Vodnik po zaščiti tiskalnikov in multifunkcijskih naprav

KYOCERA

UVOD

Naprave za tiskanje v podjetjih so od starih samostojnih naprav znatno napredovale. Današnje večopravilne naprave so vključene v omrežja, poganja jih napreden operacijski sistem. Pa vendar so v mnogih organizacijah ostale varnostne črne pege, saj se strokovnjaki za IKT v borbi z grožnjami zlonamerne programske opreme in vdori hekerjev, osredotočajo predvsem na izzive zaščite osrednje infrastrukture, kot so na primer strežniki, delovne postaje in baze podatkov.

V luči vse večje aktivnosti na področju kibernetskega kriminala, ki neposredno cilja na šibke člene sistemov, torej na naprave povezane v omrežje, zanemarjanje tiskalniških naprav predstavlja precejšnje tveganje. Organizacije morajo brez odlašanja sprejeti ukrepe in vključiti večopravilne naprave v svoje strategije varovanja podatkov, sploh ker uredbe, kot je na primer GDPR, prinašajo finančne in pravne posledice, ki so lahko uničujoče za podjetje.

Ta Kyocerin dokument ponuja praktične napotke IT strokovnjakom, kako izkoristiti vgrajene varnostne funkcije večopravilnih naprav in sprejeti dodatne, izboljšane zmogljivosti za zaščito podatkov. Osnovni, srednji in visoki nivo predlaganih zaščitnih ukrepov je zasnovan tako, da v največji možni meri oteži tako neavtoriziran vstop v omrežje organizacije prek večopravilnih naprav, kot izvajanje kriminalnih aktivnosti v primeru nepooblaščenega vstopa, če se ta zgodi.

KAKO ZAVAROVANA JE MOJA NAPRAVA?

Vsi Kyocerini tiskalniki in večopravilne naprave (MFP) imajo vgrajen operacijski sistem. Tako kot osebni računalniki so opremljeni s trdimi diski ali SSD, na katerih lahko uporabnik hrani občutljive podatke. MFP-ji so izpostavljeni številnim naprednim grožnjam, kot so na primer nepooblaščen dostop do naprav prek omrežja, spreminjanje informacij med pretokom po omrežju ali uhajanje podatkov z diskov naprav.

Kyocerine naprave uporabnikom nudijo celo paleto varnostnih funkcij. Dokument je zasnovan kot vodnik za celovito zaščito naprave in je razdeljen na tri področja:

1) **Osnovna raven:** Opisuje izvajanje ukrepov za zaščito z uporabo standardnih lastnosti in funkcionalnosti naprav.

2) **Srednja raven:** Opozori na nekatere dodatne funkcije, ki lahko izboljšajo varnost podatkov in dodatno varujejo napravo.

3) **Visoka raven zaščite:** Prikaže nadaljnje načine za zaščito naprave na ravni omrežja z uporabo dodatne strojne opreme, kot so npr. požarni zidovi.

OSNOVNA RAVEN ZAŠČITE NAPRAV ZA TISKANJE

Ukrepi v tem sklopu so najbolj preprosti in jih je mogoče hitro uvesti, obravnavajo pa zavarovanje varnostnih šibkih točk na najosnovnejši ravni. Kyocera priporoča vsem organizacijam, ki uporabljajo večopravilne naprave, da te osnovne ukrepe uvedejo in dejavno upoštevajo. Dodatni ukrepi naj bodo uvedeni poleg osnovnih in ne namesto njih.

PRIPOROČILA

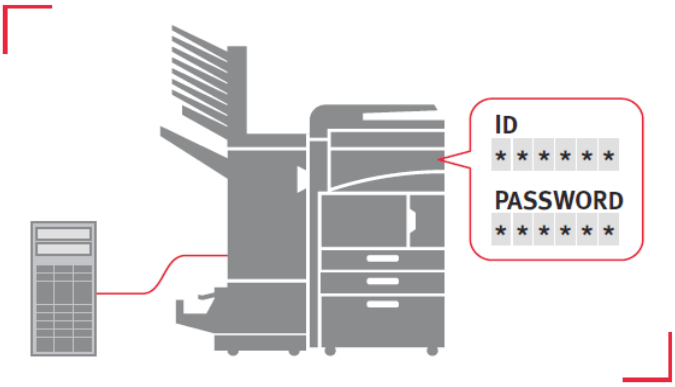
› Spremenite privzeto skrbniško geslo
› Uporabite metodo avtentikacije
› Izklopite protokole, ki niso potrebni / zaklenite neuporabljena komunikacijska vrata
› Uporabljajte varne komunikacijske protokole
› Zaklepajte nadzorno ploščo
› Onemogočite funkcije USB vrat in dodatnih vmesnikov
› Uvedite omejitve E-pošte / skeniranja / pošiljanja

Spremenite privzeto geslo skrbnika

Naprave so tovarniško opremljene s privzetim geslom. Zelo priporočljivo je, da ga spremenite. Izberite primerno močno geslo, ki je skladno z varnostno politiko podjetja. Ne uporabljajte enakega gesla ali uporabniškega imena, ki ga uporabljate za prijavo v svoj osebni računalnik. Opomba: v primeru, da pozabite geslo za prijavo v večopravilno napravo, bo naprava zahtevala, da tovarniško ponastavitev izvede Kyocerin tehnik.

Uporabite metodo avtentikacije

Naprave KYOCERA podpirajo različne načine prijave uporabnika. Dostop je razdeljen na tri ravni - uporabnik, administrator in skrbnik naprave. Stopnje zaščite lahko spreminja samo skrbnik naprave. Uporabnikom, ki se ne morejo prijaviti v napravo, lahko skrbnik dovoli uporabljati funkcije naprave v omejenem obsegu.



Lokalna avtentikacija: potrjuje uporabnike na osnovi uporabniških podatkov, ki so registrirani na lokalnem seznamu uporabnikov v tiskalniku ali večopravilni napravi. Do funkcij naprave lahko dostopajo le registrirani uporabniki.

Omrežna avtentikacija: avtentikacija preko domenskega krmilnika. Podprte so metode NTLM in Kerberos. Omogoča uvedbo politike ustvarjanja gesel, vključno s predpisano kompleksnostjo in časom veljavnosti, kot tudi z beleženjem neuspelih poskusov prijave.

