


AITOx	ITS / DIF – LM-Dokumentation	19.02.25	 Berufskolleg Ostvest
Internet-Security – Gefahren / Angriffe aus dem Internet und mögliche Gegenmaßnahmen!			

Quelle: "<https://www.security-insider.de/die-7-raffiniertesten-hacker-tricks-a-879199/>"

IT-Security – Die 7 raffiniertesten Hacker-Tricks

Hacker-Angriffe werden immer ausgefeilter: Phishing-Mails, gefakte Links oder infizierte USB-Sticks – die Tricks der Cyber-Kriminellen werden immer raffinierter. Um sich gegen sie zu schützen, hilft es, ihre Vorgehensweise zu kennen. Der nachfolgende Artikel stellt eine Übersicht der "Top-Sieben-Methoden" dar.



"Kenne deinen Feind und kenne dich selbst!" Das sagte Sunzi um 500 vor Christus über die Kriegskunst. Dieser Spruch ist aktueller denn je und findet auch im heutigen digitalen Zeitalter immer noch Anwendung, und das selbst auch dann, wenn der vermeintliche Feind nur virtuell ist. Hacker-Angriffe werden immer ausgeklügelter. Getrost der alten Weisheit ist es hilfreich, die Methoden seines Gegners zu kennen. Das IT-Unternehmen Dell-Technologies hat sieben gängige Vorgehen von Hacker zusammengefasst, die hier vorgestellt werden sollen.

1. Phishing-Mails

Fast jeder hat sie schon einmal bekommen: eine E-Mail mit dubiosen Zahlungsaufforderungen oder merkwürdigen Hinweisen. Angreifer versuchen durch solche betrügerischen Mails persönliche Daten der Empfänger zu bekommen. Oft werden diese E-Mails massenhaft versendet, jedoch gibt es durchaus auch gezielte Spear-Phishing-Mails auserlesener Opfer.

2. Verseuchte Websites und Apps

Der jüngste Skandal um die Bild-Bearbeitungs-Applikation "FaceApp" zählt zu einem solchen Angriff über infizierte Webseiten im Internet oder in App-Stores. Denn mit dem Aufrufen der Webseiten oder dem Download der App, wird auch die darin enthaltene Schadsoftware heruntergeladen, die sich dann auf dem eigenen Rechner oder im Unternehmensnetzwerk verbreiten kann.

3. USB-Sticks

Viren, Trojaner und Co. kommen nicht nur per E-Mail, sondern neuerdings auch über verseuchte USB-Sticks oder andere Datenträger in die IT-Systeme. Hacker nutzen hierbei die Schwachstelle Mensch schamlos aus. Deshalb sollten Mitarbeiter ihre privaten USB-Sticks nicht an die Firmenrechner anschließen. Der private PC ist leider oft erst recht nicht ausreichend geschützt.

4. Software-Schwachstellen

Finde die Lücke! Und die gibt es oft in der Software. Um auf direktem Weg in die Unternehmensnetze einzudringen, nutzen Cyber-Kriminelle Sicherheitslücken in den Software-Systemen der Unternehmen. Einen Schutz davor bilden regelmäßige Sicherheits-Updates. Diese schließen die Schwachstelle in der Software und verringern damit das Risiko, dem Hacker ein Hintertürchen offen zu halten.

5. "Man in the Middle"-Angriffe

Wer saß nicht schon einmal in der Mitte, wenn zwei sich über den eigenen Kopf hinweg unterhalten? Dabei nicht mitzuhören, ist schwer machbar. Und genau diese Methode nutzen Hacker, indem sie der "Man in the Middle" sind. Sie klicken sich in die Kommunikation zweier Partner ein und können den Datenverkehr mitlesen und sogar manipulieren. Wie sie das schaffen? Wenn die Kommunikation unzureichend verschlüsselt ist.

6. DDoS-Attacken

Ein DDoS-Angriff (eng "Distributed-Denial-of-Service") ist ein "verteilter" DoS-Angriff (eng. "Denial-of-Service"), der zu einer Blockade der betroffenen IT-Systeme führt. Bei dieser Art des Angriffs werden IT-Infrastrukturen mutwillig aber gezielt überlastet. Die Flut an Anfragen kann dann beispielsweise das Internet lahm legen. So können Cyber-Kriminelle Web-basierte Systeme von Unternehmen oder deren Websites ausschalten und damit große finanzielle Schäden verursachen.

7. Insider-Bedrohungen

Gefahren müssen nicht immer von außen kommen. Immer häufiger erfolgen Cyber-Attacken auch von innen. Mitarbeiter oder Angestellte von IT-Dienstleistern können ihre Zugriffsmöglichkeiten auf Unternehmen ausnutzen, um so z.B. Daten zu stehlen, zu löschen oder zu manipulieren.

Doppelt hält besser – Strategische Schutzmaßnahmen

Darüber hinaus kombinieren Cyber-Kriminelle die o.a. verschiedenen Methoden häufig. Dies sind sogenannte "Advanced Persistent Threats". Als Gegenstrategie empfehlen IT-Sicherheitsexperten daher einen umfassenden Verteidigungsansatz, der mehrere Sicherheitsebenen miteinander kombiniert. Dazu zählt u.a. der Schutz sämtlicher Internet- und Netzwerkverbindungen durch "Firewalls" und "Virenfilter". "Verschlüsselung" von Daten: Egal, ob stationär oder auf dem Übertragungsweg, Daten sollten verschlüsselt werden. Außerdem lohnt sich die "Überwachung" und Beschränkung sämtlicher Zugriffe durch ein "Identity and Access Management" (IAM). Grundsätzlich hilft es auch, die eigenen Mitarbeiter entsprechend zu schulen und für die Gefahren aus dem Netz zu sensibilisieren.

Einige nachfolgende, aktuelle Praxis-Beispiele bzgl. "Mögliche Angriffe aus dem Internet"

Die nachfolgenden Praxis-Beispiele sollen zeigen, dass auch die Cyber-Kriminalität ihre ganze Kreativität zur Corona-Pandemie oder eben auch gerade deswegen zeigt! Die Weiterentwicklung einerseits der Aktivitäten der Angriffe aus dem Internet und andererseits der Entwicklung von Gegenmaßnahmen zum Schutz vor solchen ("Cyber-")Angriffen aus dem Internet wird stetig voranschreiten und ein wohl auch nie endender Entwicklungsprozess bleiben!

Quellen: "<https://www.golem.de/news/schule-14-jaehriger-nimmt-lernplattform-vom-netz-2102-154507.html>"

25.02.21, Moritz Tremmel

Praxis-Beispiel "DoS-Attacke" – "14-Jähriger nimmt Lernplattform vom Netz!"

Der Schüler soll einen DoS-Angriff auf Moodle@RLP durchgeführt haben. Doch alleine für den Schulausfall verantwortlich war er wohl nicht.

Mit dem ersten Schultag im neuen Jahr hatten etliche Lernplattformen massive Probleme. In Rheinland-Pfalz soll nicht nur mangelhafte Infrastruktur, sondern auch ein 14-jähriger Schüler für den Ausfall der Lernplattform Moodle@RLP verantwortlich sein, wie die Generalstaatsanwaltschaft Koblenz mitteilt.



Der Schüler soll für einen "rund zwei Tage andauernden DoS-Angriff ["Denial of Service"] in der Zeit vom 19. bis 21. Januar auf das Web-Konferenzsystem Big Blue Button" verantwortlich sein. Das hätten umfangreiche Ermittlungen des Landeskriminalamtes Rheinland-Pfalz und der Generalanwaltschaft ergeben, teilte Letztere am 24. Februar mit. Durch den Angriff sei die Anmeldung bei Big Blue Button und damit auch der Online-Unterricht an den Schulen in Rheinland-Pfalz in dem genannten Zeitraum erheblich gestört gewesen.

14-Jähriger hat den DoS-Angriff gestanden!

Der 14-Jährige aus dem Landkreis Bernkastel-Wittlich habe die Tat im Anschluss an eine Hausdurchsuchung gestanden, teilte die Generalstaatsanwaltschaft mit. Neben der DoS-Attacke des Schülers habe es weitere Angriffe auf die Lernplattform Moodle@RLP, die mit der gleichnamigen Open-Source-Software Moodle betrieben wird, sowie den angebundenen Videokonferenzdienst Big Blue Button, gegeben. Hier dauerten die Ermittlungen an, schreibt die Generalstaatsanwaltschaft.

Neben der Lernplattform in Rheinland-Pfalz hatte auch der Lernraum Berlin mit vielen Zugriffen am ersten Schultag zu kämpfen, dies jedoch ohne zusätzliche DoS-Attacken. Die Probleme wurden durch neue Server und eine Modifikation der Software Moodle behoben, die dank Open Source auch den anderen Lernplattformen zugutekommt. Im vergangenen Jahr haben auch andere Lernplattformen von DDoS-Angriffen (Distributed Denial of Service) berichtet.

Quellen: "<https://www.security-insider.de ...>"

Praxis-Beispiel "Vanity-URLs" – Check Point und Zoom schließen gemeinsam Lücken

Das IT-Security-Unternehmen "Check Point" arbeitet mit Zoom, einem Anbieter von Videokonferenz-Lösungen zusammen, um das Risiko der anpassbaren "Vanity-URLs"-Funktion zu verringern. Hacker können dabei Meeting-ID-Links manipulieren und für Phishing-Zwecke nutzen.

Chats und Videokonferenzen werden durch die Coronakrise immer beliebter. Doch Sicherheitslücken in den Tools ermöglichen Hackern den Zugriff auf sensible Daten. Das US-amerikanische Softwareunternehmen Zoom verzeichnete mit seiner Videokonferenz-App zuletzt nicht nur steigende Nutzerzahlen, sondern stand aufgrund von Datenschutz- und Sicherheitsmängeln in der Kritik. Auf diese wurde mit einem Update reagiert. Jetzt arbeitet der Anbieter erneut mit dem Security-Unternehmen Check Point zusammen, um gemeinsam das Problem einer anpassbaren Vanity-URLs-Funktion zu beheben.


Eine Schwachstelle dabei kann es Hackern ermöglichen, legitim aussehende Zoom-Einladungen zu Geschäftsbesprechungen zu versenden mit dem Ziel, Malware einzuschleusen und heimlich Daten oder Zugangsinformationen von diesem Benutzer zu stehlen. Bereits im Januar haben die beiden Unternehmen kooperiert, um eine andere potenzielle Schwachstelle zu beheben, die es Hackern ermöglicht hatte, ohne Einladung an einem Meeting teilzunehmen.

Mögliche Angriffsszenarien:

Das neue Sicherheitsproblem bei "Vanity-URLs" wurde von Forschern im Anschluss an die Zusammenarbeit Anfang des Jahres festgestellt. Hacker können die Vanity-URL auf zwei Arten manipulieren. Einmal durch eine gezielte Ansprache über direkte Links. Beim Einrichten eines Treffens wird die Einladungs-URL so geändert, dass sie eine Subdomain des Hackers enthält. Ohne spezielle Schulungen tun sich Nutzer schwer solche Einladungen als Fälschungen zu entlarven.

Die andere Möglichkeit sind gezielte Zoom-Webschnittstellen, denn einige Unternehmen verfügen über eigene Konferenz-Schnittstellen. Hacker könnten versuchen, Benutzer so umzuleiten, dass dieser eine Besprechungs-ID in die gefälschte Vanity-URL und nicht in die echte Zoom-Webschnittstelle eingibt. Ohne vorherige Trainings kann die bösartige URL vom Anwender nicht identifiziert werden.

Über beide Methoden könnten Hacker versuchen, sich über die Zoom-Plattform als Mitarbeiter der anvisierten Organisation auszugeben, um einen Vektor für den Diebstahl von Zugangsdaten oder sensiblen Informationen zu öffnen.

AITOx	ITS / DIF – LM-Dokumentation	19.02.25	 Berufskolleg Ostvest
Internet-Security – Gefahren / Angriffe aus dem Internet und mögliche Gegenmaßnahmen!			

Check Point und Zoom arbeiteten nun gemeinsam an der Lösung dieser Sicherheits-Probleme. Der US-amerikanische Konzern hat sich eigenen Angaben zufolge der Schwachstellen bereits angenommen und zusätzliche Sicherheitsvorkehrungen getroffen.

Praxis-Beispiel "Cyber-Angriffe auf Cloud-Services" – Angriffe auf Cloud-Accounts steigen um das 7-fache

Aufgrund der Corona-Pandemie und der Verlagerung vieler Arbeitsplätze ins Homeoffice ist die Cloud-Nutzung in Unternehmen weltweit um 50 Prozent gestiegen. Ebenfalls gestiegen sind Cyber-Angriffe auf Cloud-Services, wie der „Cloud Adoption & Risk Report – Work-From-Home Edition“ von McAfee zeigt.

Ein Großteil des Arbeitslebens hat sich wegen Covid-19 in das Homeoffice verlagert und Unternehmen müssen plötzlich mit einer Vielzahl neuer Cloud-Tools jonglieren. Der McAfee-Report „Cloud Adoption & Risk Report – Work From Home Edition“ deckt die Zusammenhänge zwischen der stark gestiegenen Nutzung von Online-Kollaborations-Tools, wie Zoom und Slack, und dem Anstieg von Cyber-Attacken auf Cloud-Accounts auf.

