

Asiakirjojen tietoturva

Yrityksen tietojen suojaaminen

Sisältö

Johdanto	3
Taustaa	4
Ongelma	5
Suositukset	7
Yhteenveto	10
Lähteet	11

Johdanto

Organisaatioissa käsitellään päivittäin tuhansia eri muodossa olevia asiakirjoja, jotka ovat samalla vaarassa kadota, tulla varastetuiksi tai vahingoittua. Siksi ne on suojattava.

Sharpin määrittelyn mukaan asiakirjojen tietoturva tarkoittaa sellaisten tietojen tietoturvaa, jotka on saatu paperisista asiakirjoista skannaamalla tai jotka ovat sähköisinä asiakirjoina jossakin yrityksen säilytyspaikassa, kuten Microsoft Office -tiedostoissa, sähköposteissa jne. Sharpin asiakirjojen tietoturva kattaa

- asiakirjoihin liittyvät liiketoimintaprosessit
- asiakirjojen varastoinnin (fyysiset paperiasiakirjat ja sähköiset arkistot)
- asiakirjojen elinkaaren (hankinta → varastointi → hallinta → säilytys → jakaminen → integrointi).

Tässä raportissa kuvataan jokaisen yrityksen kohtaamia asiakirjojen tietoturvaan liittyviä haasteita. Käsiteltävät pääkohdat ovat

- **Tausta**

Tässä osiossa tarkastellaan asiakirjojen tietoturvan monia näkökohtia. Käydään läpi muun muassa kaikkien toimiston asiakirjojen ja tietojen tunnistaminen yleisimmissä liiketoimintaprosesseissa erikseen paperisten (fyysisten) ja sähköisten (digitaalisten) asiakirjojen osalta sekä kuvataan asiakirjojen elinkaari prosessi.

- **Ongelma**

Tässä osiossa käsitellään asiakirjojen tietoturvaan liittyviä haasteita, joita IT-vastuuhenkilöt, loppukäyttäjät ja yritysjohto voivat kohdata. Haasteet liittyvät erityisesti yrityksen luottamuksellisten asiakirjojen ja tietojen hankintaan, varastointiin ja saatavuuteen. Painopistealueet ovat

- rakenteeton data
- toimiston asiakirjoihin liittyvät manuaaliset tehtävät
- yleinen asiakirjojen tietoturva.

- **Suosituks**

Tässä osiossa kuvataan, miten Sharpin optimoidut ratkaisut, palvelut ja parhaat käytännöt auttavat luomaan asiakirjoille tietoturvallisesta ympäristön sekä välttämään asiakirjojen tietoturvaan liittyvät uhat, jotka voivat johtaa tietoturvaloukkaukseen tai häiritä prosessin toimintaa. Osiossa kerrotaan myös, miten Sharp voi auttaa ratkaisemaan yrityksen hankalia ongelmia seuraavilla alueilla:

- asiakirjaprosessien merkityksen ja roolin ymmärtäminen
- paperipohjaisten arkistojen ja sähköisten tiedostopohjaisten säilytysratkaisujen optimointi
- asiakirjan elinkaaren optimoinnin vaiheiden tunnistaminen tai oman asiakirjojen tietoturvalitiikan ja parhaiden käytäntöjen kehittäminen.

- **Yhteenveto**

Yhteenvedossa esitetään tiivistelmä käsitellyistä asioista. Painopiste on seuraavissa asioissa:

- yrityksen asiakirjoihin liittyvät keskeiset liiketoiminnalliset haasteet
- Sharpin asiantuntemukseen ja Sharpin optimoituihin tuotteisiin perustuvat tärkeimmät suositukset
- seuraavat vaiheet yhdenmukaisen asiakirjojen tietoturvalitiikan kehittämiseksi
- asiakirjojen tietoturvan liittäminen toimiston muuhun tietoturvaan, kuten verkon tietoturvaan ja tulostuksen tietoturvaan.

Taustaa

Sekä työskentelynopeutemme että luomamme ja käyttämämme tiedon määrä kasvavat nykyään suorastaan eksponentiaalisesti.

IDC-tutkimuslaitos ennustaa, että maailmanlaajuisesti tuotetun tiedon määrä kasvaa käsittämättömään 163 zettatavuun (ZB) vuoteen 2025 mennessä¹. Se on kymmenkertainen vuoteen 2017 verrattuna.

