Hvidbog om informationssikkerhed

Netværkssikkerhed

Beskyttelse af kontorets netværksenheder

www.sharp.dk

SHARP
Be Original.

Indhold

Indledning

I nutidens forbundne verden har effektiv informationssikkerhed på tværs af hele virksomhedens netværk aldrig været vigtigere.

Hver dag er der utallige ondsindede forsøge på at stjæle, modificere på ulovlig vis, opsnappe eller udbrede fortrolige dokumenter eller få uautoriseret adgang til private netværk og virksomhedsnetværk. Denne hvidbog undersøger de primære udfordringer, som virksomheder står over for, når det kommer til at beskytte deres IT-infrastruktur, hvad angår netværkstilsluttede kontorenheder som f.eks. multifunktionssystemer (MFP'er) og printere.

I denne hvidbog vil vi undersøge:

- **Baggrunden**
  Set fra et netværkssikkerhedsperspektiv står hver virksomhed over for udfordringer, men de sårbarheder, som nutidens multifunktionssystemer og printere er udsat for, er ofte overset. Hackere og cyberkriminelle bruger dem som en vej ind i organisationer for at stjæle fortrolige data, der er lagret på harddiske og andre netværkstilsluttede enheder, ligesom de også forårsager ondsindet skade eller afbryder virksomhedsaktiviteter. Indvirkningen på produktivitet og rentabilitet kan være enorm.

- **Problemet**
  Den risiko, som usikrede multifunktionssystemer og printere udgør, er ofte misforstået og ignoreret, eller virksomheden har simpelthen ikke erfaringen og ressourcerne til at løse problemet. Manglende bevidsthed blandt brugere forværrer også problemet, eftersom dårlige vaner udsætter dokumenter og data unødvendigt for risikoen for at blive kompromitteret. Virksomheder forstår de trin, de skal tage for at oprette en udskrivningssikkerhedspolitik, men det kan være en kompleks og tidsforbrugende proces.

- **Anbefalingerne**
  Vi beskriver en række hardware- og softwareløsninger samt anbefalede fremgangsmåder, der kan hjælpe dig med at bygge et sikkert udskriftsmiljø og forhindre uautoriseret adgang til og angreb på virksomhedens netværkstilsluttede enheder. Dette afsnit inkluderer specifikke svar på nogle af de primære sikkerhedsudfordringer:

  - Seks trin til at introducere og vedligeholde sikkerhedsstandarder for udskrivning ved hjælp af en kombination af Sharp-teknologi og Sharps optimerede softwareløsninger.
  - "Out of the box"-funktioner og indstillinger tilgængelige på hver netværkstilsluttede Sharp-enhed i det aktuelle sortiment, f.eks. beskyttelse med adgangskode, dataoverskrivning, kryptering osv.
  - Valgfrie løsninger, der hjælper dig med at bygge en konsistent udskrivningssikkerhedspolitik og administrere printerflåder nemt og effektivt, f.eks. Sharp Remove Device Manager (SRDM).
  - Valgfrie avancerede funktioner til multifunktionssystem/printer og ekstraudstyr, f.eks. Data Security Kit (DSK).
  - Valgfrie tjenester tilgængelige gennem den direkte Sharp-kanal, f.eks. sikkerhedsrevision, sikkerhed som en tjeneste, sletning ved lejens udløb osv.

- **Konklusionen**
  Vi giver en sammenfatning af følgende:

  - Resultaterne for virksomhedssårbarheder vedrørende hvert enkelt netværkstilsluttet multifunktionssystem og printer
  - Vores anbefalinger baseret på de indlejrede Sharp-funktioner og ekstra sikkerhedsløsninger fra Sharp.
  - De næste trin, der er nødvendige for at skabe en udskrivningssikkerhedspolitik – enten ved hjælp af en intern tilgang eller med hjælp og ekspertise fra Sharps professionelle serviceteam.

Baggrund

I løbet af de seneste år har behovet for effektiv IT-sikkerhed vundet større fremspring – men et vigtigt område er blevet overset.

