

TURVAJUHTIMISTEENUSED

Sisukord

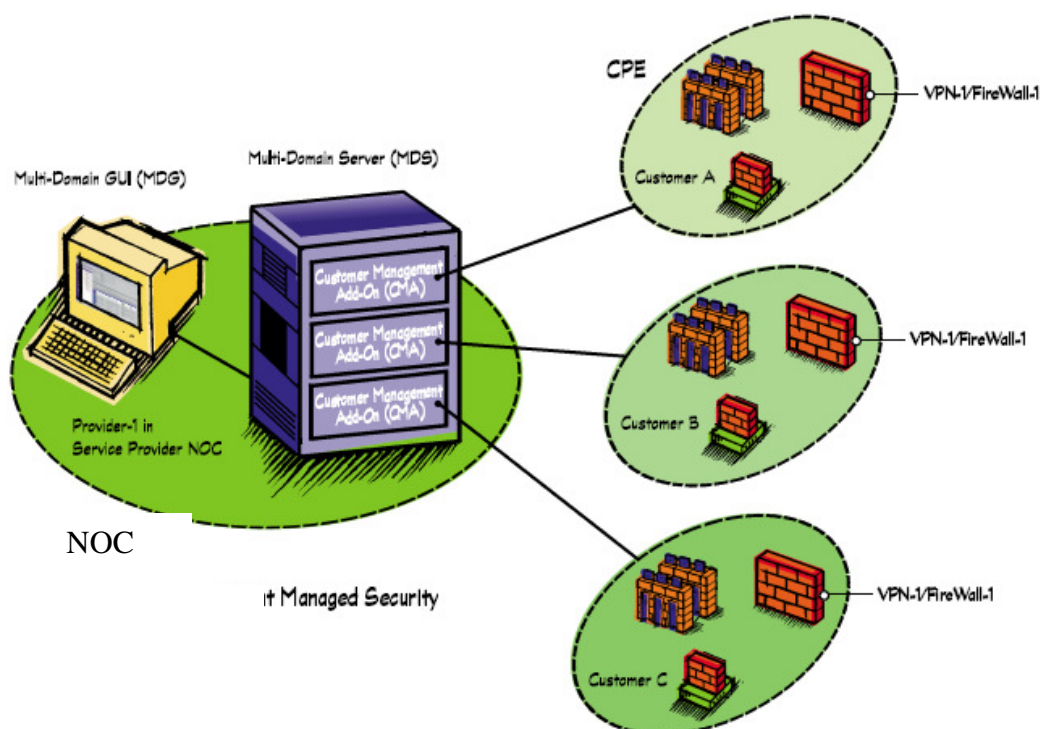
| | |
|---|---|
| Sissejuhatus..... | 1 |
| * Turvapoliitika defineerimine ja dokumenteerimine..... | 2 |
| Dokumenteerimine:..... | 2 |
| * Teenuse ettevalmistav faas | 3 |
| Loodava lahenduse struktuur | 3 |
| Lähtumine olemasolevast lahendusest..... | 3 |
| * Teenuse käitusfaas | 4 |
| Tulemüüri täishaldusteenuse eelised..... | 5 |
| Täishaldusteenuse versioonid | 6 |

Sissejuhatus

Managed Security Service (turvajuhtimisteenus) on integraalne andmeturva teenus, mis rahuldab kogu firma vajadusi turvalise elektroonse andmevahetuse järele nii firmasiseselt kui ka firmaväliste osapooltega, sh. ka Internetis.

Turvajuhtimine koosneb kahest osast:

1. Virtuaalne privaatvõrk (VPN) ja tulemüüri riist- ja tarkvara, mille tarnib teenuse osutaja, mis paiknevad kliendi ruumides, ja mida sageli tähistatakse lühendiga CPE (kliendiseadmed).
2. VPNi ja tulemüüri kaugmonitoring ja -haldus turvajuhtimislahendusi kasutades, mis paiknevad Võrguoperatsioonide keskus.



