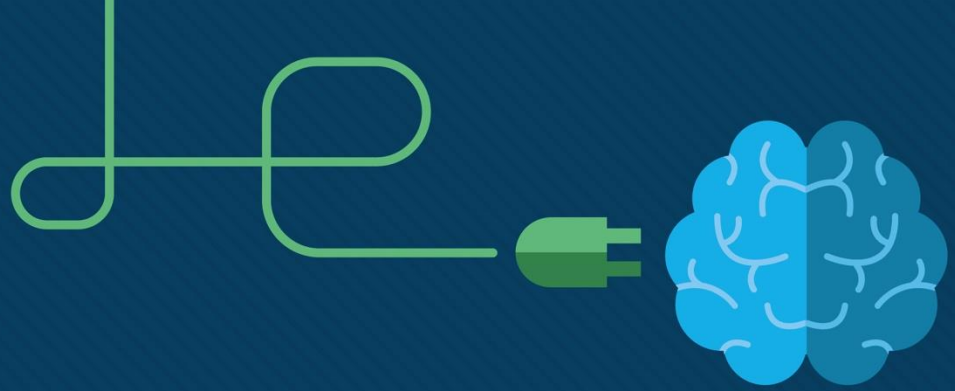


Modul 16: Grundlagen der Netzwerksicherheit

Unterlagen für Instruktoren

Einführung in Netzwerke v7.0
(ITN)

Was erwartet Sie in diesem Modul

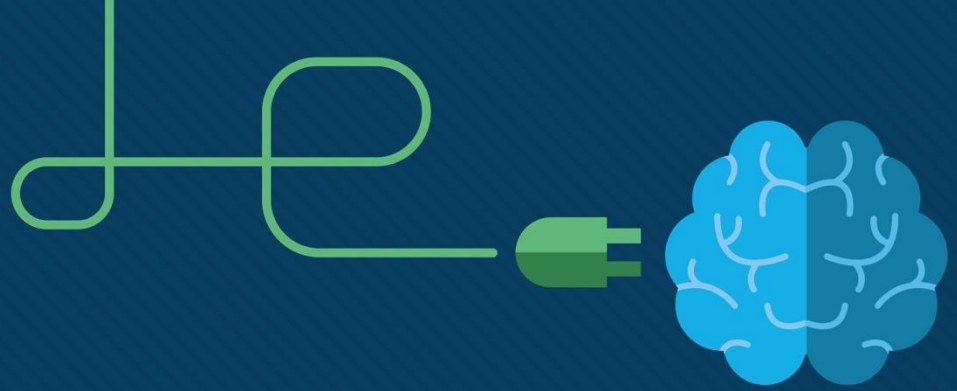
Um das Lernen zu vereinfachen, sind folgende Funktionen der grafischen Bedienoberfläche in diesem Modul enthalten:

Funktion	Beschreibung
Animationen	Den Lernenden mit neuen Fertigkeiten und Konzepten in Kontakt zu bringen.
Videos	Den Lernenden mit neuen Fertigkeiten und Konzepten in Kontakt zu bringen.
Prüfen Sie Ihr Verständnis (CYU)	Mit Hillfe der interaktiven Quizzes beurteilen die Lernenden Ihr Verständnis des Themas.
Interaktive Aktivitäten	Die Vielfalt an Formaten hilft den Lernenden ihr Verständnis einzuschätzen.
Syntaxprüfer	Über kleinere Simulation wird die Konfiguration über das Cisco command line Interface (CLI) erlernt.
Packet-Tracer (PT) Aktivitäten	Durch Simulations- und Entwurfsaufgaben entdecken und erwerben Sie neue Fähigkeiten, bereits erlernte werden gefestigt und erweitert.

Was erwartet Sie in diesem Modul (Inhalt)

Um das Lernen zu vereinfachen sind folgende Funktionen der grafischen Bedienoberfläche in diesem Modul enthalten:

Funktion	Beschreibung
Praxisorientierte Übungen	Laborübungen sind für das Arbeiten an den Geräten vorgesehen.
Gruppenaktivitäten	Sie finden diese auf den Seiten mit den Hilfsmitteln für Instruktoren Gruppenaktivitäten sollen das Lernen vereinfachen, Diskussionen fördern und Zusammenarbeit unterstützen.
Modulquizzes	Selbstüberprüfung der erlernten Begrifflichkeiten und Fertigkeiten, die während der vielfältigen Themen innerhalb des Moduls vorgestellt wurden.
Modulzusammenfassung	Kurze Wiederholung des Modulinhalts



Modul 16: Grundlagen der Netzwerksicherheit

Einführung in Netzwerke v7.0 (ITN)

Modulziele

Modultitel: Grundlagen der Netzwerksicherheit

Modul Ziel: Konfiguration von Switches und Routern mit Funktionen zur Gerätehärtung, um die Sicherheit zu erhöhen.

Thema	Ziel
Sicherheitsbedrohungen und Schwachstellen	Erläutern Sie, warum grundlegende Sicherheitsmaßnahmen auf Netzwerkgeräten erforderlich sind.
Netzwerkangriffe	Identifizierung von Sicherheitslücken.
Abwehr von Netzwerkangriffen	Identifizieren allgemeiner Risikominderungstechniken.
Gerätesicherheit	Konfigurieren Sie Netzwerkgeräte mit Gerätehärtungsfunktionen, um Sicherheitsbedrohungen zu mindern.