De fleste sikkerhedsbevidste organisationer har sikret, at deres netværks- og computeraktiver er beskyttet med den seneste teknologi: installation af firewalls, indførelse af regler vedrørende adgangskode, brugergodkendelse samt beskyttelse af krypterede og elektronisk signerede data m.m.

Nye teknologier, såsom sky og mobil, giver IT-administratorer og sikkerhedsmedarbejdere yderligere udfordringer. Nutidens intelligente multifunktionssystemer og printere er udviklet til at inkludere mange funktioner inden for netværkskommunikation og datalagring. De er i bund og grund blevet effektive computere med smarte funktioner. I henhold til IDC er der næsten 53 millioner printere og multifunktionsenheder i kontorer og private hjem i Vest- og Østeuropa[1], og de fleste er tilsluttet et netværk. Det betyder, at de er et adgangspunkt med en IP-adresse og er lige så modtagelige for malware og hackerangreb som computere og andre netværkstilsluttede endepunkter. De kræver derfor det samme niveau af sikkerhedsfunktioner for data, kommunikation og information.

25 % af brud på IT-sikkerhed, der krævede afhjælpning, involverede udskrivning.[2]

Hvis multifunktionssystemer efterlades usikrede, kan hackere få adgang til ukontrollerede porte og protokoller, hvilket kan give dem adgang til andre maskiner på netværket eller følsomme oplysninger. Kommunikation og data lagret på et multifunktionssystems harddisk eller hukommelse kan opfanges eller sendes uden tilladelse et hvilket som helst sted i verden. Netværkstilsluttede enheder vil også være åbne for DoS-angreb (Denial of Service), som er designet til at gøre netværksressourcer utilgængelige for slutbrugere med en deraf følgende påvirkning på virksomhedsproduktivitet. De kan også give en åben gateway til phishing-angreb, som er designet til at indhente fortrolige oplysninger eller at introducere vira i netværket.

Og det er ikke kun reklamegas – det er en meget reel trussel. I en nylig IDC-undersøgelse angav mere end 1 ud af 4 svarpersoner et væsentligt brud på IT-sikkerhed, der krævede afhjælpning, og mere end 25 % af disse hændelser involverede udskrivning.[2]

Mangel på at beskytte multifunktionssystemer og printere kan resultere i ødelæggende skade for en virksomhed – samt dens ry og kundetillid. Effekterne af et sådant brud kan inkludere:

- Tab af indtægt
- Tab af produktivitet uden adgang til data og netværket
- Tab af konkurrenceevne på grund af stjålne oplysninger
- Bøder på grund af ikke-overholdelse af regler
- Søgsmål
- Uautoriseret brug af udstyr og netværksressourcer.

Problem

Hackeraktiviteter og cyberangreb er blevet "normen", og uanset din virksomhedstype og -størrelse, er truslen af malware-aktivitet, der påvirker din drift, meget virkelig – og nært forestående.

Det kan overraske dig at vide, at ifølge en undersøgelse fra Quocirca indrømmede 63 % af de virksomheder, der deltog i undersøgelsen, at have oplevet et eller flere udskriftsrelaterede databrud[3].

Så hvorfor har virksomheder ikke gjort mere for at bekæmpe truslen?

Desværre er den potentielle risiko ofte overset på grund af en manglende forståelse af de sårbarheder, der skabes, når enheder som f.eks. multifunktionssystemer og printere indlejres i virksomhedens netværk. Derfor mangler mange virksomheder – eller har utilstrækkelige – udskriftssikkerhedssystemer og -værktøjer, herunderuddannet personale og sikkerhedsprocedurer vedrørende brugen af netværkstilsluttede enheder i virksomheden. Eller de bruger enheder til virksomhedsformål, som reelt er designet til hjemmebrug og har begrænsede sikkerhedsfunktioner.

Særligt har små og mellemstore virksomheder eventuelt ikke introduceret nogen sikkerhedsforanstaltninger for udskrivning og/eller undergået en sikkerhedsrevision vedrørende udskrivning. Større organisationer kan have utilstrækkelige menneskelige ressourcer eller kvalitetsværktøjer til at måle, kontrollere og forhindre cyberangreb på netværksenheder og tilsluttede teknologier.

