7: Skydd för e-post och webbläsare

Kontroll – Minimera attackytan och möjligheter för angripare att manipulera mänskligt beteende via deras användning av webbläsare och e-postsystem.

Rekommendation – MFP:er är ofta anslutna till internet så att de, till exempel, kan skicka skannat material via e-post. Säkerställ att skannat material som skickas med e-post är krypterat för att skydda känsliga data. Installera enheter och lösningar som kan autentisera användare och kontrollera åtkomst till resurser inom enheten (som webbservrar eller e-postfunktioner) baserade på en persons roll. Skapa en lista över "Tillförlitliga platser" för dina MFP:er och hantera det på lämpligt sätt för att säkerställa att endast betrodda webbplatser nås från enheten. Integrera olika autentiseringsmetoder (som PIN/PIC, LDAP eller Kerberos-autentisering) med Active Directory för strömlinjeformad hantering och ökad säkerhet. Skrivare som är anslutna till nätverket bör ha inbyggt skydd mot skadlig programvara och virus och skrivares inbyggda programvara bör uppdateras regelbundet så att de senaste skydden är på plats.

CSC 8: Skydd mot skadlig programvara

Kontroll – Kontrollera installation, spridning och utförande av skadlig programvara på flera punkter i företaget, samtidigt som du optimerar användningen av automatisering för att möjliggöra snabb uppdatering av försvar, datainsamling och korrigerande åtgärder.

Rekommendation – Välj skrivare som bara laddar ner kontrollerad, signerad kod och som har inbyggda funktioner mot skadlig programvara för att aktivt övervaka enhetens minne och göra en omstart i händelse av en attack. Ett effektivt hanteringsverktyg för skrivarsäkerhet kan automatisera din policys framtagande, installation, bedömning och åtgärdande av skrivarinställningar för hela skrivarparken. Du bör också se till att alla utskriftsprogramvarulösningar undertecknas och valideras som äkta.

CSC 9: Begränsning och kontroll av nätverksportar, protokoll och tjänster

Kontroll – Hantera (spåra, kontrollera och korrigera) den pågående operativa användningen av portar, protokoll och tjänster på nätverksenheter för att minimera sårbara fönster som är tillgängliga för angripare.

Rekommendation – Om de inte redan är inaktiverade som standard, ska du inaktivera oanvända portar och osäkra protokoll (t. ex. FTP eller Telnet) som angripare kan använda för att få tillgång till enheten. Spara IT-avdelningens tid och minska riskerna genom att distribuera ett skrivarsäkerhetsverktyg för att automatiskt hålla enhetsinställningar konstanta i hela skrivarparken. Använd administratörslösenord, autentisering och rollbaserade åtkomstkontroller för att begränsa tillgång till enhetens funktioner och inställningar.

CSC 10: Kapacitet för dataåterställning

Kontroll – Säkerhetskopiera viktig information korrekt med en beprövad metod för snabb återställning.

Rekommendation – Denna kontroll fungerar för närvarande inte för skrivare.

CSC 11: Säkra konfigurationer för nätverksenheter som brandväggar, routrar och switchar

Kontroll – Upprätta, inför och hantera aktivt (spåra, rapportera och korrigera) konfigurationssäkerheten för bärbara datorer, servrar och arbetsstationer med hjälp av en rigorös konfigurationsstyrning och ändra styrprocessen för att förhindra angripare att utnyttja sårbara tjänster och inställningar.

Rekommendation – Skrivare är anslutna till nätverket och, precis som med andra slutpunkter i nätverket, bör de konfigureras säkert. Ett effektivt hanteringsverktyg för skrivarsäkerhet kan automatisera din policys framtagande, installation, bedömning och åtgärdande av skrivarinställningar för hela skrivarparken för att hålla nätverket säkert - och samtidigt spara tid för IT-avdelningen.

CSC 12: Gränsskydd

Kontroll – Upptäck, förebygg och åtgärda informationsflödet som skickas via nätverket på olika förtroendenivåer med fokus på data som skadar säkerheten.