16.1 Sicherheitsbedrohungen und Schwachstellen

Bedrohungsarten

Angriffe auf ein Netzwerk können verheerend sein und zu Zeit- und Geldverlusten durch Beschädigung oder Diebstahl wichtiger Informationen oder Vermögenswerte führen. Eindringlinge können durch Software-Schwachstellen, Hardware-Angriffe oder durch das Erraten des Benutzernamens und Passworts einer Person Zugang zu einem Netzwerk erlangen. Eindringlinge, die sich Zugang verschaffen, indem sie Software modifizieren oder Software-Schwachstellen ausnutzen, werden als Bedrohungsakteure (threat actors) bezeichnet.

Nachdem der Bedrohungsakteur Zugang zum Netzwerk erhalten hat, können vier Arten von Bedrohungen auftreten:

- Informationsdiebstahl
- Datenverlust und Datenmanipulation
- Identitätsdiebstahl
- Dienstunterbrechung

Bedrohungsarten

Der Begriff Schwachstelle (Vulnerability) ist der Grad der Anfälligkeit in einem Netzwerk oder einem Gerät. Dieses schließt Router, Switches, Desktops, Server und sogar Sicherheitsgeräte mit ein. Netzwerkgeräte, die angegriffen werden, sind in der Regel Endgeräte wie Server und Desktopcomputer.

Es gibt drei primäre Schwachstellen:

- Technologische Schwachstellen können Schwächen des TCP/IP-Protokolls, Schwächen des Betriebssystems und Schwächen der Netzwerkausrüstung umfassen.
- Konfigurationsschwachstellen können ungesicherte Benutzerkonten, Systemkonten mit leicht zu erratenden Kennwörtern, falsch konfigurierte Internetdienste, unsichere Standardeinstellungen und falsch konfigurierte Netzwerkgeräte umfassen.
- Sicherheitslücken in Sicherheitsrichtlinien können das Fehlen einer schriftlichen Sicherheitsrichtlinie, Richtlinien, fehlende Authentifizierungskontinuität, nicht angewandte logische Zugriffskontrollen, Software- und Hardwareinstallation und Änderungen, die nicht der Richtlinie folgen, sowie einen nicht vorhandenen Notfallwiederherstellungsplan umfassen.

Alle drei dieser Schwachstellenarten können ein Netzwerk oder ein Gerät für verschiedene Angriffe zugänglich machen, darunter Angriffe mit bösartigem Code und Netzwerkangriffe.

Physische Sicherheit

Wenn Netzwerkressourcen physisch kompromittiert werden können, kann ein Bedrohungsakteur die Nutzung von Netzwerkressourcen verhindern. Die vier Klassen physischer Bedrohungen sind folgende:

- **Hardware-Bedrohungen -** Dazu gehören physische Schäden an Servern, Routern, Switches, Verkabelungen und Workstations.
- **Bedrohungen durch extreme Umgebungsbedingungen -** Dazu gehören Temperaturextreme (zu heiß oder zu kalt) oder Feuchtigkeitsextreme (zu nass oder zu trocken).
- **Elektrische Bedrohungen -** Dazu gehören Spannungsspitzen, unzureichende Versorgungsspannung (Spannungsabfälle), ungefilterte Spannungsversorgung (Rauschen) und totaler Stromausfall.
- **Bedrohungen durch unsachgemäße Wartung -** Dazu gehören schlechte Handhabung wichtiger elektrischer Komponenten (elektrostatische Entladung), Mangel an kritischen Ersatzteilen, fehlerhafte Verkabelung und unzureichende Kennzeichnung.

Um diese Probleme anzugehen, muss ein guter Plan für die physische Sicherheit erstellt und umgesetzt werden.

16.2 Netzwerkangriffe

Arten von Malware

Malware ist die Kurzform für bösartige (=malicious) Software. Es handelt sich dabei um Code oder Software, der bzw. die speziell dafür entwickelt wurde, Daten zu stehlen, Daten, Hosts oder Netzwerke zu beschädigen, Störungen zu verursachen oder unerlaubte bzw. rechtswidrige Aktionen in Verbindung mit diesen auszuführen. Die folgenden sind Arten von Malware:

- **Viren -** Ein Computervirus ist eine Art von Malware, die dadurch verbreitet wird, dass sie eine Kopie von sich selbst in ein anderes Programm einfügt und dadurch Teil des Programms wird. Ein Virus verbreitet sich von einem Computer auf andere und infiziert diese so.
- **Würmer -** Computerwürmer ähneln Viren insofern, als dass sie funktionsfähige Kopien von sich selbst replizieren und die gleiche Art von Schaden verursachen können. Im Gegensatz zu Viren, die die Verbreitung einer infizierten Host-Datei erfordern, sind Würmer jedoch Standalone-Software und benötigen kein Host-Programm oder menschliche Unterstützung, um sich zu verbreiten.
- **Trojanische Pferde -** Es handelt sich hierbei um schädliche Software, die harmlos und legitim aussieht. Anders als Viren und Würmer vervielfältigen sich Trojaner nicht, indem sie andere Dateien infizieren. Sie replizieren sich selbst. Trojaner müssen durch die Interaktion von Benutzern verbreitet werden, z.B. das Öffnen eines E-Mail-Anhangs oder das Herunterladen und Ausführen einer Datei aus dem Internet.

