TECHNOTRADE - TECHNOTRADE BIZTONSÁGI IRAT-KEZELÉSI ÉS FELÜGYELETI RENDSZERE

A JÖVŐ ITT ÉS MOST

A bizalmas adatok és információk védelme minden szervezet számára alapkövetelmény. A XXI.-ik században az adatvédelem leggyengébb pontja az EMBER lett! A bizalmas, üzleti adatok a felhasználók közvetítésével jóval könnyebben kerülnek ki, mintsem a számítástechnikai rendszer „feltörésével" próbálkoznának. Sajnos napjaink közélete egyre gyakrabban kényszeríti ki a multifunkciós eszközök által érintett adtok védelmét, azok tartalmában való keresési, szűrési képesség meglétét, az ilyen jellegű vizsgálatok azonnali elvégzését is.

A jellemző problémák az alábbiak:

- Nem tudni, ki és mit másol, szkennel, faxol, hova küldi
- Nem tudni, milyen belső titkokat szerzett és osztott meg valaki
- Nem tudni, mi marad a gép merevlemezén
- Nem tudni, ki mennyit használta az eszközöket
- Nem tudni, ki mekkora költséget termel

A hálózati rendszerek széleskörű lehetőséget adnak a biztonságos adatforgalom és adattárolás megvalósítására.

Megoldás:

Teljeskörű Biztonsági Iratkezelési és Felügyeleti Rendszer, TSMP Transcript Security Monitoring Package ©, amely megvásárolható a KEF központosított közbeszerzés keretében is

A Technotrade, mint az irodatechnikai és informatikai piac meghatározó szereplője, a **nyomtatott és elektronikus dokumentumkezelés** területén jelentős áttörést ért el. A fenti problémák gyakorlati megoldására a **forgalmazott TOSHIBA multifunkciós készülékek mellé egy olyan biztonsági, költség-, dokumentum- és üzemeltetés-menedzsment rendszert kínál**, mely a gyakorlatban már számos területen bizonyított.

A TSMP dokumentumkezelés biztonsági rendszer két témakörre koncentrál:

1. Felhasználói azonosítás, hozzáférés és költségmenedzsment
2. A felhasználók által kezelt dokumentumok biztonsági rögzítése

A teljes rendszer használatának mérhető előnyei

- ***Költség megtakarítás***: Csökken a nem munkavégzést szolgáló eszközhasználat. (Magán célú másolások, nyomtatások)
- ***Tervezhető dokumentumkészítési költségek***: Az eszközhasználat limitálhatósága biztosítja, hogy a felhasználó nem tud a költségkereteénél többet költeni.
- ***Bizalmas dokumentumkezelés***: A felhasználót „követő" nyomtatás, hitelesített azonosítás és az eszközhasználat naplózása a bizalmas dokumentumkezelés megvalósításában elengedhetetlen funkciók..
- ***Beazonosítható tevékenység***: Nem csak a kezelt (nyomtatott, másolt …) oldalak száma kerül rögzítésre, hanem a dokumentumok tartalma (oldalképe és visszafejtett szövege) is. Így egy bizalmasan kezelt, de „kiszivárgott információról" azonnal tudható: ki, mikor, hol másolta , szkennelte, faxolta.
- ***Adatszivárgás felderítése***: riasztás jelleggel vagy utólag elemezve az adatszivárgás azonosítható

A rendszer által felügyelt tevékenységek:

Nyomtatás, Másolás, Szkennelés, Faxolás, Levelezés (opcionálisan állományok felügyelete, hanganyag kezelés, levelezés audit log)

A rendszer alapját képező, bevizsgált, a rendszer biztonságának érdekében speciális átalakításon átesett homogén géppark azonos műszaki színvonalat és használatot biztosít a felhasználók számára, akik szabadon választhatnak valamennyi készülék közül szkennelés, másolás, faxolás és nyomtatás esetén. A személyi azonosításhoz kötött tevékenység elvégzésével párhuzamosan a rendszer automatikusan készít egy biztonsági másolatot elektronikus formátumban (pl. PDF) és azt a felhasználó adataival kiegészítve elmenti egy háttértárolóra.

Ezt követően lehetővé válik majd a szövegtartalom alapján történő – akár full textes – szűrés, keresés. Ezáltal **megoldható az adatvédelem legkritikusabb részének figyelemmel kísérése** is, hiszen a háttérmásolatoknak köszönhetően most már az is pontosan visszakereshető hogy kii, mikor és milyen papír alapú dokumentummal dolgozott, **s az mit is tartalmazott**. A rendszer biztonsági szempontból gyakorlatilag megkerülhetetlen, s már önmagában ez a tudat is komoly visszatartó erőt jelent.