Rekommendation – Använd kryptering för att skydda data när de skickas (skrivar- eller skanningsjobb som skickas till eller från skrivaren) och är i vila på enhetens hårddisk. Välj skrivare och lösningar med förmåga att autentisera användare och kontrollera åtkomst till funktionalitet baserat på en persons roll så att, till exempel, endast auktoriserade användare kan skicka skanningsjobb via e-post eller skicka filer till molndestinationer. Konfigurera betrodda webbplatser i en lista över "Tillförlitliga platser" på enheten för att förhindra åtkomst till skadliga webbplatser. Säkra mobila utskriftslösningar kan göra det enkelt för användare att skriva ut från sina mobila enheter samtidigt som de även skyddar nätverket.

CSC 13: Dataskydd

Kontroll – Förhindra dataexfiltration, mildra effekterna av exfiltrerade data och säkerställ integriteten för känslig information.

Rekommendation – Använd kryptering för att skydda data när de skickas (skrivar- eller skanningsjobb som skickas till eller från skrivaren) och är i vila på enhetens hårddisk. Installera pull print-lösningar för att undvika att känsliga handlingar lämnas kvar i utmatningsfacken. Se till att data som lagras på enhetens hårddiskar raderas säkert innan leasade enheter återlämnas eller återvinns i slutet av sin livslängd.

CSC 14: Kontrollera åtkomst baserat på nivåbehov

Kontroll – Spåra, kontrollera, förhindra, åtgärda och skydda åtkomst till viktiga tillgångar (t. ex. uppgifter, resurser och system) i enlighet med det formella beslutet över vilka personer, datorer och program som har ett behov och rätt att få tillgång till dessa viktiga tillgångar baserat på en godkänd klassificering.

Rekommendation – Välj skrivare och lösningar med förmåga att autentisera användare och kontrollera åtkomst till funktionalitet baserat på en persons roll. Integrera olika autentiseringsmetoder (som PIN/PIC, LDAP eller Kerberos-autentisering) med Active Directory för strömlinjeformad hantering och ökad säkerhet. Pull print-lösningar kan skydda känsliga dokument från att hamna i fel händer.

CSC 15: Trådlös åtkomstkontroll

Kontroll – Spåra, kontrollera, förhindra och korrigera säkerhetsanvändningen av trådlösa lokala nätverk (LAN), åtkomstpunkter och trådlösa klientsystem.

Rekommendation – Ett effektivt hanteringsverktyg för skrivarsäkerhet kan automatisera driftsättning, bedömning och åtgärdande av skrivarinställningar, inklusive inställningar för trådlöst, för hela skrivarparken. Använd lösningar för åtkomstkontroll för att begränsa tillgången till enhetens funktioner, som skanning till e-post, baserat på användarens roll. Säkra mobila utskriftslösningar kan göra det enkelt för användare att skriva ut från sina mobila enheter samtidigt som de även skyddar nätverket. Till exempel enheter som stöder trådlös utskrift peer-to-peer och som tillåter användare av mobila enheter att skriva ut direkt till en skrivares diskreta trådlösa signal – utan tillgång till företagets nätverk eller trådlösa tjänster.

CSC 16: Övervakning och kontroll av konton

Kontroll – Hantera aktivt livscykeln för system- och programkonton – skapande, användning, vila, radering – i syfte att minimera möjligheterna för angripare att utnyttja dem.

Rekommendation – Välj skrivare och lösningar med förmåga att autentisera användare och kontrollera åtkomst till funktionalitet baserat på en persons roll. Integrera autentisering med Active Directory för centraliserad hantering och ökad säkerhet. Se regelbundet över användarkonton och inaktivera onödiga sådana, och använd spårningslösningar för att övervaka kontoanvändningen. Kryptera kontots användarnamn och inloggningsuppgifter, både när ett jobb skickas och är i vila på lagringsenheten. Säkerhetskonsulter kan hjälpa dig att utforma en omfattande skrivarsäkerhetsplan för att minimera riskerna – och i vissa fall hjälpa dig att hantera säkerhet, inklusive kontoövervakning och kontroll.