Funkcije za goste: ko je omogočena administracija za prijavo, se lahko uvede status gosta. V tem načinu je mogoče dostopati do omejenega nabora funkcij brez prijave v napravo. Način je primeren tudi za zmanjševanje stroškov tiskanja. V načinu za goste lahko, na primer, omejimo tiskanje v barvah, tako da je funkcija barvnega tiskanja rezervirana le za registrirane uporabnike. Ta raven varnosti lahko zaščiti napravo pred uhajanjem informacij, hkrati pa ohranja uporabniško prijaznost.

Uporaba protokola za omrežno avtentikacijo je učinkovita metoda za zagotavljanje varne komunikacije. Tiskalniki in večopravilne naprave Kyocera podpirajo omrežno avtentikacijo IEEE802.1x, avtentikacijo SMTP in protokol POP pred SMTP, kadar uporabljate funkcijo ‘send to email’ **(glej prilogo A – Protokoli za avtentikacijo).**

Izklopite protokole, ki niso potrebni / zaklenite neuporabljena komunikacijska vrata

Stopnja varnosti omrežja: tiskalniki in večopravilne naprave Kyocera lahko omejujejo komunikacije v omrežju za sprejem / posredovanje na določenem obsegu IP naslovov in številk vrat.

Filter IP naslovov: omejuje omrežni dostop do tiskalnikov in MFPjev. Kot nezaželen lahko določite izbor naslovov IP ali vrst protokolov. **(glej Dodatek B - Vrata in protokoli).**

Uporabljajte varne protokole

Varni komunikacijski protokoli zagotavljajo varno zaščito omrežnega komunikacijskega kanala. Glede na namen ali načrt kodiranja so na voljo različni komunikacijski protokoli, ki
učinkovito ščitijo podatke pred spremembami ali uhajanjem prek omrežja. **(Glejte Dodatek C - Protokoli za varno komunikacijo).**

Zaklepajte nadzorno ploščo

S funkcijo delnega zaklepanja lahko onemogočite izbrane funkcije. Ima tri nivoje: uporaba nadzorne plošče, upravljanje opravil tiskanja in izvedba naročila tiskanja ter nastavitve dela s papirjem. Zaklepanje nadzorne plošče omogoča blokiranje dostopa do nastavitev sistema in nastavitev brisanja opravil.

Onemogočite funkcije USB vrat in dodatnih vmesnikov

Če je preko USB vhoda na večopravilno napravo povezan zunanji disk za hrambo podatkov, obstaja tveganje izgube podatkov ali nepooblaščenega dostopa do podatkov, shranjenih v napravi. Administrator ima možnost izključiti funkcijo USB Storage Class, ki onemogoči uporabo naprav za shranjevanje, obenem pa dovoljuje priključitev drugih USB naprav, kot so na primer čitalci kartic, tipkovnice in podobno. Za preprečevanje namestitve neavtoriziranih vmesnikov pa lahko administrator onemogoči funkcijo Optional Interfaces (Reži 1 & 2).

Nastavite omejitve E-pošte / skeniranja / pošiljanja

Z uporabo funkcije Email Send Restriction lahko administrator omeji dovoljenje za pošiljanje na izbrane e-poštne naslove. Naslovi, na katere je pošiljanje dovoljeno, se vnaprej registrirajo, kakor tudi naslovi, na katere pošiljanje ni dovoljeno.

Sprejemanje elektronske pošte lahko omejite s funkcijo omejevanja pošiljatelja e-pošte na podlagi predregistracije. Naslovi pošiljateljev, ki jim dovolite, da vam pošiljajo e-pošto, so vnaprej registrirani, tako da se lahko e-poštna sporočila sprejemajo le od pošiljatelja, ki je na seznamu dovoljenih. Zavrnjeni naslovi pošiljateljev so tudi vnaprej registrirani, tako da bodo zavrnjena tudi vhodna e-poštna sporočila s seznama nedovoljenih naslovov. Kyocerine naprave so opremljene tudi s funkcijo tiskanja datotek, ki so pripete k e-poštnim sporočilom.

PDF geslo in kodiranje: funkcija Encrypted PDF omogoča uporabnikom, da za format datoteke določijo PDF ali kompresiran PDF, ki ponujata dodatno zaščito s kodiranjem in nastavljanjem gesla. Omejevanje se izraža tako, da mora uporabnik pri odpiranju, tiskanju ali spreminjanju prejete datoteke PDF vnesti pravilno geslo.

SREDNJA RAVEN ZAŠČITE NAPRAV ZA TISKANJE

Ukrepi, opisani v tem delu, dopolnjujejo prvo raven zaščite. Predlagamo, da najprej izvedete osnovne ukrepe zaščite in nato v nadaljevanju opisane dodate kot dodatno zavarovanje sistema in podatkov. Na voljo so kot dodatni moduli za vse Kyocerine večopravilne naprave.

PRIPOROČILA

› Omogočite zaščito podatkov na HDD / SSD
› Dostop z uporabo kartic ID / RFID
› Zaščitite shrambo opravil za tiskanje
› Uporabite varno tiskanje
› Omogočite zaščito pred kopiranjem

Omogočite zaščito podatkov na HDD / SSD

Na trdem ali SSD disku v napravi so lahko shranjeni občutljivi ali zaupni podatki podjetja. Zato je možno uvesti dodatne varnostne ukrepe, ki so v skladu s standardom ISO 15408. Ti ukrepi vključujejo:

HDD/SSD KODIRANJE

Funkcija kodiranja HDD / SSD je varnostna funkcija. Kodira dokumente, uporabniške nastavitve in podatke o napravi, shranjene na trdem disku ali SSD. Kodiranje se uporablja za podatke z uporabo 128-bitnih in 256-bitnih algoritmov AES (Advanced Encryption Standard: FIPS PUB 197). Če je trdi disk ali SSD disk odstranjen iz večopravilne naprave, občutljivi ali zaupni podatki, shranjeni na trdem disku ali SSD, ne bodo dostopni.

HDD PREPIS IN IZBRIS PODATKOV

HDD Overwrite-Erase (prepis in izbris) je varnostna funkcija, ki onemogoči tretjim osebam dostop do podatkov, kot so na primer uporabniške nastavitve, podatki o napravi in podatki o slikah shranjenih na disku naprave.
Pri tiskanju in kopiranju se skenirani podatki začasno shranijo na trdem disku naprave. Uporabniki tudi vnesejo različne nastavitve, kot so na primer destinacija skeniranja in e-naslovi, ki so shranjeni v napravi. Ti podatki ostanejo shranjeni na disku dokler niso prepisani z drugimi podatki, tudi potem ko uporabnik dokument natisne ali izbriše z diska. Obstaja možnost, da se podatki, ki ostanejo na disku, z uporabo posebnih orodij in pripomočkov obnovijo, kar predstavlja varnostno grožnjo.