Felügyelve:

Nyomtatás

Másolás

Szkennelés

Faxolás

Levelezés

TSMP:

A digitális őrszem

Így felkészülhet arra is amire nem lehet!

Rendszerintegrációs lehetőségek
A TSMP rendszer funkcionalitásai kiterjeszthetőek a levelezőrendszerekre, a teljes irat és dokumentumkezelési folyamatra, és a vállalatirányítási rendszerekben (pl: SAP) keletkező dokumentumok védelmére is.
A rendszerintegrációs lehetőségekről a http://www.technotrade.hu/dokumentumkezeles/images/stories/easy_2011_11_07.pdf linken tájékozódhat.

A rendszer bevezetésének és használatának előfeltételei

Toshiba multifunkciós eszköz
- Csak a bevizsgált típusok, a biztonság érdekében a multifunkciós irodagép kezelőfelülete is „speciális átalakításon" megy át

Scrambler Board: Multifunkciós gép merevlemez tartalmának titkosítása 128bites titkosító kóddal
- Merevlemez írása titkosítva történik
- Merevlemez az MFP-ből kiemelve olvashatatlan

Hozzáférés-engedélyező és költségkövető rendszer megléte
- TOSHIBA termék (felhasználó azonosítására, tevékenység engedélyezésére vagy tiltására, költséghelyre való elszámolásra, limitek kezelésére)

A rendszer certifikált részei:
TSMP © jogilag védett, amerikai eredetű szoftver megoldás, amely integrálva van a KPMG által auditált manipulálhatatlan digitális archívummal, és melybe beleépül a 24/2006 rendelet szerint certifikált, a magyar iratkezelési előírásoknak megfelelő iktatási workflow.

A TSMP megoldásról, az alkalmazott tárolásról és visszakeresésről bővebb információ a www.technotrade.hu/dokumentumkezeles oldalon található.

A rendszer működésének rövid leírása:

A multifunkcionális gépek kezelőfelülete és szükséges elemei olyan módosításon esnek át, melynek eredményeként a felhasználók nem tudják kikerülni azt, hogy tevékenységüket a rendszer teljes mértékben és TARTALMI tekintetben is kövesse. Ez a különbség a szokásos költségkövető rendszerekkel szemben, amelyek a TARTALOM kezelésére nem alkalmasak.

Így a FELHASZNÁLÓ minden tevékenységének eredménye eredeti bináris formájában ÉS a megfelelő, jól skálázható teljesítményű központi szerveren elvégzett optikai karakter felismerés eredményeként előállított „kereshető pdf" formátumban is tárolásra kerül. Ez a tevékenység nem a MFP készüléken zajlok, nem annak munkáját lassítja, hanem a szerver erőforrásait használja fel.

A felhasználó tevékenységére vonatkozó METAADATOK (melyik gépen, mikor, milyen címzettel megosztva, stb) és az állományok egymástól nem elválaszthatóak, azokat a rendszer automatikusan menti, tehát NEM CSAK a felhasználó kapja meg a munkája eredményét, HANEM a központi digitális archívum is. Ezt a felhasználó sem kikapcsolni, sem megkerülni sem módosítani nem tudja. A rendszer megőrzi az eredeti állományokat is (.tif, .ps, esetenként pcl) és a belőlük készített kereshető pdf-et is.

Ezek az adatok egy olyan digitális archívumba kerülnek, amely „kőbe vésve" őrzi őket. Tehát nem érhetők el a file rendszerből sem, és nincs olyan jogosultságú egyén, aki képes lenne azokat megmódosítani. Az alkalmazott jogosultsági rendszer lehetővé teszi, hogy egy felhasználó a saját munkáinak eredményét lássa, abban kereshessen, de ne is legyen tudomása más felhasználók azonos vagy hasonló munkáinak létezéséről sem. A rendszer egésze egy olyan átfogó workflow jogosultságkezelő dokumentumkezelő megoldáson alapul, amely bármely dokumentumkezelési feladatra, ideértve az iratkezelés speciális formáit is, alkalmas.
Opcionálisan lehetőség van file rendszerbeli állományok felügyelete (törlés előtti állapot archiválása), hanganyag kezelés, CRM rendszerhez való integrálással, elektronikus levelezés audit log kezelésre.

TSMP +:

A digitális őrszem

- File törlés ellen

-Hanganyag, CRM integráció

- e-mail audit log

Referenciák:
Pénzügyminisztérium 73 gép, 900 használó
BKK Budapesti Közlekedési Központ 9 gép 120 használó