Aufklärungsangriffe (Reconnaissance Attacks)

Netzwerke sind nicht nur durch Schadcode bedroht – sie können Ziel unterschiedlicher Netzwerkangriffe werden. Netzwerkangriffe fallen in drei Hauptkategorien:

- **Reconnaissance-Angriffe** – Die Erkennung und Zuordnung von Systemen, Diensten oder Schwachstellen.
- **Zugriffsangriffe (Access attacks)** – Die unbefugte Manipulation von Daten, Systemzugriff oder Benutzerrechten
- **Denial of Service (DoS)** – Die Deaktivierung oder Beschädigung von Netzwerken, Systemen oder Diensten

Für Reconnaissance-Angriffe können externe Angreifer Internet-Tools wie **nslookup** und **whois** verwenden, um auf einfache Weise den einer bestimmten Firma oder Organisation zugeordneten IP-Adressbereich zu ermitteln. Nach dem Bestimmen des IP-Adressbereichs kann ein Bedrohungsakteur einen Ping an die öffentlich verfügbaren IP-Adressen senden, um die aktiven Adressen zu identifizieren.

Zugriffs-Angriffe

Zugriffsangriffe nutzen bekannte Schwachstellen in Authentifizierungs-, FTP- und Webdiensten aus, um Zugriff auf Web-Konten, vertrauliche Datenbanken und andere vertrauliche Informationen zu erhalten.

Zugangsangriffe fallen in vier Kategorien:

- **Passwort-Angriffe -** Implementiert mit Brute-Force, Trojanern und Paket-Sniffern
- **Vertrauensausnutzung —** Ein Bedrohungsakteur nutzt nicht autorisierte Berechtigungen, um Zugriff auf ein System zu erhalten, was möglicherweise das Ziel gefährdet.
- **Port-Umleitung**: - Ein Bedrohungsakteur nutzt ein kompromittiertes System als Basis für Angriffe auf andere Ziele. Zum Beispiel ein Bedrohungsakteur, der SSH (Port 22) verwendet, um sich mit einem kompromittierten Host A zu verbinden. Host A wird von Host B als vertrauenswürdig eingestuft, daher kann der Bedrohungsakteur Telnet (Port 23) verwenden, um darauf zuzugreifen.
- **Mann in der Mitte (Man-in-the middle) -** Der Bedrohungsakteur befindet sich zwischen zwei Systemen, um die Daten zu lesen oder zu ändern, die zwischen diesen beiden Parteien ausgetauscht werden.

Denial of Service Angriff

Denial of Service (DoS)-Angriffe sind die bekannteste Art von Angriffen und gehören mit zu den Angriffen, die extrem schwer zu beseitigen sind. Aber gerade weil sie so einfach angewendet werden können und dennoch bemerkenswerten Schaden anrichten, verdienen DoS-Angriffe besondere Aufmerksamkeit bei Sicherheitsadministratoren.

- DoS-Angriffe treten in vielen unterschiedlichen Formen auf. DoS-Angriffe verhindern, dass Personen einen Dienst nutzen können, indem Sie Systemressourcen verbrauchen. Um DoS-Angriffe zu vermeiden, ist es wichtig, stets die neuesten Sicherheits-Updates für Betriebssysteme und Anwendungen zu installieren.
- DoS-Angriffe stellen ein erhebliches Risiko dar, da sie die Kommunikation stören und so zu großen Geld- und Zeitverlusten führen können. Diese Art von Angriffen lässt sich selbst von einem wenig versierten Angreifer leicht durchführen.
- Ein Distributed-DoS-Angriff (DDoS) ähnelt einem DoS-Angriff, erfolgt aber von mehreren, koordinierten Quellen. Ein Bedrohungsakteur baut beispielsweise ein Netzwerk infizierter Hosts auf, die als Zombies bezeichnet werden. Ein Netzwerk von Zombies wird Botnet genannt. Der Bedrohungsakteur verwendet ein Command and Control (CnC)-Programm, um das Botnetz von Zombies anzuweisen, einen DDoS-Angriff durchzuführen.