Funkcija HDD Overwrite-Erase deluje tako, da področja na disku, kjer so bili zapisani podatki, prepiše z nizom naključnih in nesmiselnih podatkov in tako prepreči obnavljanje za podjetje pomembnih informacij. Ukrep prepisovanja in izbrisa se izvaja samodejno, tako da zagon procesa s strani uporabnika ni potreben. Podatki na trdem disku se prepišejo takoj, tudi če je bilo opravilo med izvedbo preklicano ali neposredno po končanem opravilu.

Za večopravilne naprave Kyocera so na voljo tri metode prepisa in izbrisa podatkov s trdega diska.

ENKRATEN PREPIS IN IZBRIS

Območje na disku s podatki, ki jih več ne potrebujemo, je prepisano enkrat, z ničlami (null data) in jih je zelo težko obnoviti.

TRIKRATEN PREPIS IN IZBRIS

Območje na disku s podatki, ki jih več ne potrebujemo, je prepisano dvakrat z naključnimi podatki in nato še enkrat z ničlami (null data). Trikratno prepisovanje območja na disku učinkovito onemogoči obnovitev, tudi v primeru uporabe sofisticiranih tehnik obnavljanja podatkov in je znatno bolj zanesljiva od enkratne metode. V primeru brisanja večje količine podatkov, lahko postopek traja nekoliko dlje.

U.S. DEPARTMENT OF DEFENCE DOD 5220.22-M (TRIJE PREPISI)

Metoda DoD 5220.22-M s tremi prehodi prepisovanja pomeni v primerjavi z zgoraj opisanima najvišji nivo zaščite. Z uporabo te metode je možnost uhajanja informacij znatno zmanjšana.

Dostop z uporabo kartic ID / RFID

V organizacijah, kjer za dostop v objekt ali za upravljanje z delovnim časom, uporabljajo kartice ID, lahko te uporabijo tudi za prijavo na tiskalnike ali večopravilne naprave. Niihova uporaba je priročna in ponuja dodatno učinkovitost.

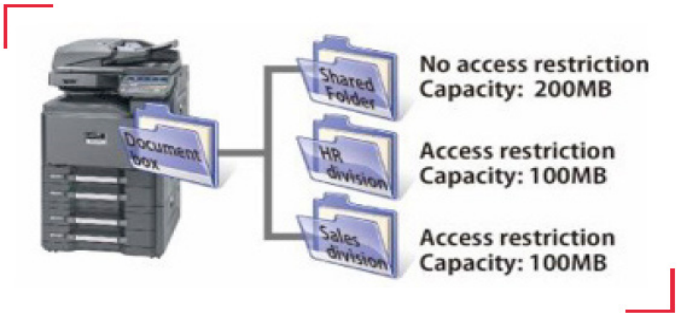
V kombinaciji s funkcijo Job Storage (Nabiralnik opravil), ki je na voljo v operacijskem sistemu večopravilnih naprav, lahko tako uporabniki varno dostopajo do svojih dokumentov, ki so jih poslali v izpis.

Nabiralnik opravil (Job Storage)

Na večopravilnih napravah lahko uporabniki ustvarijo različne nabiralnike v katerih se hranijo prejeti in že natisnjeni podatki. Dostop do podatkov, ki se v njih hranijo, je mogoče omejiti.

NABIRALNIK UPORABNIKA (User Box)

Uporabniki lahko ustvarijo lastne nabiralnike, v katerih hranijo svoje podatke. Za posamične nabiralnike lahko nastavijo omejitve uporabe, čas hrambe podatkov in gesla.



V User Box lahko vstopa le uporabnik, ki je registriran kot lastnik nabiralnika, neavtoriziran vstop ni možen. V primeru, da bi želel omogočiti dostop drugim osebam, mora uporabnik ustvariti Skupni nabiralnik (Shared Box).
Po časovnem obdobju, ki ga določi skrbnik, se lahko shranjeni podatki dokumenta samodejno izbrišejo, kar omogoča učinkovito samodejno upravljanje s trdim diskom in varnostjo podatkov.

NABIRALNIK OPRAVIL (Job Box)

Podatki o zasebnem tiskanju, hitrem kopiranju, shranjenih opravilih ali za funkcijo Proof and Hold, se lahko shranijo v nabiralniku opravil. Job Boxa uporabnik ne more sam ustvariti ali brisati. Dostop do nabiralnika opravil lahko zaščitite s kodo PIN. Shranjeni podatki o dokumentu se lahko po določenem času samodejno izbrišejo, kar omogoča učinkovito samodejno upravljanje s trdim diskom in varnostjo podatkov.

NABIRALNIK FAKS SPOROČIL (Fax Box)

V tem nabiralniku se zbirajo podatki o faks sporočilih. Hrambo podatkov v Fax Boxu nastavite z uporabo funkcije Memory Forward. Podatki bodo dodeljeni v posamezne nabiralnike na osnovi podnaslova pošiljatelja ali faks številke. Uporabnik lahko podatke o prejetih faks sporočilih preveri v predogledu na nadzorni plošči večopravilne naprave in se odloči ali bo sporočilo takoj natisnil, neželena sporočila pa lahko tudi izbriše.

Varno tiskanje (Secure Print)

Secure Print je funkcija tiskanja na tiskalnikih ali večopravilnih napravah in se uporablja za tiskanje zaupnih ali zasebnih dokumentov. Funkcija zagotavlja, da na odlagalnih policah naprave, kjer bi bili na voljo nepooblaščenim osebam, ne ostajajo natisnjeni dokumenti.

ZASEBNO TISKANJE (Private Print)

Private print je funkcija, ki zadržuje naročila tiskanja, poslana z uporabnikovega računalnika na tiskalnik ali večopravilno napravo, vse dotlej, dokler ni vnešeno ustrezno geslo na nadzorni plošči naprave. Uporabnik mora v gonilniku tiskalnika pred pošiljanjem opravila iz delovne postaje nastaviti kodo za dostop in jo znova vnesti na napravi pred tiskanjem dokumenta.