Finanzsektor und industrieller Fertigung im Cloud-Fieber:

Von Januar bis April konnte in Unternehmen weltweit ein Anstieg von 50 Prozent bei der Cloud-Nutzung festgestellt werden. Dazu gehören auch Unternehmen des Finanzsektors und der industriellen Fertigung (Wachstum um 144 Prozent), die in der Regel mehr als andere auf Legacy-Anwendungen, lokale Netzwerke und Sicherheit angewiesen sind. Auch der Einsatz von Cloud-Kollaborations-Tools wie WebEx, Zoom und Slack, stieg um 600 Prozent, wobei hier der Bildungssektor das meiste Wachstum verzeichnen konnte. Dieser Anstieg kann auf vermehrtes Home-Schooling und E-Learning zurückgeführt werden.

Cyber-Kriminelle halten mit:

Nicht unbemerkt bleibt die vermehrte Cloud-Nutzung bei Cyberkriminellen, die Massen-Cloud-Migration für ihre eigenen Vorteile nutzen. So verdreifachte sich zum einen die Anzahl anormaler Login-Versuche in Cloud-Services innerhalb der ersten vier Monate des Jahres. Es ist davon auszugehen, dass dieser Anstieg auf den erhöhten Cloud-Einsatz von Unternehmen zurückzuführen ist. Zum anderen stiegen externe Angriffe auf Cloud-Services zwischen Januar und April um das Siebenfache, die auf Versuche der Daten-Exfiltration hindeuten. Die meisten dieser Angriffe richteten sich auf Kollaborations-Tools wie Microsoft 365 und versuchten großflächig, Zugangsdaten zu ergattern. Zudem haben sich weitere Einfallstore für Cyber-Kriminelle ergeben, denn der Zugriff auf Cloud-Accounts via nicht-verwaltete, private Geräte der Mitarbeiter verdoppelte sich.

„Um die Covid-19-Pandemie zu überstehen, demonstriert die Welt eine unglaubliche Menge an Mut und gutem Willen. Gleichzeitig mussten wir aber leider auch feststellen, dass viele Cyber-Kriminelle versuchen aus der Krise, und dem damit einhergehenden Wechsel ins Homeoffice, Profit zu schlagen“, sagt Rajiv Gupta, Senior Vice President für den Bereich Cloud-Sicherheit bei McAfee. „Das Risiko, das durch Cyber-Kriminelle Angriffe auf Cloud-Umgebungen entsteht, ist weitaus höher als jenes, das von Mitarbeitern ausgeht, die sich an das neue Arbeitsumfeld gewöhnen müssen. Die Eindämmung dieses Datenverlust-Risikos erfordert Lösungen, die Transparenz und Sicherheitskontrollen für alle Cloud-Dienste bieten.“

Praxis-Beispiel "reCaptcha-Abfragen" als neue Phishing-Methode – Kein Mensch, kein Bot – ein Hacker!

Eine neue Phishing-Methode manipuliert vermehrt "reCaptcha-Abfragen", um zu verhindern, dass automatisierte URL-Analysesysteme auf den eigentlichen Inhalt von Phishing-Seiten zugreifen können. Wie man die Methode erkennen und sich davor schützen kann.

Auch wenn die stationären Geschäfte langsam wieder öffnen, der Online-Kauf hat Hochkonjunktur. Viele seriöse Unternehmen sichern ihre Webseiten durch eine so genannte reCaptcha-Abfrage ab.

Im Dauer-Clinch zwischen Cybersicherheit und Cyberkriminalität finden Hacker erfahrungsgemäß immer wieder neue Methoden, persönliche oder Unternehmensdaten abzugreifen. Seit kurzem fällt auf, dass Hacker in Phishing-Kampagnen zum Zweck der Manipulation von Mail-Konten zunehmend reCaptcha-Mauern einsetzen. Damit wollen sie verhindern, dass automatisierte URL-Analysesysteme auf den eigentlichen Inhalt von Phishing-Seiten zugreifen können.


Was eine "reCaptcha"-Abfrage ist:

reCaptcha ist ein von Google betriebener Sicherheitsdienst, der prüft, ob eine bestimmte Handlung im Internet von einem Menschen oder von einem Computerprogramm bzw. einem Bot vorgenommen wird. Das Akronym steht für "Completely Automated Public Turing test to tell Computers and Humans Apart" (dt. "Vollständig automatisierter öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen"). Der Turing-Test geht zurück auf Alan Turing, der im Jahr 1950 der Frage nachging, ob ein Computer bzw. eine Maschine, ein dem Menschen gleichwertiges Denkvermögen besäße.

Endbenutzer sind i.d.R. sehr vertraut mit solchen Sicherheitsabfragen seriöser Unternehmen, die sie auffordert, ein reCaptcha zu lösen und damit zu klären, dass es sich um einen Menschen handelt. Entsprechend glaubwürdig kommt eine böswillige Phishing-Webseite daher, die ein echtes reCaptcha missbraucht, um den Benutzer auszutricksen.

128.000 E-Mail mit gefälschten Microsoft-Log-ins:

Während einige Methoden die reCaptcha-Box nur simulieren, wird die Verwendung der genuinen reCaptcha-API immer üblicher. Ein zweifellos wirksamerer Ansatz, um automatisierte Scanner zu täuschen, da eine nur gefälschte reCaptcha-Box recht einfach identifizierbar wäre. Entsprechend haben Barracuda-Sicherheitsanalysten im April

AITOx	ITS / DIF – LM-Dokumentation	19.02.25	 Berufskolleg Ostvest
Internet-Security – Gefahren / Angriffe aus dem Internet und mögliche Gegenmaßnahmen!			

lediglich eine E-Mail mit einer gefälschten reCaptcha-Box identifiziert, jedoch über 100.000 E-Mails, die die echte reCaptcha-API verwendeten, entdeckt.

Bei einem Phishing-Angriff auf E-Mail-Konten wurden im gleichen Zeitraum mehr als 128.000 E-Mails verschickt, die gefälschte Microsoft-Anmeldeseiten zeigten. Darin wird mitgeteilt, der Benutzer habe eine Sprachnachricht erhalten. Zudem enthielten diese E-Mails einen HTML-Anhang, der auf eine Seite mit einer reCaptcha-Mauer weiterleitet.

Die Seite enthält nichts anderes als das reCaptcha. Da dieses Format auch für legitime reCaptchas gebräuchlich ist, hat die Täuschung beste Chancen, keinen Argwohn beim Benutzer aufkommen zu lassen.

Sobald der Benutzer jedoch das reCaptcha löst, wird er auf die eigentliche Phishing-Seite umgeleitet, die wiederum das Aussehen einer gewöhnlichen Microsoft-Anmeldeseite imitiert. Auch, wenn das Erscheinungsbild der Seite mit dem legitimen Mailserver des Benutzers nicht übereinstimmen mag, ist es für den Angreifer durchaus möglich, weitere Informationen zu erhalten, um die Phishing-Seite für spätere Zwecke noch überzeugender zu gestalten.

Tipp – Einem reCaptcha nicht bedingungslos vertrauen:

Es ist unabdingbar, die Benutzer vor der Bedrohung durch böswillige reCaptcha-Mauern aufzuklären und ihnen zu vergegenwärtigen, einem reCaptcha nicht bedingungslos zu vertrauen und blind davon auszugehen, dass die dahinterliegende Seite sicher sei.

Dabei führt kein Weg daran vorbei, sich das reCaptcha genauer anzusehen und auf Anomalien zu überprüfen. Wie bei jedem E-Mail-basierten Phishing hilft die Suche nach verdächtigen Absendern, URLs und Anhängen, einen Angriff zu erkennen, bevor sie auf das reCaptcha gelangen. Auch ein reCaptcha, das einem neu erscheint, da vorher keine legitime re-Captcha-Abfrage bestand, sollte den Benutzer alarmieren.

Eine Schulung des Sicherheitsbewusstseins der Benutzer ist eine solide Basis dafür, Phishing-Angriffe frühzeitig zu erkennen. Denn die E-Mail selbst ist immer noch ein Phishing-Angriff und kann von E-Mail-Security-Lösungen erkannt werden. Letztendlich wird jedoch keine Sicherheitslösung alles abfangen, deshalb ist die Fähigkeit der Benutzer, verdächtige E-Mails und Websites zu erkennen, entscheidend.

Praxis-Beispiel zur Erhöhung der WLAN-Sicherheit durch "WPA3" – Was ist hierin "SAE"?

SAE repräsentiert einen neuen Authentifizierungs- und Verschlüsselungsstandard für WLANs!

Definition von "SAE" = "Simultaneous Authentication of Equals":

SAE basiert auf dem "Dragonfly-Handshake"-Protokoll und ermöglicht den sicheren Austausch von Schlüsseln Passwort-basierter Authentifizierungsmethoden. SAE ersetzt in WPA3 die bisherige Methoden zur Aushandlung der Sitzungsschlüssel mittels "Pre-Shared Key" (PSK) und kommt auch in WLAN-Mesh-Implementierungen zum Einsatz. Die Abkürzung SAE steht für Simultaneous Authentication of Equals und bezeichnet ein sicheres Schlüsseltauschverfahren für Passwort-basierte Authentifizierungsmethoden. Es handelt sich um eine Variante des im RFC 7664 spezifizierten "Dragonfly-Key-Exchange"-Protokolls, das wiederum auf dem "Diffie-Hellmann"-Schlüsselaustausch basiert.

U.a. kommt SAE bei WPA3 (Wi-Fi Protected Access 3) zum Einsatz und ersetzt die bisherige Methode zur Aushandlung der Sitzungsschlüssel mittels Pre-Shared Key. Darüber hinaus wird Simultaneous Authentication of Equals in WLAN-Mesh-Netzwerken nach IEEE 802.11s während des Discovery-Prozesses der Peers verwendet. SAE verbessert die Sicherheit des Schlüsselaustauschs im Handshake-Verfahren. Selbst bei der Verwendung von schwachen Kennwörtern ist die Authentifizierung geschützt. Wörterbuch- oder Brute-Force-Angriffe und Angriffsmethoden wie KRACK (Key Reinstallation Attack) sind bei Nutzung von Simultaneous Authentication of Equals praktisch unmöglich.

Die Motivation für Simultaneous Authentication of Equals:

WPA2-basierte WLANs sind anfällig für die im Jahr 2017 bekannt gewordene Angriffsmethode auf die WPA2-Verschlüsselung durch "KRACK". Angreifer können hiermit in den Besitz der Schlüssel gelangen und die übertragenen Daten manipulieren oder mitlesen. KRACK nutzt eine Schwachstelle des mehrstufigen Handshake-Prozesses zur Aushandlung der Sitzungsschlüssel. Ein häufiges Sicherheitsproblem in WLANs ist zudem, dass schwache oder sehr kurze Passwörter verwendet werden. Diese lassen sich relativ schnell mittels Wörterbuch- oder **Brute-Force-Angriffe** herausfinden. SAE soll WLANs gegen diese Schwachstellen absichern und den Datenverkehr in Mesh-Netzwerken schützen. Simultaneous Authentication of Equals erhöht die Sicherheit bei schwachen Kennwörtern und macht Rückschlüsse auf verwendete Schlüssel durch das Aufzeichnen des Handshakes unmöglich. Zudem unterstützt das Schlüsselaustauschprotokoll Perfect Forward Secrecy (PFS) und verhindert Sitzungsschlüssel im Nachhinein zu rekonstruieren. Selbst das nachträgliche Bekanntwerden eines WLAN-Passworts gestattet es nicht, aufgezeichnete Datenpakete zu entschlüsseln.

Die Funktionsweise von SAE:

SAE nutzt nach wie vor übereinstimmende Passwörter, mit denen Clients Zugang zu einem WLAN erhalten. Allerdings wird aus den Passwörtern ein eindeutiger und bei jedem Client anderer Pairwise Master Key (PMK) abgeleitet. Trotz Verwendung eines für alle Clients gleichen Passworts erhält jeder Client einen eigenen PMK. Aus dem PMK werden mittels Vier-Wege-Handshake zwischen WLAN-Client und dem Authentifikationsserver Pairwise Transient Keys (PTK) abgeleitet, mit denen die eigentliche Verschlüsselung der Daten erfolgt.

Die Verwendung von SAE:

Eine der wichtigsten Anwendungen von SAE ist der Authentifizierungs- und Verschlüsselungsstandard für WLANs WPA3. Bei WPA3 ist die von WPA2 verwendete Methode zur Aushandlung von Sitzungsschlüsseln mit Pre-Shared Keys (PSK) durch Simultaneous Authentication of Equals ersetzt. Da Schlüssel nicht mehr über die Funkverbindungen übertragen werden, sind Rückschlüsse auf die Schlüssel durch Mitlesen des Handshakes so gut wie unmöglich. Sitzungsschlüssel zwischen WLAN-Client und Accesspoint lassen sich sicher aushandeln. Durch Perfect Forward Secrecy (PFS) ist zudem sichergestellt, dass sich aufgezeichnete Datenpakete nachträglich nicht mehr entschlüsseln lassen, selbst wenn ein Angreifer in Besitz eines WLAN-Passworts gelangt.

Auch in WLAN-Mesh-Netzwerken wird SAE verwendet. Der Standard IEEE 802.11s definiert, wie sich WLAN-Geräte verbinden, um ein vermaschtes WLAN zu bilden. Die Peers nutzen SAE während des Discovery-Prozesses und stellen mithilfe der abgeleiteten paarweisen Schlüssel sichere Verbindungen her.

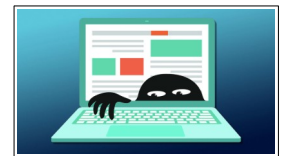
Quellen: "<https://winfuture.de/news,128926.html>"



01.04.22, Autor: Nadine Juliana Dressler

Praxis-Beispiel "Rootkit" – "Hackerangriffe: Neues Windows-Rootkit versteckt sich gekonnt!"