Übung– Recherchieren von Sicherheitsbedrohungen für Netzwerke

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- Teil 1: Erkunden der SANS-Website
- Teil 2: Identifizieren von aktuellen Sicherheitsbedrohungen für Netzwerke
- Teil 3: Erklären einer bestimmten Sicherheitsbedrohung für Netzwerke

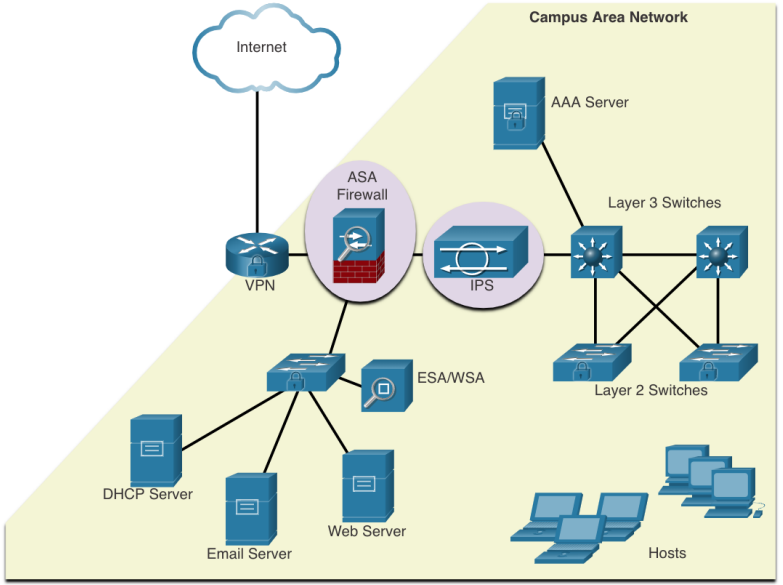
16.3 Abwehr von Netzwerkangriffen

Der tiefgreifende Verteidigungsansatz

Um Netzwerkangriffe zu minimieren, müssen Sie zuerst Geräte wie Router, Switches, Server und Hosts sichern. Die meisten Organisationen verwenden einen tiefgreifenden Ansatz (auch als mehrschichtiger Ansatz bezeichnet) für die Sicherheit. Dies erfordert eine Kombination von Netzwerkgeräten und Diensten, die zusammen arbeiten.

Mehrere Sicherheitsgeräte und -dienste werden implementiert, um die Benutzer und Ressourcen einer Organisation vor TCP/IP-Bedrohungen zu schützen:

- VPN
- ASA Firewall
- IPS
- ESA/WSA
- AAA Server



Backups aufbewahren

Eine Datensicherung der Gerätekonfigurationen und -daten ist eine der wirksamsten Möglichkeiten, einen folgenreichen Datenverlust zu vermeiden. Backups sollten in regelmäßigen Abständen durchgeführt werden, basierend auf den Sicherheitsrichtlinien. Daten-Backups werden in der Regel extern aufbewahrt, um den Schutz der Backup-Medien auch bei einem Brand oder sonstigen katastrophalen Ereignissen zu gewährleisten.

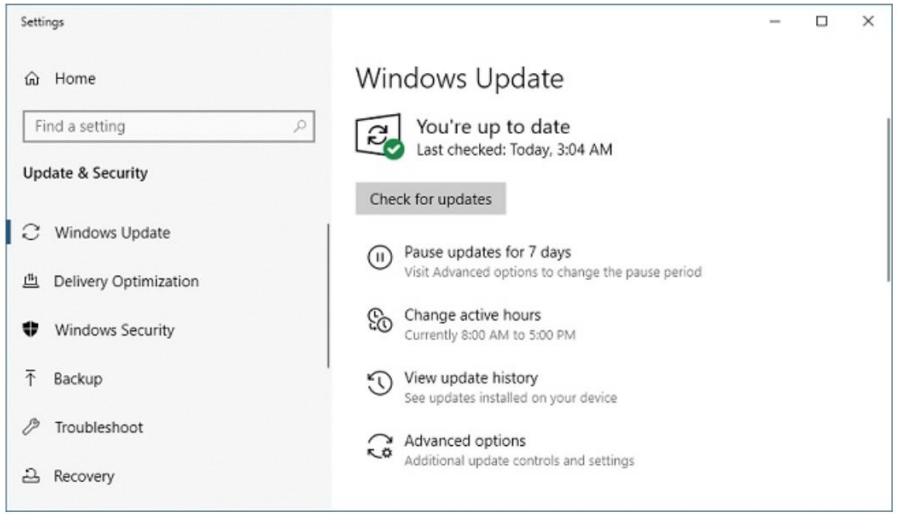
Die Tabelle listet einige Strategien auf, die bei der Erstellung einer Backup-Richtlinie betrachtet werden sollten, mit entsprechenden Beschreibungen.

Erwägung	Beschreibung
Häufigkeit	•Führen Sie regelmäßig Sicherungen durch, wie in der Sicherheitsrichtlinie angegeben. •Vollständige Sicherungen können zeitaufwändig sein. Führen Sie daher monatliche oder wöchentliche Sicherungen mit häufigen Teilsicherungen geänderter Dateien durch.
Storage	•Überprüfen Sie Backups immer, um die Integrität der Daten zu gewährleisten, und validieren Sie die Dateiwiederherstellungsverfahren.
Sicherheit	•Backups sollten je nach Sicherheitsrichtlinien in einem täglichen, wöchentlichen oder monatlichen Wechsel zu einem genehmigten externen Lagerort transportiert werden.
Validierung	•Sicherungen sollten mit starken Kennwörtern geschützt werden. Das Kennwort ist erforderlich, um die Daten wiederherzustellen.

Upgrade, Update und Patch

Unternehmen müssen ihre Antivirus-Software auf dem neuesten Stand halten, um mit neu veröffentlichter Malware Schritt zu halten.