Teenuse elutsükkel on võimalik jaotada tingimuslikult mitmeks faasiks:

1. Ettevalmistav faas, mis omakorda on jaotatud:
 - a. Turvapoliitika defineerimine ja dokumenteerimine
 - b. Installeerimine ja/või integreerimine
2. Igapäevane opereerimine

Sõltuvalt konkreetse firma vajadustest ja hetkeolukorrast võib nende faaside kestvus olla erinev. Allpool kirjeldame me faase üksikasjalikumalt.

*** Turvapoliitika defineerimine ja dokumenteerimine**

Ühekordsed üritused turvalist andmesidet ei taga. Andmeside turvalisuse tagamiseks tuleb pidevalt teostada monitooringut ja värskendada turvalahendusi sõltuvalt uute tehnoloogiate arengust ja loomulikult sõltuvalt ka avastatud rünnete laadist. Aga enne kui on võimalik rakendada abinõusid turvapoliitika juurutamiseks, tuleb turvapoliitika defineerida ja samuti normikohaselt dokumenteerida. Sellel eesmärgil teostatakse ekspertanalüüs hindamaks firma andmeturvanõudmisi.

Turvapoliitika defineerimise käigus:

- Kõik kasutajad jaotatakse omaduste poolest sarnastesse rühmadesse oma õiguste ja kasutatavate ressursside põhjal;
- Firma ressursid grupeeritakse selle alusel, kui olulised konkreetset andmed on – olulised äriandmed (näiteks finantsandmed, kliendipakkumised, jne.) ja vähemolulised ressursid (näiteks kodulehekülg jne.);
- Firma ressursid grupeeritakse nende kättesaadavuse alusel;
- Kasutajad jaotatakse nende juurdepääsuõiguste alusel - juurdepääs ainult Intraneti piires, juurdepääs ainult väljastpoolt Intranetti jne.
- Määratakse kindlaks, millistele ressurssidele on juurdepääs ainult Intranetist, millistele nii Intranetist kui ka välisvõrgust;
- Defineeritakse kasutaja autentimise mehhanismid ning nende turvalisus.

Lisaks antakse turvariskide minimeerimiseks soovitusel seoses teiste antud firma IT osadega, näiteks infrastruktuuriga, kasutatavate erakanalitega jne.

Dokumenteerimine:

Firma turvapoliitika dokumenteeritakse kõige ülalkirjeldatu alusel ning selle tulemusel kujuneb firma turvapoliitika. Turvapoliitika on aluseks turvalahenduse nõudmistele ja parameetrite kindlaksmääramisele juhul, kui tuleb koostamisel uus turvalahendus. Igal juhul kasutatakse turvapoliitika edaspidi kogu turvalahenduse juhtimiseks. Loomulikult toimub pidevalt turvapoliitika arendamine ja värskendamine.

Lisaks kehtestatakse vormid ja reeglid selle kohta, kuidas toimub infovahetus kliendi ja teenuse pakkuja vahel, kellel on õigus saata päringuid teenuse pakkuja tulemüüri täishaldusteenuse osutamise ajal, kellel on õigus anda juhiseid kasutajate lisamiseks või kasutajaõiguste muutmiseks. Kehtestatakse spetsiaalsed vormid, mille abil teenuse osutaja informeerib klienti kliendi vastu suunatud rünnetest.

*** Teenuse ettevalmistav faas**

Kasutada saab põhiliselt kahte versiooni sõltuvalt kliendi poolt eelnevalt kasutatud tulemüüri lahendusest:

1. Alustades uue lahenduse väljaarendamist nullist või
2. Värskendades kasutatud lahendust teenuse osutamiseks vajalike komponentidega.