Derudover er dårlig brugerpraksis ofte en alvorlig udfordring for IT-administratorer, da det kan forårsage alvorlige sikkerhedsproblemer for virksomheden. Disse kan inkludere usikret udskrivning, efterlade dokumenter ubevogtet på multifunktionssystemet/printerudkastbakkerne, udskrivning fra usikrede USB-drev, udskrivning uden endepunkt til endepunkt-kryptering eller lagring af følsomme dokumenter på multifunktionssystemets/printerens harddisk.

Næsten to tredjedele af virksomheder har oplevet et udskriftsrelateret databrud.[3]

For mange organisationer kan bortskaffelsen af data, når en kontrakt ophører, også været et reelt problem. Udskrivningsprocessen kan efterlade en kopi af data, som er blevet udskrevet på enheden, på multifunktionssystemets/printerens harddisk. Hvad sker der med dataene, når kontrakten ophører?

Det at opsætte et konsistent netværkssikkerhedssystem eller at introducere en udskrivningssikkerhedspolitik for at registrere og forhindre uautoriseret adgang til en flåde af netværkstilsluttede multifunktionssystemer og printere kan være en kompleks og tidsforbrugende opgave. Du skal med al sandsynlighed gennemgå følgende nøglefaser:

- Forudsige og evaluere potentielle implikationer ved ikke at have et netværkssikkerhedssystem
- Anerkende eksistensen af potentielle sårbarheder, og hvordan de kan skade netværksinfrastrukturen
- Forstå den komplicerede natur af udfordringen, som unægtelig vil variere fra virksomhed til virksomhed
- Finde en intern eller ekstern ressource, der kan hjælpe dig med at håndtere udfordringen
- Identificere værktøjer, der kan overvåge hele flåder af multifunktionssystemer/printere, forhindre uautoriseret adgang til netværkstilsluttede aktiver og advare dig om eventuel mistænkelig aktivitet
- Opsætte og vedligeholde et pålideligt netværkssikkerhedssystem, der omfatter alle de unikke udfordringer, din virksomhed står over for.

Anbefalinger

Hvis alt dette har gjort dig bekymret om din egen netværkssikkerhed, så … OK! Din virksomheds risiko bør ikke undervurderes. Men vær ikke bange.

Vores mål er et præsentere en enkelt måde til at introducere omfattende udskrivningssikkerhedsforanstaltninger for din virksomhed og indikere, hvordan Sharp kan hjælpe dig med at forstå og hæve dine netværkssikkerhedsniveauer nemt og uden besvær.

Slå øjeblikkelig beskyttelse til

En undersøgelse foretaget af brancheanalytikeren IDC har vist, at "Hardcopyadministrerede teknologiudbydere af udskrift- og dokumenttjenester koncentrerer deres bestræbelser på udskrivningsenhedssikkerhed, der forhindrer hackere i at trænge ind i virksomhedsnetværk via udskrivningsenheder."[4] Mange virksomheder overser dog eller opsætter ikke sikkerhedsindstillinger korrekt, hvilket kan gøre dem sårbare for angreb.

Følgende er en liste over sikkerhedsfunktioner og -indstillinger, der er tilgængelig "out of the box" på alle Sharps multifunktionssystemer og printere, som kan give en "hurtig løsning". De kan alle hurtigt slås til eller fra eller justeres af IT-administratoren for at ændre standardsikkerhedsniveauerne og give et mere effektivt beskyttelsesniveau for dine særlige virksomhedsbehov:

- Lokale administrationsindstillinger, herunder: ændring af administratoradgangskode, adgang til enhedswebside, ekstern driftssikkerhed
- Standardmæssig opsætning af sikkerhedsfunktioner: portkontrol, protokolindstillinger, SNMP MIB-indstilling, adgangsfiltre, SSL, S/MIME, IPSEC, IEEE802.1X, aktivering/deaktivering af mobile udskriftsprotokoller, eksterne serviceindstillinger, offentlig mappe – netværksadresseret server (delt disk), sporings-ID (sporingsinformation vedrørende udskrivning), brugerindstillinger, aktivering/deaktivering af midlertidige løsninger vedrørende brugersikkerhed, automatisk sletning af lagrede filer, sletning af hele spool-køen ved fejl
- Forbedrede sikkerhedsfunktioner (i standardsikkerhedstilstand): overskrivning af HDD-data (sletning af harddisk) efter hver kopi/udskrivning/scanning/fax, lagerkryptering, beskyttelse med adgangskode
- I den samme gruppe er der forskellige avancerede, valgfrie indstillinger. Disse indstillinger kan give IT-administratorer adgang til avancerede Sharp-sikkerhedsfunktioner, som er nyttige for organisationer, der kræver de højeste sikkerhedsniveauer, som f.eks. militær eller statslige organer eller enhver virksomhed, der ønsker at hæve sikkerheden til det højeste niveau:

    - Data Security Kit (DSK) inkluderer: installation af Data Security Kit, datasikkerhedsforbedringer, udskriftsikkerhedsforbedringer, firmware-validering
    - Avancerede Data Security Kit (Advanced DSK) inkluderer: HCD-PP-certificeret avanceret sikkerhedstilstand (inkluderer Data Security Kit), forbedring af lagerkryptering, forbedring af krav om adgangskode, kontrol af firmware-sikkerhed

Seks enkle trin

De følgende seks trin, der ser på sikkerheden fra et langsigtet perspektiv, giver en struktureret måde til at udvikle og introducere dine egne rammer for konsistent netværkssikkerhed.

1. **Sikr adgangen til netværket**
   Alle enheder, der er tilsluttet netværket, er kun så sikre som det mest sårbare punkt på netværket. Derfor er det vigtigt at kontrollere brugen af porte og protokoller for at fastholde netværkssikkerheden. Gennem følsom kalibrering kan IT-administratorer forhindre uønskede aktiviteter og potentielle angreb på infrastrukturen. Teknikkerne til at sikre sikker kommunikation mellem hver enhed og netværket inkluderer:

- Brug af IP-filtrering for at begrænse adgangen til specifikke IP-adresser samt filtrering af medieadgangskontrol (MAC, Media Access Control). Dette hjælper med at beskytte dit netværk og dine kommunikationskanaler ved kun at tillade adgang gennem specificerede IP-adresse eller områder.
- Deaktivering af ubrugte porte (så kun de nødvendige porte virker) giver et ekstra sikkerhedslag og giver dig mere kontrol over dit netværk ved at forhindre uautoriseret adgang til alle tilsluttede aktiver.
- Sørg for, at IPSec (internetprotokolsikkerheden for sikker og krypteret dataudveksling), TLS (Transport Layer Security for krypteret dataoverførsel) og HTTPS (Hypertext Transfer Protocol Secure for sikker netværkskommunikation) er konfigureret for det højeste beskyttelsesniveau.

2. Sikr enheden (for at beskytte dine data)
Der er to måder til at sikre, at dataene, der er lagret på harddiskene (HDD) på multifunktionssystemer og printere, forbliver sikre:

- Datakryptering er proceduren eller funktionaliteten, der krypterer dokumenter ved hjælp af en kompleks 256-bitalgoritme
- Dataoverskrivning er muligheden for datasletning for en enheds harddisk. Den sikrer, at alle data, der allerede er lagret på drevet og eventuelle elektroniske billeder af udskrevne dokumenter, slettes permanent ved at blive overskrevet op til 10 gange.

For ekstra ro i sindet tilbyder Sharp også en servicemulighed ved lejens udløb, der sikrer, at eventuelle data på enheden slettes, og at den fysiske harddisk destrueres.