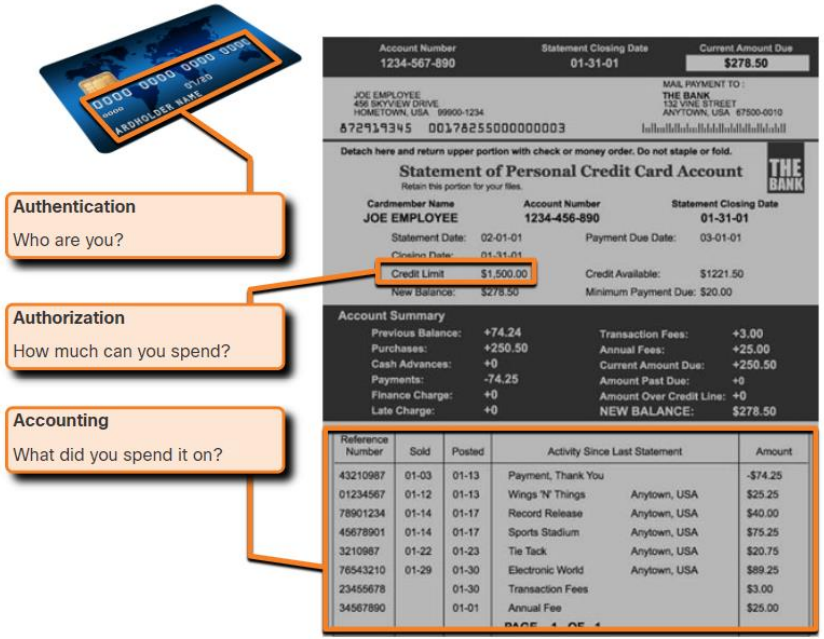
- Die wirksamste Methode zur Abwehr eines Wurm-Angriffs besteht darin, Sicherheits-Updates von der Website des Betriebssystem-Anbieters herunterzuladen und alle anfälligen Systeme zu patchen.
- Eine Lösung für die Verwaltung kritischer Sicherheits-Patches besteht darin, sicherzustellen, dass alle Endsysteme automatisch Updates herunterladen.



Authentifizierung, Autorisierung und Abrechnung

Die AAA-Netzwerk-Sicherheitsdienste (Authentication Authorization, and Accounting oder „Triple-A“) bilden das Hauptgerüst für die Einrichtung der Zugriffskontrolle auf Netzwerkgeräten.

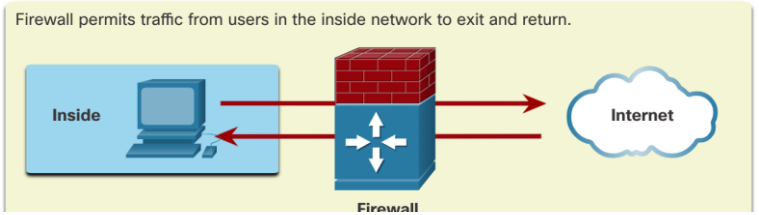
- AAA ist eine Möglichkeit, zu kontrollieren, 1. wer berechtigt ist, auf ein Netzwerk zuzugreifen (Authentifizieren), 2. was diejenigen Personen machen können, wenn sie sich im Netzwerk befinden (Autorisieren), und 3. nachzuverfolgen, welche Aktionen die Personen durchführen, während sie auf das Netzwerk zugreifen (Accounting).
- Das AAA-Konzept ähnelt der Verwendung einer Kreditkarte Die Kreditkarte identifiziert, wer sie benutzen kann, wie viel der Benutzer ausgeben kann und führt Buch darüber, wofür der Benutzer Geld ausgegeben hat.

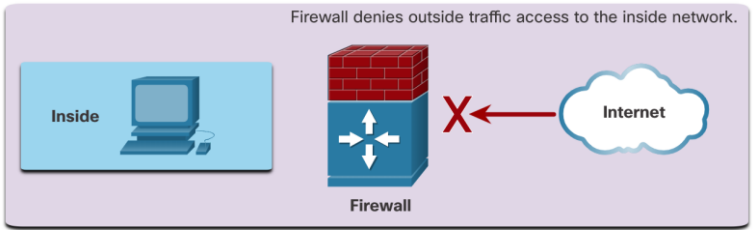


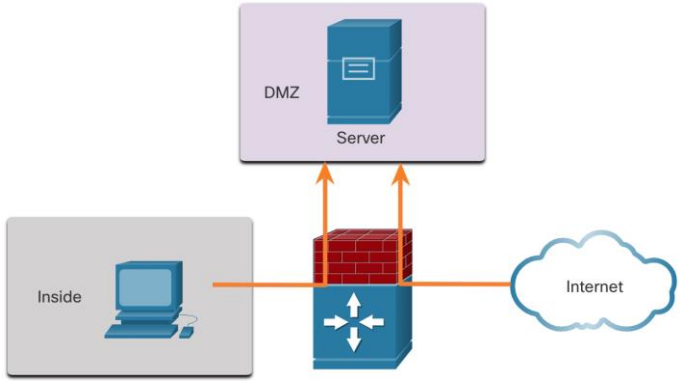
Firewalls

Netzwerk-Firewalls befinden sich zwischen zwei oder mehr Netzwerken, kontrollieren den Datenverkehr zwischen diesen und verhindern nicht autorisierte Zugriffe.