Die Hackergruppe "**Deep Panda**" meldet sich jetzt mit einem neuen Rootkit zurück. Bei den Angriffen wird ihre Malware mit gültigen digitalen Zertifikaten signiert, so dass die Erkennung durch Sicherheitssoftware umgangen und ohne Warnungen in Windows geladen wird.



Das melden die Sicherheitsspezialisten von "Fortinet" (via Bleeping Computer). Fortinet hat aufgedeckt, dass die berüchtigte chinesische Hackergruppe "Deep Panda" es jetzt mithilfe eines "**Log4Shell-Exploits**" (s. "Log4j2-Bug") auf VMware-Horizon-Server abzielt. Solche nicht-gepatchten Server werden aufgespürt, um dort dann ein neuartiges Rootkit namens "**Fire Chili**" einzusetzen.

Dieses Rootkit ist mit einem Zertifikat von "**Frostburn Studios**", einem Spiele-Entwickler, oder einem Zertifikat der Sicherheitssoftware "**Comodo**" digital signiert, um die Erkennung durch AV-Tools zu umgehen. Laut Fortinet hat "Deep Panda" die Zertifikate von den genannten Softwareentwicklern direkt gestohlen oder sie von Datendieben übernommen.

Das "**Fire-Chili-Rootkit**" umgeht die Erkennung auf kompromittierten Systemen durch die legitimen Zertifikate, das ist aber noch lange nicht alles, was die Malware gegen ihre Entdeckung macht.

Noch mehr fiese Versteck-Tricks – Raffiniert!

Für diese "**Verschleierung**" verwendet die Malware dann gefälschte Input/Output Control System Calls, kurz "**IOCTLs**". Um beispielsweise seine eigenen böartigen TCP-Verbindungen vor "**netstat**" zu verbergen, fängt das Rootkit routinemäßige IOCTL-Aufrufe ab, ruft die vollständige Liste aller Netzwerkverbindungen auf, filtert seine eigenen heraus und gibt schließlich eine bereinigte Struktur zurück. So ist das Rootkit auch in Betrieb nahezu unsichtbar.

Einmal auf dem System ihrer Opfer angelangt, prüft Fire Chili zunächst, ob es nicht auf einer simulierten Umgebung läuft. Das Ziel des Rootkits ist es, Datei-Operationen, Prozesse, Ergänzungen von Registrykeys und böartige Netzwerkverbindungen vor dem Benutzer und jeglicher Sicherheitssoftware zu verbergen, die auf dem kompromittierten Computer ausgeführt werden könnte.

Siehe auch:

- **Microsoft Defender-Schwachstelle** verrät Hackern das beste Einfallstor
- **Log4j2-Bug**: Microsoft warnt vor größerer Schwachstelle als SolarWinds
- **Microsoft-Lizenzen** aus dem Supermarkt - Legal, illegal oder scheißegal?

Quellen: "<https://winfuture.de/news,128938.html>"



03.04.22, Autor: Nadine Juliana Dressler


Praxis-Beispiel "Trojaner" (Spyware) – "Russische Android-Spyware überträgt massenhaft Daten an Unbekannte"

Sicherheitsforscher von "**Lab52**" warnen jetzt vor einem Daten-stehlenden Android-Trojaner, dessen Hinterleute in Russland sitzen. Der Trojaner geht dabei besonders gemein vor, denn er versteckt sich und fordert eine Vielzahl an Zugriffs-Berechtigungen an.



Dabei sind die Sicherheitsforscher derzeit noch bei der Analyse, was der neue Android-Trojaner alles auf dem Kerbholz hat. Das berichtet das Online-Magazin "Bleeping Computer". Was man bislang weiß ist, dass der Android-Trojaner in direkter Verbindung zu der russischen Hackergruppe "**Turla**" steht. Lab52 hat dabei eine "**App**" entdeckt, die sich "**Process Manager**" nennt und im Hintergrund die Infrastruktur nutzt, die zuvor den Bedrohungsakteuren von Turla zugeschrieben wurde. Turla ist eine vom russischen Staat unterstützte Hackergruppe, die mit maßgeschneiderter Malware europäische und amerikanische Systeme angreift, vor allem zu Spionagezwecken.

Die nun entdeckte "**App**" "**Process Manager**" ist eine klassische Android-Spyware. Sie sammelt Daten und schickt alle Informationen heimlich an ihre Entwickler.

AITOx	ITS / DIF – LM-Dokumentation	19.02.25	 Berufskolleg Ostvest
Internet-Security – Gefahren / Angriffe aus dem Internet und mögliche Gegenmaßnahmen!			

Bösartige Schadsoftware nennt sich "Process Manager"

Bisher ist nicht bekannt, wie die Spyware verbreitet wird. Lab52 geht davon aus, dass man den Trojaner selbst nicht im Google Play Store findet. Die Hacker nutzen vor allem "**Phishing**", um Opfer dazu zu bringen, den Trojaner zu laden. Nach der Installation versucht die bösertige App "Process Manager", sich auf einem Android-Gerät zu verstecken, indem sie vortäuscht, eine "Systemkomponente" zu sein. Dazu wird ein Zahnrad-förmiges Symbol angezeigt, das an die Einstellungen erinnert.

Beim ersten Start fordert die App den Nutzer auf, ihr eine Vielzahl an Berechtigungen zu erteilen. Dazu gehört der Zugriff auf Speicherort, Feinstandort, Netzwerkstatus und WLAN-Status. Zudem sollen Berechtigungen für Kamera, Internet, das Ändern der Audioeinstellungen, SMS lesen und senden, Anrufprotokoll lesen, Kontakte lesen und Audio aufzeichnen gegeben werden. Damit ist die App ein ernsthaftes Risiko nicht nur in Sachen Privatsphäre. Nachdem die App diese Berechtigungen erhalten hat, entfernt sich die Spyware vom Home-Bildschirm und läuft danach ständig resident im Hintergrund.

Die vom Gerät gesammelten Informationen, einschließlich Listen, Protokolle, SMS, Aufnahmen und Ereignis-Benachrichtigungen, werden im "JSON"-Format (JASON = "JavaScript Object Notation", this is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays) an den "Command-and-Control-Server" der Cyber-Gangster gesendet.

Bei der Untersuchung der App fand das Lab52-Team auch heraus, dass sie zusätzliche Nutzdaten auf das Gerät herunterlädt, und fand einen Fall einer App, die direkt aus dem Play Store geholt wurde. Es handelt sich dabei um "**Roz Dhan: Earn Wallet Cash**". Es ist möglich, dass dies ein Teil der Taktik ist, um Spuren zu verwischen und Sicherheitsforscher zu verwirren. Laut Lab52 können die Hacker über "Roz Dhan: Earn Wallet Cash" aber auch im Hintergrund Geld verdienen.

Quelle: **Cisco-ITN-Curriculum, Kapitel 11.2: "Netzwerksicherheit"**

Kapitel 11.2 Netzwerksicherheit

Kapitel 11.2.1 Sicherheitsbedrohungen und Schwachstellen

Kapitel 11.2.1.1 Arten von Bedrohungen

Computernetzwerke sind ein wesentlicher Bestandteil täglicher Aktivitäten. Dies gilt sowohl für kabelgebundene als auch für Wireless-Netzwerke. Menschen verlassen sich ebenso auf ihre Computer und Netzwerke wie Unternehmen. Eindringversuche nicht autorisierter Personen können zu teuren Netzwerkausfällen und zum Verlust von Arbeitsergebnissen führen. Angriffe auf ein Netzwerk können verheerende Auswirkungen haben und Zeit und Geld kosten, wenn wichtige Informationen oder Vermögenswerte beschädigt oder gestohlen werden.

Eindringlinge können sich durch Softwareschwachstellen, Hardware-Angriffe oder durch Erraten des Benutzernamens und Kennworts einer Person Zugriff auf ein Netzwerk verschaffen. Eindringlinge, die sich durch Softwareänderungen oder die Ausnutzung von Schwachstellen in Software Zugriff verschaffen, werden häufig als Hacker bezeichnet.

Wenn ein Hacker Zugriff auf ein Netzwerk erlangt, können vier Arten von Bedrohungen entstehen, wie im Bild unten gezeigt wird. Klicken Sie auf die einzelnen Bilder, um weitere Informationen anzuzeigen.

 Informationsdiebstahl	 Datenverlust und -manipulation	Informationsdiebstahl Hierbei verschafft sich eine Person Zugriff auf einen Computer, um vertrauliche Informationen zu erhalten. Die Informationen können verwendet oder für verschiedene Zwecke verkauft werden. Beispiel: Diebstahl von proprietären Informationen eines Unternehmens wie Informationen zu Forschung und Entwicklung.
 Identitätsdiebstahl	 Dienstunterbrechung	

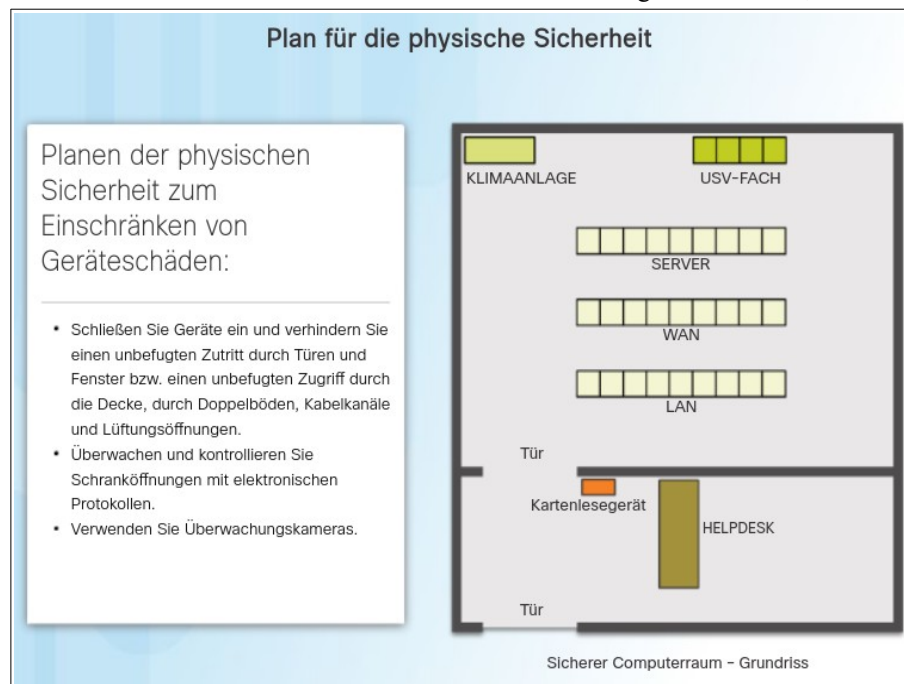
Datenverlust und -manipulation Hierbei verschafft sich eine Person Zugriff auf einen Computer, um Datensätze zu zerstören oder zu ändern. Beispiele für einen Datenverlust: Senden eines Virus, der die Festplatte des Computers neu formatiert. Beispiele für Datenmanipulation: Unbefugter Zugriff auf ein Datensatzsystem, um Informationen zu ändern, z. B. den Preis eines Artikels.	Identitätsdiebstahl Dies ist eine Form des Informationsdiebstahls, bei der persönliche Daten gestohlen werden, um die Identität einer anderen Person anzunehmen. Mithilfe dieser Informationen kann sich eine Person Rechtsdokumente verschaffen, einen Kredit beantragen und nicht autorisierte Online-Einkäufe tätigen. Identitätsdiebstahl ist ein wachsendes Problem, das pro Jahr Milliarden von Euro kostet.	Dienstunterbrechung Hierbei wird verhindert, dass legitime Benutzer auf Dienste zugreifen können, zu deren Nutzung sie berechtigt sind. Beispiele: Denial-of-Service (DoS)-Angriffe auf Server, Netzwerkgeräte oder Netzwerkkommunikationsverbindungen.
---	--	---

Kapitel 11.2.1.2 *Physische Sicherheit*

Eine ebenso wichtige Schwachstelle ist die physische Sicherheit von Geräten. Ein Angreifer kann dafür sorgen, dass Netzwerkressourcen nicht genutzt werden können, wenn es ihm gelingt, diese Ressourcen physisch zu kompromittieren. Physische Bedrohungen fallen in vier Kategorien. Diese Kategorien sind wie folgt:

- **Hardware-Bedrohungen** – Physische Beschädigung von Servern, Routern, Switches, Kabeln und Workstations.
- **Bedrohungen durch extreme Umgebungsbedingungen** – Extreme Temperaturen (zu heiß oder zu kalt) oder extreme Luftfeuchtigkeit (zu feucht oder zu trocken).
- **Elektrische Bedrohungen** – Spannungsspitzen, unzureichende Versorgungsspannung (Spannungseinbrüche), schwankende Leistung (Rauschen) und totaler Stromausfall.
- **Bedrohungen durch unsachgemäße Wartung** – Unsachgemäße Handhabung von sehr wichtigen elektrischen HW-Komponenten (elektrostatische Entladung), Fehlen wichtiger Ersatzteile, fehlerhafte Verkabelung und unzureichende Kennzeichnung.

Diese Probleme müssen durch Unternehmensrichtlinien abgedeckt werden, wie das nachfolgende Bild zeigt.



Kapitel 11.2.1.3 *Arten von Schwachstellen*

Der Begriff "Schwachstelle" bezieht sich auf ein gewisses Maß an Anfälligkeit, das bei jedem Netzwerk und Gerät zu verzeichnen ist. 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 hierbei wie folgt drei primäre Schwachstellen:

- Technologische Schwachstellen, wie in Abb. 1 gezeigt.
- Konfigurationsschwachstellen, wie in Abb. 2 gezeigt.
- Schwachstellen bei Sicherheitsrichtlinien, wie in Abb. 3 gezeigt.