CSC 17: Bedömning av säkerhetskunskaper och lämplig utbildning för att fylla luckorna

Kontroll – Identifiera de specifika kunskaper, färdigheter och förmågor som behövs för att stödja företagets skydd, utveckla och genomföra en integrerad plan för att bedöma, identifiera och åtgärda brister med hjälp av en policy, organisatorisk planering, utbildning och informationsprogram för alla funktionella roller i organisationen.

Rekommendation – Skrivarsäkerhetskonsulter har specialkunskaper för att hjälpa dig att bedöma dina säkerhetsrisker, utveckla en övergripande säkerhetspolicy och planera och implementera rekommenderade processer och teknik. Vissa säkerhetstjänster kan även hantera utskriftssäkerhet och efterlevnad åt dig.

CSC 18: Säkerhet för applikationer och program

Kontroll – Hantera säkerhetens livscykel för alla egenutvecklade och förvärvade programvaror för att förebygga, upptäcka och åtgärda säkerhetsbrister.

Rekommendation – Följ bästa praxis för säker utveckling av alla utvecklade utskriftslösningar. Välj programvarulösningar som har signerats och godkänts som äkta.

CSC 19: Ansvar för och hantering av incidenter

Kontroll – Skydda företagets information, liksom dess rykte, genom att utveckla och genomföra en infrastruktur för incidenthantering (t. ex. planer, roller, utbildning, kommunikation och ledningsöversyn).

Rekommendation – Bekräfta att din skrivarmiljö tas upp i incidentplanen.

CSC 20: Penetrationstester och Red Team-övningar

Kontroll – Testa den totala styrkan i en organisations försvar (teknik, processer och människor) genom att simulera en angripares mål och åtgärder.

Rekommendation – Inkludera din utskriftsmiljö när du kör penetrationstester. Utvärdera regelbundet din utskriftsmiljö för sårbarheter och uppdatera din säkerhet för att åtgärda dessa brister.

Ta nästa steg

Att genomföra rekommendationerna i denna vitbok kan hjälpa dig stärka skrivarsäkerheten och uppfylla efterlevnadskrav. Behöver du hjälp? Hantering av och rådgivning kring utskriftssäkerhet kan hjälpa dig att utveckla en plan och installera processer och teknik för att förbättra säkerheten för dina skrivare, data och dokument.

Bilaga A: HPs utskriftssäkerhetsfunktioner, lösningar och tjänster

De säkerhetsfunktioner som är inbyggda i HP-enheter, tillsammans med branschledande programvarulösningar och tjänster, kan hjälpa dig att uppfylla regulatoriska och juridiska efterlevnadskrav och skydda din företagsinformation från säkerhetshot.

Inbyggda säkerhetsfunktioner i HP Enterprise-skrivare och MFP:er skyddar mot skadlig programvara och kan automatiskt upptäcka attacker och återställa skrivaren efteråt. Endast HPs skrivarsäkerhet erbjuder realtidsupptäckt, automatisk övervakning och inbyggd programvaruvalidering för att stoppa hot i samma ögonblick som de sker.[5] (hjälper till att leva upp till CSC 2, 4, 6 och 8.) hp.com/go/PrintersThatProtect

HP Access Control -lösningar ger en mängd olika autentiserings- och rollbaserade åtkomstkontroller för att minska potentiella säkerhetsöverträdelser, samt spårning av jobb och redovisning. (hjälper till att leva upp till CSC 5, 7, 10, 12, 13, 14, 15 och 16.) hp.com/go/hpac

Kryptering och **HP JetAdvantage arbetsflödeslösningar** skydda data både när de lagras på HP Enterprise-enheter och även när de skickas till eller från skrivare eller molnet. (hjälper till att leva upp till CSC 12 och 13.) hp.com/go/upd, hp.com/go/documentmanagement

HP pull print-lösningar skyddar konfidentiella dokument genom att lagra utskriftsjobb på en skyddad server, i molnet eller på din dator. Användare behörighetsverifierar sig på den skrivare de valt för att hämta och skriva ut sitt jobb. (hjälper till att möta CSC 10, 13 och 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect ger enkelt mobila användare tillgång till utskrift från smarttelefoner och plattor med den bibehållna säkerhet och administrativa kontroll du behöver. (hjälper till att leva upp till CSC 12 and 15.) hp.com/go/JetAdvantageConnect

HPs data för skrivarhändelser kan skickas till SIEM-verktyg, som ArcSight, Splunk eller SIEMonster. Ditt säkerhetsteam kan enkelt se skrivarslutpunkter som en del av det bredare IT ekosystemet och kan vidta korrigerande åtgärder. (hjälper till att leva upp till CSC 4 och 6.)

