

Ciscon tietoturvastrategia: vastustuskykyiset tietoverkot



Millainen on vastustuskykyinen verkko?

Voiko tietoverkko puolustaa itse itseään? Lyhyt vastaus on "Kyllä voi!" Verkkojen tietoturva on kehittynyt vähitellen yksittäisistä erillistuotteista järjestelmätason ratkaisuksi. Nykyaikaisen tietoverkon on pysyttävä hengissä ja toimintakuntoisena, kohdistuipa siihen minkälainen hyökkäys tahansa.

Yritysten tietoverkot ja niihin kohdistuvat hyökkäykset ovat muuttuneet entistä monimutkaisemmiksi, eikä tietoturvassa sen vuoksi voida luottaa mihinkään yksittäiseen mekanismiin. Tästä on syntynyt monitasoisen puolustuksen käsite, jonka nojaa ennakoiviin ja mukautuviin tietoturva-ratkaisuihin. Vastustuskykyisen verkon luonteeseen kuuluvia ominaisuuksia ovat:

- Verkkopalveluiden saatavuus ja käytettävyys on oltava turvattu myös mahdollisen hyökkäyksen aikana
- Käyttäjien on päästävä turvallisesti verkkoon mistä tahansa



- Verkkoon kytkettävät laitteet ja käyttäjät on voitava tunnistaa, niiden tietoturvan tila on voitava määrittää, jonka perusteella ne voidaan valtuuttaa
- Verkon tietoturvan on oltava tietoinen sovelluksista ja tarvittaessa voitava vaikuttaa sovellusten käyttöön
- Suojata päätelaitteita tehokkaasti erilaisia tunnettuja ja tuntemattomia hyökkäyksiä vastaan
- Mahdolliset hyökkäykset on havaittava nopeasti ja niiden eteneminen voitava rajoittaa

Miten vastustuskykyinen tietoverkko rakennetaan?

Ciscon vastustuskykyinen tietoverkko on uudenlainen järjestelmätason ratkaisu, jonka avulla voidaan pienentää tietoturva-avoittuvuuksien aikaikkunaa, hyökkäysten vaikutusta ja parantaa verkon käytettävyyttä ja luotettavuutta. Vastustuskykyisen verkon rakentaminen perustuu kolmeen teemaan.

Ensimmäinen teema on *integroitu tietoturva*, eli tietoturvan ulottaminen koko verkon yli. Verkon jokainen komponentti, reitittimet, kytkimet jne. ovat mahdollisia hyökkäyksen kohteita tai välineitä ja niiden suojaaminen on mahdollista ainoastaan integroimalla tietoturva osaksi kyseistä verkko-laitetta.

Toinen teema on *yhteistoiminnallisuus*. Kun tietoturva muuttuu järjestelmätason ratkaisuksi tarvitaan yhteistoiminnallisuutta eri komponenttien, kuten verkon ja tietoturvan välille, sekä myös yhteistyökumppaneiden välille. Esimerkkinä verkon pääsynvalvonta, joka voi olla tietoinen mahdollisesta virusten aiheuttamasta tietoturvauhasta ja sen perusteella rajoittaa verkkoon pääsyä.

Kolmas teema on *mukautuva tietoturva*, jonka tavoitteena on tarjota entistä dynaamisempaa, monikerroksista suojaa päätelaitteille, käyttäjille ja sovelluksille. Uudentyyppisillä Anti-X palveluilla (anti-virus, anti-spyware, anti-mato, anti-phishing) ja sovellustietoisella tietoturvalla voidaan suojata jokainen sovellusvuo tai paketti, joka verkossa liikkuu. Verkon tietoturva- ja sovellustietoisuutta lisäämällä voidaan nopeammin tai jopa automaattisesti pysäyttää tunnetut ja tuntemattomat hyökkäykset.

Cisco on sitoutunut jatkuvasti kehittämään myös uusia tietoturvamekaniismeja ja -ratkaisuja, joilla saadaan entistäkin parempi tietoisuus tietoturvan kokonaistilasta verkossa ja parempi kontrolli verkossa oleviin laitteisiin, käyttäjiin ja sovelluksiin.

Vastustuskykyisen verkon hyödyt liiketoiminnalle ja tietoturvan ammattilaisille

- Auttaa täyttämään lainsäädännölliset vaatimukset
- Suojaa yritysten ja organisaatioiden kriittisen tiedon
- Turvaa liiketoiminnan jatkuvuuden
- Auttaa liiketoiminnan ja IT:n riskienhallinnassa
- Auttaa valvomaan tietoturvapolitiikan noudattamista
- Suojaa tietoverkkoa turvatomilta tai saastuneilta päätelaitteilta
- Mukautuu nykyisiin ja tuleviin uhkiin

Lisätietoja

www.cisco.com/go/security

www.cisco.com/go/selfdefend

Cisco keskeisten tietoturvaluotteiden avainominaisuudet



Cisco MARS (Security Monitoring, Analysis and Response System)

- Lokitiedon analysointityökalu
- Tunnistaa korreloimalla uhkia ja suosittelee mahdollisia torjuntamenetelmiä
- L2/L3 -verkkotopologian tuntemus visualisoi hyökkäysten kulun ja parhaat torjuntapaikat verkossa
- Tuki useille laitevalmistajille
- Mukautettavat haku- ja raportointiominaisuudet

Security Auditor -ohjelmisto

- Auttaa organisaatioita täyttämään lain asettamat vaatimukset
- Havaitsee verkon tietoturvassa olevia aukkoja
- Automatisoi verkon auditointiprosessia ja antaa konfiguraatio-suosituksia
- Laaja ja joustava raportointi
- Sisältää tietoturvapoliitikoiden tarkistuksia tunnettujen käytäntöjen pohjalta (NSA, CIS, Cisco SAFE)