Zaščita kopiranja

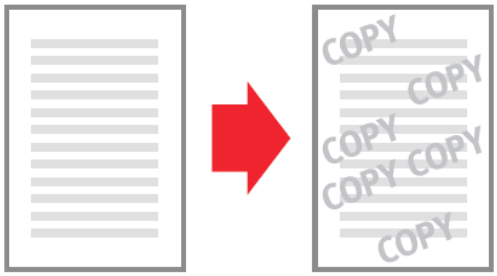
Pri kopiranju vam bodo funkcije z dodatnimi možnostmi zaščite dokumentov, ki so opisane v nadaljevanju, pomagale preprečiti nepooblaščeno kopiranje.

TEKSTUALNE OZNAKE / OZNAKE BATES

Glede na vrsto dokumenta, ki ga uporabnik namerava natisniti, lahko izbira med oznakami (žigi) “Confidential”, “Do Not Duplicate” in “Privacy”. Oznake so natisnjene preko besedila ali slike dokumenta. Uporabniki lahko besedilo oznake po želji spreminjajo. Oznaka Bates “Serial Number” bo na dokument natisnila serijsko številko naprave na kateri je dokument izpisan in oštevilčila strani dokumenta. Poleg tega pa so na voljo še možnosti za dodajanje datuma in uporabniškega imena.

VODNI ŽIG

V natisnjeni dokument lahko uporabniki vgradijo tudi vodni žig z varnostnim vzorcem ali besedilom. V primeru, ko kopiranje dokumenta ni dovoljeno, bo vodni žig postal viden, kar jasno pokaže na nepooblaščeno kopiranje.



DOCUMENT GUARD KIT

Document Guard Kit je dodatna funkcija, ki v dokument vgradi varnostni vzorec. V primeru, da uporabnik poskuša kopirati, skenirati ali faksirati dokument, ki je opremljen s to funkcijo, bo naprava prenehala z delovanjem in tako preprečila nedovoljeno dejanje. Tako učinkovito preprečuje uhajanje dragocenih podatkov podjetja. Če Document Guard Kit na napravi ni nameščen, se bo pojavil vodni žig z varnostnim vzorcem, ki opozarja, da gre za nepooblaščeno kopija dokumenta.

VISOKA RAVEN ZAŠČITE NAPRAV ZA TISKANJE

Zadnja skupina ukrepov prinaša smernice o vrstah naprednih varnostnih zmogljivosti, povezanih z večopravilnimi napravami, ki so na voljo ob uporabi komplementarnih rešitev. Uporabnikom svetujemo, da jih uveljavijo kot dopolnilo k temeljnim ukrepom, ki so podrobno opisani na osnovni in srednji ravni.

PRIPOROČILA

› Uveljavite rešitve za nadzor tiskanja
› Uporabite povezave VPN
› Omogočite spremljanje omrežnih podatkov

Rešitve za nadzor tiskanja

Obstaja veliko različnih vrst nadzornih sistemov za tiskanje, ki ponujajo prihranke in nadzor. Prav tako vsi ponujajo tudi načine za zagotavljanje varnosti podatkov v prenosu po omrežju.

Osnovna predpostavka rešitev za nadzor tiskanja je, da uporabnik pošlje opravilo v skupno »virtualno« čakalno vrsto, ki je shranjena na centralnem tiskalnem strežniku. Naročilo je shranjeno na strežniku, dokler se uporabnik ne prijavi na napravo in izbere opravila, ki jih želi natisniti. Nato je opravilo tiskanja poslano na napravo, ki izpiše izbrane dokumente, na strežniku pa se zapišejo revizijski podatki za namene poročanja.

Metoda ponuja številne prednosti:

› Opravila tiskanja so dostavljena šele, ko je uporabnik prisoten pri napravi.
› Informacije niso shranjene na napravi.
› Možne so nastavitve omejitev za posamezne uporabnike.
› Zmanjšani so stroški tiskanja.
› Ponuja izboljšano varnost naprav.

NUANCE

myQ

KYOCERA Net Manager

Cirrato
Reimagine printing

drivve | print

PaperCut

CENTRALIZIRANI TISKALNIŠKI STREŽNIKI / TISKANJE IZ ZASEBNEGA OBLAKA

V zadnjem času so se nekateri sistemi za nadzor tiskanja še dodatno nadgradili in rešujejo težave izkoriščanja pasovne širine v povezavi z varnostjo podatkov pri tiskanju na zunanje strežnike oziroma na strežnike nameščene v oblaku.

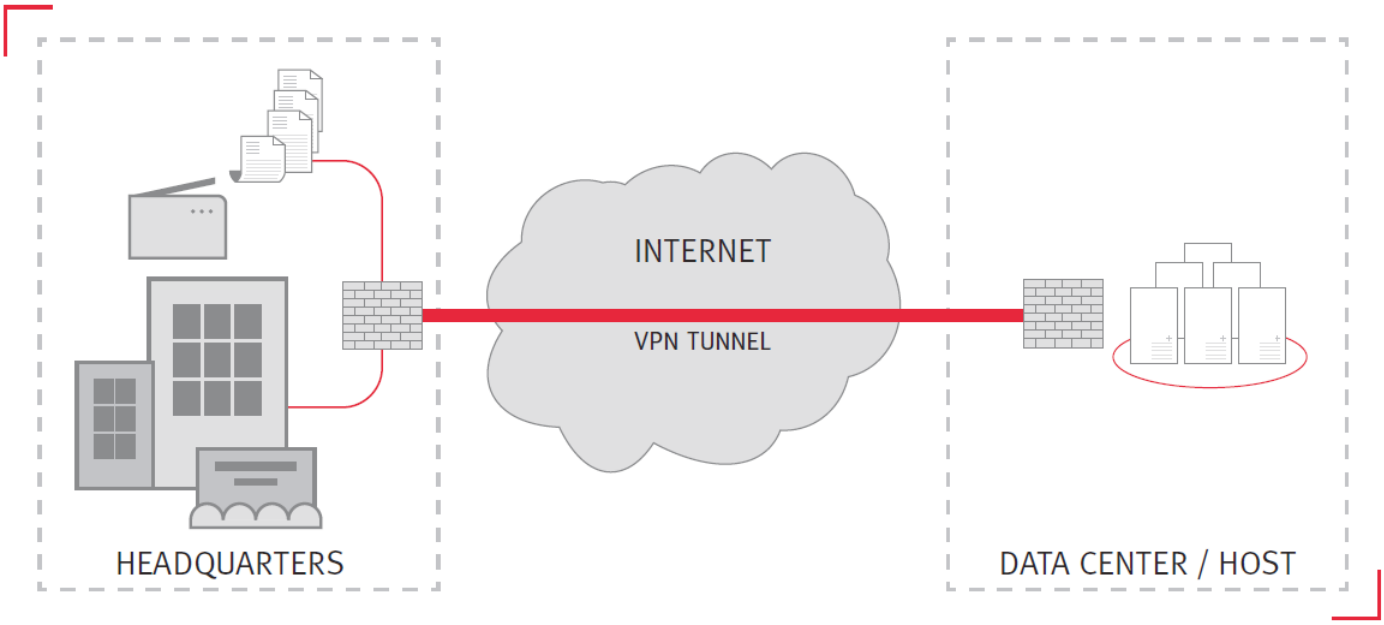
V ta namen se uporablja proces imenovan Local Print Spooling – pošiljanje opravila v vmesno shrambo. Dokument ostane shranjen v lokalnem omrežju, na uporabnikovem osebnem računalniku ali izbrani večopravilni napravi, na strežnik pa se pošlje le revizijske podatke in informacije o načinu tiskanja. Zadržano opravilo je poslano v izpis šele, ko se uporabnik na napravi identificira. Ta metoda izdatno zmanjšuje uporabo pasovne širine in ohranja dokument znotraj lokalnega omrežja. Lahko se uporabi tudi dodatni sekundarni lokalni strežnik, ki upravlja naprave, uporabnike in revizijske podatke, ki jih je mogoče sinhronizirati z osrednjim glavnim strežnikom.