Eine Firewall könnte externen Benutzern den kontrollierten Zugriff auf bestimmte Dienste ermöglichen. Beispielsweise befinden sich Server, die für externe Benutzer zugänglich sind, normalerweise in einem speziellen Netzwerk, das als demilitarisierte Zone (DMZ) bezeichnet wird. Die DMZ ermöglicht es einem Netzwerkadministrator, bestimmte Richtlinien für Hosts anzuwenden, die mit diesem Netzwerk verbunden sind.







Typen von Firewalls

Firewall-Produkte werden in Form unterschiedlicher Pakete angeboten. Diese Produkte verwenden unterschiedliche Techniken, um zu bestimmen, was einen zulässigen und was einen unberechtigten Zugriff auf ein Netzwerk darstellt. Die folgenden Anwendungen sind enthalten:

- **Paketfilterung** - Verhindert oder erlaubt den Zugriff basierend auf IP- oder MAC-Adressen
- **Anwendungsfilterung** - Verhindert oder erlaubt den Zugriff durch bestimmte Anwendungstypen auf der Grundlage von Port-Nummern
- **URL-Filterung** - Verhindert oder ermöglicht den Zugang zu Websites auf der Grundlage bestimmter URLs oder Schlüsselwörter
- **Stateful packet inspection (SPI)** - Eingehende Pakete müssen gültige Antworten auf Anfragen von internen Hosts sein. Unerwünschte Pakete werden blockiert, wenn sie nicht explizit zugelassen werden. SPI kann auch die Fähigkeit beinhalten, bestimmte Arten von Angriffen, wie z.B. Denial of Service (DoS), zu erkennen und herauszufiltern.

Endpunktsicherheit (Endpoint Security)

Ein Endgerät oder Host ist ein einzelnes Computersystem oder Gerät, das als Netzwerk-Client fungiert. Gängige Endgeräte sind Laptops, Desktops, Server, Smartphones und Tablets.

Das Sichern von Endgeräten gehört zu den anspruchsvollsten Aufgaben für Netzwerkadministratoren, da hierbei der Faktor „menschliche Natur“ eine Rolle spielt. Ein Unternehmen muss über gut dokumentierte Sicherheitsrichtlinien verfügen und die Mitarbeiter müssen diese Regeln kennen.

Die Mitarbeiter müssen bezüglich der richtigen Nutzung des Netzwerks geschult werden. Sicherheitsrichtlinien umfassen häufig den Einsatz von Antivirus-Software und Host-Intrusion-Prevention (Schutz vor Eindringlingen). Umfassendere Endgeräte-Sicherheitslösungen setzen auf die Netzwerkzugriffskontrolle.

16.4 Gerätesicherheit

Cisco AutoSecure

Beim Installieren eines neuen Betriebssystems auf einem Gerät werden die Sicherheitseinstellungen auf die Standardwerte gesetzt. In den meisten Fällen ist dieses Maß an Sicherheit unzureichend. Für Cisco Router kann die Funktion Cisco AutoSecure zum Schutz des Systems verwendet werden.

Außerdem gibt es einige einfache Schritte, die ausgeführt werden sollten und die für die meisten Betriebssysteme gelten:

- Standard-Benutzernamen und -Kennwörter sollten sofort geändert werden.
- Der Zugriff auf Systemressourcen sollte ausschließlich auf die Personen beschränkt werden, die zur Nutzung dieser Ressourcen berechtigt sind.
- Alle nicht benötigten Dienste und Anwendungen sollten deaktiviert und nach Möglichkeit deinstalliert werden.
- Häufig werden Geräte nach der Auslieferung durch den Hersteller eine Zeit lang in einem Lager aufbewahrt und verfügen nicht über aktuelle Patches. Es ist wichtig, vor der Implementierung die gesamte Software zu aktualisieren und alle Sicherheits-Patches zu installieren.

Passwörter

Zum Schutz von Netzwerkgeräten ist es wichtig, sichere Kennwörter zu verwenden. Folgende Standardrichtlinien sollten hierzu befolgt werden:

- Verwenden Sie eine Passwortlänge von mindestens acht Zeichen, vorzugsweise 10 oder mehr Zeichen.
- Erstellen Sie komplexe Kennwörter. Verwenden Sie eine Mischung aus Groß- und Kleinbuchstaben, Zahlen, Symbolen und Leerzeichen, falls zulässig.
- Vermeiden Sie Kennwortwiederholungen, sowie allgemeine Wörter aus Wörterbüchern, Buchstaben- oder Zahlenfolgen, Benutzernamen, Namen von Verwandten oder Haustieren, biografische Informationen wie Geburtsdatum, Ausweisnummern, Namen von Vorfahren oder andere leicht zu erratende Informationen.
- Absichtlich falsch geschrieben Kennwörter. Zum Beispiel Smith = Smyth = 5mYth oder Security = 5ecur1ty.
- Ändern Sie Kennwörter häufig. Falls ein Kennwort unwissentlich kompromittiert wurde, ist das Zeitfenster, in dem der Angreifer das Kennwort verwenden kann, begrenzt.
- Schreiben Sie Kennwörter nicht auf und bewahren Sie sie nicht an offensichtlichen Stellen wie dem Schreibtisch oder am Monitor auf.