3. Sikr brugeradgangen (gennem brugeridentifikation og -autorisation)
Et af de vigtigste trin er at få alle brugere under kontrol ved at introducere brugeradministration og -autorisation. I denne kategori består de vigtigste aktiviteter af:

- Brugeridentificering er processen, gennem hvilken administratorer kun giver registrerede brugere adgangsrettigheder til multifunktionssystemer og printere. De skal identificere brugere enten gennem lokal godkendelse baseret på den lokale brugerliste eller netværksgodkendelse gennem autentificeringsserveren.
- Brugergodkendelse anvendes til at give adgang til organisationens netværksaktiver og kontrollere deres brug. Baseret på hver brugers identifikation kan de begrænse adgangen til specifikke personer eller enhedsfunktioner eller helt blokere adgangen. Administratoren kan også konfigurere adgangen til enheden gennem ID-kort, som indeholder brugeridentifikationsdataene.

4. Udskriv fortrolige oplysninger sikkert
Fortrolige dokumenter bør kun udskrives ved hjælp af en sikkerhedsprocedure, der forhindrer uautoriseret adgang og kopiering. Typisk, når et udskriftsjob sendes, placeres det på enhedens harddisk og frigives kun, når brugeren indtaster en PIN-kode, som er blevet konfigureret tidligere. Når dokumentet er blevet udskrevet, slettes alle data automatisk fra harddisken.

5. Kontrollér netværksaktiviteten
Netværkssikkerhedsværktøjer, hvis de indføres korrekt, kan give IT-administratorer fuld kontrol over alle netværkstilsluttede enheder direkte fra deres computere. De kan dermed kontrollere en hel flåde af multifunktionssystemer og printere og også fjernopsætte og -administrere de fleste af de potentielle sikkerhedstrusler. Muligheden for at klone enheder effektiviserer også administratorernes arbejde og giver ekstra ro i sindet, da eventuelle ændringer i enhedsindstillinger nemt kan foretages på tværs af hele flåden.

6. Vælg den rette partner
Der er mange virksomheder, der tilbyder professionelle tjenester i forbindelse med udskrivningssikkerhed, men ekspertiseniveauet kan variere væsentligt. Sharp tager netværkssikkerhed meget alvorligt, og det er centrum for hver enkelt nye produktudvikling. Som producent evalueres vores udstyr ved hjælp af retningslinjer, der er specificeret for den omfattende Common Criteria-certificering. Som resultat heraf er vores netværkstilsluttede multifunktionssystemer med indlejrede datasikkerhedsmuligheder blevet uafhængigt evalueret af det globalt anerkendte japanske system til evaluering og certificering af IT-sikkerhed (JISEC). De er blevet certificeret for at overholde den seneste beskyttelsesprofil for v1.0-standarden for hardcopy-enheder (HCD-PP v1.0) for Common Criteria, hvilket betyder, at vi kan hjælpe mange kunder med at håndtere de mest følsomme data i verden.

Få eksperthjælp

Mens meget af dette kan virke skræmmende, er det vigtigt at huske, at du ikke er alene – der er altid eksperthjælp tilgængelig.

Særligt tilbyder Sharp forskellige løsninger, værktøjer og tjenester for at kontrollere og måle dine netværkssårbarheder, forberede forbedringsplanen og designe mulige scenarier tilgængelige for dig:

- **Seminar om udskriftssikkerhed**
  Vi kan anvende en række værktøjer og teknikker, der kan hjælpe din organisation med at forstå sikkerhedstruslerne, angive konklusionerne og bygge en skræddersyet forbedringsplan.