Joka päivä yrityksissä laaditaan sopimuksia, laskuja, tarjouksia ja monia muita asiakirjoja lukuisissa eri formaateissa. Kaikki niistä ovat kriittisen tärkeitä yrityksen toiminnalle.

Esimerkiksi sopimuksissa määritellään organisaation ja sen asiakkaiden välinen liikesuhde, kun taas maksetut laskut tuovat yritykseen liikevaihtoa. Kaiken tämän tiedon hallitseminen ja säilyttäminen sekä sen saatavuuden varmistaminen oikeille ihmisille organisaatiossa muodostavat yrityksen menestyksen avaimen.

Yrityksen luoman ja käyttämän tiedon suuri määrä, monimutkaisuus ja monimuotoisuus aiheuttavat haasteita hallintaan ja valvontaan.

90 % tämän päivän datasta on luotu viimeksi kuluneiden kahden vuoden aikana. Se tekee 2,5 triljoonaa tavua dataa päivässä.²

Tilanteen ratkaisemiseksi yrityksen on ymmärrettävä ja kartoitettava asiakirjojen tyypit - miten niitä käytetään, miten ne ovat vuorovaikutuksessa liiketoimintaprosessien kanssa sekä miten asiakirjoja varastoidaan, hallitaan, jaetaan ja säilytetään.

Useimmat näistä haasteista liittyvät suoraan kolmeen ongelmaan:

- **Rakenteeton data**

Rakenteeton data on tietoa, johon ei liity ennalta määriteltyä tietomallia tai jota ei ole järjestetty ennalta määritellyllä tavalla. Käyttäjät säilyttävät transaktioasiakirjoja, kuten sähköposteja tai Office-tiedostoja usein itse luomissaan kansiorakenteissa, joita ei ole nimetty minkään vakiomuotoisen nimeämiskäytännön mukaan tai joihin ei liity mitään kuvailevaa metadataa.

Siksi on hyvin hankalaa saada asiakirjoista yhtenäistä kokonaiskuvaa ja seuraaviin kysymyksiin on vaikea saada vastausta:

- Miten asiakirjoja säilytetään, hallitaan ja valvotaan?
- Miten helposti asiakirjat voidaan löytää, tarkastaa ja jakaa?
- Miten käyttöoikeudet ja tiedostojen käyttöluvat toimivat?

- **Toistuvat manuaaliset tehtävät**

Toistuvia manuaalisia tehtäviä joudutaan tekemään jokseenkin jokaisessa yrityksessä. Kyseessä voi olla laskujen ja kulujen käsittely tai henkilöstöhallinnon asiakirjojen hallinta. Tekniikan avulla näitä prosesseja voidaan automatisoida, jolloin tietoturvan paranemisen lisäksi myös tehokkuus, tarkkuus ja jäljitettävyyden paranevat.

- **Yrityksen asiakirjojen elinkaaren ymmärtäminen**

Jokainen asiakirja tai asiakirjalaji noudattaa omaa elinkaartaan asiakirjan syntymisestä sen hävittämiseen asti. Eri asiakirjalajien elinkaarten ymmärtämisen, kartoittamisen ja optimoinnin avulla voidaan varmistaa oikeiden tietoturvatöiden käyttö määräysten edellyttämällä tavalla, ja samalla pidetään toiminta riittävän joustavana tehokkaan työnteon mahdollistamiseksi.

Nämä ovat tärkeimmät osa-alueet, joita jokaisen yrityksen pitäisi pohtia määritellesään ja toteuttaessaan organisaation asiakirjojen tietoturvalitiikkaa.

Ongelma

Nykyaikaisissa yrityksissä käsitellään paljon tietoja, mutta useinkaan ei välttämättä ole todellista käsitystä siitä, miten tiedot tuotetaan ja varastoidaan ja miten niihin pääsee käsiksi. Tästä voi aiheutua tietoturvariskejä.

Useimmissa organisaatioissa luodaan ja varastoidaan sisältöjä digitaalisesti. Asiakirjoja kuitenkin usein varastoidaan sekä sähköisessä (digitaalisessa) muodossa että paperisina:

- **Paperiset asiakirjat**

Paperiset asiakirjat tai muut pysyvätulosteet ovat huomattava tietoturvariski, sillä niiden alkuperää on usein vaikea selvittää tai osoittaa selkeää jäljitysketju. Siten niiden jäljitettävyyttä voi olla hyvin heikko. Lisäksi fyysinen tietoturva jätetään usein liian vähälle huomiolle. Luottamukselliset asiakirjat saattavat esimerkiksi kadota tai joutua vahingossa säilytettäväksi väärään paikkaan, joka ei ole turvallinen.

