Intelligent sikkerhed i netværket

Perimeter-beskyttelse udfordret af nyt trusselsbillede

Omfattende hackingangreb på store organisationer med værdifuld data er blevet dagligdag. I Danmark er der mange eksempler på sofistikerede angreb, der har kompromitteret større virksomheder med tillids- og datatab til følge. Dette til trods for store sikkerhedsinvesteringer.

Traditionel perimeter-beskyttelse, der fokuserer på at forhindre indtrængen udefra, kan ikke alene håndtere de nye sikkerhedsudfordringer. Mange trusler kommer i dag indefra, og ikke alle enheder kan styres, sikres eller kontrolleres ved at anvende klientsoftware. Der findes ikke én løsning, der kan sikre virksomheden 100% imod angreb, og derfor bør man som sikkerhedsansvarlig stille

? Hvilke muligheder findes i dag, når en hacker har brudt virksomhedens forsvar?

Hvordan opnår virksomheden tilstrækkelig viden om et sikkerhedsbrud, så skadens omfang og konsekvenser kan vurderes og forhindres i fremtiden?

sig følgende spørgsmål:

Svaret på disse spørgsmål kan være at anvende selve netværket som forsvar. Det stigende antal DDoS, malware og APT-angreb kræver nemlig, at virksomheder og organisationer anvender nye mere intelligente teknikker og metoder for at opnå viden og visibilitet i og omkring netværket. Når først angrebene eller truslerne er identificerede, kan de prioriteres, adresseres og fjernes.

Netværket som garant for sikkerhed i infrastrukturen

For at kunne beskytte sig mod kendte trusler er det nødvendigt at have en robust og skalérbar infrastruktur, som ikke alene kan adressere sårbarheder men også give løbende overblik over netværkets tilstand. Viden om netværkets trafikmønster gør det muligt at opdage f.eks. port-scanning fra klient til klient på det lokale netværk eller ”zero day”-angreb, der ellers vil flyde sammen med den almindelige netværkstrafik.

Conscia kan hjælpe dig til at få et netværk, der er så intelligent og fleksibelt som muligt, og som samtidig er dit bedste værn mod det nye trusselsbillede. Det er netværket, der binder infrastrukturen sammen, og det er her de vigtige beslutninger om trafikhåndtering skal foretages. Netværket ser alle brugere, applikationer, klienter og servere og er derfor det naturlige udgangspunkt for at skabe visibilitet og ikke mindst sikkerhed i it infrastrukturen.

Visibilitet end-to-end med Cisco Cyber Threat Defense

Conscia og Cisco kan hjælpe dig med at styrke sikkerheden i dit netværk. Som førende på netværks- og datacenterområdet er Ciscos teknologier nemlig stærkt positioneret til at tage kampen op imod det nye trusselsbillede.

Cisco Cyber Threat Defense giver nemt og enkelt et centralt og præcist overblik af hele infrastrukturen - fra det kablede og trådløse access-lag, gennem distributions- og core-infrastruktur til det moderne datacenter med virtuelle driftsmiljøer.

Cyber Threat Defense er et unikt værktøj, som opsamler, skaber sammenhæng og præsenterer realtidsadfærd end-to-end i infrastrukturen. Dette øger netværks- og sikkerhedsteamets effektivitet, samtidig med at driftsomkostninger reduceres og den overordnede sikkerhedssituation forbedres.

Conscia hjælper dig

Conscia er Cisco Gold Partner og har mange års erfaring med at levere Cisco infrastruktur – netværk, datacenter og sikkerhed. Sammen med vores kunder arbejder vi målrettet for at få det størst mulige udbytte af de nyeste teknologier.
Vil du vide mere om, hvad Conscia kan gøre for din organisation på sikkerhedsområdet:
Kontakt din Conscia account manager, eller send en mail til conscia-sikkerhed@conscia.dk.