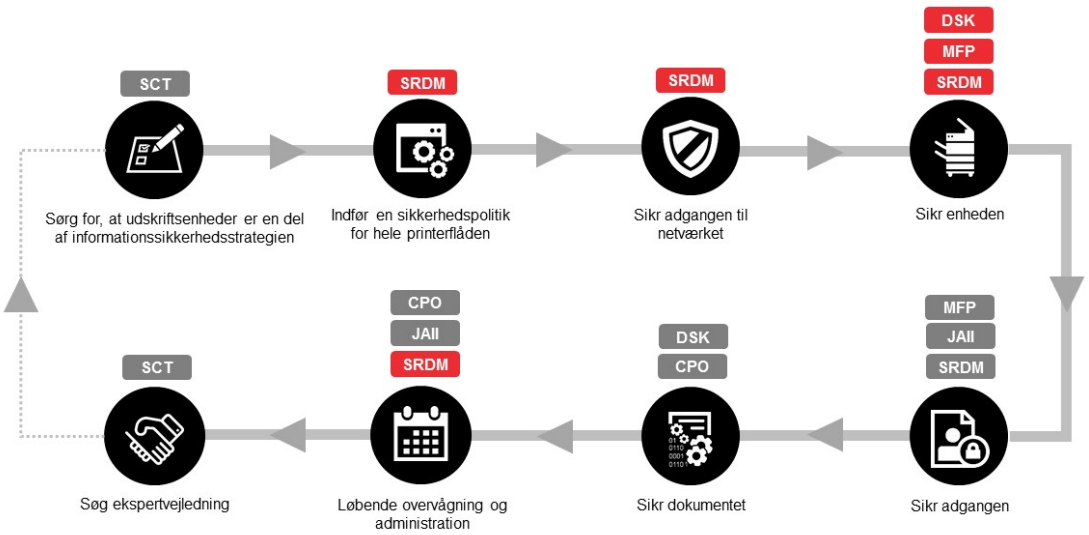
  Revisionen fokuserer på alle netværkstilsluttede enheder og deres sikkerhed. Vi måler alle standardfunktioner og avancerede funktioner, der er tilgængelige for disse enheder, samt værktøjer til effektiv opdagelse og forhindring af trussel. Vi kontrollerer også, om de enheder, du bruger i din virksomhed, er egnet til formålet og kan levere maksimal sikkerhedsbeskyttelse for din virksomhed og brugere. Derudover angiver udskriftssikkerhedsrevisionen de "næste trin" for at introducere en konsistent udskrivningssikkerhedspolitik og dække alle sikkerhedsaspekter i din virksomhed, herunder:

  - Netværkssikkerhed – som beskrevet i dette dokument
  - Printsikkerhed – dækker alle aktiviteter i forbindelse med dokumentudkast, såsom udskrivning, scanning, faxning og e-mailing
  - Dokumentsikkerhed – rettet mod administrationen af elektroniske filer og papirfiler anvendt i dit kontor
  - GDPR-overholdelse – sikrer overholdelse af de seneste EU-bestemmelser vedrørende sikkerhed og beskyttelse af personlige data.

- **Sikkerhedspakke**
  Dette kombinerer et kundeseminar og installation af Sharp Remote Device Manager samt konfiguration af valgfrit udkastadministrationssystem og udrulning for at dække mere af kontorsikkerheden – Netværkssikkerhed og printsikkerhed.

- **Sharp Remote Device Manager (SRDM)**
  Dette Sharp-værktøj hjælper dig med at implementere vigtige sikkerhedsindstillinger på sekunder. Implementeringen leveres som en service af et uddannet Sharp-team. Baseret på dine behov og krav vil alle relevante sikkerhedsindstillinger blive introduceret i dit IT-miljø, og alle multifunktionssystemer og printere fra Sharp vil være under kontrol.

Skabe en udskrivningssikkerhedspolitik og Sharps netværkssikkerhedsløsninger



SCT – Sharps konsulentteam, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – Multifunktionssystem, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Konklusion

Så hvad har vi lært? Den gode nyhed er, at det ikke alt sammen er dårlige nyheder!

Omend multifunktionssystemer og printere udgør en alvorlig (og i øjeblikket undervurderet) trussel mod virksomheder, er der nogle klare trin, du kan tage for at afbøde risikoen.