Najnovejše aplikacije lahko nadzorujejo tudi dostop do skeniranja, omejijo destinacije in nastavitve z dovoljenji za dostop. Dovoljenja lahko določajo za vse uporabnike, skupine ali le za posameznike.

KYOCERA lahko pomaga pri izbiri najboljših rešitev za zahteve vaše organizacije. Za več informacij se obrnite na lokalne predstavnike.

Povezave VPN (Virtual Private Network)

Virtualno zasebno omrežje (VPN) je zelo varen način povezovanja pisarniške omrežne infrastrukture v javnem omrežju. Vsi podatki, ki potujejo po teh povezavah, so kodirani, zato ga je varno uporabljati tudi v javnih omrežjih. VPN zahteva specializirano opremo, namestiti pa ga mora usposobljeno osebje, da ustvari varen VPN tunel. V uporabi sta dve vrsti VPN-ov: Site to Site in Client Based Connection. Slednja se uporablja kot “ad-hoc” način povezave med posameznima klientoma prek mobilne naprave, medtem ko je Site to Site navadno uporabljena za povezovanje pisarniške infrastrukture.



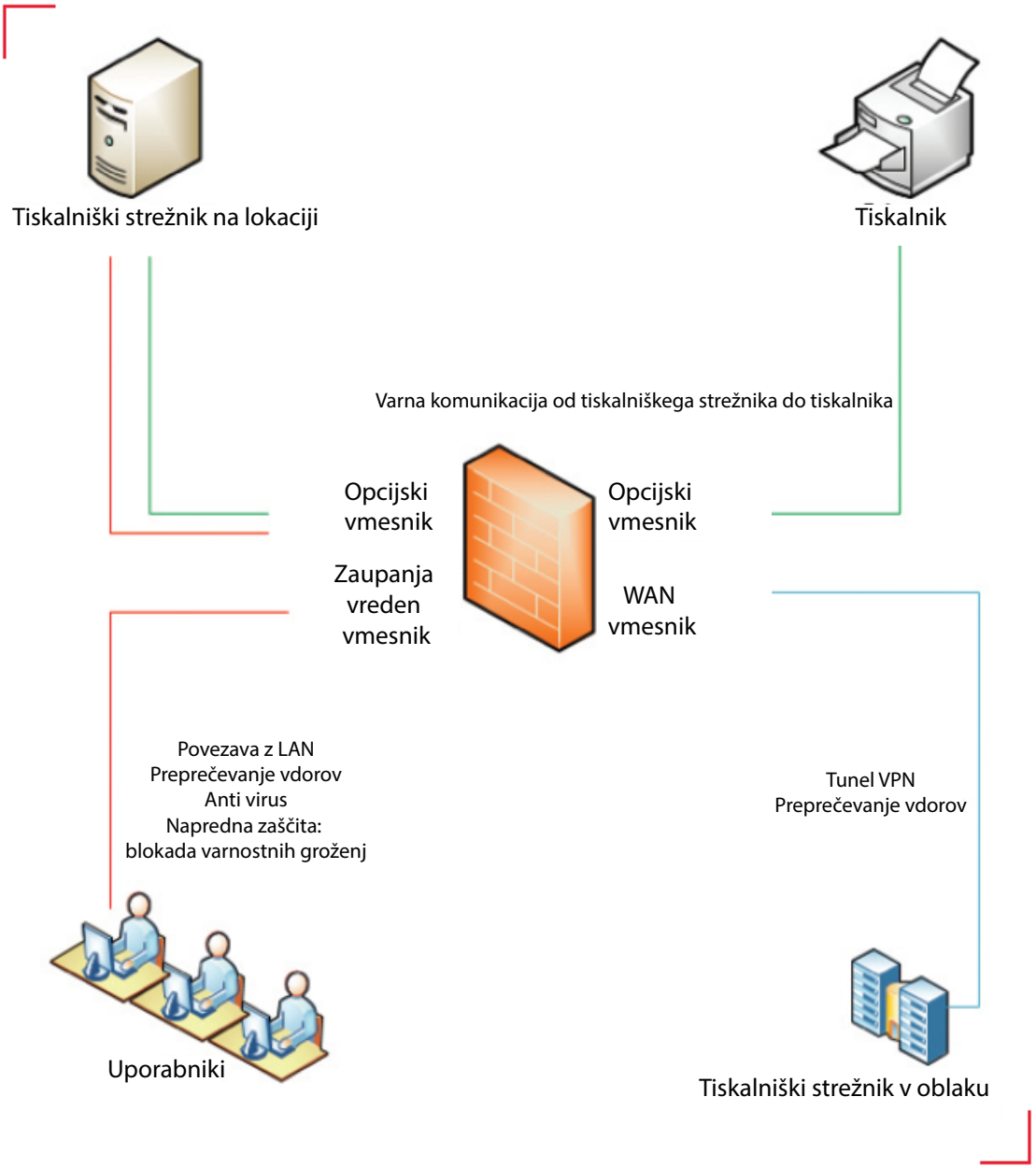
SPREMLJANJE OMREŽNIH POVEZAV

Dejanske in potencialne grožnje varnosti večopravilnih naprav povezanih v omrežje so neizogibne. Kibernetni kriminalci si prizadevajo pridobiti trajno in čimbolj celovito prisotnost v omrežju. Večopravilne naprave uporabljajo napredne operacijske sisteme, zato so lahko potencialne tarče za krajo podatkov, kot tudi poverilnic uporabnikov in omrežja.

