Cloud-baseret sikkerhed i DNS-laget

Cisco Umbrella

80 mio. forespørgsler blokeret dagligt

Cisco Umbrella (tidligere OpenDNS) er den tjeneste efter Google, der varetager næstflest internetforespørgsler. I en kombination med Threat Intelligence fra Ciscos Security Lab stilles data til rådighed på en Cloud-platform, der giver brugere øjeblikkelig indsigt i trusselsbilledet - set fra et DNS-perspektiv.

Cisco Umbrella har overblik over, hvilke DNS-infrastrukturer, IP-netværk, Autonomous-systemer og DNS-registranter, der distribuerer malware, styrer botnets og phishing-kampagner.

Dette Big Data-baserede overblik resulterer i, at der blokeres mere end 80 millioner forespørgsler om dagen.

Meget mere end en DNS-server

Cisco Umbrella er langt mere end en DNS-service, og porteføljen indeholder en række stærke sikkerhedsydelser.

Udgangspunktet for ydelserne er at tilbyde effektiv beskyttelse og rapportering med baggrund i den unikke adgang til Cisco Umbrellas enorme datasæt.

Én af mulighederne er fx at få adgang til et investigate-modul, det giver et dybere indblik i det datagrundlag, som sikkerhedsbeslutningerne bliver truffet ud fra. Investigate-modulet kan integreres med egne sikkerhedslog-systemer, hvilket styrker efterforskningen af sikkerhedsrelaterede hændelser i virksomhederne.

Conscia - eneste Cisco Umbrella Elite Partner i Norden

Conscia er specialiseret i Cisco Umbrellas produktportefølje, og vi er, som de eneste i Norden, certificeret Elite Partner. Vi giver dig indblik i, hvordan DNS-baseret Big Data kan styrke din virksomheds sikkerhedsindsats og samtidig skabe viden, visibilitet og overblik over hele infrastrukturen før, under og efter et angreb.

Kontakt marketing@conscia.com, hvis du vil høre mere om vores sikkerhedsløsninger.

Beskyttelse før, under og efter et malware-angreb

Download	Call-back	Krypteringsnøgle	Karantæne
Reklamer på nettet eller et link i en email sender DNS-forespørgslen afsted, inden siden med malware tilgås. DNS-forespørgslen registreres, og er den kendt som ondsindet, blokeres forespørgslen.	Hvis malware når ind på et system, analyserer den ofte dette, inden den sender en forespørgsel tilbage for at modtage en ransomeware-pakke. Callback-forsøg genkendes og forhindres, og der er samtidig udviklet algoritmer, der kan opdage og forudsige callback-destinationer til malware-pakker.	Hvis det alligevel lykkes ransomeware at inficere maskinen, benytter denne ofte DNS-initieret callback til fx at modtage en krypteringsnøgle. Et eksempel er CryptoLocker. Netop CryptoLocker blev stoppet ved at hindre den i at lave callback til sin botnet controller.	Nogle ransomeware-varianter behøver ikke lave callback, før løsesummen skal indbetales. Her begrænses skaden ved at forhindre den inficerede enhed i at forbinde sig til flere enheder og sprede malware.