Loodava lahenduse struktuur

Turvalahenduse jaoks valitakse optimaalsed komponendid sõltuvalt koostatavast või olemasolevast turvaprofiilist:

- Sobiv tulemüüritarkvara;
- Sobiv tulemüüri riistvara;
- Vajadusel lahenduse dubleerimiseks vajalikud komponendid;
- Nõutavad VPNi (virtuaalse privaatvõrgustiku) komponendid firma harukontorite ühendamiseks;
- Nõutavad VPNi komponendid kodustöötajatele või liikuvatele töötajatele;
- Nõutavad vahendid valitakse kasutajate autentimiseks nii Intranetist ja vajadusel välisvõrgust;
- Vajalik haldustarkvara;
- Muud vajalikud komponendid.

Valik ülalnimetatud komponente paigaldatakse kliendi bürosse ja harukontoritesse ja vajadusel samuti kodustöötajate ja liikuvate töötajate sülearvutitesse. Turvalahendus luuakse vastavalt turvaprofiilis määratud nõudmistele.

Lähtumine olemasolevast lahendusest

Vastavalt koostatud või olemasolevale Turvaprofiilile täiendatakse tulemüüri lahendust vajalike puuduvate komponentidega:

- Sobiv tulemüüritarkvara;
- Sobiv tulemüüri riistvara;

- Vajadusel lahenduse dubleerimiseks vajalikud komponendid;
- Nõutavad VPNi komponendid firma harukontorite ühendamiseks
- Nõutavad VPNi komponendid kodustöötajatele või liikuvatele töötajatele;
- Nõutavad vahendid valitakse kasutajate autentimiseks nii Intranetist ja vajadusel välisvõrgust;
- Muud vajalikud komponendid.

Lisaks asendatakse või värskendatakse järgmisi mooduleid, mida vajatakse täishaldusteenuse pakkumiseks:

- Teenusepakkuja halduskonsool;
- Teenusepakkuja seirekonsool;
- Muud

Valik ülalnimetatud komponente paigaldatakse kliendi bürosse ja harukontoritesse ja vajadusel samuti kodustöötajate ja liikuvate töötajate sülearvutitesse. Turvalahendus luuakse vastavalt turvaprofiilis määratud nõudmistele.

*** Teenuse käitusfaas**

Pärast installeerimist ja seadistamist toimub lahenduse käivitamine. Teenuse käitusfaas koosneb järgmiste igapäevaste rutiinsete tegevuste administreerimisest:

- Lahenduse seire;
- Tarkvarauuenduste lisamine;
- Tootja poolt väljaarendatud tarkvarauuenduste lisamine uute rünnakute ärahoidmiseks;
- Kasutajate lisamine vastavalt kliendi poolt antud juhistele;
- Kasutajaõiguste muutmine vastavalt kliendi poolt antud juhistele;
- Uute ressursside lisamine vastavalt kliendi poolt antud juhistele;
- Pidev turvapoliitika hindamine;
- Vajadusel kasutatud riistvara uuendamine;
- Sammud, mis on vajalikud SLA s (teenuste taseme leping) sätestatud teenuseparameetrite tagamiseks. Näiteks riistvara asendamine ettenähtud aja jooksul ja spetsialisti kohalejõudmine kliendi bürosse, kui see osutub vajalikuks.
- Toimunud muudatuste dokumenteerimine.
- Turvaprofiili pidev uuendamine vastavalt teostatud ülesannetele ning kasutajate nimekirja muudatuste ning kasutajaõiguste muudatuste pidev uuendamine.
- Klienti puudutavate logide arhiveerimine.

Sõltuvalt kliendi vajadustest ja soovidest võib mõned halduse komponendid jagada kliendi ja teenuse osutaja spetsialistide vahel. Näiteks uute kasutajate lisamine ja kasutajaõiguste muutmine võivad kuuluda kliendi spetsialistide ülesannete hulka. Sellisel juhul täidab Adventus ülalnimetatud funktsiooni, kui kliendi spetsialist on pikemat aega ära või selle funktsiooni täitmine on Adventuse poolt pakutavat teenust kasutades tõhusam ja kiirem. Samas on muudatuste dokumenteerimine endiselt Adventuse ülesanne.