VMS-hallintajärjestelmä (CiscoWorks VPN / Security Management Solution)

- VPN-reitittimien, palomuurien ja IPS-laitteiden keskitetty hallintajärjestelmä
- Käyttäjien roolipohjainen pääsyhallinta
- Auto Update Server mahdollistaa etäkäytössä olevien palomuurien sääntöjen ja ohjelmistoversioiden päivittämisen

Network Admission Control (NAC)

- Lisää kaikenkokoisten verkkojen tietoturvaa varmistamalla verkkoon pyrkivien laitteiden tietoturvan ajantasaisuuden
- Ennakoiva suojaus virusten, matojen ja haittakoodien leviämiseksi
- Laajentaa verkkoinfrastruktuuriin ja päätelaitteiden tietoturvahallinnan käyttömahdollisuuksia
- Käytettävissä kytkinverkoissa, reititinverkoissa, langattomissa verkoissa ja VPN-etäyhteyksille
- Toteutus mahdollinen joko NAC-erillisjärjestelmällä tai olemassa olevaan järjestelmään integroimalla

NAC-erillislaitte (Cisco Clean Access)

- Pakettiratkaisu, jossa on valmis tuki virustorjunta ym. tietoturvasovelluksille sekä Microsoft-päivityksille
- Sopii kaiken kokoisille yrityksille ja organisaatioille
- Täydentää integroitua NAC-järjestelmää

Integroitu NAC-ratkaisu

Tarjoaa saman toiminnallisuuden kun Clean Access ja lisäksi

- Uudenlainen arkkitehtuuri ja toteutus
- Yhdistää keskitetyn tietoturvapoliitiikan hallinnan, älykkään verkon ja ratkaisut yli 50:ltä johtavalta virustorjunta ja tietoturvalaitevalmistajalta

Cisco Security Agent - tietoturva-agentti

- Päätelaitteiden tietoturvaratkaisu tuntemattomien tietoturvaohjelmien torjuntaan
- Päivitysvapaa arkkitehtuuri
- Ohjelmistojen ja päivitysten inventointi
- Yksityiskohtainen säännösten hallinta ja mahdollisuus NAC-integraatioon.

Cisco ASA 5500 tieturvalaitte (Adaptive Security Appliance)

- Yhdistetty palomuuuri, IPS, verkkovirusten torjunta, IPSec- ja SSL VPN -palvelut
- Integroitu ratkaisu yksinkertaistaa ja tuo kustannussäästöjä
- Helppo ottaa käyttöön ja hallita
- Monipuoliset ominaisuudet ja laajennettavuus myös tulevaisuudessa



VPN 3000 -keskitin

- Cisco Secure Desktop (CSD) tarjoaa edistykselliset tietoturva-ominaisuudet SSL VPN -yhteyksien suojaamiseksi
- Laaja tuki käytännössä kaikille sovelluksille SSL VPN client -ohjelmistolla
- Citrix-tuki
- Mahdollisuus integroida IPSec -yhteydet NAC-järjestelmään



AVS 3110 Application Velocity System

- Web-pohjaisten sovellusten optimointi, suorituskyvyn ja turvallisuuden parantaminen
- Minimoi verkon viiveen ja tarjoaa 2 - 5 kertaisesti parantuneet vasteajat
- Vähentää kaistan tarvetta 70-90%
- Vähentää servereiden kuormitusta jopa 80%

ISR 800, 1800, 2800, 3800 -monipalvelureitittimet

- Integroitu tilatietoinen palomuuuri, VPN, IPS, Access-listat, NAT ja PAT – ideaalinen haarakonttoreiden, pienten yritysten ja palvelun tarjoajien laite
- Edistykselliset VPN-tekniologia tukee mm. VoIP, Multicast, QoS ja DMVPN -ominaisuuksia
- Integroidut palvelut uusille teknologioille, kuten puheelle, langattomuudelle, SSL VPN, NAC, Anti-X
- Web-pohjainen laitehallinta, SDM



PIX 501 / 506 / 535 -palomuuuri

- Kustannustehokas ja helppo ottaa käyttöön
- Käyttäjien ja sovellusten tietoturvan hallinta, hyökkäysten torjunta ja turvalliset yhteydet
- Tilatietoinen palomuuuri, VPN, dynaaminen NAT ja PAT
- Helppokäyttöinen web-pohjainen hallinta, PDM



IPS 4200 hyökkäyksen tunnistuslaitteet

- Parempi suojaus edistyksellisellä tarkkuudella
- Tarkka matojen tunnistus integroidulla tapahtumien korreloinnilla
- Riskilähtöinen uhkaluokitus
- Sovellustarkitus vakoilu- ja mainosohjelmille sekä P2P-liikenteelle



Catalyst 6500 / 7600 tieturvalaitepalvelumoduulit

- WebVPN, FW, IPS, IPSec VPN, DDoS, SSL -palvelumoduulit tarjoavat laajennettavat ja yhtenäiset tietoturvapalvelut palveluntarjoajille ja suuryrityksille
- Hyvä investointien suoja ja alemmat kokonaiskustannukset
- Palveluiden virtualisointi helpottaa käyttöönottoa, vähentää monimutkaisuutta ja alentaa käyttökustannuksia



Lisätietoja: www.cisco.com/go/security

Cisco Systems Finland Oy, Lars Sonckin kaari 16, 02600 Espoo. Puh: 0204 7061, faksi: 0204 706300, www.cisco.fi