simac

Internetveiligheid met Cisco Umbrella: Blokkeren is beter dan genezen

Het is de nachtmerrie voor elke organisatie. Plots werkt internet traag en komt er een massa spamberichten binnen. Of erger nog, hackers gaan er met privacygevoelige informatie vandoor, en dat terwijl er toch maatregelen waren getroffen in de vorm van een firewall en virusscanners.

Daarom is het verstandig om een extra verdedigingslinie op te werpen tegen cybercriminelen. Een makkelijke manier om dat te doen is Umbrella van Cisco gebruiken. Deze toepassing zorgt ervoor dat bedreigingen uw netwerk niet bereiken. Het beschermt tegen malware, ransomware, phishing en met virussen geïnfecteerde apparatuur die met uw netwerk contact willen maken.

Wat is Cisco Umbrella?

Cisco Umbrella is een toepassing die bescherming biedt tegen cybercriminelen, waar gebruikers zich ook bevinden. Het maakt gebruik van DNS, oftewel het Domain Name System. Een soort telefoonboek voor internet, dat domeinnamen vertaalt naar IP-adressen. Het zorgt ervoor dat als u gaat zoeken op internet gewoon 'Google' kunt intikken in plaats van een ingewikkelde getallencombinatie. Vergelijk het maar met de contactenlijst op uw mobiele telefoon, die zorgt er ook voor dat u niet alle 06-nummers uit uw hoofd hoeft te leren. Umbrella grijpt in nog voor de ingegeven domeinnaam contact legt met het IP-nummer, mocht dat nummer niet te vertrouwen zijn.

Er zijn verschillende manieren waarop hackers gebruikers naar een 'foute' site proberen te krijgen:

Social Engineering

Door gebruik te maken van menselijke 'zwaktes', zoals nieuwsgierigheid, hebzucht, of onoplettendheid. Social Engineering heet dat. Phishing is hier een voorbeeld van. Hackers gaan tegenwoordig heel ver, ze kunnen zich via sms of WhatsApp voordoen als een bekende. Er zijn al heel wat mensen opgelicht, omdat ze dachten dat een vriend hen om geld vroeg. Maar ze kunnen u natuurlijk ook verleiden op een 'verkeerde' link te klikken. Soms kan een typefoutje al genoeg zijn (Go0gle in plaats van Google) om op een pagina terecht te komen vol malware, advertenties waar een hacker aan verdient of politieke boodschappen.

1.

Domein kapen

Een andere bedreiging is dat wanneer uw domeinnaam wordt gekaapt, bezoekers worden doorgesluisd naar een perfect nagebouwde site. Als mensen daar bijvoorbeeld hun creditcardgegevens achterlaten, kunnen hackers daar vervolgens heel gemakkelijk misbruik van maken.

2.

DDoS-aanval

Hackers kunnen ook grote hoeveelheden data naar uw systeem sturen. In dat geval kan het compleet stil komen te liggen. Dat gebeurt bijvoorbeeld bij een DDoS-aanval. DDoS staat voor 'Distributed Denial of Service'. In zo'n geval raakt het systeem compleet verstopt en kan er geen informatie meer in of uit.

3.

Wat doet Cisco Umbrella hiertegen?

Umbrella blokkeert de weg naar 'foute' sites en voorkomt dus onjuiste verbindingen. Zo kun je bijna alle bedreigingen buiten de deur houden. Continu wordt door mens en machine in de gaten gehouden welke adressen in het 'telefoonboek' te vertrouwen zijn en welke niet.

Kracht zit in de schaalgrootte

De kracht van Cisco Umbrella zit hem vooral in de schaalgrootte. Cisco werkt samen met meer dan 500 internetproviders en ziet zo elke dag enorm veel internetactiviteit. Experts houden bovendien het gedrag van de miljoenen Umbrella-gebruikers in de gaten, ook als ze niet aan het bedrijfsnetwerk zijn gekoppeld. Dat levert een schat aan informatie op. Daardoor is vaak al vooraf in te schatten dat er een cyberaanval gaat komen en welke IP-adressen en domeinnamen daarmee gemoeid zijn. Die komen dan op de 'zwarte lijst'.

Gebruikers van Umbrella kunnen ook zelf overzicht krijgen in internetbedreigingen die op hen afkomen. Dat inzicht kan een extra hulpmiddel zijn om diefstal van data te voorkomen. Elk lek in de beveiliging kan immers grote gevolgen hebben. In een ziekenhuis bijvoorbeeld, kan het een kwestie van leven of dood zijn, als criminelen aan internet gekoppelde medische apparatuur stil kunnen leggen.

Privacy

De zorg is een sector waar veel persoonsgegevens digitaal worden opgeslagen. Als medische dossiers op straat komen te liggen, kan de autoriteit persoonsgegevens besluiten torenhoge boetes opleggen. Dat wil zeggen, als gebleken is dat de beveiliging niet op het juiste niveau was gebracht.

Een bekende gebruiker van Cisco Umbrella is de RAI in Amsterdam. Die zorgt er op die manier voor dat bezoekers van een beurs of congres het internet op kunnen, zonder dat ze hoeven te vrezen dat hun mobiele apparatuur besmet raakt of dat anderen bij daarop opgeslagen bestanden kunnen.

Cloud

Een bijkomend voordeel van Umbrella is dat het werkt vanuit de cloud. Gebruikers hoeven daardoor geen hardware te installeren om updates te ontvangen en ook geen software, want wijzigingen worden automatisch doorgevoerd.

Wat doet Simac?

Simac kan ervoor zorgen dat Cisco Umbrella al binnen een uur draait, zonder dat IT'ers binnen uw organisatie er naar om hoeven te kijken. Mede omdat de toepassing goed kan samenwerken met andere applicaties, kan deze worden ingepast in een complete beveiligingsstrategie. Simac kan helpen die op te zetten. Meestal wordt daarbij eerst gekeken naar waar zwakke plekken zitten, waar de kern van een organisatie zit, waar het echt pijn doet als uw organisatie wordt geraakt. Vervolgens bedenkt Simac een op maat gesneden oplossing om de veiligheid van uw organisatie optimaal te maken.

Wilt u meer weten over Cisco Umbrella? Neem dan contact op met Simac, dat kan telefonisch via **040-2582944** of mail **info@simac.com**

simac

cisco Gold Partner