

SARM



„Az egyre kifinomultabb fenyegetettségek, az iparági szabályozások folyamatos szigorításai felerősítették azt az igényt, hogy a vállalatvezetők minden pillanatban tudják: ki, mikor, milyen bizalmas adatokhoz férhet hozzá”

A felhasználók személyazonosságának és vállalati erőforrás elérésüknek felügyelete egyre fontosabb szemponttá és egyre nagyobb kihívássá válik napjainkban. Növekszik azon vásárlók, alkalmazottak, partnerek és beszállítók száma, akik jogosultak hozzáférni egy adott szervezet kritikus fontosságú információs erőforrásaihoz.

A hozzáférési jogosultságok meghatározása egyrészt a szervezeti hierarchia, másrészt a személyes tevékenységet meghatározó feladatkör függvénye. Az azonosság- és hozzáférés kezelési megoldások feladata a folyamatot támogató funkciók szolgáltatása, ami technikailag segíti a vezetői elképzelés kompetenciafüggő, összehangolt érvényre jutását, és ellenőrzött fennmaradását.

A SARM RENDSZER

- Önállóan is alkalmazható komponensei révén képes biztonságosabbá tenni a néhány fős, kis cégek működését, ellenőrizhetővé és átláthatóvá téve az ott is elengedhetetlen jogosultság menedzselési munkát, azaz „megmutatja”, kinek mihez van jogosultsága.
- Segít feltárni a változásokat, támogatva a vezetői szándék következetes megvalósulását egy, a jelen gyakorlat szerint csupán az informatikusok jó szándékán és precízégén múló, ugyanakkor elképesztően kritikus tevékenység körben.
- Nagyvállalati körben workflow támogatást ad a több személyt, szervezetet érintő jogosultsági kérdések dokumentált meghatározásához

A SARM hatékonyan gyűjti össze a vállalat kiszolgáló eszközein (hálózati infrastruktúra és szerverek) elérhető informatikai rendszerek jogosultsági beállításait, az adatok feldolgozása után a tárolt információkon monitorozó, illetve jelentéskészítési funkciókat biztosít. A rendszer képes megmutatni, hogy egy adott felhasználó vagy csoport milyen informatikai jogosultságokkal bír a vállalat egészét, vagy egy részterületét illetően





A RENDSZER RÉSZEI

SECURITYDISCOVERER (ADATGYŰJTŐ MODUL)

Feladata a jogosultsági adatok felderítése, begyűjtése a különböző rendszerekből. Távrolról konfigurálható, felügyelhető a rendszer működése. Új kiszolgálóra való telepítése a központi modulból végezhető. Az adatokat lokálisan is képes tárolni (hálózat kiesési puffer), majd lehetőség szerint továbbítani a központi szervernek (SecurityStore). Az adattovábbítás SOAP-on keresztül történik.

SECURITYSTORE (ADATTÁROLÓ MODUL)

Input oldali feladata a gyűjtőmodulokból érkező adatok fogadása SOAP-on keresztül. Érkeztetés után rendszerezi, csoportosítja és eltárolja őket az adatbázisba, ideértve a SecurityDiscoverer programok konfigurációs bejegyzéseit is. Az adatok összefüggéseinek ellenőrzését végző üzleti logika réteg is ebben a program modulban helyezkedik el. Output oldalon kiszolgálja a SecurityMonitor adatkéréseit is, amik a lekérdezések és riportok alapjául szolgálnak.

SECURITYMONITOR (ADATMEGJELENÍTŐ MODUL)

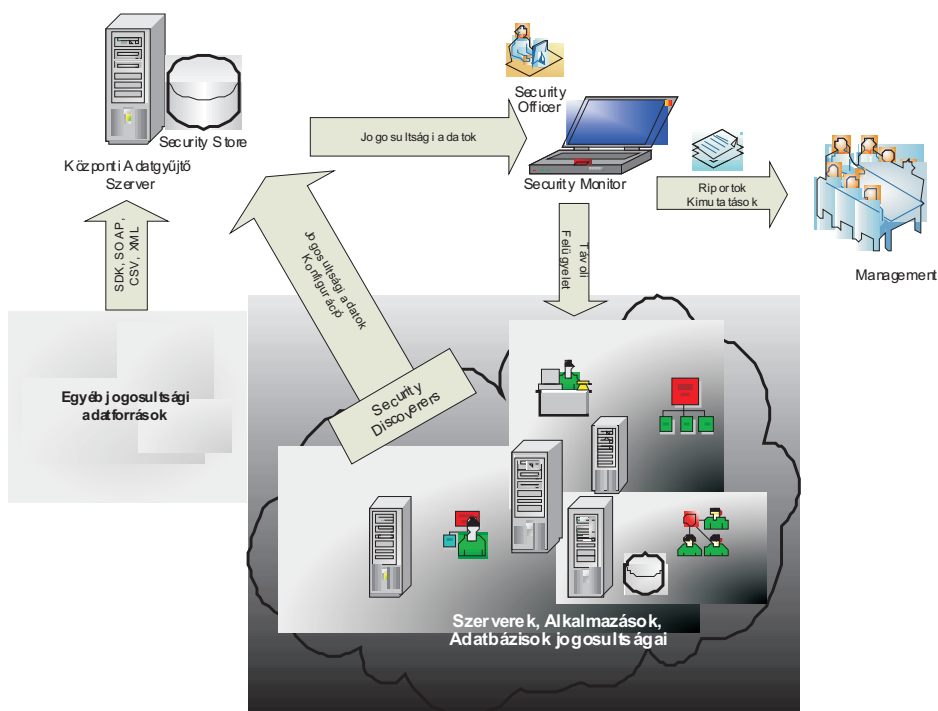
A modul feladata a klasszikus felhasználói funkciók biztosítása, úgymint:

- lekérdezések, riportok futtatása
- figyelmeztetések menedzselése
- rendszergazdai felület
- belső jogosultságkezelés
- SecurityDiscoverer programok távmenedzselése.

A különböző rendszerek adatainak egyesítését végzi, így egy felületen látható a megfigyelt felhasználó összes jogosultsága, amit a program kezelője néhány kattintással meg tud jeleníteni.

SARMAUTHORITYREQUEST (JOGOSULTSÁGIGÉNYLŐ MODUL)

A modul feladata, hogy a felhasználók a jogosultsági igényeiket elektronikusan egységes formában továbbítsák a megfelelő szervezetek felé. Ezzel kiindulási pontként szolgál igények engedélyezési/jóváhagyási folyamatának.



Seacon europe

8000 Székesfehérvár
Kertalja út 11.
Telefon: (06) 22 / 501-632
Fax: (06) 22 / 501-633
<http://www.seacon.hu>
seacon@seacon.hu