- **Sähköiset asiakirjat**

Hajautettuihin ja toisinaan eristettyihin varastointijärjestelmiin tallennettuihin sähköisiin asiakirjoihin liittyy omat tietoturvaasteensa. Ne johtuvat usein jo pelkästään asiakirjojen määrästä sekä käytettävissä olevien säilytysjärjestelmien ja -paikkojen määrästä. Asiakirjojen elinkaaren ymmärtäminen on ainoa mahdollinen lähtökohta koko yrityksen kattavien prosessien ja tietoturvamennettelyjen käyttöönotolle.

Asiakirjojen tietoturvan ylläpito

Asiakirjojen tietoturvan (tai sen puutteen) määritelmä on hyvin laaja. Sitä tulisi tarkastella asiakirjan elinkaaren näkökulmasta ja ottaa erityisesti huomioon esimerkiksi tietoturvaloukkaukset, rakenteettomat tiedot, suojaamattomat tiedostot, inhimilliset erehdykset ja luvaton tietojen varastointipaikkaan pääsy.

Asiakirjan elinkaari koostuu kuudesta päävaiheesta, jotka ovat hankinta, varastointi, hallinta, säilytys, jakaminen ja integrointi.

- **Vaihe 1: Hankinta**

Hankinta on prosessin vaihe, jossa tiedot "otetaan haltuun". Kyseessä voi olla paperiasiakirjojen skannaus, sähköpostilaatikon seuraaminen tai asiakirjojen luominen ja tallennus sovelluksesta käsin.

- **Skannaus** on tavallinen tapa muuntaa paperiasiakirjat sähköiseen muotoon. Skannaus on kieltämättä kätevää, mutta siihen voi liittyä ongelmia tietoturvan ja lainmukaisuuden kannalta. Valvomattomana prosessi ei ole jäljitettävissä, joten asiakirjoilta saattaa puuttua todistusvoima ja kelpoisuus laillisena asiakirjana.
- **Indeksointi** on asiakirjojen kuvailumenetelmä, jossa käytetään metaselostusta tai koko sisältöä (tekstiä). Indeksointi nopeuttaa tiedostojen hakua ja tietojen löytämistä - erittäin käyttökelpoista, kun tarkastellaan sisältöä tietoturvan tai vaatimustenmukaisuuden näkökulmasta.
- **Reititys** on prosessi, jossa muodostetut asiakirjat toimitetaan oikeaan varastointipaikkaan. Ilman reititystä asiakirjat saattavat vahingossa päätyä väärään tai jopa suojaattomaan säilytyspaikkaan.

- **Vaihe 2: Varastointi**

Asiakirjojen turvallinen varastointi voi perustua paperiasiakirjoihin tai sähköisiin tiedostoihin. Monet yritykset eivät kuitenkaan kiinnitä tarpeeksi huomiota varastointitapaan, paikkaan eikä tarpeelliseen tietoturvaan:

- Paperipohjaiset varastointijärjestelmät ovat edelleen hyvin yleisiä, mutta niistä puuttuu usein tietoturvan edellyttämä valvonta. Lisäksi on hyvin hankalaa esittää mitään paperisiin asiakirjoihin liittyviä auditointitietoja.
- Sähköiseen varastointiin perustuvaa järjestelmää pidetään usein

automaattisesti parempana. Jos varastointia ei kuitenkaan suunnitella eikä hallita asianmukaisesti, sähköiseenkin varastointiin liittyy haasteita. Pitäisi päättää, miten järjestelmä suojataan yrityksen verkossa, miten perustetaan käyttöoikeudet ja miten valvotaan tai rajoitetaan järjestelmän käyttöä.