Uporaba naprav za spremljanje omrežja, kot je na primer WatchGuard, in povezovanje naprav v ločena podomrežja, omogoča enoti, da deluje kot prehod za dohodni in izhodni promet do tiskalniških naprav. Obenem pa naprava podpira spremljanje podatkovnih paketov, da se preko njih ne vnašajo potencialne grožnje.

Zlonamerna programska oprema je že zdavnaj prehitela tradicionalne viruse kot najbolj razširjeno grožnjo varnosti. Nove vrste napredne programske opreme poznamo tudi po imenu Advanced Persistent Threats (Napredne stalne grožnje - APTs).

Naprava WatchGuard sproti dobiva posodobitve in opise najnovejših groženj iz shrambe v oblaku in v primeru, da zazna zlonamerno programsko opremo, jo takoj blokira na požarnem zidu. V nekaterih primerih, ko grožnja izkorišča neznano luknjo v sistemu, ki še ni znana in opisana v shrambi v oblaku, se lahko zgodi, da se izogne blokadi, medtem pa poteka analiza v oblaku. V takih primerih lahko sistem WatchGuard takoj zagotovi opozorila, da je v omrežju sumljiv del kode in osebje v oddelku IT organizacije lahko po svoji presoji ukrepa.

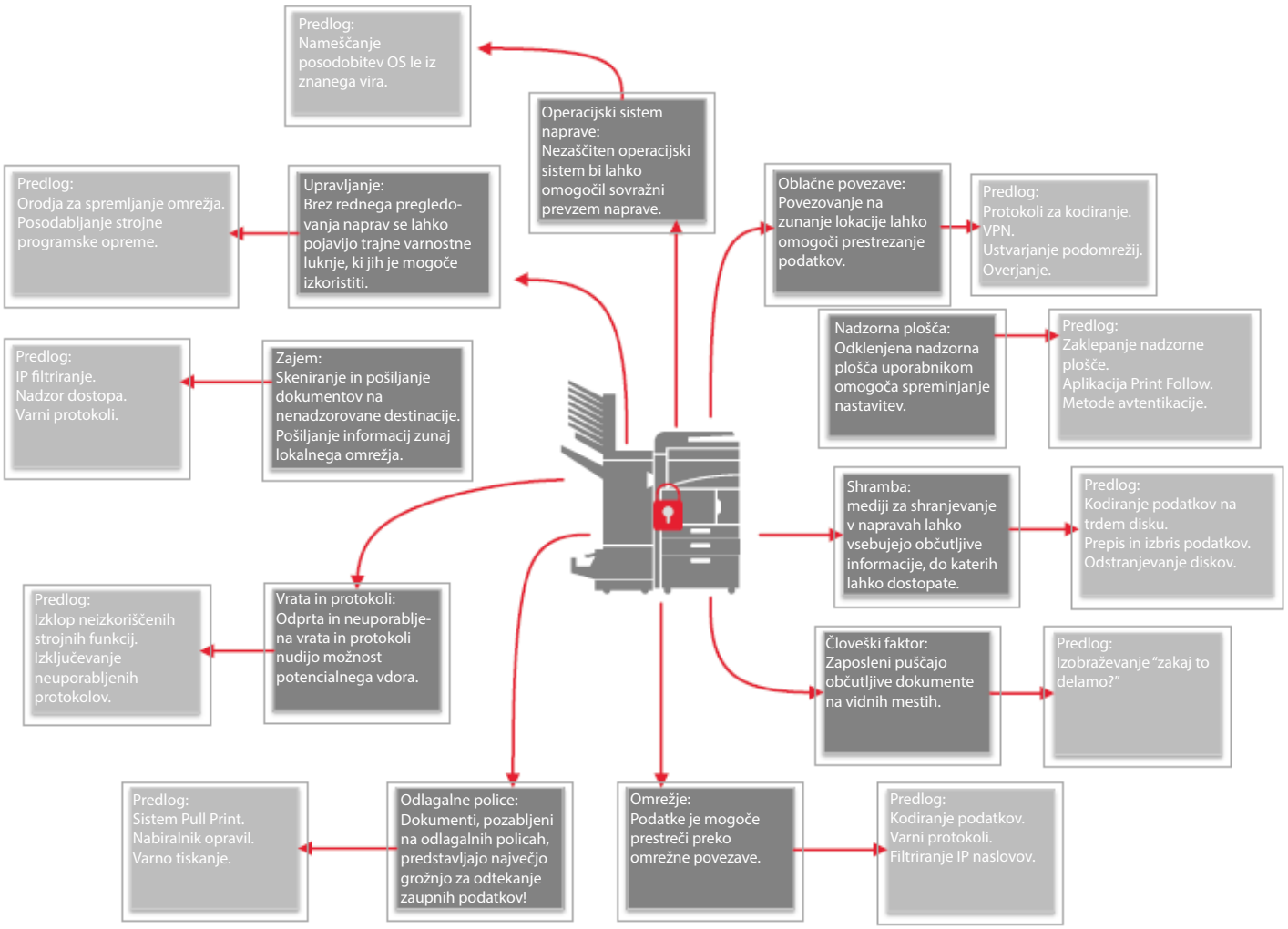


ZAKLJUČEK

Strokovnjaki IT morajo upoštevati večopravilne naprave kot del strateškega pristopa k varnosti omrežij in podatkov. Organizacije lahko začnejo z najpreprostejšimi koraki, opisanimi v tem dokumentu, in si po potrebi prizadevati za bolj poglobljene ukrepe ter si s tem zagotoviti varnost občutljivih podatkov pred napadi kibernetskih kriminalcev.

Poleg tega morajo strokovnjaki za informacijske tehnologije v kontekstu vse bolj intenzivnih razprav o zagotavljanju varnosti »interneta stvari«, kot tudi zagotavljanju skladnosti z uredbami o varovanju podatkov, kot je npr. GDPR, izkoristiti prvo razpoložljivo priložnost za pretvorbo večopravilnih naprav iz varnostne slepe pege v vidno komponento svoje omrežne informacijske infrastrukture.

