Grundlagen der Netzwerksicherheit für KMU

Was ist Netzwerksicherheit?

Netzwerksicherheit ist eine beliebige Aktivität, welche die Funktionsfähigkeit und Integrität Ihres Netzwerks und Ihrer Daten schützt. Sie umfasst sowohl Hardware- als auch Softwaretechnologien. Eine effektive Netzwerksicherheit verwaltet den Zugriff auf das Netzwerk. Sie geht eine Vielzahl von Bedrohungen an und hält sie davon ab, in Ihr Netzwerk einzudringen oder sich dort zu verbreiten.

Wie funktioniert Netzwerksicherheit?

Netzwerksicherheit kombiniert mehrere Verteidigungsebenen am Netzwerk-Edge und im Netzwerk. Jede Netzwerksicherheitsebene implementiert Richtlinien und Kontrollen. Autorisierte Benutzer erhalten Zugriff auf Netzwerkressourcen, Angreifer werden jedoch davon abgehalten, Exploits und Bedrohungen in Umlauf zu bringen.

Wie profitiere ich von Netzwerksicherheit?

Die Digitalisierung hat unsere Welt verwandelt. Die Art, wie wir leben, arbeiten, spielen und lernen hat sich verändert. Jede Organisation, die von Kunden und Mitarbeitern geforderte Services bereitstellen möchte, muss ihr Netzwerk schützen. Netzwerksicherheit hilft Ihnen auch dabei, Ihre urheberrechtlich geschützten Informationen vor Angriffen zu schützen. Letztendlich dient dies dem Schutz Ihres Rufs.

6 Schritte zum Schutz Ihres Netzwerks

1. Überwachen Sie den Datenverkehr von und zur Firewall und lesen Sie die Berichte sorgfältig. Verlassen Sie sich nicht darauf, dass Sie Warnungen über gefährliche Aktivitäten erhalten. Stellen Sie sicher, dass eine Person in Ihrem Team die Daten lesen kann und bereit ist, die erforderlichen Maßnahmen zu ergreifen.
2. Achten Sie auf neue Bedrohungen, sobald diese entdeckt und online publik gemacht werden. Die TrendWatch-Website von Trend Micro verfolgt beispielsweise aktuelle Bedrohungsaktivitäten nach.
3. Führen Sie regelmäßige Updates Ihrer Firewall und Antivirus-Software durch.
4. Schulen Sie Mitarbeiter regelmäßig, damit diese über jegliche Änderungen an Ihren Richtlinien zur akzeptablen Nutzung informiert sind. Fördern Sie zudem eine Art „Nachbarschaftswache“ als Sicherheitsansatz. Wenn ein Mitarbeiter etwas Verdächtiges bemerkt, etwa wenn er sich nicht sofort bei seinem E-Mail-Konto anmelden kann, sollte er oder sie umgehend den richtigen Ansprechpartner benachrichtigen.
5. Installieren Sie eine Datenschutzlösung. Dieser Gerätetyp kann Ihr Unternehmen vor Datenverlust schützen, falls die Sicherheit Ihres Netzwerks kompromittiert ist.
6. Ziehen Sie zusätzliche Sicherheitslösungen in Betracht, die ebenfalls zum Schutz Ihres Netzwerks beitragen und die Fähigkeiten Ihres Unternehmens erweitern.

Option B

Grundlagen der Netzwerksicherheit für KMU

Arten von Netzwerksicherheit

Zugriffskontrolle

Nicht jeder Benutzer sollte auf Ihr Netzwerk zugreifen können. Um potenzielle Angreifer fernzuhalten, müssen Sie jeden Benutzer und jedes Gerät kennen. Danach können Sie Ihre Sicherheitsrichtlinien durchsetzen. Sie können nicht konforme Endgeräte blockieren oder Ihnen nur begrenzten Zugriff gewähren. Dieser Prozess wird als Network Access Control (NAC) bezeichnet.

Antivirus- und Malwareschutz-Software

„Malware“, bzw. bösartige Software, umfasst Viren, Würmer, Trojaner, Ransomware und Spyware. Manchmal infiziert Malware ein Netzwerk, bleibt dann aber tage- oder sogar wochenlang inaktiv. Die besten Malwareschutzprogramme scannen nicht nur Malware bei ihrem Eintreten, sondern verfolgen Dateien laufend nach, um Anomalien aufzuspüren, Malware zu entfernen und Schäden zu beheben.

Anwendungssicherheit

Jede Software, die Sie für den Betrieb Ihres Unternehmens ausführen, muss geschützt werden, und zwar unabhängig davon, ob Ihr IT-Personal sie entwickelt oder ob Sie sie kaufen. Leider kann jede Anwendung Sicherheitslücken oder Schwachstellen beinhalten, durch die Angreifer in Ihr Netzwerk eindringen können. Anwendungssicherheit umfasst die Hardware, Software und Prozesse, die Sie zum Schließen dieser Lücken verwenden.