Tulemüüri täishaldusteenuse eelised

Tulemüüri täishaldusteenus on parim lahendus firmale:

- mis on otsustanud spetsialiseeruda kitsas ärivaldkonnas;
- mis tunnistab kõrge turvataseme vajadust andmevahetuse osas, kuid kus ei ole palgal IT turvaeksperte;
- mis tunnistab kõrge turvataseme vajadust andmevahetuse osas, kuid eelistab leida alternatiive kõrgetele alginvesteeringutele turvalahendustesse;
- kus soovitakse täiendada oma IT spetsialistide poolt pakutavat turvateenust ekspertide abiga;
- kus soovitakse minimeerida kiiresti muutuvast IT maailmas uute tehnoloogiate ja lahendustega kaasnevaid riske.

Tulemüüri täishaldusteenuse kasutamise alustamine on hõlbus. Selleks on vaja ainult selgelt väljendatud soovi omada tipptasemel ekspertjuhtimisega turvalahendust.

Tulemüüri täishaldusteenus sisaldab kõiki kohustuslikke turvapoliitika ja turvajuhtimise komponente, mis jäävad sageli katmata väikestes ja keskmise suurusega firmades ebapiisava väljaõppe, kogemuse ja väga sageli ka IT spetsialistide ajapuuduse tõttu. Tulemüüri täishaldusteenus sisaldab järgmist:

- Turvapoliitika väljatöötamine;
- Kasutajate ja kasutajaõiguste kontrollimine, kasutajaõiguste vastavus valitud turvapoliitikale;
- Juurdepääsureeglid erinevatele ressurssidele;
- Turvariskide perioodiline analüüs;
- Kogu lahenduse ja sisseviidud muudatuste ja täienduste dokumenteerimine.

Antud teenus sobib ka praegustele CheckPointi kasutajatele. Isegi kui firma juba kasutab tulemüüri täishaldusteenust, ei kaota klient oma eelnevaid investeeringuid, kuna ka täishaldusteenuse korral on võimalik kasutada enamikku komponentidest. Sellisel juhul väheneb kliendi jaoks täishaldusteenuse teenustasu, kuna teenuse pakkuja investeeringuga seotud riskid on väiksemad, kuna lisada tuleb ainult haldusmoodul.

Kui klient liigub arenguspiraali mööda edasi ja jõuab punkti, kus on vajalik või mõnel muul kaalutlusel põhjendatud oma ekspertide ja juhtrühma palkamine, saab klient ikkagi kasu tulemüüri täishaldusteenuse kasutamisest. Nimelt:

- Ei ole vaja maha kanda eelmistel perioodidel tehtud investeeringuid.

- Halduse ülevõtmisel on võimalik üle võtta kogu operatsioonisüsteem ning puudub vajadus investeerida uue turvakontseptsiooni väljatöötamisse.
- Kliendile edastatakse täielikult dokumenteeritud lahendus.
- Kliendile edastaks dokumenteeritud ajalugu.
- Võimalik on teenuse osutaja kasutuses olevad lahenduse komponendid välja osta jääkväärtusega.

Täishaldusteenuse versioonid

Tulemüüri haldamise täisteenust on võimalik osutada kahe mudeli alusel.

Esimesel juhul osutatakse täishaldusteenust, kus kogu vajalik lahendus ja oskusteave tulevad teenuse pakkujalt, k.a. vajalikud tarkvaramoodulid ja riistvara.

Teisel juhul osutatakse segmenteeritud teenust, kus sõltuvalt kehtestatud turvapoliitikast jagatakse ülesanded ja õigused teenuse pakkuja ja kliendi spetsialistide vahel. See versioon sobib klientidele, kes tahavad omada litsentse ja seadmeid või kes juba kasutavad CheckPoint tulemüüri lahendust, kuid soovivad delegeerida osa või kõik haldusprotseduurid teenuse pakkuja ehk firma Adventus Solutions spetsialistidele.