Biztonságosan a nyomtatástól a dokumentummenedzsmentig

Pap Kornél
Rendszermérnök

xerox

Négy „komponens”

Végfelhasználói eszközök
(szerver, laptop, PC, tablet, telefon)

Kommunikációs csatorna

Végrehajtó eszközök
(nyomtató, MFP, szkenner)

Szoftverek (driverek, eszközfelügyelet, nyomtatásfelügyelet, digitalizálás,DMS)

xerox

Kapcsolódó feladatok

Dokumentum – információvédelem

Hozzáférés-védelem

Adatvédelem az eszközökön

Kommunikációs csatorna védelme

xerox

Dokumentum - információvédelem

- Classification és ennek megfelelő kezelés
  - vízjel, QR kód, digitális aláírás használata a dokumentumokon az azonosításhoz, eredetiségigazoláshoz
  - megfelelő iratmegsemmisítési szabályozás a fizikai dokumentumok kezeléséhez
- Megfelelő formátumok használata
  - PDF, PDF-A, XPS
- Jelszavas védelem

Hozzáférésvédelem I.

- Multifunkciós nyomtatóeszközökön (MFP vagy MFD) a szolgáltatások használatának szabályozása, zárolása
  - Kiemelten figyelve a másolásra és a szkennelésre (pl.: USB eszközre szkennelés tiltása, Emailbe szkennelés csak saját email címre)
- Nyomtatók és MFP eszközök webes adminisztrációs felületének lezárása, hozzáférés vezérlése
  - Gyári admin megváltoztatása
  - Admin szintek definiálása
  - Szervízmérnök hozzáférésének „vezérlése”

xerox

Hozzáférésvédelem II.

- A nyomtató és MFP eszközök ne jelenítsenek meg semmilyen felhasználható információt (pl.: IP cím, hostnév, fw verzió)
- Használ szoftvermegoldások is képesek legyenek a differenciált jogosultságkezelésre
  - Dokumentum, adat, szoftverfunkció jogosultságkezelése
  - ACL-ek (csoportjogosultságok) használata egy a többhöz kapcsolattal (egy felhasználó több csoport tagja is lehet)
  - Minden jogosultsági feladat csoportra legyen definiálva soha ne felhasználóra

xerox

Adatvédelem az eszközökön I.

- Merevlemez törlés
- Merevlemez titkosítás
- FIPS
- Malwarevédelem
- Up-to-date firmware-ek használata
- A feladatok nevének elrejtése
  (pl.: kinomytatott dokumentumok neve is lehet érzékeny információ)
- Naplózás (jogosultságkezelés a megtekintéshez!)

xerox

Adatvédelem az eszközökön II.

- Backupolás (minimum a konfigurációt)
- Tartományszűrések
  (pl.: email szkennelés esetében kiszolgálandó domain-ek meghatározása)
- IP white / blacklistek használata
- Többlépcsős hitelesítés (szoftvermegoldások esetében)
- Mentés, archiválás, visszaállítás (főleg a szoftvermegoldások esetében)
- Automatikus értesítési, riasztási funkciók
  (szintén első sorban a szoftvermegoldások esetében)

Kommunikációs csatorna védelme I.

- HTTPS használata ahol csak lehetséges
  - Nyomtató és MFP webfelület, kommunikáció kifelé, szkennelések, nyomtatás
- SNMPv3 használata felügyelethez
- IPsec
- 802.1x végponthitelesítés
- Secure LDAP, SMTP
- Külső tanúsítvány
  (amennyiben használatban van saját tanúsítvány kiszolgáló)

xerox

Kommunikációs csatorna védelme II.

- Auto discovery protokollok tiltása (pl.: WSD)
- Nyomtató portneve ne az - alapértelmezetten használt - IP cím legyen
- Mobil elérési lehetőségek (Airprint, Mopria, Google Cloud print) szabályozása, tiltása, mobil nyomtatásra központosított alternatívák használata
- Driveres titkosítás (pl.: AES 256 tikosítással ellátni a driver által előállított nyomtatási állományt)
- Proxy használata (pl.: kifelé történő kommunikációnál)

xerox