- **Vaihe 3: Hallinta**

Asiakirjahallinta käsittää luvat, versionhallinnan sekä jäljitysketjun:

- Lupien avulla hallitaan käyttäjien oikeuksia päästä käsiksi asiakirjoihin, joten ne ovat avainasemassa tietoturvallisen asiakirjaympäristön ylläpidossa. Vaikka lupa on käsitteenä helppo ymmärtää, ilman asianmukaisia järjestelmiä niiden käyttöönotto ja hallinta voi olla vaikeaa. Jotta lupakäytäntö olisi tehokas, yrityksessä on ensin ymmärrettävä, miten käyttäjien toiminta liittyy heidän tarvitsemiinsa tietoihin ja niihin prosesseihin, joissa he ovat mukana.
- Versionhallinnalla varmistetaan, että käyttäjillä on käytössä asiakirjojen uusimmat versiot, vaikka myös aikaisempia versioita voidaan tarvittaessa säilyttää. Tämä on erityisen tarpeellista strategisissa tai juridisissa tilanteissa, kun asiakirjan alkuperä voidaan todistaa asiakirjan aikaisempien versioiden avulla. Versionhallinta on avain tietoturvalliseen ja juridisesti hyväksyttävään digitaaliseen asiakirja-arkistoon.
- Jäljitysketjuun tallennetaan tieto jokaisesta asiakirjaan kohdistuvasta toiminnasta ja tapahtumasta, kuten asiakirjan luoja, muokkaaja, katselija tai uudelleenversioija. Jäljitysketjujen avulla voidaan todistaa kaikkiin varastoituihin asiakirjoihin liittyvä toiminta, ja jäljitysketjut ovat avainasemassa tietoturvan ylläpitämisessä etenkin tietoturvaloukkausten yhteydessä

- **Vaihe 4: Säilytys**

Asiakirjojen ja tietojen säilyttäminen on myös tärkeä osa tietoturvallisen asiakirjaympäristön ylläpitoa. Perinteisiin tai sähköisiin arkistoihin varastoituja asiakirjoja on kuitenkin ylläpidettävä jatkuvasti, koska käytettävissä oleva tila on rajallinen. Siksi seuraavat menettelyt ovatkin ratkaisevan tärkeitä:

- **Asiakirjan säilytys**

Joitakin asiakirjoja on (lain mukaan) säilytettävä tietty aika. Tähän liittyviä haasteita ovat

- luettelon ylläpito, jolla varmistetaan asiakirjojen poistaminen säilytysajan päätyttyä
- sen varmistaminen, että kaikki säilytettäväksi määritellyt asiakirjat ovat löydettävissä
- päätös, hallitaanko asiakirjoja keskitetysti vai paikallisesti.

- **Asiakirjojen hävittäminen**

Yritysten on laadittava menettelytavat kaiken paperilla olevan tiedon, sähköisten tiedostojen ja sähköisten kirjastojen hävittämiseksi, kun ne ovat vanhentuneet tai vaadittu säilytysaika on päättynyt.

- Fyysinen asiakirjojen tuhoaminen jonkin DIN-turvaluokan mukaisesti on paperisten asiakirjojen perinteinen hävittämistapa. Tämä voi olla kallista ja aikaa vievää.
- Sähköinen tuhoaminen tarkoittaa varmaa ja todennettavaa sähköisten asiakirjojen poistamista kiintolevyiltä, DVD:iltä, levykkeiltä jne.

- **Vaihe 5: Jakaminen**

Tässä vaiheessa määritellään tavat, joilla sähköinen asiakirja voidaan jakaa muille käyttäjille tai liikekumppaneille. Erityisesti on otettava huomioon seuraavaa:

- Asiakirjojen jakaminen toteutetaan usein jaettujen kansioiden tai levyjen avulla. Jos tätä ei hallita asianmukaisesti, luvattomat käyttäjät tai käyttäjäryhmät saattavat löytää asiakirjat, päästä niihin käsiksi ja käyttää niitä.
- Asiakirjojen käyttö mobiililaitteilla voi myös kuulua tähän vaiheeseen. Se aiheuttaa paljon mutkikkaampia käytön suojaamiseen liittyviä kysymyksiä.

- **Vaihe 6: Integrointi**

Integraatioprosessissa tietoja vaihdetaan muiden liiketoimintasovellusten kanssa (esimerkiksi kirjanpito- tai toiminnanohjausjärjestelmä).

Jokaisen edeltävän vaiheen tarkkuus ja täydellisyys on kriittisen tärkeää integraation onnistumiselle, jotta data on yhdenmukaista ja

luotettavaa. Missä tahansa kohdassa esiintyvä ongelma vaikuttaa suoraan liiketoimintaprosessiin.