Auf Cisco Routern werden führende Leerzeichen für Kennwörter ignoriert, Leerzeichen nach dem ersten Zeichen sind jedoch zulässig. Deshalb besteht eine Methode zum Erstellen eines sicheren Kennworts darin, Leerzeichen zu verwenden und einen Satz aus vielen Wörtern zu bilden. Dies wird als Passphrase bezeichnet. Eine Passphrase ist oft leichter zu merken als ein einfaches Passwort. Sie ist außerdem länger und schwerer zu erraten.

Zusätzliche Passwortsicherheit

Es gibt mehrere Schritte, mit denen Sie sicherstellen können, dass Passwörter auf einem Cisco Router und Switch geheim bleiben einschließlich dieser:

- Verschlüsseln Sie alle Klartext-Passwörter mit dem **service password-encryption** Befehl.
- Legen Sie mit dem Befehl „ **min-length“ eine akzeptable Mindestkennwortlänge** fest.
- Schrecken Sie Brute-Force-Passwort-Erraten-Angriffen mit dem **Login-Block-for # attempts # *within* #** -Befehl ab.
- Deaktivieren Sie einen inaktiven privilegierten EXEC-Modus nach einer bestimmten Zeit mit dem Befehl **exec-timeout**.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

SSHaktivieren

Es ist möglich, ein Cisco-Gerät mit den folgenden Schritten für die Unterstützung von SSH zu konfigurieren:

1. **Konfigurieren Sie einen eindeutigen Hostnamen**. Ein Gerät muss über einen anderen eindeutigen Hostnamen als den Standardnamen verfügen.
2. **Konfigurieren Sie den richtigen IP-Domänennamen**. Konfigurieren Sie den IP-Domänennamen des Netzwerks im globalen Konfigurationsmodus mit dem Befehl **ip domain-name**.
3. **Generieren Sie einen Schlüssel zum Verschlüsseln von SSH-Datenverkehr**. SSH verschlüsselt den Datenverkehr zwischen Quelle und Ziel. Um dies zu tun, muss jedoch ein eindeutiger Authentifizierungsschlüssel generiert werden, indem der globale Konfigurationsbefehl **crypto key generate rsa general-keys modulus** *bits*. Die modulus *bits* bestimmen die Größe des Schlüssels und können von 360 Bit bis 2048 Bit konfiguriert werden. Je größer der Bitwert ist, desto sicherer ist der Schlüssel. Bei größere Bitwerten dauert es jedoch auch länger, um Informationen zu verschlüsseln und zu entschlüsseln. Die empfohlene Mindestlänge ist 1024 Bit.
4. **Überprüfen oder erstellen Sie einen lokalen Datenbankeintrag**. Erstellen Sie mit dem globalen Konfigurationsbefehl **username** einen Benutzernameneintrag in der lokalen Datenbank.
5. **Authentifizieren Sie sich für die lokale Datenbank**. Verwenden Sie den line-Konfigurationsbefehl **login local** , um die vty-Verbindung über die lokale Datenbank zu authentifizieren.
6. **Aktivieren von eingehenden SSH-Sitzungen über line vty**. Standardmäßig ist keine eingehende Sitzung für line vty zulässig. Sie können mehrere Protokolle, einschließlich Telnet und SSH, mit dem Befehll **transport input [ssh | telnet] angeben.**

Ungenutzte Dienste deaktivieren

Cisco Router und Switches starten mit einer Liste aktiver Dienste, die möglicherweise in Ihrem Netzwerk erforderlich sind oder nicht. Deaktivieren Sie alle nicht verwendeten Dienste, um Systemressourcen wie CPU-Zyklen und RAM zu freizugeben, und verhindern Sie, dass Bedrohungsakteure diese Dienste nutzen.

- Der Typ der Dienste, die standardmäßig aktiviert sind, hängt von der IOS-Version ab. Beispielsweise hat IOS-XE in der Regel nur HTTPS- und DHCP-Ports geöffnet. Sie können dies mit dem Befehl **show ip ports all** überprüfen.
- IOS-Versionen vor IOS-XE verwenden den Befehl **host open-ports show control-plane** .

Packet Tracer – Konfigurieren Sie sichere Kennwörter und SSH

In dieser Paket-Tracer-Übung konfigurieren Sie Passwörter und SSH:

- Der Netzwerkadministrator hat Sie gebeten, RTA und SW1 für den Einsatz vorzubereiten. Bevor die Geräte mit dem Netzwerk verbunden werden können, müssen Sicherheitsmaßnahmen aktiviert werden.

Labor – Konfigurieren Sie sichere Kennwörter und SSH

Diese Übung beinhaltet folgende Lernziele:

- Teil 1: Konfigurieren von Gerätegrundeinstellungen
- Teil 2: Konfigurieren des Routers für den SSH-Zugriff
- Teil 3: Konfigurieren des Switches für den SSH-Zugriff
- Teil 4: SSH von der CLI auf dem Switch

16.5 Modul Übung und Quiz

Paket-Tracer — Sichere Netzwerkgeräte

In dieser Aktivität konfigurieren Sie einen Router und einen Switch basierend auf einer Liste von Anforderungen.

