Tjänstebeskrivning: Umbrella DNS-skydd

Av denna Tjänstebeskrivning framgår vad som gäller för tjänsten Umbrella DNS-skydd vilken är en tilläggstjänst till Bredband2s Internettjänster Fiber City (FC) respektive Fiber Business (FB).

Kundens avtalade servicenivå (SLA) för FC/FB gäller för tjänsten.

Umbrella DNS-skydd

Är en molnbaserad säkerhetstjänst som detekterar och blockerar misstänkta eller svartlistade domäner som används för malware, C2 callbacks, phishing- och ransomware-attacker. Med en kombination av artificiell intelligens och de drygt 120 miljarder domänförfrågningarna som dagligen analyseras av systemet stoppas både kända skadliga domäner samt de som förutspås bli skadliga domäner.

Riskreducering

Genom att alla kundens DNS-anrop passerar via Umbrellas DNS-skydd så skyddas klienterna från elakartade domäner. Tjänsten skyddar automatiskt de enheter som befinner sig på kundens LAN. För de enheter som befinner sig utanför LAN:et ingår klientskydd som kan installeras på enheter med följande operativsystem: Windows, macOS eller ChromeOS.

Policy

Det finns möjlighet att själv sätta regler och göra kundspecifika policys via webbportal såsom:

- Olika regler på grupp- respektive användarnivå genom AD-integration.
- Blockera trafik till domäner som anses vara riskabla.
- Skapa egna blockeringssidor för skadliga domäner.
- Blockera användande av s.k. Molntjänster såsom Dropbox m.m.
- Blockera hela kategorier av webbsajter såsom spelsajter, pornografi m.m.
- Blockering av enstaka webbsajter.
- Välja var loggfilernas ska sparas; Europa alternativt USA.

Rapporter

I webbportalen kan kunden generera rapporter på besökta- respektive blockerade domäner:

- Realtidsstatistik och schemalagda utskick.
- Sorterade på användare och/eller enheter respektive externa IP-adresser.
- Sorterade på olika typer av säkerhetskategorier (malware, phishing m.m).
- Sorterade på vilka molntjänster som används av användarna.
- Öppet API som ger möjlighet att integrera plattformen i andra rapportverktyg eller säkerhetslösningar.

Tekniska förutsättningar

Tjänsten kräver ingen utrustning och klientskyddet som ingår installeras på kundens egna enheter (kräver ett av följande operativsystem: Windows, macOS eller ChromeOS). Tjänsten förutsätter att kundens FC-/FB-tjänst levereras med en statisk IP-adress.