Suosituksset

Sharp tarjoaa useita ratkaisuja ja sovelluksia, joiden avulla organisaatiot voivat laatia tarvitsemansa tietoturvapoliitiikan.

Asiakirjojen tietoturva on hyvin monimutkainen kysymys. Asiakirjan elinkaaren rakenteen määrittely kuitenkin selkiyttää ja helpottaa asian ymmärtämistä sekä sen jälkeen muutos- tai parannustoimien toteuttamista:

- Prosessien parantaminen tai asiakirjojen tietoturvan määrittely alusta lähtien voi olla melkoisen hankalaa ja aikaa vievää, erityisesti kun kartoitetaan prosesseja ja hankitaan kaikki tarpeellinen tieto prosesseista ja liiketoimintarooleista. Sharp Professional Services -ammattilaispalveluissa hyödynnetään sekä Sharpin kokemusta asiakirjaratkaisuista että sen kehittyneitä työkaluja asiakirjojen ja tietojen selvittämiseen ja työnkulkujen kartoittamiseen.
- Sharp auttaa vaiheittaisen prosessin avulla yrityksiä selvittämään asiakirjojensa nykyisen elinkaaren ja siihen liittyvät haasteet. Niiden perusteella kehitetään prosessit ja menettelytavat asiakirjojen tietoturvan optimoinnin kahta päätavoitetta varten:
 - Rakenteistamattoman tiedon rakenteistaminen
 - Toistuvien tehtävien nopeuttaminen ja rationalisointi

Nopea ja turvallinen aloitus

- Sharp auttaa asiakkaita kehittämään vahvan turvallisuuspolitiikan ja asiakirjaympäristön. Sharpin ratkaisut perustuvat Sharpin monitoimilaitteisiin asiakirjojen muodostamisessa sekä optimoituihin sovellusratkaisuihin asiakirjojen varastoinnissa ja hallinnassa. Nämä ratkaisut antavat asiakkaille mielenrauhaa, koska niiden avulla asiakirjainfrastruktuuri on tietoturvallinen ja jäljitettävä.
- Aluksi voi olla kyse vain muutoksista erittäin paljon paperia käyttävien osastojen (henkilöstö-, talous- tai lakiasiainosasto)

prosessissa, ja myöhemmin ratkaisut laajennetaan suunnitellusti yrityksen muiden osa-alueiden prosesseihin ja menettelytapoihin.

Asiakirjojen muodostamisen ja varastoinnin yksinkertaistaminen

- Skannauksen tietoturvan varmistamiseksi Sharp suosittelee erittäin painokkaasti, että asiakkaat skannaavat ainoastaan tietoturvalle sisäisiin säilytyspaikkoihin sekä valikoiduille sähköpostiryhmille tai käyttäjille, jotka IT-pääkäyttäjät voivat konfiguroida Sharpin monitoimilaitteisiin. Tämä on erityisen tärkeää GDPR:n noudattamisen kannalta.
- Kun tarvitaan kehittyneempiä ominaisuuksia esimerkiksi laillisen kelpoisuuden varmistamiseksi, käytettävissä on Sharpin optimoitujen ratkaisujen valikoima. Sharp tarjoaa valikoiman ratkaisuja, jotka nopeuttavat prosesseja pienissä, keskikokoisissa ja suurissa yrityksissä sekä mahdollistavat suoran integraation liiketoimintasovelluksiin.
- Sharpin optimoidut ratkaisut tarjoavat mahdollisuuden indeksoida kaikki muodostetut asiakirjat:
 - Lisätään metadataa suoraan monitoimilaitteesta
 - Lisätään metadataa sovellusrajapinnassa ennen varastointia ja käsittelyä.
- Sharpin optimoidut sovellusratkaisut sisältävät reititysmahdollisuuksia, joilla varmistetaan, että kaikki käyttäjät toimivat skannauksessa samalla rakenteisella tavalla ja ohjaavat siten asiakirjat oikeisiin paikkoihin ja luotettaviin sovelluksiin.