Potrebni ukrepi so sorazmerno preprosti in poceni, toda posledice neukrepanja bi se lahko izkazale za zelo boleče.



PRILOGA A

Avtentikacijski protokoli

IEEE802.1x
Pri povezovanju z omrežjem ta protokol omogoča vzpostavitev komunikacije samo pooblaščenim uporabnikom (in overjenim napravam) in preprečuje, da bi se nepooblaščene naprave povezale v omrežje. Naprave KYOCERA podpirajo protokol IEEE802.1x, ki nepooblaščenim strankam ne dovoljuje dostopa do omrežja in občutljivih podatkov. Tiskalniki in večopravilne naprave KYOCERA uporabljajo šest načinov avtentikacije, kot je opisano spodaj.

PEAP-TLS/PEAP (Protected Extensible Authentication Protocol-Transport Layer Security)
Klient je overjen na podlagi uporabniškega imena in certifikata, hkrati pa protokol preveri tudi certifikat avtentikacijskega strežnika.

EAP-PEAP (Extensible Authentication Protocol-Protocol Extensible Authentication Protocol)
Klient je overjen na podlagi uporabniškega imena in gesla, hkrati preveri le splošno ime certifikata avtentikacijskega strežnika.

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling)
EAP-FAST je metoda za preverjanje pristnosti IEEE802.1.x / EAP, ki jo je razvil Cisco Systems, Inc. Medsebojna avtentikacija se izvaja za odjemalca in avtentikacijski strežnik, temelji pa na uporabniškem imenu in geslu.
PAC (Protected Access Credential) vzpostavlja predor za uporabnika na podlagi edinstvenega skupnega tajnega ključa.

EAP-TTLS (Extensible Authentication Protocol-Tunnelled Transport Layer Security)
Klient je overjen na podlagi uporabniškega imena in gesla, hkrati pa protokol preveri tudi avtentikacijski strežnik na podlagi elektronskega certifikata.

Za preverjanje pristnosti pri uporabi protokola EAP-TLS sta potrebna elektronska certifikata odjemalca in strežnika, za EAP-TTLS pa uporabniško ime in geslo namesto certifikata klienta. Zaradi tega je EAP-TTLS lažje uvesti v primerjavi z EAP-TLS. Elektronska potrdila se uporabljajo za dokazovanje veljavnosti avtentikacijskega strežnika. Zato pomaga izboljšati varnost komunikacije.

Avtentikacija SMTP
SMTP avtentikacija je funkcija, ki omogoča pošiljanje e-pošte le, če sta uporabniško ime in geslo uspešno potrjena na strežniku SMTP. Z omejevanjem dostopa do strežnika SMTP, preprečuje nepooblaščenim uporabnikom pošiljanje e-poštnih sporočil prek strežnika SMTP.

POP pred SMTP
POP pred SMTP opravi preverjanje pristnosti protokola POP pred pošiljanjem e-poštnih sporočil s strežnika SMTP. E-poštna sporočila se lahko pošljejo v določenem obdobju po zaključku preverjanja pristnosti POP. Preverjanje pristnosti POP pred pošiljanjem e-pošte preprečuje maskiranje.

PRILOGA B

Vrata in protokoli

Protokol	Št. vrat	Nastavitev	Opomba
Strežnik FTP	TCP 21	Enable/Disable	Strežnik FTP server je protokol za prejemanje dokumentov.
HTTP	TCP 80	Enable/Disable	HTTP je protokol, ki se uporablja pri prejemanju in pošiljanju podatkov s spletne strani med strežnikom www in brskalnikom.
NetBEUI	TCP 139	Enable/Disable	NetBEUI je protokol za majhno omrežje, ki se uporablja za izmenjavo datotek in storitev tiskanja.
HTTPS	TCP 443	Enable/Disable	HTTPS je protokol, ki izvaja kodiranje s pomočjo SSL/TLS.
IPP over SSL/TLS	TCP 443	Enable/Disable	IPP over SSL/TLS je protokol, ki združuje SSL/TLS, ki kodira SSL/TLS kanal in IPP, ki se uporablja za internetno tiskanje. Poleg tega ima lahko IPP over SSL/TLS veljaven certifikat.
LPD	TCP 515	Enable/Disable	LPD je protokol, ki se uporablja za tiskanje.
IPP	TCP 631	Enable/Disable	IPP je protokol, ki nadzoruje pošiljanje / sprejemanje podatkov o tiskanju prek TCP / IP, vključno z internetom ali tiskalniškimi napravami.
ThinPrint	TCP 4000	Enable/Disable	ThinPrint je tehnologija za tiskanje, ki je na voljo v okolju tankih odjemalcev (Thin client) in podpira tudi SSL / TLS.
WSD Scan	TCP 5358	Enable/Disable	Windows Vista WSD je protokol, ki pripravi tiskalnike ali večopravilne naprave za omrežno povezavo. Prav tako uporabnikom omogoča prepoznavo (namestitev) tiskalniške naprave ali olajša pošiljanje / prejemanje podatkov. Izvorna slika dokumentacije, ki jo optično preberete prek MFP-ja, se lahko shrani v WSD PC kot datoteka.
WSD Print	TCP 5358	Enable/Disable	Windows Vista WSD je protokol, ki pripravi tiskalnike ali večopravilne naprave za omrežno povezavo. Prav tako uporabnikom omogoča prepoznavo (namestitev) tiskalniške naprave ali olajša pošiljanje / prejemanje podatkov.
Enhanced WSD	TCP 9090	Enable/Disable	Izboljšani WSD izvede postopek za lažje povezovanje različnih, v omrežje povezanih naprav in njihovo uporabo. Skozi vrata 9090 je tudi mogoče spremljati status in stanje tiskalniških naprav v omrežju.
Enhanced WSD over SSL/TLS	TCP 9091	Enable/Disable	Enhanced WSD (SSL/TLS) je nadgrajen varnostni protokol, ki zagotavlja kodiranje, avtentikacijo in varnost (Protect against alteration).