- **Du er ikke alene – trusler er alle steder.** Hver dag hører vi om databrud, cyberangreb, vira og anden ondsindet aktivitet i virksomheder af alle størrelser. Det vigtigste er at forstå, hvordan din virksomhed kan blive påvirket, hvis den bliver angrebet, og stille spørgsmålet: "Er min virksomhed virkelig forberedt til at forsvare sig selv?"
- **Løsningen er ikke altid enkel.** Det kan tage lang tid at forstå, konfigurere og udføre passende sikkerhedsforanstaltninger og -funktioner, og det kan forårsage reelle implementeringsproblemer. Eftersom hver organisation er forskellig, skal du anvende forskellige værktøjer og introducere unikke strategier, der tackler de specifikke trusler for din virksomhed. Men uanset hvad dine specielle behov er, kan Sharp hjælpe dig med at skabe en effektiv sikkerhedsløsning for at beskytte dine multifunktionssystemer og printere.
- **Hvis din virksomhed ikke er forberedt, så prøv at forstå problemet.** Hvorfor er din virksomhed sårbar? Har den tilstrækkelige værktøjer og ressourcer til at introducere eller forbedre dit netværk og udskrivningssikkerhedspolitik? Eller skal du anvende Sharp-specialister til at gennemgå dine netværk og netværksenheder og introducere relevante sikkerhedsværktøjer i virksomhed.
- **Opsæt dine egne sikkerhedsmål.** For at forstå dine potentielle sårbarheder og det, du behøver for at beskytte dig, skal du besvare spørgsmålet "Hvor skal min organisation være om nogle få år fra nu af?" og "Hvordan kan jeg forberede min virksomhed til at tage de nødvendige trin for at introducere de passende foranstaltninger og værktøjer til at forhindre cyberangreb, malware osv. i fremtiden?".

Sharps sikkerhedsstruktur

- **Ørg for, at du har den rette ekspertise.** Hvis du har de nødvendige ressourcer internt, kan du opbygge din egen udskrivningssikkerhedspolitik. Eller du kan bruge Sharps professionelle serviceteam som hjælp til at opbygge et effektivt sikkerhedssystem og introducere værktøjer, der er relevante for din virksomhedstype og -behov, herunder:

  - Sharps sikre netværksenheder, som er kompatible med de seneste sikkerhedscertifikater.
  - Sharps sikkerhedssoftware, løsninger og tjenester, der hjælper med at skabe en udskrivningssikkerhedspolitik: DSK, SRDM, sikkerhedsrevision af udskrivning osv.

- **Vi er her for at hjælpe.** Vi kan sørge for, at du ikke vil lide under uventede forsinkelser i gennemgangen og implementeringen af din udskrivningssikkerhedspolitik. Sharp-repræsentanter er klar til at hjælpe dig med at forstå dit aktuelle

virksomhedssikkerhedsniveau, gennemgå det og foreslå en strategi, der vil levere en konsistent udskrivningssikkerhedspolitik, som passer til din organisations behov og krav. Vores specialister vil hjælpe dig med at vælge de relevante værktøjer og tjenester fra følgende:

- Sharps standardsikkerhedsfunktioner
- Valgfrie værktøjer, f.eks. SRDM
- Valgfrie forbedringer, f.eks. DSK
- Sharps netværkssikkerhedspakke
- Sharps sikkerhedsrevision
- Udskrivningssikkerhedspolitik.

- **Overvej altid det større billede.** For at undgå potentielle sårbarheder i andre områder af din organisation kan vi hjælpe dig med at indføre yderligere sikkerhedsforanstaltninger fra Sharp-porteføljen, så du kan levere 360-graders sikkerhedsbeskyttelse for ethvert aspekt af din virksomhed:

  - Netværkssikkerhed
  - Printsikkerhed
  - Dokumentsikkerhed
  - Overholdelse af GDPR.

Du kan læse mere om alle vores sikkerhedsløsninger i vores hvidbogsbibliotek eller i afsnittet Informationssikkerhed på vores website: https://www.sharp.dk/cps/rde/xchg/dk/hs.xsl/-/html/informationssikkerhed.htm

Alternativt kan du kontakte Sharps løsningskonsulentteam.

Referencer

1. Rapporten "Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years", IDC, 4. kvartal 2018
2. "IT and Print Security Survey 2015", IDC, september 2015
3. "Printing: a false sense of security", Quocirca, 2013
4. "Transformative Technology in Document Security", IDC, maj 2015

www.sharp.dk

SHARP

Be Original.