Käyttäjien roolit ja luvat

Asiakirjojen tietoturvapoliittikan rakentamisessa käyttäjien luvilla ja rooleilla on tärkeä merkitys luottamuksellisuuden ja valvonnan säilyttämiselle

- Sharp neuvoo käyttämään yhtä keskitettyä asiakirjahallintajärjestelmää, jossa "roolit" on liitetty työntekijöiden työhön liittyviin tarpeisiin. Esimerkiksi näin:
 - Vain hallituksen jäsenillä on pääsy yrityksen kaikkiin asiakirjoihin
 - Vain henkilöstöosastolla on pääsy työntekijöiden tietoihin
 - Projektipäälliköillä on projektiin liittyvien asiakirjojen käyttöoikeus
 - Myyjillä on käyttöoikeus myyntiin liittyviin tiedostoihin, kuten esitteisiin, kaavakkeisiin jne.
- Luvat määritellään rooli- tai ryhmäkohtaisesti ja niillä valvotaan käyttäjien asiakirjojen käyttöä (luominen, katselu, muuttaminen, poistaminen) tai voidaan antaa vain osittaiset käyttöoikeudet, kuten asiakirjojen katseluoikeus ilman muita oikeuksia.
- Versionhallinta on olennaisen tärkeää. Sharpin optimoitujen ratkaisujen avulla käyttäjä voi tarkistaa, mikä versio hänellä on käytössä, sekä tarkastella tai palauttaa asiakirjan vanhempia versioita.
- Samanaikainen käyttö pysyy hallinnassa asiakirjahallinnan avulla: jos joku työntekijä on parhaillaan muokkaamassa asiakirjaa, muut työntekijät voivat ainoastaan lukea sitä.
- Tietoturvan vaatimustenmukaisuuden varmistamiseksi IT-pääkäyttäjillä on käytettävissään edistynyt jäljitysketjutyökalu (jäljitysloki), johon kirjataan kaikki asiakirjoihin kohdistuva toiminta: milloin asiakirjaa on muutettu, kuka teki muutoksen ja miten pitkän aikaa tietty käyttäjä on käyttänyt asiakirjaa.

Oikeita tietoja säilytetään oikean mittainen aika

- Laaditaan asiakirjojen lajiin ja tietoja käsittelevään osastoon perustuva asiakirjojen säilytysmenettely.
- Asiakirjojen hävittäminen on asiakirjojen säilytysmenettelyn päätepiste. Käytetystä säilytyspaikasta riippuen tarjolla on eri

vaihtoehtoja kaikkien tietojen poistamiseksi järjestelmästä:

- Paperiasiakirjoille Sharp suosittelee käyttämään ammattimaista tuhoamispalvelua, jonka DIN-turvaluokka on vähintään 5.
- Sähköisessä muodossa oleville tiedoille Sharp puolestaan suosittelee ammattimaista sähköisen datan hävityspalvelua.
- Kiintolevylle tallennetuille tiedoille (käytössä talon sisäinen asiakirjahallinta ja sisäiset säilytyspaikat) Sharp suosittelee kaksivaiheista prosessia eli tietojen pyyhkimistä ja sen jälkeen fyysistä tuhoamista sen varmistamiseksi, että kiintolevyllä olevat tiedot eivät ole enää käytettävissä.

Saumaton tietojen saatavuus ja jakaminen

Yrityksen käyttöön ottamassa asiakirjojen tietoturvapoliitikassa on aina kuvattava, miten käyttäjät/työntekijät saavat asiakirjat käyttöönsä ja miten he voivat jakaa niiden tietoja muiden kanssa.

Sharpin optimoiduissa ratkaisuissa on tarjolla useita menetelmiä asiakirjojen jakamiseksi asiakirjahallinta-alustojen kautta:

- Ensimmäinen vaihtoehto on lähettää vastaanottajalle sähköpostitse tiedostoon linkki, joka vanhenee tietyn ajan kuluttua. Jakamistapahtuman yksityiskohdat kirjataan lokiin, ja linkki voidaan tehdä toimimattomaksi tarpeen mukaan tai ennalta määritellyn ajan kuluttua.
- Toinen vaihtoehto on jakaa kansioita järjestelmän sisällä saman organisaation rekisteröityneiden käyttäjien kanssa. Vastaanottajien käyttöoikeudet kansion asiakirjoihin voidaan määritellä ja asettaa – luku; luku ja kirjoitus; tai luku, kirjoitus ja poisto. Nämä oikeudet ja säännöt voidaan määritellä myös suunniteltaessa asiakirjahallintajärjestelmän yleissääntöjä ja asiakirjojen tietoturvapoliittikkaa.
- Useimmat järjestelmän toiminnot voidaan tarjota myös mobiilikäyttäjille (Android tai iOS). Sharp suosittelee, että yritykset pohtivat turvallisen mobiiliyöskentelyn etuja.