HP JetAdvantage Security Manager är branschens enda policybaserade efterlevnadsverktyg för skrivarsäkerhet.[6] Det hjälper dig att etablera en säkerhetspolicy för hela skrivarparken, automatisera justering av enhetsinställningar och installera och förnya unika certifikat samtidigt som du får de rapporter du behöver för att bevisa efterlevnaden. Lösningens direktaktiverade säkerhet konfigurerar automatiskt nya enheter när de adderas till nätverket eller efter en omstart. (hjälper till att leva upp till CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 och 15.) hp.com/go/securitymanager

HP Secure Managed Print Services ger branschens starkaste, mest övergripande skrivarsäkerhetsskydd.[7] Skrivarsäkerhet kan vara komplicerad. Låt HP hantera skrivarsäkerheten från skrivaren och uppdatera till avancerade säkerhetslösningar som behandlar människor, processer och efterlevnadskrav. (hjälper till att leva upp till CSC 2, 3, 12, 16, 17, 18 och 19.) hp.com/go/SecureMPS

HP Print Security Professional Services tillhandahåller experter på säkerhet för att hjälpa dig att bedöma din utskriftsmiljö, proaktivt fastställa säkerhetsregler och hålla din säkerhetsplan aktuell. Vi kan även hantera utskriftssäkerhet och efterlevnad åt dig. (hjälper till att leva upp till CSC 2, 3, 12, 16, 17 och 19.) hp.com/go/SecureMPS

Fotnoter

[1] Ponemon Institute, "2015 Global Cost of Cyber Crime Study," oktober 2015.

[2] Källa: PWC, "Global Economic Crime Survey," 2016.

[3] Källa: IDtheftcenter.org, juni 2015.

[4] 26,2 % av de som svarade i undersökningen upplevde ett större IT-säkerhetsintrång som krävde åtgärder och mer än 26,1 % av dessa incidenter involverade skrivare. IDC, "IT and Print Security Survey 2015" IDC #US40612015, september 2015.

[5] Gäller HP Enterprise-klassenheter som introducerades 2015 och är baserad på HPs granskning av inbäddade säkerhetsfunktioner som publiceras 2016 hos konkurrerande skrivare i klassen. Endast HP erbjuder en kombination av säkerhetsfunktioner för integritetskontroll under BIOS med självreparerande möjligheter. En uppdatering av ditt FutureSmart-service pack kan krävas för att aktivera säkerhetsfunktioner. En lista över skrivare hittar du här: hp.com/go/PrintersThatProtect. Mer information finns på hp.com/go/printersecurityclaims.

[6] HP JetAdvantage Security Manager måste köpas separat. Mer information finns på hp.com/go/securitymanager. Påståendet om jämförelser baseras på HPs interna undersökning av konkurrenternas erbjudande (Device Security Comparison, januari 2015) och Solutions Report on HP JetAdvantage Security Manager 2.1 från Buyers Laboratory LLC, februari 2015.

[7] Inkluderar skrivar-, data- och dokumentsäkerhetskapacitet genom ledande leverantörer av hanterade utskriftstjänster. Baserat på HPs genomgång av publikt tillgänglig information 2015-2016 om säkerhetstjänster, säkerhet och programvara och inbäddade säkerhetsfunktioner för deras konkurrenskraftiga skrivare i klassen. Mer information finns på hp.com/go/MPSsecurityclaims eller hp.com/go/mps.

Anmäl dig för uppdateringar
hp.com/go/getupdated

4AA6-8821SVE, november 2016