Basisinformatie over netwerkbeveiliging voor MKB-bedrijven

Wat is netwerkbeveiliging?

Netwerkbeveiliging omvat elke activiteit die is bedoeld om de bruikbaarheid en integriteit van uw netwerk en gegevens te beschermen. Dit betreft zowel hardware- als softwaretechnologieën. Met effectieve netwerkbeveiliging wordt de toegang tot het netwerk beheerd. Hierbij worden diverse bedreigingen gestopt zodat deze zich niet verder kunnen verspreiden op uw netwerk en hackers geen toegang krijgen.

Hoe werkt netwerkbeveiliging?

Bij netwerkbeveiliging worden meerdere beveiligingslagen bij de edge en in het netwerk gecombineerd. Op elke netwerkbeveiligingslaag worden beleidsregels en controles geïmplementeerd. Geautoriseerde gebruikers krijgen toegang tot netwerkresources, maar kwaadwillenden worden geblokkeerd zodat ze geen exploitaties en bedreigingen kunnen uitvoeren.

Hoe profiteer ik van netwerkbeveiliging?

Digitalisering heeft onze wereld getransformeerd. Onze manier van leven, werken, spelen en leren is veranderd. Elke organisatie die de services wil leveren waar klanten en werknemers om vragen, moet zijn netwerk beschermen. Netwerkbeveiliging helpt u ook om eigendomsinformatie tegen aanvallen te beschermen. Uiteindelijk beschermt u daarmee uw reputatie.

Zes stappen om uw netwerk te beveiligen

1. Bewaak het via de firewall binnenkomende en uitgaande verkeer en neem de gemelde kwesties zorgvuldig door. Vertrouw niet op waarschuwingen om gevaarlijke activiteiten te markeren. Zorg dat iemand van uw team de gegevens begrijpt en de nodige actie kan ondernemen.
2. Blijf alert op nieuwe bedreigingen die worden ontdekt en online worden gepost. Op de TrendWatch-site van Trend Micro worden bijvoorbeeld actuele bedreigingsactiviteiten gevolgd.
3. Voer regelmatig updates uit van uw firewall- en antivirussoftware.
4. Geef werknemers regelmatig training zodat zij op de hoogte zijn van eventuele wijzigingen in uw beleid voor aanvaardbaar gebruik. Stimuleer ook een 'buurtwacht'-aanpak van beveiliging. Als een werknemer iets verdachts opmerkt (hij/zij kan zich bijvoorbeeld niet direct aanmelden bij een e-mailaccount), moet deze de juiste persoon hiervan onmiddellijk op de hoogte stellen.
5. Installeer een oplossing voor gegevensbescherming. Dit type apparaat kan uw bedrijf beschermen tegen gegevensverlies als er sprake is van een inbreuk op de netwerkbeveiliging.
6. Overweeg de inzet van aanvullende beveiligingsoplossingen om uw netwerk verder te beschermen en de mogelijkheden van uw bedrijf uit te breiden.

Optie – B

Basisinformatie over netwerkbeveiliging voor MKB-bedrijven

Typen netwerkbeveiliging

Toegangscontrole

Niet elke gebruiker zou toegang tot uw netwerk moeten hebben. Om potentiële aanvallers buiten te houden, moet u elke gebruiker en elk apparaat kunnen herkennen. U kunt dan uw beveiligingsbeleid afdwingen. U kunt endpointapparaten die niet aan het beleid voldoen, blokkeren of slechts beperkte toegang verlenen. Dit proces wordt netwerktoegangsbeheer (NAC) genoemd.

Antivirus- en antimalwareprogramma's

Malware (afkorting van 'malicious software', kwaadaardige software) omvat virussen, wormen, trojans, ransomware en spyware. Soms kan malware een netwerk besmetten en vervolgens dagen of zelfs weken sluimerend aanwezig blijven. De beste antimalwareprogramma's scannen niet alleen op malware op het moment dat deze binnendringt, maar blijven bestanden ook daarna volgen om abnormaliteiten te detecteren, malware te verwijderen en schade te herstellen.

Toepassingsbeveiliging

Alle software die wordt gebruikt bij het uitvoeren van uw bedrijfsactiviteiten moet worden beschermd, ongeacht of de software door uw IT-personeel is ontwikkeld of door u is gekocht. Toepassingen kunnen echter 'gaten' (kwetsbaarheden) bevatten die aanvallers kunnen misbruiken om uw netwerk te infiltreren. Toepassingsbeveiliging omvat de hardware, de software en de processen die u gebruikt om die gaten te dichten.