Optimaalinen arvo datasta

Sharp on kehittänyt erilaisia integraatioita, niin että Sharpin monitoimilaitteista, esimääritellyistä kansioista tai järjestelmään liitetystä sovelluksista peräisin oleva data voi integroitua yrityksen järjestelmiin, kuten Sage, QuickBooks, SharePoint ja niin edelleen.

Seuraavassa esimerkkejä osa-alueista, joihin Sharp on erikoistunut:

- **Optimoitu työnkuluohjelmisto ostoreskontraan**

Ratkaisussa data poimitaan yritykseen tulleista laskuista optisen merkintunnistuksen (OCR) avulla, ja laskujen validointi- ja hyväksymisprosessi on automatisoitu. Se parantaa ostoreskontraosaston tuottavuutta ja tarkkuutta ja takaa saumattoman tehokkuuden.

Lue lisää ostoreskontraintegraatiosta [täältä](#) (esimerkki UK:sta).

- **Digitaalisen postinkäsittelyn optimoitu työnkulkuratkaisu**

Ratkaisussa kerätään sekä painettu että digitaalinen posti ja reititetään sähköisessä muodossa oikealle henkilölle tai tämän

sijaiselle, jos vastaanottajalla on "Out of Office" -asetus aktiivisena. Ratkaisun avulla yritykset pystyvät lajittelemaan ja jakamaan suuren postimäärän nopeasti ja tehokkaasti sekä maksimoimaan henkilöstön tuottavuuden.

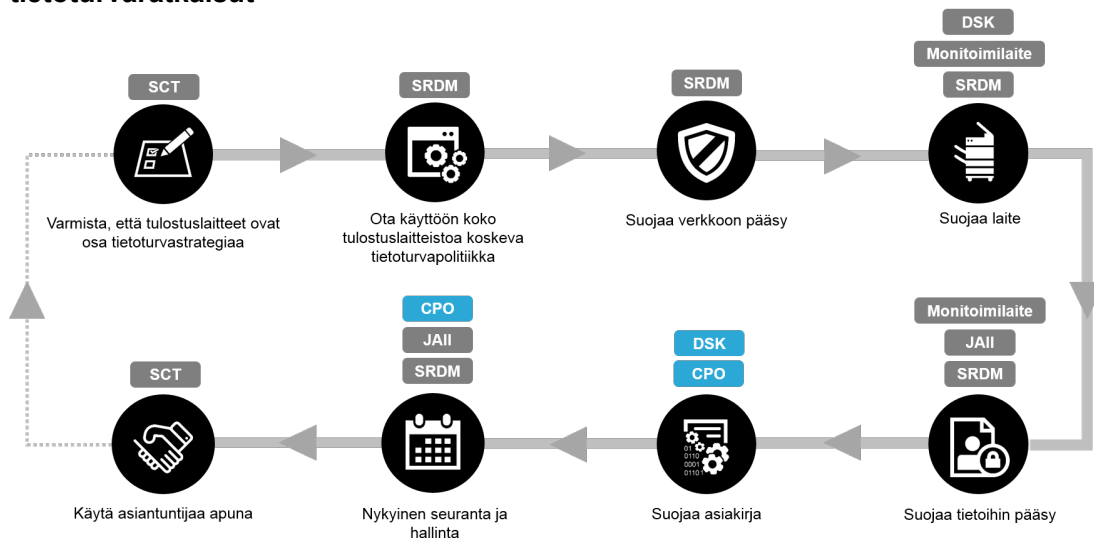
Lue lisää digitaalisen postituksen optimoidusta työnkuluohjelmistosta [täältä](#) (esimerkki UK:sta)

- **Henkilöstöhallinnon optimoitu työnkuluohjelmisto**

Tämä ratkaisu perustuu luottamuksellisten henkilöstötietojen erittäin turvalliseen ja tehokkaasti hallittuun säilytykseen. Yritykset voivat rationalisoida henkilöstöhallinnon asiakirjojen käsittelyn sekä valvoa asiakirjojen käyttöä, ja samalla täytetään tietosuojan ja salassapitoon liittyvät määräykset.