Labor — Sichere Netzwerkgeräte

Diese Übung beinhaltet folgende Lernziele:

- Konfigurieren der Gerätegrundeinstellungen
- Konfigurieren von grundlegenden Sicherheitsmaßnahmen auf dem Router
- Konfigurieren von grundlegenden Sicherheitsmaßnahmen auf dem Switch

Was habe ich in diesem Modul gelernt?

- Wenn der Bedrohungsakteur Zugriff auf das Netzwerk erhält, können vier Bedrohungsarten die Folge sein: Informationsdiebstahl, Datenverlust/-manipulation, Identitätsdiebstahl und Dienstunterbrechung.
- Es gibt drei primäre Schwachstellen oder Schwächen: Technologie, Konfiguration und Sicherheitsrichtlinie.
- Die vier Klassen physischer Bedrohungen sind: Hardware, Umwelt, Elektrik und Wartung.
- Malware ist die Kurzform für bösartige (=malicious) Software. Es handelt sich dabei um Code oder Software, der bzw. die speziell dafür entwickelt wurde, Daten zu stehlen, Daten, Hosts oder Netzwerke zu beschädigen, Störungen zu verursachen oder unerlaubte bzw. rechtswidrige Aktionen in Verbindung mit diesen auszuführen. Viren, Würmer und Trojaner sind Arten von Malware.
- Netzwerkangriffe lassen sich dabei in drei Hauptkategorien einteilen: Reconnaissance-, Zugriffs- und DoS-Angriffe (Denial of Service).
- Um Netzwerkangriffe zu minimieren, müssen Sie zuerst Geräte wie Router, Switches, Server und Hosts sichern. Die meisten Unternehmen setzen einen tiefgreifenden Sicherheitsansatz ein. Dies erfordert eine Kombination von Netzwerkgeräten und -diensten, die zusammenarbeiten.
- Mehrere Sicherheitsgeräte und -dienste sind implementiert, um die Benutzer und Ressourcen einer Organisation vor TCP/IP-Bedrohungen zu schützen: VPN, ASA-Firewall, IPS, ESA/WSA und AAA-Server.

Was habe ich in diesem Modul gelernt? (Forts.)

- Infrastrukturgeräte sollten Backups von Konfigurationsdateien und IOS-Images auf einem FTP oder ähnlichen Dateiserver haben. Wenn der Computer oder eine Router-Hardware ausfällt, können die Daten oder Konfiguration mithilfe der Sicherungskopie wiederhergestellt werden.
- Die wirksamste Methode zur Abwehr eines Wurm-Angriffs besteht darin, Sicherheits-Updates von der Website des Betriebssystem-Anbieters herunterzuladen und alle anfälligen Systeme zu patchen. Um wichtige Sicherheitspatches zu verwalten, um sicherzustellen, dass alle Endsysteme automatisch Updates herunterladen.
- AAA ist eine Möglichkeit, zu kontrollieren, wer berechtigt ist, auf ein Netzwerk zuzugreifen (Authentifizieren), was diejenigen Personen machen können, wenn sie sich im Netzwerk befinden (Autorisieren), und nachzuverfolgen, welche Aktionen die Personen durchführen, während sie auf das Netzwerk zugreifen (Accounting).
- Netzwerk-Firewalls befinden sich zwischen zwei oder mehr Netzwerken, kontrollieren den Datenverkehr zwischen diesen und verhindern nicht autorisierte Zugriffe.
- Das Sichern von Endpunktgeräten ist für die Netzwerksicherheit von entscheidender Bedeutung. Ein Unternehmen muss über gut dokumentierte Richtlinien verfügen, einschließlich der Verwendung von Antivirensoftware und der Host-Intrusion Prevention. Umfassendere Endgeräte-Sicherheitslösungen setzen auf die Netzwerkzugriffskontrolle.

Was habe ich in diesem Modul gelernt? (Forts.)

- Für Cisco Router kann die Funktion Cisco AutoSecure zum Schutz des Systems verwendet werden. Bei den meisten Betriebssystemen sollten Standardbenutzernamen und Kennwörter sofort geändert werden, der Zugriff auf Systemressourcen sollte nur auf Personen beschränkt sein, die zur Verwendung dieser Ressourcen berechtigt sind. Unnötige Dienste und Anwendungen sollten nach Möglichkeit deaktiviert und deinstalliert werden.
- Zum Schutz von Netzwerkgeräten ist es wichtig, sichere Kennwörter zu verwenden. Eine Passphrase ist oft leichter zu merken als ein einfaches Passwort. Sie ist außerdem länger und schwerer zu erraten.
- Verschlüsseln Sie bei Routern und Switches alle Klartextkennwörter, legen Sie eine akzeptable Mindestkennwortlänge fest, verhindern Sie das Brute-Force-Kennwortraten und deaktivieren Sie nach einer bestimmten Zeit einen inaktiven privilegierten EXEC-Modus.
- Konfigurieren Sie geeignete Geräte zur Unterstützung von SSH und deaktivieren Sie nicht verwendete Dienste.


CISCO