Alle drei Schwachstellen können unterschiedlichen Angriffen ausgesetzt sein, darunter Angriffe durch Schadcode und Netzwerkangriffe.

Schwachstellen – Technologie

Network Security Weaknesses

Schwachstellen beim TCP/IP-Protokoll

- Das Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) und Internet Control Message Protocol (ICMP) sind prinzipiell unsicher.
- Das Simple Network Management Protocol (SNMP) und Simple Mail Transfer Protocol (SMTP) haben eine ähnliche, prinzipiell unsichere Struktur wie die, auf der TCP basiert.

Schwachstellen beim Betriebssystem

- Jedes Betriebssystem hat Sicherheitsprobleme, die berücksichtigt werden müssen.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- Sie sind in den CERT-Archiven (Computer Emergency Response Team) unter <http://www.cert.org> dokumentiert.

Schwachstellen bei Netzwerkgeräten

Verschiedene Arten von Netzwerkgeräten wie Router, Firewalls und Switches haben Sicherheitslücken, die erkannt und abgesichert werden müssen. Zu den Schwachstellen gehören Kennwortschutz, fehlende Authentifizierung, Routing-Protokolle und Firewall-Lücken.

Schwachstellen – Konfiguration

Konfigurationsschwachstellen	Wie die Schwachstelle ausgenutzt wird
Unsichere Benutzerkonten	Benutzerkontodaten können unsicher über das Netzwerk übertragen werden, sodass Benutzernamen und Kennwörter Schnüffelfprogrammen (Snoopers) ausgesetzt sind.
Systemkonten mit leicht zu erratenden Kennwörtern	Dieses weit verbreitete Problem ist das Ergebnis falsch ausgewählter und leicht zu erratender Benutzerkennwörter.
Falsch konfigurierte Internetdienste	Ein häufiges Problem ist das Aktivieren von JavaScript in Webbrowsern. Hierdurch werden Angriffe durch schädliche JavaScript-Programme ermöglicht, wenn der Benutzer auf nicht vertrauenswürdige Websites zugreift. Andere potenzielle Schwachstellen sind falsch konfigurierte Terminaldienste, FTP oder Webserver (z. B. Microsoft-Internetinformationsdienste (IIS), Apache HTTP-Server).
Ungesicherte Standardeinstellungen in Produkten	Viele Produkte haben Standardeinstellungen, die Sicherheitslücken verursachen.
Falsch konfigurierte Netzwerkgeräte	Fehlkonfigurationen der Geräte selbst können erhebliche Sicherheitsprobleme verursachen. Zum Beispiel können falsch konfigurierte Zugriffslisten, Routing-Protokolle oder SNMP-Community-Zeichenfolgen die Ursache für umfangreiche Sicherheitslücken sein.

Schwachstellen – Richtlinien

Richtlinienschwachstellen	Wie die Schwachstelle ausgenutzt wird
Fehlen schriftlicher Sicherheitsrichtlinien	Ungeschriebene Richtlinien können nicht konsequent angewandt oder durchgesetzt werden.
Firmenpolitik	Auseinandersetzungen bzgl. der Firmenpolitik und Streitigkeiten hinsichtlich der Zuständigkeit können eine konsistente Umsetzung von Sicherheitsrichtlinien erschweren.
Fehlende Kontinuität bei der Authentifizierung	Falsch ausgewählte, einfach zu hackende oder Standardkennwörter können den unbefugten Zugriff auf das Netzwerk ermöglichen.
Nicht angewendete logische Zugriffskontrollen	Mangelhaftes Überwachen und Auditing lassen Angriffe und die unbefugte Nutzung weiterhin zu, wodurch Unternehmensressourcen verschwendet werden. Die Folge davon können rechtliche Schritte gegen IT-Techniker, das IT-Management oder sogar die Unternehmensführung sein, die zulassen, dass diese unsicheren Bedingungen fortbestehen, bis hin zu deren Kündigung.
Software- und Hardware-Installationen und -Änderungen folgen nicht den Richtlinien	Unberechtigte Änderungen an der Netzwerktopologie oder die Installation von nicht genehmigten Anwendungen verursachen Sicherheitslücken.
Kein Disaster-Recovery-Plan	Das Fehlen eines Disaster-Recovery-Plans führt zu Chaos, Panik und Verwirrung, wenn ein Angriff auf das Unternehmen stattfindet.

Kapitel 11.2.1.4 Aktivität – Sicherheitsbedrohungen und Schwachstellen

Übung 1:

Aktivität – Teil 1: Sicherheitsbedrohungen und Schwachstellen

Anweisungen

Lesen Sie sich die Szenarien für Sicherheitsbedrohungen und Schwachstellen durch. Ziehen Sie jedes Szenario auf die entsprechende Sicherheitsbedrohung.

<div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Senden eines Virus zum Neuformatieren einer Festplatte</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Verhindern, dass berechtigte Benutzer Datendienste nutzen können</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Stehlen der Benutzerdatenbank eines Unternehmens</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Tätigen illegaler Online-Einkäufe</div>	<div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Ändern von Datensätzen</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Stehlen wissenschaftlicher Forschungsberichte</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Überlasten eines Netzwerks, um Benutzern den Zugriff zu verweigern</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Sich als jemand anderes ausgeben, um einen Kredit zu erhalten</div>
--	---

Prüfen
Zurücksetzen

Informationsdiebstahl

Identitätsdiebstahl

Datenverlust/-manipulation

Dienstunterbrechung

Lösung:

Aktivität – Teil 1: Sicherheitsbedrohungen und Schwachstellen

Anweisungen

Lesen Sie sich die Szenarien für Sicherheitsbedrohungen und Schwachstellen durch. Ziehen Sie jedes Szenario auf die entsprechende Sicherheitsbedrohung.

<div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Stehlen der Benutzerdatenbank eines Unternehmens</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Stehlen wissenschaftlicher Forschungsberichte</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Senden eines Virus zum Neuformatieren einer Festplatte</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Ändern von Datensätzen</div>	<div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Tätigen illegaler Online-Einkäufe</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Sich als jemand anderes ausgeben, um einen Kredit zu erhalten</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Verhindern, dass berechtigte Benutzer Datendienste nutzen können</div> <div style="border: 1px solid #007bff; padding: 5px; margin-bottom: 5px;">Überlasten eines Netzwerks, um Benutzern den Zugriff zu verweigern</div>
--	---

Prüfen
Zurücksetzen

Informationsdiebstahl

✓

Stehlen der Benutzerdatenbank eines Unternehmens

✓

Stehlen wissenschaftlicher Forschungsberichte

Identitätsdiebstahl

✓

Tätigen illegaler Online-Einkäufe

✓

Sich als jemand anderes ausgeben, um einen Kredit zu erhalten

Datenverlust/-manipulation

✓

Senden eines Virus zum Neuformatieren einer Festplatte

✓

Ändern von Datensätzen

Dienstunterbrechung

✓

Verhindern, dass berechtigte Benutzer Datendienste nutzen können

✓

Überlasten eines Netzwerks, um Benutzern den Zugriff zu verweigern

Übung 2:

Aktivität – Teil 2: Sicherheitsbedrohungen und Schwachstellen

Anweisungen

Lesen Sie sich die praktischen Maßnahmen zum Sicherheitsmanagement durch. Ziehen Sie alle praktischen Managementmaßnahme auf den entsprechenden Sicherheitsmanagamentyp.

Beschriften wichtiger Kabel und Komponenten

Kontrolle von Temperatur und Luftfeuchtigkeit

Steuerung des Zugriffs auf Konsolen-Ports

Einsatz von Überwachungskameras

Einrichten eines positiven Luftstroms

Installieren redundanter Stromversorgungen

Installieren von USV-Systemen

Einschließen von Geräten – Verhindern von unberechtigtem Zugriff

Prüfen

Zurücksetzen

Hardware

Umgebung

Elektrisch

Wartung

Lösung:

Aktivität – Teil 2: Sicherheitsbedrohungen und Schwachstellen

Anweisungen

Lesen Sie sich die praktischen Maßnahmen zum Sicherheitsmanagement durch. Ziehen Sie alle praktischen Managementmaßnahme auf den entsprechenden Sicherheitsmanagamentyp.

Beschriften wichtiger Kabel und Komponenten

Kontrolle von Temperatur und Luftfeuchtigkeit

Steuerung des Zugriffs auf Konsolen-Ports

Einsatz von Überwachungskameras

Einrichten eines positiven Luftstroms

Installieren redundanter Stromversorgungen

Installieren von USV-Systemen

Einschließen von Geräten – Verhindern von unberechtigtem Zugriff

Prüfen


Zurücksetzen

Hardware

Umgebung

Elektrisch

Wartung

AITOx	ITS / DIF – LM-Dokumentation	19.02.25	 Berufskolleg Ostvest
Internet-Security – Gefahren / Angriffe aus dem Internet und mögliche Gegenmaßnahmen!			

Kapitel 11.2.2 Netzwerkangriffe

Kapitel 11.2.2.1 Arten von Malware

Malware oder Schadcode (Malcode, Schadsoftware) ist die Kurzform für bösartige 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 typische Arten von Malware. Klicken Sie auf die Wiedergabeschaltfläche (s.u. Abbildungen hierzu!), um sich eine Animation für diese drei Bedrohungen anzusehen.

Was ist ein Intrusion Detection System (Abk. "IDS")?

Intrusion Detection ist eine wichtige Sicherheitstechnologie zum Schutz gegen Cyber-Angriffe. Ein IDS (Intrusion Detection System) überwacht den Netzwerkverkehr auf verdächtige Aktivitäten und schlägt Alarm, wenn es einen Einbruchversuch bemerkt. Die fortschrittlichsten Lösungen zur Erkennung (Intrusion Detection) und zur Unterbindung (Intrusion Prevention) von Angriffen nutzen Echtzeit-Verhaltensanalysen und maschinelles Lernen.

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. Der Schweregrad eines Angriffs durch Viren kann sehr unterschiedlich sein und reicht von einem einfachen Ärgernis bis hin zur Beschädigung von Daten oder Software und Denial-of-Service (DoS)-Zuständen. Fast alle Viren sind an eine ausführbare Datei angehängt. Das bedeutet, dass der Virus auf einem System vorhanden sein kann, jedoch erst aktiv wird oder sich verbreiten kann, wenn ein Benutzer die bösartige Host-Datei oder das bösartige Host-Programm öffnet oder ausführt. Beim Ausführen des Host-Codes wird der Virencode ebenfalls ausgeführt. Normalerweise bleibt das Host-Programm funktionsfähig, nachdem es durch den Virus infiziert wurde. Einige Viren überschreiben jedoch andere Programme mit Kopien von sich selbst, wodurch das Host-Programm vollständig zerstört wird. Viren verbreiten sich, wenn die Software oder das Dokument, an die bzw. das sie angehängt sind, über das Netzwerk, einen Datenträger, durch Dateifreigabe oder infizierte E-Mail-Anhänge von einem Computer auf einen anderen übertragen wird.

Würmer:

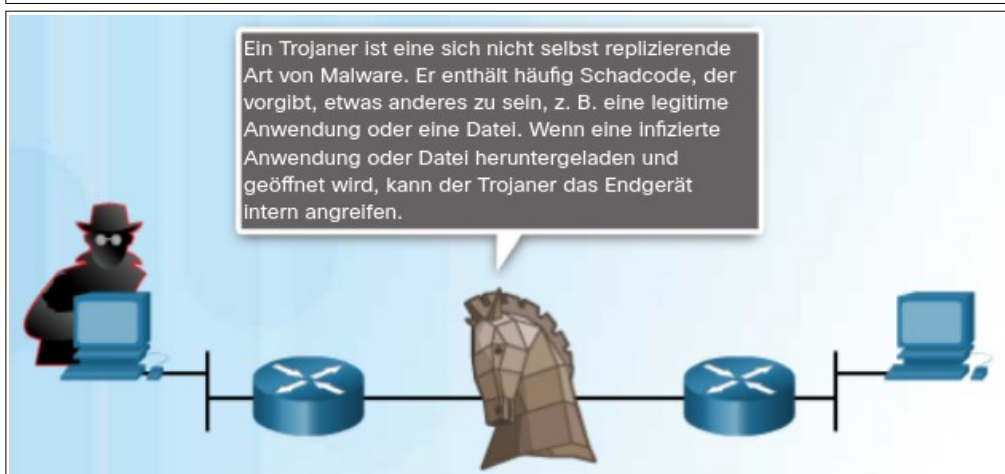
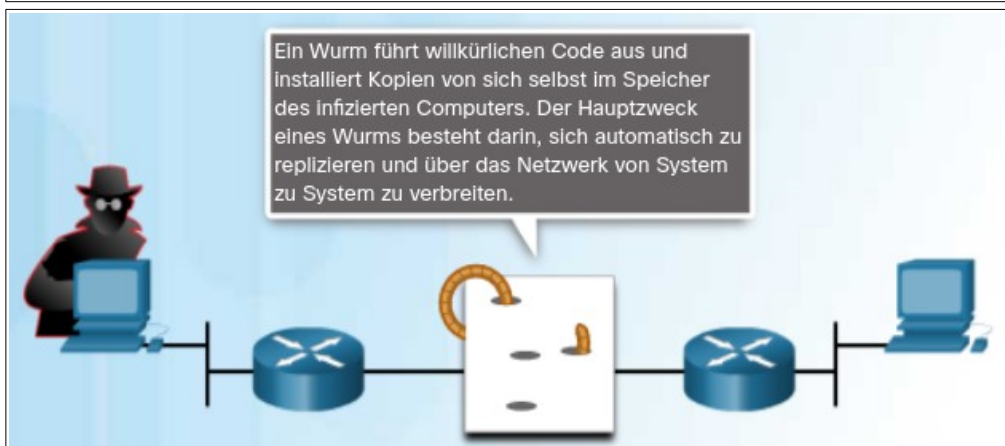
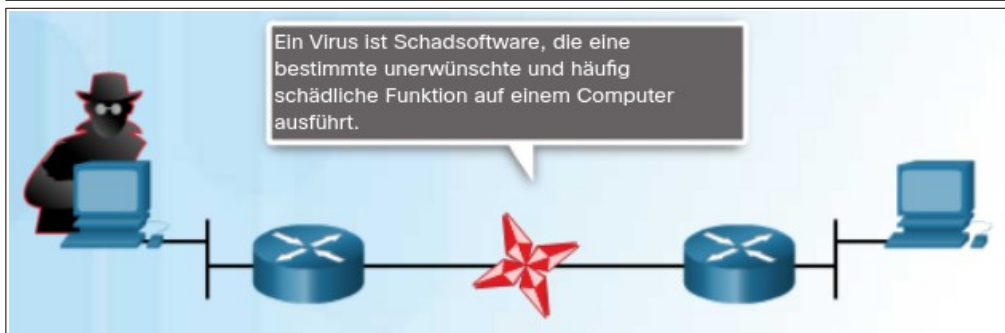
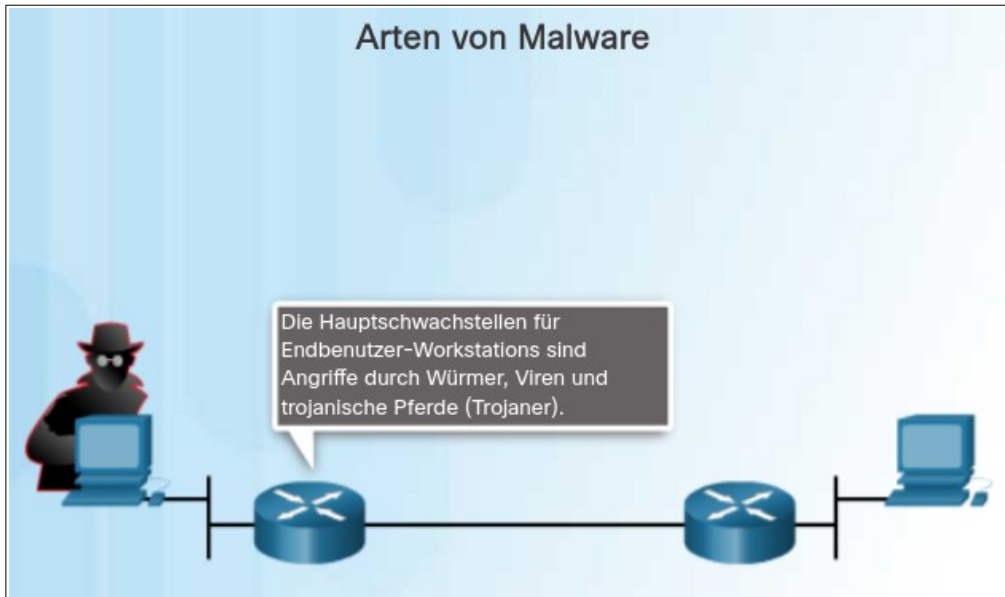
Computerwürmer ähneln Viren insofern, als dass sie funktionsfähige Kopien von sich selbst replizieren und die gleiche Art von Schaden verursachen können. Im Gegensatz zu Viren, die die Verbreitung einer infizierten Host-Datei erfordern, sind Würmer jedoch Standalone-Software und benötigen kein Host-Programm oder menschliche Unterstützung, um sich zu verbreiten. Ein Wurm muss nicht an ein Programm angehängt sein, um einen Host zu infizieren und über eine Schwachstelle im System in einen Computer einzudringen. Würmer nutzen Systemfunktionen, um sich ohne Hilfe über das Netzwerk zu verbreiten.

Trojanische Pferde:

Ein trojanisches Pferd (kurz Trojaner) ist eine weitere Malware-Art, benannt nach dem hölzernen Pferd der Griechen, mit dessen Hilfe diese in Troja eindringen. Es handelt sich hierbei um schädliche Software, die harmlos und legitim aussieht. Benutzer werden i.d.R. dazu verleitet, die Software zu laden und auf ihren Systemen auszuführen. Nach seiner Aktivierung kann ein Trojaner beliebig viele Angriffe auf den Host starten, angefangen vom Ärgern des Benutzers durch Einblenden von Fenstern oder Ändern des Desktops bis hin zur Beschädigung des Hosts durch Löschen von Dateien, Stehlen von Daten oder Aktivieren und Verbreiten anderer Malware wie Viren. Trojaner sind auch dafür bekannt, dass sie Hintertüren erstellen, über die sich böswillige Benutzer Zugriff auf das System verschaffen können.

Anders als Viren und Würmer reproduzieren sich Trojaner nicht, indem sie andere Dateien infizieren, und sie replizieren sich auch nicht 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.

Arten von Malware



This video shows two PCs. Each PC is connected to a router and the routers are connected. There is an attacker working on one of the computers. The attacker is sending malicious code to the other PC in the form of worms, viruses, and a Trojan horse.

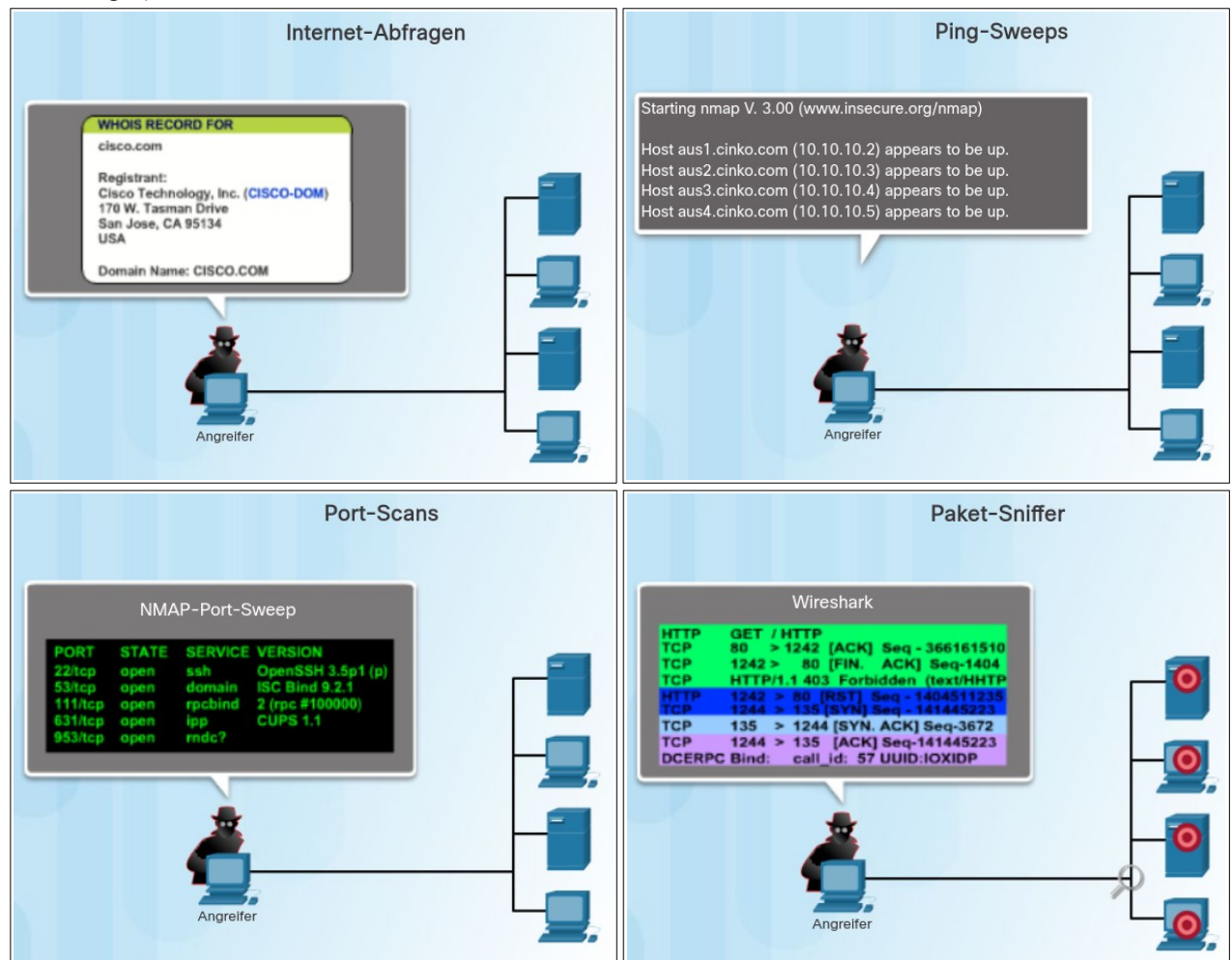
Kapitel 11.2.2.2 Reconnaissance-Angriffe

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

- **Reconnaissance-Angriffe** – Die Erkennung und Zuordnung von Systemen, Diensten oder Schwachstellen.
- **Zugriffsangriffe** – 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 die Dienstprogramme "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 Angreifer ein "Ping" an die öffentlich verfügbaren IP-Adressen senden, um die aktiven Adressen zu identifizieren. Zur Automatisierung dieses Schritts kann ein Angreifer ein "Ping-Sweep-Tool" wie "fping" oder "gping" verwenden, das systematisch ein Ping an alle Netzwerkadressen in einem bestimmten Bereich oder Subnetz sendet. Dies ist vergleichbar mit dem Durchsuchen eines Adressbuchs und dem Anrufen jeder betreffenden Nummer, um damit herauszufinden, wer antwortet.

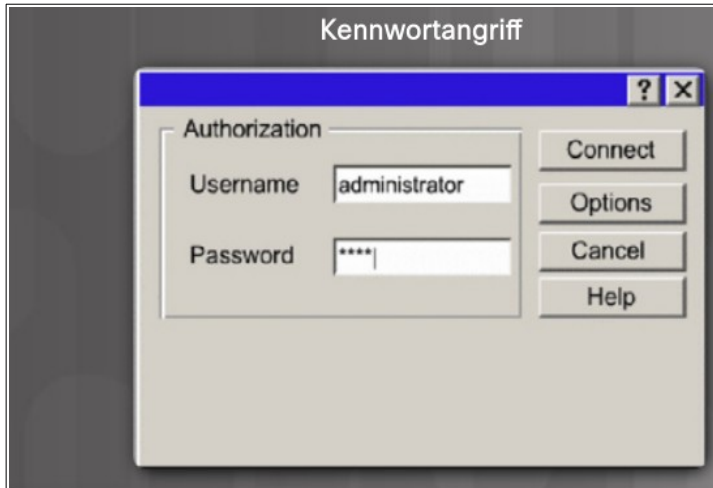
Klicken Sie auf die einzelnen Tools für Reconnaissance-Angriffe, um sich eine Animation des Angriffs anzusehen (s.u. Abbildungen).



Kapitel 11.2.2.3 Zugriffsangriffe

Zugriffsangriffe nutzen bekannte Schwachstellen in Authentifizierungs-, FTP- und Webdiensten aus, um Zugriff auf Web-Konten, vertrauliche Datenbanken und andere vertrauliche Informationen zu erhalten. Ein Zugriffsangriff ermöglicht einer Person unbefugten Zugriff auf Informationen zu erhalten, zu deren Ansicht sie nicht berechtigt ist. Zugriffsangriffe fallen in vier Kategorien:

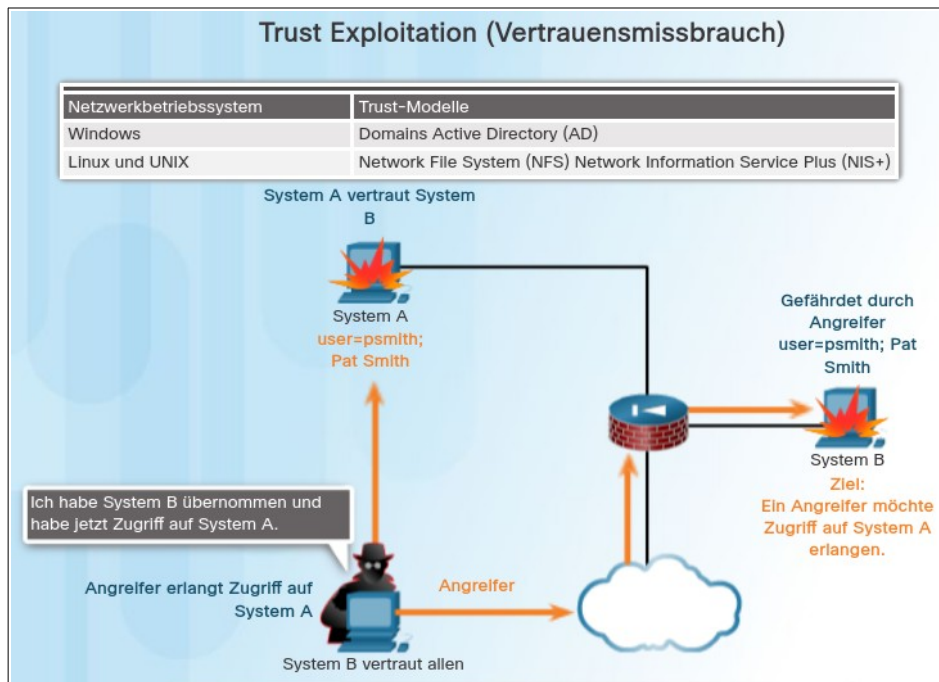
- Kennwortangriffe (Abb. 1).
- Trust Exploitation-Angriffe (Vertrauensmissbrauch) (Abb. 2).
- Port-Umleitung (Abb. 3).
- Man-in-the-Middle-Angriffe (Abb. 4).



