



Firewall Protection

De cyberdreiging is de afgelopen jaren sterk toegenomen en dagelijks worden er nieuwe manieren gevonden om IT infrastructuur aan te vallen en gegevens te stelen. De firewall protection van Sharp IT Services is gebaseerd op onze best-practices voor het inrichten van Security. Dankzij deze aanpak zijn wij in staat om bedreigingen op meerdere lagen tegen te gaan. Dit is een vast onderdeel van onze Cyber Essentials suite, die is geaccrediteerd in het Verenigd Koninkrijk.

Het beschermen van organisaties en gegevens tegen de dreiging van hackers, malware en virussen is een serieuze taak. Met zoveel kritische gegevens op de servers, in de Cloud, op laptops, desktopcomputers en handapparatuur hebben bedrijven een geïntegreerde beveiligingsoplossing nodig. We hebben een breed aanbod van beveiligingsoplossingen voor onze klanten en beschikken over een breed netwerk aan deskundigheid en ervaring met betrekking tot de belangrijkste beveiligingstools en -technologieën.

De Firewall Protection van Sharp is een zakelijke oplossing voor de beveiliging van organisaties. Zo verzekeren wij dat onze klanten over de beste beveiliging beschikken. Deze service is opgebouwd rond een firewall en op alle PC's, laptops en services wordt software geïnstalleerd om verdacht gedrag te monitoren.

De firewall en beveiligingsservices worden binnen de Firewall Protection-service door het IT-team van Sharp gemonitord. Verdacht gedrag wordt aan ons IT team doorgegeven, waarna actie wordt ondernomen, vaak nog voordat er hinder wordt veroorzaakt. Wij maken regelmatig een verslag. Daarnaast zorgen we voor nieuwe releases die gepaard gaan met updates.

Belangrijkste functies



Preventie van binnendringing

Software waarmee een netwerk proactief wordt gemonitord en waarmee preventieve maatregelen worden getroffen tegen verdachte activiteiten.



Detectie van binnendringing

Software waarmee een netwerk proactief wordt gemonitord en waarmee de gebruiker wordt gewaarschuwd als verdachte activiteiten worden waargenomen.



Filteren van webpagina's

Software waarmee de websites die gebruikers op hun computer kunnen bezoeken worden beperkt.



Contentfilter

Software waarmee de content waartoe gebruikers toegang kunnen hebben, wordt beperkt of geregeld.



Filteren op malware

Software waarmee gebruikers tegen kwaadaardige software worden beschermd.



Preventie van gegevensverlies

Software waarmee potentiële datalekken worden gedetecteerd en voorkomen door gevoelige gegevens te monitoren, te detecteren en te blokkeren.



Op reputatie gebaseerde verdediging

Beoordeelt de bestemming van uitgaande verbindingen en bepaalt het dreigingsniveau aan de hand van ingevoerde informatie. Met behulp van de dreigingsscore die dit oplevert, worden bekende dreigingen geblokkeerd en veilige bestemmingen toegestaan.



Gateway Antivirus

Met Gateway Antivirus kunnen applicaties bestanden op virussen controleren. De webservice waarmee dit wordt gedaan, maakt gebruik van SOAP (Simple Object Access Protocol).