Lue lisää [täältä](#) (esimerkki UK:sta)

Tulostuksen tietoturvaliikkeen kehittäminen ja Sharpin tarjoamat asiakirjojen tietoturvaratkaisut



Yhteenveto

Kellään ei ole varaa laiminlyödä tietoturvaa, etenkin kun on kyse asiakirjoista. Asiakirjat ovat jokaisen organisaation immateriaaliomaisuutta, jonka menettämällä voi olla kohtalokkaat seuraukset

Asiakirjojen tietoturva on tietoturvan tärkeimpiä osa-alueita kaikissa yrityksissä. Asiakirjojen tietoturvapolitiikan laatiminen voi kuitenkin olla aikaa vievä ja monimutkainen prosessi. Tässä Sharp voi auttaa.

Sharpilla on vuosien kokemus asiakirjaratkaisuista. Kokemuksensa avulla Sharp on kehittänyt yritysten tietoturvaan kokonaisvaltaisen ratkaisun, joka kattaa verkon tietoturvan, tulostuksen tietoturvan sekä asiakirjojen tietoturvan.

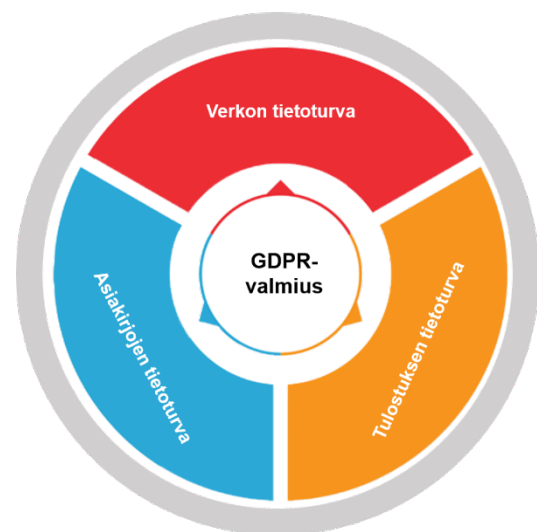
Sharp haluaa käyttää asiantuntemustaan ja asemaansa maailmanlaajuisesti tunnustettuna johtajana toimiston tietoturvaratkaisuissa auttaakseen asiakkaita varmistamaan kestävä ja määräysten mukaisen tietoturvan asiakirjoihin liittyvissä liiketoimintaprosesseissa.

Käyttämällä todistetusti toimivaa lähestymistapaansa asiakirjojen tietoturvaan Sharp auttaa yrityksiä rakentamaan ainutlaatuisia ja mittojen mukaan suunniteltuja järjestelmiä ja prosesseja jokaiseen asiakirjan elinkaaren vaiheeseen (hankinta, varastointi, hallinta, säilytys, jakaminen ja integrointi). Samalla Sharp auttaa näitä organisaatioita täyttämään uusimmat tietoturvamääräykset, kuten EU:n yleisen tietoturva-asetuksen (GDPR) sisältämät määräykset.

Sharpin optimoidut ratkaisut on suunniteltu huomioiden maksimaalinen toiminnallisuus ja tietoturva sekä antamaan nopeasti tuottoa sijoitukselle.

Sharpin tärkeimpiä toimialoja ovat hallinto-, koulutus-, laki-, talous-, terveydenhoito-, ravintola- ja matkailu- sekä yrityssektori, mutta tilaustyönä

Sharpin tietoturvan runko



toteutettuja kestäviä ratkaisuja voidaan toimittaa mille tahansa toimialalle.

Organisaationne muilla alueilla mahdollisesti esiintyvien haavoittuvuuksien torjumiseksi voimme auttaa valitsemaan muita tietoturvamenettelyjä Sharpin portfolioista, niin että voitte varmistaa täydellisen kattavan suojan kaikille yrityksenne osa-alueille:

- Asiakirjojen tietoturva
- Verkon tietoturva
- Tulostuksen tietoturva
- GDPR-asetuksen noudattaminen

Edellä käsitellyistä aiheista on lisätietoja Sharpin White Paper -kirjastossa tai Tietoturva-osiossa verkkosivustolla:

<https://www.sharp.fi/cps/rde/xchg/fi/hs.xsl/-/html/tietoturvallisuus.htm>

Voit myös ottaa yhteyttä Sharp Solutionsin konsultointitiimiin.

Lähteet

1. "Data Age 2025", IDC, maaliskuu 2017
2. "Data Never Sleeps 5.0", DOMO, 2018

www.sharp.fi

SHARP
Be Original.