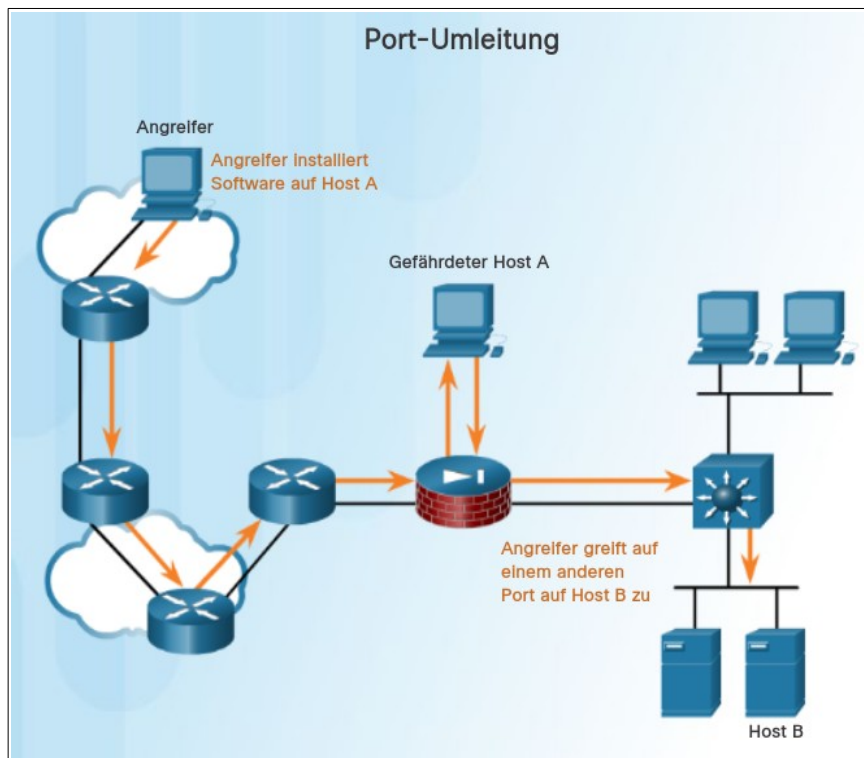
Angreifer können Kennwortangriffe unter Verwendung verschiedener Methoden durchführen:

- Brute-Force-Angriffe
- Trojaner-Programme
- Paket-Sniffer

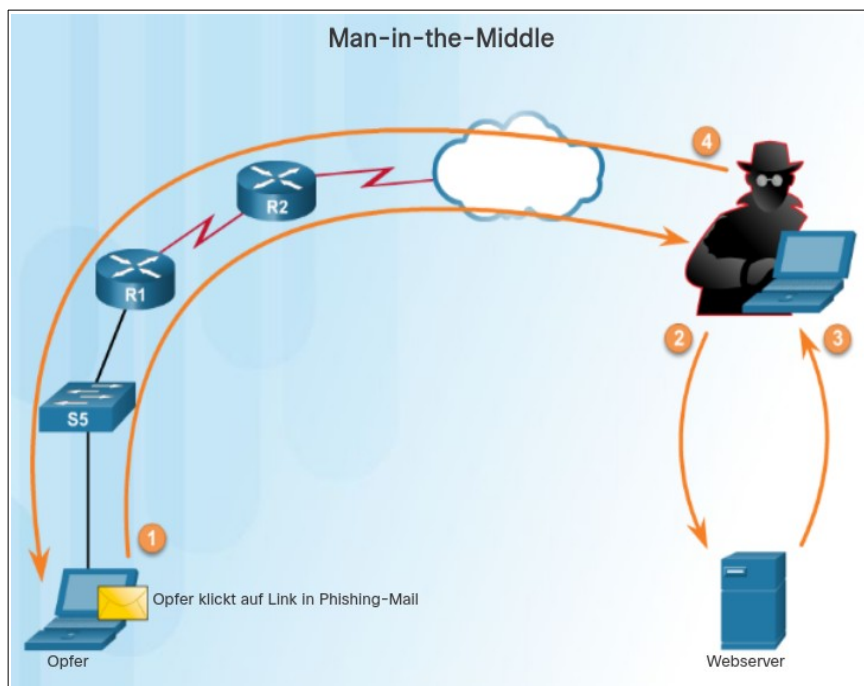
(Abb. 1)



(Abb. 2)



(Abb. 3)



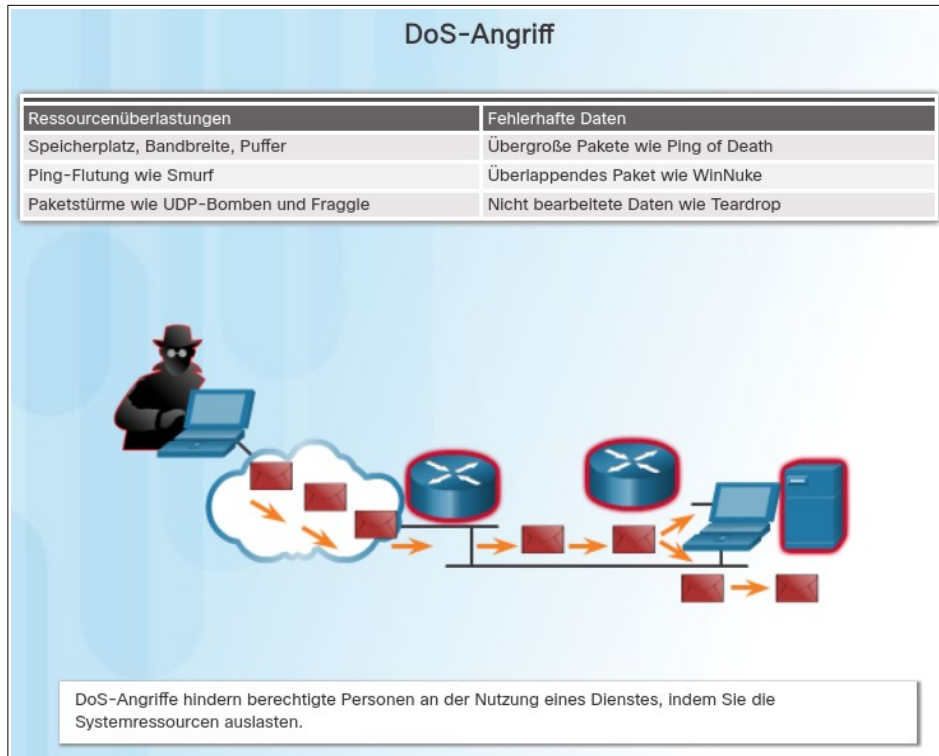
(Abb. 4)

Kapitel 11.2.2.4 DoS-Angriffe

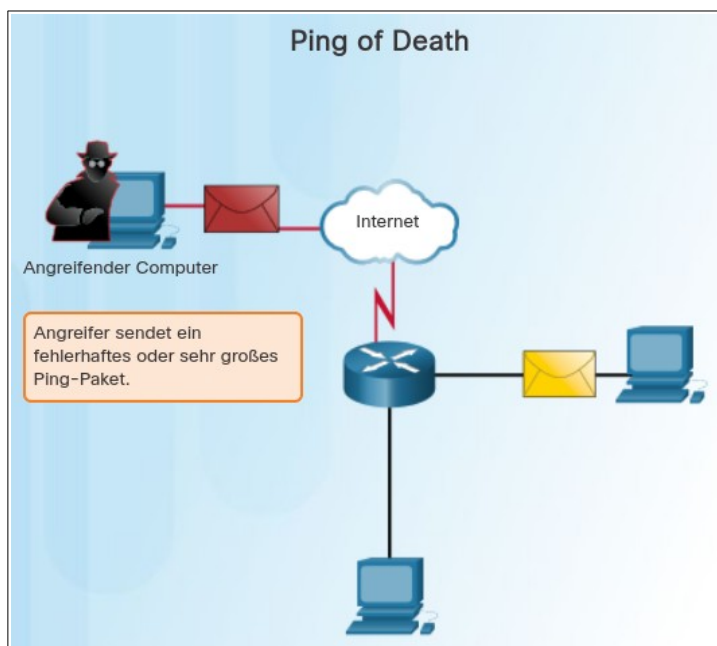
Denial of Service (DoS)-Angriffe sind die bekannteste Art von Angriffen und gehören mit zu den Angriffen, die extrem schwer zu beseitigen sind. Selbst in der Hacker-Community werden DoS-Angriffe als trivial angesehen und gelten als schlechter Stil, weil ihre Durchführung so wenig Aufwand erfordert. Aber gerade weil sie so einfach angewendet werden können und dennoch bemerkenswerten Schaden anrichten, verdienen DoS-Angriffe eine besondere Aufmerksamkeit von Sicherheitsadministratoren.

DoS-Angriffe treten in vielen unterschiedlichen Formen auf. DoS-Angriffe verhindern, dass Personen einen Dienst nutzen können, indem Sie Systemressourcen verbrauchen. Klicken Sie auf die Schaltflächen im Bild unten, um einige Beispiele für DoS- und DDoS-Angriffe anzuzeigen.

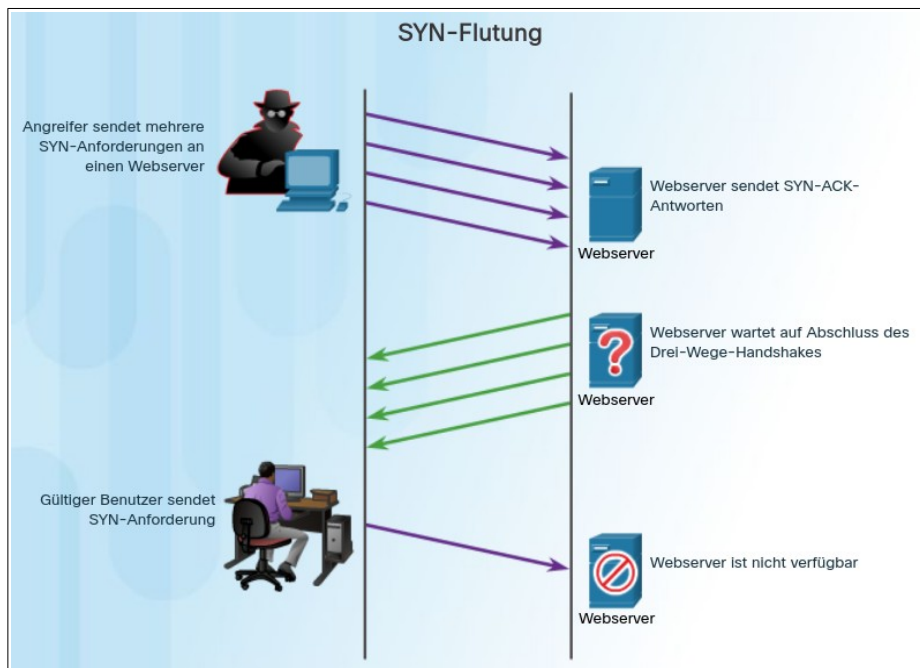
Um DoS-Angriffe zu vermeiden, ist es wichtig, stets die neuesten Sicherheits-Updates für Betriebssysteme und Anwendungen zu installieren. So stellt z. B. das „Ping of Death“ keine Bedrohung mehr dar, da Updates für Betriebssysteme die Schwachstelle behoben haben, die von diesem Angriff ausgenutzt wurde.



