Napotki za ureditev varnosti na sistemih, kjer je nameščen Saop

V tem prispevku

Zadnja sprememba 27/07/2023 10:22 am CEST | Objavljeno 03/12/2020

Podatki in podatkovni strežnik so last stranke, kar pomeni, da za varnost in administracijo strežnika, omrežja in podatkovnih baz skrbi stranka sama, oz. njihov vzdrževalec opreme. Seyfor kot ponudnik programske rešitve skrbi, da je njihova programska oprema varna in da je varno implementirana.

Program Saop zadostuje zahtevam varnosti, saj za svoje delovanje na odjemalcih potrebuje samo »Uporabniške privilegije na sistemu«. Novo verzijo se lahko namesti samo z uporabniškimi privilegiji. Saop je aplikacija, nameščena lokalno na računalnikih ali strežniških mapah v skupni rabi. Podatki zajeti - vneseni preko programa Saop so shranjeni v podatkovnem strežniku Microsoft SQL server. Na podatkovni strežnik se Saop priključi z SQL Uporabnikom, kateri potrebuje minimalne pravice na strežniku. Ta uporabnik je aplikacijski uporabnik, zato naj bi ga uporabljala samo aplikacija.

Za administracijo in podporo SQL strežnika naj bi se uporabljali namenski SQL uporabniki. Enako velja za SQL uporabnike, ki so namenjeni izmenjavi / integraciji podatkov med različno programsko opremo. Kaj uporablja in kakšna dovoljenja ima SQL uporabnik, določijo razvijalci programske opreme, ki je izvor podatkov, saj v nasprotnem primeru ne morejo jamčiti konsistence podatkov.

Za svetovanja in podporo se uporablja ISL , kjer stranka in svetovalec vidita namizje stranke. Za diagnoze, odkrivanje in odpravljanje napak ter posege v podatke se, v kolikor je na voljo, po predhodnem dogovoru uporabi neposreden dostop na daljavo. V primeru drugačnih zahtev, so mogoči tudi drugi dostopi, kot so nadzorovani, naročeni, itd..

Varovanje strežnika, dostope do Windows strežnika in podatkovnega strežnika ureja pri stranki za to zadolžena oseba. Ta skrbi za izdelavo in nemoteno dnevno izdelovanje varnostnih kopij, kreiranje in dodeljevanje pravic SQL uporabnikom, dodeljevanje dostopov do Windows strežnika in podatkovnega strežnika, ...

Specifične SQL uporabnike za integracijo različne programske opreme ureja administrator strežnika, po navodilih dobavitelja programske opreme. Glede funkcij in procedur za integracijo s Saop lahko ta del (pravice za dostop do Saop baz) uredi tehnična podpora Seyfor.

Ko je na enem strežniku več informacijskih sistemov in vsi nudijo podporo z oddaljenimi dostopi, je potrebno vsakemu nastaviti določene / omejene

pravice, saj so v nasprotnem primeru vse varnostne nastavitve brezpredmetne. V kolikor ima uporabnik, ki nudi podporo administratorske pravice, lahko naredi vse in dostopi do vsega sam. Seveda se to lahko rešuje tudi z nadzorovanimi dostopi, server auditing (logiranje).

Poleg tega je na nivoju Windows sistemov in aplikacij potrebno skrbeti za ustrezno politiko in varovanje dostopnih gesel.

Kako lahko v iCentru pokrijemo zahteve po varnosti:

- Nastavitev enkripcije povezave med SQL in klientom.
- Konverzija vseh podatkov v SQL bazo (verzija 6.27 + ročna konverzija dokumentov v FILESTREAM – izvaja Seyfor tehnična podpora).
- Pravice za SAOPapp – potrebuje samo guest, bulk admin in database creator. SAOPapp mora bit db.owner vseh SAOP baz, oz. na njih imeti owner pravice.
- SQL strežnik naj teče pod virtualnim računom (privzet račun ob namestitvi SQL 2012) ali pod user računom (userja se kreira v ad, oz. win in se ga spremeni skoz SQL server configuration manager, ker na tak način SQL že sam nastavi minimalne zahtevane sistemske pravice, ki jih SQL potrebuje).
- Menjava privzetega gesla aplikacijskega uporabnika (SAOPapp).
- Nastavitev večkratnega dnevnega sistema za izdelavo rezervnih kopij in obveščanja o uspešnosti.
- Možnost uporabe drugega aplikacijskega uporabnika (novo verzijo se že vedno namesti kot SAOPapp – vklop SQL uporabnika pred namestitvijo, izklop po namestitvi).
- Menjava gesla skrbnika.
- Varna nastavitev Saop privzeto vse zaprto (parameter v nastavitvah okolja SEC_VSE NE).

Omejitve postavitve visoke varnosti:

- Za implementacijo visoke varnosti so zahtevana urejena domenska okolja.
- Vsaka specifična potreba stranke, ki zahteva drugačne nastavitve, privzeto visoko varnost izključuje in je potrebno iz visoke varnosti dodeljevati izključna dovoljenja za posamezne specifike.