Verhaltensanalysen

Um ungewöhnliches Netzwerkverhalten erkennen zu können, müssen Sie wissen, was normales Verhalten ist. Tools zur Analyse von Verhaltensanalysen erkennen automatisch Aktivitäten, die von der Norm abweichen. Ihr Sicherheitsteam kann damit Anzeichen für Kompromittierungen besser identifizieren, die ein potenzielles Problem darstellen, und Bedrohungen schnell beseitigen.

Schutz vor Datenverlust

Organisationen müssen sicherstellen, dass ihre Mitarbeiter keine vertraulichen Informationen außerhalb des Netzwerks versenden. DLP-Technologien (Data-Loss-Prevention; Schutz vor Datenverlust) können Mitarbeiter davon abhalten, kritische Informationen auf unsichere Weise hochzuladen, weiterzuleiten oder sogar auszudrucken.

E-Mail-Sicherheit

E-Mail-Gateways sind der erste Angriffsvektor für eine Sicherheitsverletzung. Angreifer nutzen persönliche Daten und Social-Engineering-Taktiken, um komplexe Phishing-Kampagnen aufzubauen und damit Empfänger zu täuschen und sie auf Websites mit Malware zu locken. Eine Anwendung für E-Mail-Sicherheit blockiert Angriffe und steuert ausgehende Nachrichten, um den Verlust vertraulicher Daten zu verhindern.

Firewalls

Firewalls bilden eine Barriere zwischen Ihrem vertrauenswürdigen internen Netzwerk und nicht vertrauenswürdigen externen Netzwerken, wie dem Internet. Sie verwenden eine Reihe von festgelegten Regeln, mit denen Datenverkehr zugelassen oder blockiert werden kann. Eine Firewall basiert entweder auf Hardware, auf Software oder auf einer Kombination aus beidem. Cisco bietet Unified Threat Management-Geräte (UTM) und bedrohungsorientierte Next-Generation-Firewalls.

Intrusion Prevention-Systeme

Ein Intrusion-Prevention-System (IPS) scannt den Netzwerkverkehr, um Angriffe aktiv zu blockieren. Next-Generation IPS-Appliances (NGIPS) von Cisco korrelieren zu diesem Zweck riesige Volumen an globaler Threat-Intelligence, wodurch nicht nur schädliche Aktivitäten blockiert werden sondern auch der Verlauf von verdächtigen Dateien und Malware im Netzwerk nachverfolgt wird, um die Ausbreitung von Infektionen und Neuinfektionen zu vermeiden.

Grundlagen der Netzwerksicherheit für KMU

Sicherheit für Mobilgeräte

Cyber-Kriminelle nehmen zunehmend Mobilgeräte und Apps ins Visier. In den nächsten 3 Jahren werden möglicherweise 90 Prozent der IT-Abteilungen unternehmenseigene Apps auf persönlichen Mobilgeräten unterstützen. Natürlich müssen Sie Kontrolle darüber haben, welche Geräte auf Ihr Netzwerk zugreifen dürfen. Sie werden auch ihre Verbindungsarten konfigurieren müssen, um den Netzwerkverkehr zu schützen.

Netzwerksegmentierung

Bei der softwaredefinierten Segmentierung wird der Netzwerkverkehr unterschiedlichen Klassifizierungen zugeordnet, was die Durchsetzung von Sicherheitsrichtlinien erleichtert. Im Idealfall basieren Klassifizierungen auf der Identität des Endpunkts, und nicht nur auf den IP-Adressen. Sie können Zugriffsrechte basierend auf der Rolle, dem Standort und vielem mehr zuweisen, sodass jeder den passenden Zugriff erhält und verdächtige Geräte eingegrenzt und beseitigt werden.

VPN

Ein virtuelles privates Netzwerk verschlüsselt die Verbindung von einem Endgerät zu einem Netzwerk häufig über das Internet. Normalerweise nutzt ein Remote-Zugriff-VPN IPSec oder Secure Sockets Layer, um die Kommunikation zwischen Gerät und Netzwerk zu authentifizieren.

Web-Sicherheit

Eine Websicherheitslösung überwacht die Internetnutzung Ihrer Mitarbeiter, blockiert webbasierte Bedrohungen und verweigert schädlichen Websites den Zugriff. Sie schützt Ihr Web-Gateway vor Ort oder in der Cloud. „Websicherheit“ bezieht sich auch auf die Schritte, die Sie zum Schutz Ihrer eigenen Website ergreifen.

Wireless-Sicherheit

Wireless-Netzwerke sind nicht so sicher wie kabelgebundene. Ohne strenge Sicherheitsmaßnahmen kann die Installation eines Wireless LAN ausufern und dazu führen, dass überall Ethernet-Ports integriert werden. Damit sich ein Exploit nicht festsetzen kann, benötigen Sie Produkte, die speziell für den Schutz des Wireless-Netzwerks konzipiert wurden.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices.**