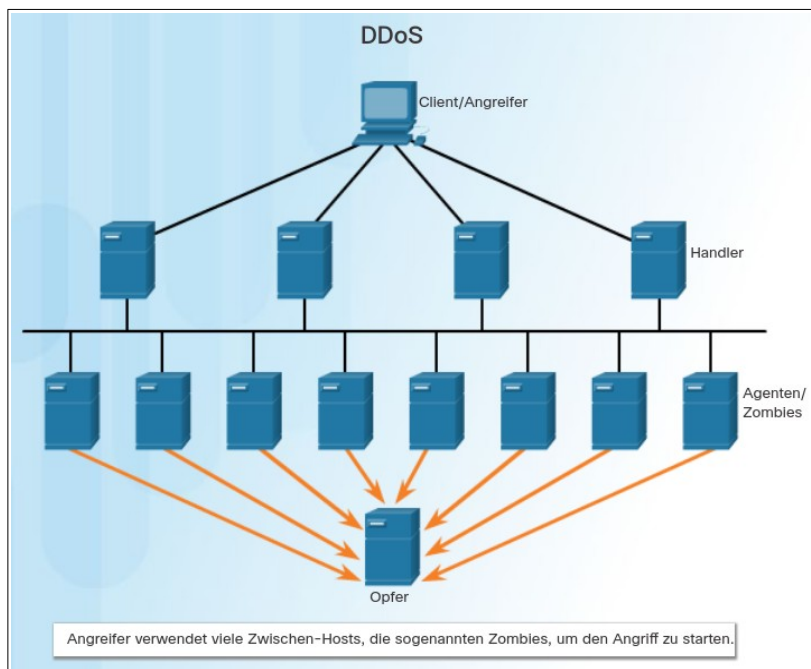
(Abb. 1)



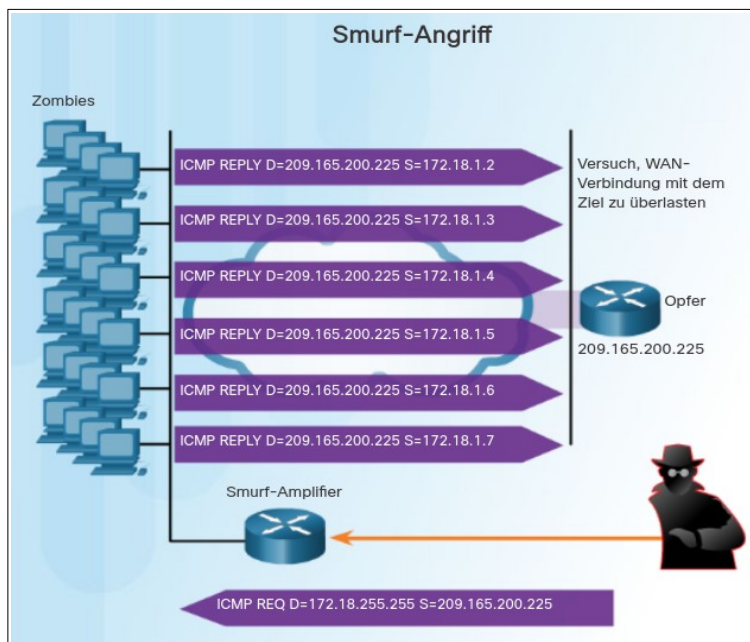
(Abb. 2)



(Abb. 3)



(Abb. 4)



(Abb. 5)

Kapitel 11.2.2.5 Aktivität – Angriffstypen

Übung 1:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Wurm

Zugriff

Virus

Trojaner

Reconnaissance-Angriff

Denial of Service (DoS)

Angriffstyp	Sicherheitsangriffsszenario
	Ein Computer wird als Druckserver für ACME Inc. verwendet. Die IT-Mitarbeiter haben seit mehr als 60 Tagen keine Sicherheits-Updates mehr auf diesen Computer angewendet. Jetzt arbeitet der Druckserver langsam und sendet eine hohe Anzahl schädlicher Pakete an seine Netzwerkkarte.
	Sabine, eine interne IT-Mitarbeiterin bei ACME Inc., hat bei der Überprüfung der von der Firewall generierten Sicherheitsprotokolle einige verdächtige Pakete bemerkt. Eine Handvoll IP-Adressen im Internet haben falsch formatierte Pakete an eine Reihe unterschiedlicher IP-Adressen und mehrere zufällige Port-Nummern bei ACME Inc. gesendet.

Lösung:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Zugriff

Virus

Trojaner

Denial of Service (DoS)

Angriffstyp	Sicherheitsangriffsszenario
✓ <div style="border: 1px solid black; padding: 5px; display: inline-block;">Wurm</div>	Ein Computer wird als Druckserver für ACME Inc. verwendet. Die IT-Mitarbeiter haben seit mehr als 60 Tagen keine Sicherheits-Updates mehr auf diesen Computer angewendet. Jetzt arbeitet der Druckserver langsam und sendet eine hohe Anzahl schädlicher Pakete an seine Netzwerkkarte.
✓ <div style="border: 1px solid black; padding: 5px; display: inline-block;">Reconnaissance-Angriff</div>	Sabine, eine interne IT-Mitarbeiterin bei ACME Inc., hat bei der Überprüfung der von der Firewall generierten Sicherheitsprotokolle einige verdächtige Pakete bemerkt. Eine Handvoll IP-Adressen im Internet haben falsch formatierte Pakete an eine Reihe unterschiedlicher IP-Adressen und mehrere zufällige Port-Nummern bei ACME Inc. gesendet.

Übung 2:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Wurm

Zugriff

Virus

Trojaner

Reconnaissance-Angriff

Denial of Service (DoS)

Angriffstyp	Sicherheitsangriffsszenario
	<p>Jens surfte mit seinem PC im Internet, als ihm von einer beliebigen Website ein kostenloses Programm zum Bereinigen seines Systems angeboten wurde. Nachdem er die ausführbare Datei heruntergeladen und ausgeführt hatte, stürzte das Betriebssystem ab. Wichtige Betriebssystemdateien waren beschädigt und es musste eine vollständige Festplattenformatierung und Neuinstallation des Betriebssystems für Jens' Computer durchgeführt werden.</p>
	<p>Andrea fand auf dem Parkplatz eines Einkaufszentrums ein Flash-Laufwerk. Sie fragte ein wenig herum, konnte aber den Besitzer nicht ermitteln. Sie beschloss, das Laufwerk zu behalten, und schloss es an ihren Laptop an. Dabei fand sie einen Ordner mit Fotos. Neugierig öffnete Andrea einige Fotos, bevor sie das Flash-Laufwerk für ihre eigenen Zwecke formatierte. Danach bemerkte Andrea, dass die Kamera ihres Laptops aktiviert war.</p>

Lösung:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Wurm

Zugriff

Reconnaissance-Angriff

Denial of Service (DoS)

Angriffstyp	Sicherheitsangriffsszenario
<div style="display: flex; align-items: center; justify-content: center;"> ✓ <div style="border: 2px solid blue; padding: 5px; background-color: #e0f0ff;">Virus</div> </div>	<p>Jens surfte mit seinem PC im Internet, als ihm von einer beliebigen Website ein kostenloses Programm zum Bereinigen seines Systems angeboten wurde. Nachdem er die ausführbare Datei heruntergeladen und ausgeführt hatte, stürzte das Betriebssystem ab. Wichtige Betriebssystemdateien waren beschädigt und es musste eine vollständige Festplattenformatierung und Neuinstallation des Betriebssystems für Jens' Computer durchgeführt werden.</p>
<div style="display: flex; align-items: center; justify-content: center;"> ✓ <div style="border: 2px solid blue; padding: 5px; background-color: #e0f0ff;">Trojaner</div> </div>	<p>Andrea fand auf dem Parkplatz eines Einkaufszentrums ein Flash-Laufwerk. Sie fragte ein wenig herum, konnte aber den Besitzer nicht ermitteln. Sie beschloss, das Laufwerk zu behalten, und schloss es an ihren Laptop an. Dabei fand sie einen Ordner mit Fotos. Neugierig öffnete Andrea einige Fotos, bevor sie das Flash-Laufwerk für ihre eigenen Zwecke formatierte. Danach bemerkte Andrea, dass die Kamera ihres Laptops aktiviert war.</p>

Übung 3:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Wurm

Zugriff

Virus

Trojaner

Reconnaissance-Angriff

Denial of Service (DoS)

Angriffstyp	Sicherheitsangriffsszenario
	Angela, eine IT-Mitarbeiterin bei ACME Inc., bemerkt, dass die Kommunikation mit dem Webserver der Firma sehr langsam ist. Sie überprüft dies und stellt fest, dass der Webserver so langsam reagiert, weil ein Computer im Internet eine große Anzahl von falsch formatierten Web-Anfragen an den Webserver von ACME sendet.
	Georg musste ein Video für einen Kollegen freigeben. Aufgrund der Größe der Videodatei beschloss er, auf seiner Workstation einen einfachen FTP-Server auszuführen, um die Videodatei seinem Kollegen bereitzustellen. Um das Ganze zu vereinfachen, erstellte George ein Konto mit dem einfachen Kennwort „Datei“ und gab dieses am Freitag an seinen Kollegen weiter. Ohne die entsprechenden Sicherheitsmaßnahmen oder ein sicheres Kennwort waren die IT-Mitarbeiter nicht überrascht, am Montag zu erfahren, dass Georgs Workstation kompromittiert worden war und versuchte, Arbeitsdokumente in das Internet hochzuladen.

Lösung:

Aktivität – Angriffstypen

Anleitung

Bestimmen Sie die Typen der beschriebenen Sicherheitsangriffe. Ziehen Sie alle Sicherheitsangriffe auf das entsprechende Szenario.

Wurm

Zugriff

Virus

Trojaner

Reconnaissance-Angriff

Angriffstyp	Sicherheitsangriffsszenario
<div style="color: green; font-weight: bold;">✓</div> <div style="border: 2px solid blue; padding: 2px; display: inline-block;">Denial of Service (DoS)</div>	Angela, eine IT-Mitarbeiterin bei ACME Inc., bemerkt, dass die Kommunikation mit dem Webserver der Firma sehr langsam ist. Sie überprüft dies und stellt fest, dass der Webserver so langsam reagiert, weil ein Computer im Internet eine große Anzahl von falsch formatierten Web-Anfragen an den Webserver von ACME sendet.
<div style="color: green; font-weight: bold;">✓</div> <div style="border: 2px solid blue; padding: 2px; display: inline-block;">Zugriff</div>	Georg musste ein Video für einen Kollegen freigeben. Aufgrund der Größe der Videodatei beschloss er, auf seiner Workstation einen einfachen FTP-Server auszuführen, um die Videodatei seinem Kollegen bereitzustellen. Um das Ganze zu vereinfachen, erstellte George ein Konto mit dem einfachen Kennwort „Datei“ und gab dieses am Freitag an seinen Kollegen weiter. Ohne die entsprechenden Sicherheitsmaßnahmen oder ein sicheres Kennwort waren die IT-Mitarbeiter nicht überrascht, am Montag zu erfahren, dass Georgs Workstation kompromittiert worden war und versuchte, Arbeitsdokumente in das Internet hochzuladen.

Kapitel 11.2.2.6 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

Übung – Recherchieren von Sicherheitsbedrohungen für Netzwerke (s. Online-Curriculum!).



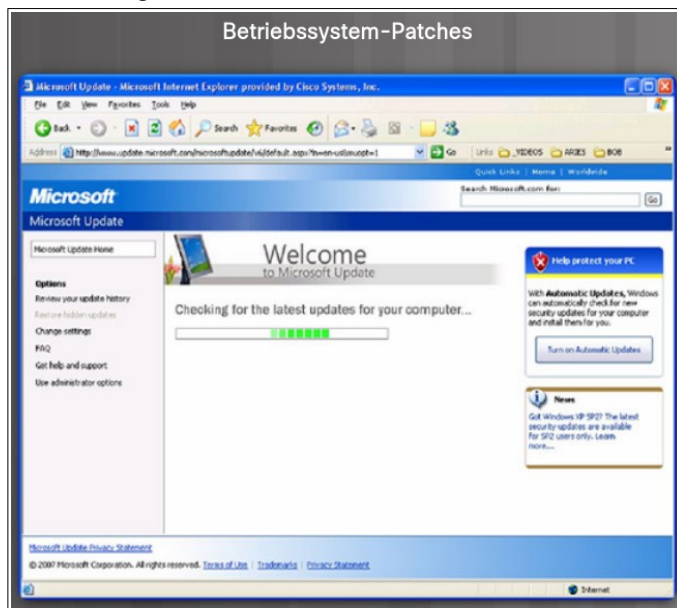
Kapitel 11.2.3 Abwehr von Netzwerkangriffen

Kapitel 11.2.3.1 Backup, Upgrade, Update und Patch

Wenn Sie über aktuelle Entwicklungen auf dem Laufenden sind, können Sie sich effektiver gegen Netzwerkangriffe verteidigen. 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. Das Verwalten zahlreicher Systeme erfordert das Erstellen eines Standard-Software-Abbilds (Betriebssystem und Anwendungen, die für den Einsatz auf Client-Systemen zugelassen sind), das auf neuen oder aktualisierten Systemen bereitgestellt wird. Sicherheitsanforderungen können sich jedoch ändern, und auf bereits bereitgestellten Systemen müssen möglicherweise aktualisierte Sicherheits-Patches installiert werden.

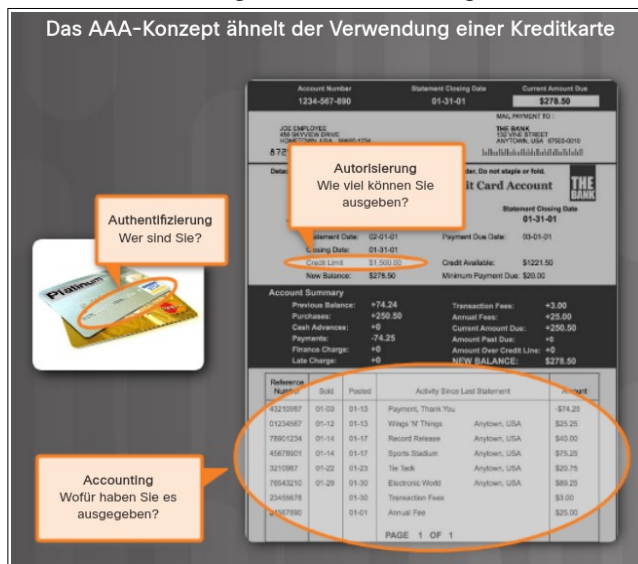
Eine Lösung für die Verwaltung kritischer Sicherheits-Patches ist das Einrichten eines zentralen Patch-Servers, mit dem alle Systeme nach einem festgelegten Zeitraum kommunizieren müssen, wie in der Abbildung gezeigt. Alle Patches, die noch nicht auf einen Host angewendet wurden, werden automatisch vom Patch-Server heruntergeladen und ohne Benutzereingriff installiert.