RAW	TCP 9100	Enable/Disable	Protokol RAW za tiskanje uporablja drugačne korake kot LPR. V splošnih 9103, tiskalniki ali večopravilne naprave uporabljajo vrata številka 9100, hkrati pa uporabljajo SNMP ali MIB za konfiguracijo in spremljanje stanja tiskalniških naprav.
SNMPv1/v2	UDP 161	Enable/Disable	SNMP protokol se uporablja v sistemih za upravljanje omrežij. Normalna komunikacija bo izvedena z uporabo imen skupnosti za zapisovanje in branje.
SNMPv3	UDP 161	Enable/Disable	SNMP protokol se uporablja v sistemih za upravljanje omrežij. Normalna komunikacija bo izvedena z uporabo uporabniškega imena in gesla. Možna je uporaba možnosti za avtentikacijo in kodiranje.
DSM Scan		Enable/Disable	DSM (Distributed Scan Management) uporablja Windows Server 2008 R2, s pomočjo katerega obdelujejo velike količine uporabniških podatkov v veliki organizaciji.
FTP Client		Enable/Disable	FTP odjemalec je komunikacijski protokol za posredovanje datotek prek omrežja.
LDAP		Enable/Disable	Imenik na strežniku LDAP se imenuje zunanji adresar. Kot destinacija sta lahko izbrana številka faksa in poštni naslov.
POP3		Enable/Disable	POP3 je standardni protokol za prejemanje elektronske pošte.
POP3 over SSL / TLS		Enable/Disable	POP3 over SSL / TLS je protokol, ki združuje POP3, ki se uporablja za SSL / TLS prejemanje e-pošte in SSL / TLS, ki je potreben za kodiranje kanala.
SMTP		Enable/Disable	SMTP je protokol za pošiljanje e-pošte.
SMTP over SSL/TLS		Enable/Disable	Protokol SMTP over SSL/TLS združuje SMTP, ki se uporablja za pošiljanje e-pošte in SSL / TLS, ki je potreben za kodiranje kanala.
SMB Klient		Enable/Disable	SMB je protokol, ki omogoča deljenje datotek ali tiskalnikov prek omrežja.
eSCL		Enable/Disable	eSCL je protokol, ki se uporablja za oddaljeno skeniranje iz operacijskega sistema Mac OS X.
eSCL over SSL/TLS		Enable/Disable	eSCL over SSL je eSCL komunikacijski protokol, ki uporablja SSL certifikat. Vsa eSCL over SSL komunikacija je kodirana.
LLTD		Enable/Disable	LLTD je protokol za odkrivanje topologije omrežja in za diagnostiko kakovosti storitev.
REST		Enable/Disable	REST je programska arhitektura za izmenjavo podatkov med spletnimi storitvami.
REST over SSL/TLS		Enable/Disable	REST over SSL je REST komunikacijski protokol, ki uporablja SSL certifikate. Vsa REST over SSL komunikacija je kodirana.

PRILOGA C

Varni komunikacijski protokoli

SNMP v3
SNMP je standardni protokol, ki spremlja in nadzira naprave, ki se povezujejo v omrežje. Poleg tega SNMPv3 zagotavlja možnost varovanja zaupnosti podatkov z avtentikacijo in kodiranjem.

IPv6
KYOCERA je pridobila status IPv6 Ready do nivoja Phase2. Podpora za IPv6, ki je na voljo v KYOCERA tiskalnikih in večopravilnih napravah, se lahko poveže z usmerjevalniki in uporablja osnovni kontrolni protokol, kot je npr. ping. Poleg zgoraj omenjenih osnovnih povezav je zagotovljena varnejša povezava z izvajanjem strogih varnostnih ukrepov.

IPSec
Protokol IPSec s kodiranjem posameznih paketov IP ščiti podatke v tranzitu. Kodiranje z uporabo IPSec se uporablja za podatke o naročilih tiskanja, poslanih iz računalnika v tiskalnik ali večopravilno napravo in optično prebranih podatkov, ki jih je potrebno poslati iz večopravilne naprave v računalnik. Torej, IPSec podpira varnejšo izmenjavo podatkov.

SSL/TLS
SSL/TLS je sistem za kodiranje podatkov za prenose v omrežju, kot je na primer spletni dostop. Ima tudi funkcijo, da preveri ali so stranke zanesljive za medsebojno komunikacijo. KYOCERA MFP / tiskalniki podpirajo SSL / TLS kodirne protokole, vključno s SSL3.0, TLS1.0, TLS1.1, TLS1.2 in s tem preprečujejo dostopanje do podatkov v omrežju in njihovo spreminjanje.

IPP over SSL/TLS
Protokol za tiskanje v spletu, ki deluje kot kombinacija IPP, ki je namenjen izmenjavi podatkov o tiskanju na internetu ali omrežju TCP / IP in SSL / TLS, katerega naloga je kodiranje komunikacijskega kanala. Tako uporabnikom omogoča varno pošiljanje prek omrežja naročil tiskanja dokumentov v tiskalnik ali večopravilno napravo.

HTTP over SSL/TLS
Protokol, ki deluje kot kombinacija HTTP, ki je namenjen pošiljanju in sprejemanju podatkov v ali iz spletnih brskalnikov ali drugih v omrežju TCP / IP in SSL / TLS, katerega naloga je kodiranje komunikacijskega kanala. Pri prenosu podatkov med osebnim računalnikom in tiskalnikom ali večopravilno napravo zmanjša tveganje za spremembe s strani nepooblaščenih uporabnikov ali uhajanja podatkov.

FTP over SSL/TLS
Protokol, ki deluje kot kombinacija FTP, ki se uporablja za posredovanje datotek v omrežju TCP / IP in SSL / TLS, ki je namenjen kodiranju komunikacijskega kanala. Pri pošiljanju skeniranih podatkov iz tiskalnika ali večopravilne naprave s protokolom FTP je kanal kodiran s SSL / TLS protokolom. FTP preko SSL / TLS tako omogoča bolj varne prenose.

SMTP over SSL/TLS
Protokol, ki deluje kot kombinacija e-poštnega prenosa in SSL / TLS, ki je namenjen kodiranju komunikacijskega kanala med strežnikom in tiskalnikom ali večopravilno napravo. S tem je onemogočeno maskiranje ali spreminjanje podatkov v tranzitu.

POP3 over SSL/TLS
Protokol je kombinacija POP3, ki je protokol za prejemanje e-poštne in SSL / TLS, ki je namenjen kodiranju komunikacijskega kanala med strežnikom in MFP / tiskalnikom. S tem je onemogočeno maskiranje ali spreminjanje podatkov v tranzitu.

KYOCERA
Document Solutions

Xenon forte d.o.o.
Letališka c. 29, Ljubljana

Tel.: 01 5484 800
E-pošta: prodaja@xenon-forte.si

www.xenon-forte.si
www.kyoceradocumentsolutions.si