Gedragsanalyses

Om abnormaal netwerkgedrag te kunnen detecteren, moet u eerst weten wat normaal netwerkgedrag is. Met tools voor gedragsanalyse worden activiteiten die afwijken van de norm automatisch gedetecteerd. Uw beveiligingsteam kan vervolgens aanwijzingen van besmetting die een potentieel probleem vormen, beter identificeren en bedreigingen snel verwijderen.

Voorkoming van gegevensverlies

Organisaties moeten ervoor zorgen dat hun werknemers geen gevoelige informatie buiten het netwerk verzenden. Technologieën ter voorkoming van gegevensverlies (DLP) kunnen helpen voorkomen dat cruciale informatie op een onveilige manier wordt geüpload, doorgestuurd of zelfs afgedrukt.

E-mailbeveiliging

E-mailgateways vormen de belangrijkste bedreigingsvector voor een beveiligingsinbreuk. Aanvallers gebruiken persoonlijke informatie en social engineeringtechnieken om geraffineerde phishingcampagnes op te zetten om ontvangers te misleiden en naar sites met malware te sturen. Met een toepassing voor e-mailbeveiliging worden inkomende aanvallen geblokkeerd en worden uitgaande berichten gecontroleerd om verlies van gevoelige gegevens te voorkomen.

Firewalls

Firewalls vormen een barrière tussen uw vertrouwde interne netwerk en niet-vertrouwde externe netwerken, zoals het internet. Hierbij wordt een set gedefinieerde regels gebruikt om verkeer toe te laten of te blokkeren. Een firewall kan hardware, software of beide zijn. Cisco biedt UTM-apparaten (Unified Threat Management) en bedreigingsgerichte firewalls van de volgende generatie.

Inbraakpreventiesystemen

Een inbraakbeveiligingssysteem (IPS) scant netwerkverkeer om aanvallen actief te blokkeren. Cisco NGIPS-applicaties (Next-Generation IPS) doen dit door enorme hoeveelheden wereldwijde bedreigingsinformatie te correleren en niet alleen kwaadaardige activiteit te blokkeren, maar ook de voortgang van verdachte bestanden en malware te volgen over het netwerk om de verspreiding van uitbraken en herinfectie te voorkomen.

Basisinformatie over netwerkbeveiliging voor MKB-bedrijven

Beveiliging van mobiele apparaten

Cybercriminelen richten hun pijlen steeds meer op mobiele apparaten en apps. Binnen de komende drie jaar zal 90% van de IT-organisaties zakelijke toepassingen op persoonlijke mobiele apparaten ondersteunen. Natuurlijk moet u kunnen bepalen en controleren welke apparaten toegang hebben tot uw netwerk. En u moet hun verbindingen configureren om netwerkverkeer privé te houden.

Netwerksegmentering

Met softwaregedefinieerde segmentering wordt het netwerkverkeer geclassificeerd, waardoor het handhaven van beveiligingsbeleid eenvoudiger wordt. Idealiter worden de classificaties gebaseerd op de identiteit van endpoints, niet alleen op IP-adres. U kunt toegangsrechten verlenen op basis van rol, locatie en meer, zodat het juiste toegangsniveau wordt toegewezen aan de juiste personen en verdachte apparaten worden ingeperkt en hersteld.

VPN

Bij een virtueel particulier netwerk (VPN) wordt de verbinding met een netwerk via een endpoint, vaak via het internet, versleuteld. Bij een VPN voor externe toegang wordt gebruikgemaakt van IPsec of Secure Sockets Layer om de communicatie tussen apparaat en netwerk te verifiëren.

Webbeveiliging

Met een webbeveiligingsoplossing wordt het webgebruik van uw werknemers beheerd, worden webgebaseerde bedreigingen geblokkeerd en wordt toegang tot kwaadaardige websites geweigerd. Uw webgateway op locatie of in de cloud wordt beschermd. ‘Webbeveiliging’ heeft ook betrekking op de stappen die u neemt om uw eigen website te beschermen.

Draadloze beveiliging

Draadloze netwerken zijn minder beveiligd dan bekabelde. Zonder strenge beveiligingsmaatregelen is het installeren van een draadloos LAN net zoiets als overal Ethernet-poorten plaatsen (inclusief parkeerplaats). Om succesvolle exploitaties tegen te gaan, moet u producten gebruiken die speciaal zijn ontwikkeld om een draadloos netwerk te beschermen.

Hoofdkantoor Amerika
Cisco Systems, Inc.
San Jose, CA

Hoofdkantoor Zuidoost-Azië
Cisco Systems (USA) Pte. Ltd.
Singapore

Hoofdkantoor Europa
Cisco Systems International BV Amsterdam,
Nederland

Cisco beschikt wereldwijd over meer dan 200 kantoren. Adressen, telefoonnummers en faxnummers vindt u op de Cisco-website op **www.cisco.com/go/offices.**