Kapitel 11.2.3.2 Authentifizierung, Autorisierung und Accounting (Nutzungsverfolgung per "AAA")

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

Das AAA-Konzept ähnelt der Verwendung einer Kreditkarte. Die Kreditkarte identifiziert, wer sie benutzen darf, wie viel der Benutzer ausgeben darf und verfolgt, wofür der Benutzer sein Geld ausgibt, wie nachfolgendes Bild zeigt.




Kapitel 11.2.3.3 Firewalls


Eine Firewall ist eines der wirksamsten verfügbaren Sicherheits-Tools, um Benutzer vor externen Bedrohungen zu schützen. Netzwerk-Firewalls befinden sich zwischen zwei oder mehr Netzwerken, kontrollieren den Datenverkehr zwischen diesen und verhindern nicht autorisierte Zugriffe. Host-basierte Firewalls oder persönliche Firewalls werden auf Endsystemen installiert. Firewalls verwenden unterschiedliche Techniken, um zu bestimmen, was einen zulässigen und was einen unberechtigten Zugriff auf ein Netzwerk darstellt. Diese Techniken sind wie folgt:

- **Paketfilterung** – Verhindert oder gestattet den Zugriff auf Hosts auf der Basis von IP- oder MAC-Adressen.
- **Anwendungsfilterung** – Verhindert oder gestattet den Zugriff auf bestimmte Anwendungstypen auf der Basis von Port-Nummern.
- **URL-Filterung** – Verhindert oder gestattet den Zugriff auf Websites auf der Basis von spezifischen URLs oder Schlüsselwörtern.
- **Stateful Packet Inspection** (Abk. SPI) – Eingehende Pakete müssen zulässige Antworten auf Anfragen interner Hosts sein. Unerwünschte Pakete werden blockiert, wenn sie nicht explizit zugelassen werden. SPI kann darüber hinaus die Funktion beinhalten, spezielle Angriffsformen wie Denial of Service (DoS) zu erkennen und herauszufiltern.


Firewalls können eine oder mehrere dieser oben genannten Filterfunktionen unterstützen. Firewall-Produkte werden in Form unterschiedlicher Pakete angeboten, wie die nachfolgende Abbildung zeigt. Klicken Sie auf die einzelnen Pakete, um weitere Informationen anzuzeigen.




Cisco Security-Appliances



Serverbasierte Firewall



Cisco WRP500 Wireless-Breitband-Router



Persönliche Firewall

Cisco Security-Appliances

Dedizierte Firewall-Geräte sind spezielle Computer ohne Peripheriegeräte oder Festplatten. Appliance-basierte Firewalls können den Datenverkehr schneller untersuchen und sind weniger fehleranfällig.

Serverbasierte Firewall

Firewall-Anwendung mit einer Kombination aus SPI-Firewall und Zugriffskontrolle auf Basis von IP-Adressen oder Anwendungen. Serverbasierte Firewalls können aufgrund der Schwachstellen gängiger Betriebssysteme weniger sicher als dedizierte Appliance-basierte Firewalls sein.

Cisco WRP500 Wireless-Breitband-Router

Die meisten Home-Router verfügen über integrierte grundlegende Firewall-Funktionen, die eine Paket-, Anwendungs- und Website-Filterung unterstützen. Hochwertigere Router, auf denen spezielle Betriebssysteme wie das Cisco Internetwork Operating System (IOS) ausgeführt werden, haben zudem Firewall-Funktionen, die konfiguriert werden können.

Persönliche Firewall

Clientseitige Firewalls, normalerweise eine SPI-Filterung nutzend. Der Benutzer kann aufgefordert werden, bestimmten Anwendungen das Herstellen einer Verbindung zu gestatten, oder er kann eine Liste mit automatischen Ausnahmen erstellen. Persönliche Firewalls werden häufig genutzt, wenn ein Host-Gerät direkt mit einem ISP-Modem verbunden ist. Die Firewall kann den Zugriff auf das Internet behindern, wenn sie nicht richtig konfiguriert wurde. Es wird davon abgeraten, jeweils mehr als eine persönliche Firewall zu nutzen, da dies zu Konflikten zwischen Firewalls führen könnte.

The figure shows four pictures of different firewall devices. These devices are Cisco security appliance, server based firewall, wireless router with integrated firewall, and personal firewall built into the operating system. When you click each image a description appears below.

Kapitel 11.2.3.4 Endgeräte-Sicherheit

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



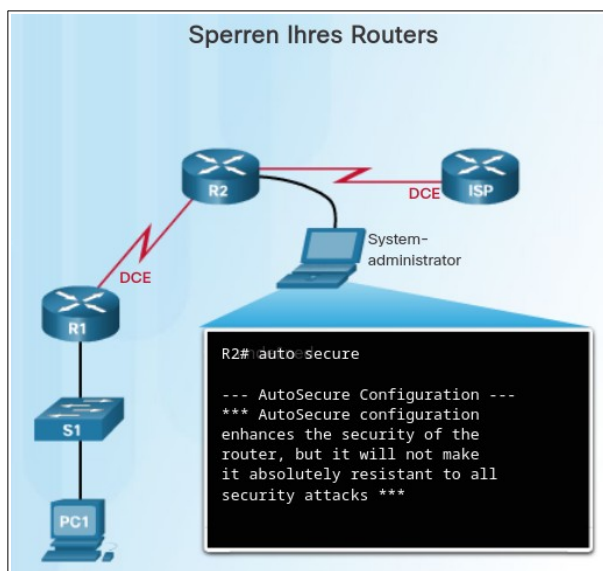
Kapitel 11.2.4 Gerätesicherheit

Kapitel 11.2.4.1 Gerätesicherheit im Überblick

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, wie in der Abbildung gezeigt. 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.



Kapitel 11.2.4.2 Kennwörter

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

- Verwenden Sie eine Kennwortlänge von mindestens acht Zeichen, besser noch zehn Zeichen oder mehr. Ein längeres Kennwort ist ein besseres Kennwort.
- 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 geschriebene 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.

Die Abbildung unten zeigt Beispiele für sichere und unsichere Kennwörter.

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 einzelnes Kennwort. Sie ist außerdem länger und schwerer zu erraten.

Unsichere und sichere Kennwörter	
Unsicheres Kennwort	Warum es unsicher ist
Geheim	Einfaches Wort aus dem Wörterbuch
schmitt	Mädchenname der Mutter
toyota	Automarke
bob1967	Name und Geburtsjahr eines Benutzers
Blueleaf23	Einfache Wörter und Zahlen
Sicheres Kennwort	Warum es sicher ist
b67n42d39c	Kombiniert alphanumerische Zeichen
12^h u4@1p7	Kombiniert alphanumerische Zeichen, Symbole und beinhaltet außerdem ein Leerzeichen

Figure shows two tables; one table contains weak passwords and the reasons why they are weak. Reasons include it is a simple dictionary word, a mother's maiden name, a make of car, or other simple words. The other table contains strong passwords that are made from a combination of letters numbers and symbols. They appear random.

Kapitel 11.2.4.3 Grundlegende Sicherheitspraktiken

Zusätzliche Kennwortsicherheit

Sichere Kennwörter sind nur nützlich, wenn sie geheim sind. Es gibt mehrere Schritte, mit denen Sie sicherstellen können, dass Kennwörter geheim (verschlüsselt) bleiben. Mithilfe des globalen Konfigurationsbefehls **service password-encryption** kann verhindert werden, dass nicht autorisierte Einzelpersonen unverschlüsselte Kennwörter in der Konfigurationsdatei anzeigen können, wie das Bild unten zeigt. Dieser Befehl verschlüsselt alle bisher nicht verschlüsselten Kennwörter.

Um sicherzustellen, dass alle konfigurierten Kennwörter eine festgelegte Mindestlänge haben, verwenden Sie zusätzlich den Befehl **security passwords min-length** im globalen Konfigurationsmodus.

Eine weitere Möglichkeit für Hacker, Kennwörter herauszufinden, sind Brute-Force-Angriffe, wobei viele Kennwörter ausprobiert werden, bis eines funktioniert. Diese Art von Angriffen kann verhindert werden, wenn die Anmeldeversuche für ein Gerät blockiert werden, sobald eine bestimmte Anzahl von Fehlversuchen innerhalb eines gewissen Zeitraums auftritt.

Router(config)# login block-for 120 attempts 3 within 60

Dieser Befehl blockiert Anmeldeversuche 120 Sekunden lang, wenn innerhalb von 60 Sekunden 3 Anmeldeversuche fehlschlagen.

Exec Timeout (Ausführungszeitüberschreitung)

Eine weitere Empfehlung besteht darin, Ausführungszeitüberschreitungen festzulegen. Durch Festlegen einer Zeitüberschreitung wird das Cisco Gerät angewiesen, Benutzer auf einer Leitung automatisch zu trennen, wenn diese für die Dauer des eingestellten Werts nicht aktiv waren. Ausführungszeitüberschreitungen können im Leitungskonfigurationsmodus auf Konsolen-, VTY- und AUX-Ports mit dem Befehl **exec-timeout** konfiguriert werden.

Router(config)# line vty 0 4

Router(config-line)# exec-timeout 10

Dieser Befehl konfiguriert das Gerät so, dass Benutzer nach zehn Minuten Inaktivität getrennt werden.

```

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)# exec-timeout 10
Router(config-line)# end
Router# show running-config
- more -
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login

```


The figure shows router output for configuring encrypted line passwords and setting restrictions on password length or failed attempts. Commands entered include “security password-encryption”, “security password min-length 8”, login block-for 120 attempts 3 within 60”, and “exec-timeout 10” on the VTY lines.

Kapitel 11.2.4.4 Aktivieren von SSH

Telnet ist kein sicheres Protokoll. Daten in einem Telnet-Paket werden unverschlüsselt übertragen. Um einen sicheren Remote-Zugriff zu gewährleisten, sollte daher auf Geräten unbedingt SSH aktiviert werden. Die Unterstützung von SSH auf einem Cisco Gerät kann, wie im Bild unten gezeigt, in 4 Schritten konfiguriert werden.

- **Schritt 1:** Stellen Sie sicher, dass der Router einen eindeutigen Hostnamen aufweist und konfigurieren Sie anschließend im globalen Konfigurationsmodus den IP-Domännennamen des Netzwerks mit dem Befehl **ip domain-name**.
- **Schritt 2:** Für Router müssen Einweg-Geheimschlüssel generiert werden, um SSH-Datenverkehr zu verschlüsseln. Um den SSH-Schlüssel zu generieren, verwenden Sie im globalen Konfigurationsmodus den Befehl **crypto key generate rsa general-keys**. Die genaue Bedeutung der verschiedenen Teile dieses Befehls ist sehr komplex und geht über den Rahmen dieses Kurses hinaus. Beachten Sie lediglich, dass der Modul die Größe des Schlüssels bestimmt und als ein Wert zwischen 360 Bit und 2.048 Bit konfiguriert werden kann. Je größer der Modul, umso sicherer ist der Schlüssel, aber umso länger dauert das Verschlüsseln und Entschlüsseln von Informationen. Die empfohlene Mindestlänge ist 1.024 Bit.
- **Schritt 3:** Erstellen Sie mit dem globalen Konfigurationsbefehl **username** einen Benutzernameneintrag in der lokalen Datenbank.
- **Schritt 4:** Aktivieren Sie eingehende SSH-Sitzungen mit den „line vty“-Befehlen **login local** und **transport input ssh**.

Der Remote-Zugriff auf den Router ist jetzt nur noch mit SSH möglich.



```

R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit

```

Schritt 1: Konfigurieren des IP-Domännennamens
 Schritt 2: Generieren von unidirektionalen Geheimschlüsseln
 Schritt 3: Überprüfen oder Erstellen eines lokalen Datenbankeintrags
 Schritt 4: Aktivieren eingehender VTY-SSH-Sitzungen

Figure shows the commands to configure SSH. The steps are listed in a text box.

Kapitel 11.2.4.5 Packet Tracer – Konfigurieren von sicheren Kennwörtern und SSH

Der Netzwerkadministrator bittet Sie, einen Router für den Einsatz vorzubereiten. Bevor das Gerät mit dem Netzwerk verbunden werden kann, müssen Sicherheitsmaßnahmen aktiviert werden.

- * Packet Tracer – Konfigurieren von sicheren Kennwörtern und SSH – Anleitung.
- * Packet Tracer – Konfigurieren von sicheren Kennwörtern und SSH – PKA.

(s. Online-Curriculum).



Kapitel 11.2.4.6 Übung – Zugreifen auf Netzwerkgeräte mit SSH

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- * Teil 1: Konfigurieren von Gerätegrundeinstellungen.
- * Teil 2: Konfigurieren des Routers für den SSH-Zugriff.

Übung – Zugreifen auf Netzwerkgeräte mit SSH (s. Online-Curriculum).



Kapitel 11.2.4.7 Übung – Untersuchen von Telnet und SSH in Wireshark

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- * Teil 1: Untersuchen einer Telnet-Sitzung mit Wireshark.
- * Teil 2: Untersuchen einer SSH-Sitzung mit Wireshark.

Übung – Untersuchen von Telnet und SSH in Wireshark (s. Online-Curriculum).



Kapitel 11.2.4.8 Übung – Sichern von Netzwerkgeräten

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- * Teil 1: Konfigurieren von Gerätegrundeinstellungen.
- * Teil 2: Konfigurieren von grundlegenden Sicherheitsmaßnahmen auf dem Router.
- * Teil 3: Konfigurieren von grundlegenden Sicherheitsmaßnahmen auf dem Switch.

Übung – Sichern von Netzwerkgeräten (s. Online-Curriculum).

