Beispiele für typische Attacken aus dem Internet

Inhaltsangabe:

1. ***Malware – "Was ist das?"***
2. ***DoS vs. DDoS***
3. ***Formen der DDoS-Attacken***
4. ***Motive für DDoS-Attacken***
5. ***Maßnahmen gegen DDoS-Attacken***
6. ***DDoS & Botnets***
7. ***Weitere typische Attacken aus dem Internet***
   - ***"Brute-Force"-Angriffe***
   - ***"Spoofing"-Angriffe***
   - ***"SYN-Flooding"***
   - ***"Man-in-the-Middle-Attacken"***
   - ***"Phishing"***
   - ***"Botnets"***
   - ***"Ransomware" (Verschlüsselte Trojaner bzw. Erpressungssoftware)***

Beispiele für typische Attacken aus dem Internet

1. Malware – "Was ist das?"

- ***Arten von Bedrohungen: (s.)***
  - – Informationsdiebstahl,
  - – Datenverlust/-manipulation,
  - – Identitätsdiebstahl,
  - – Dienstunterbrechung.
- ***Arten von Schwachstellen, die durch … :***

  * … Unternehmensrichtlinien und -maßnahmen abgedeckt bzw. berücksichtigt sein sollten:
    - – HW-Bedrohung (z.B. HDD-Defekt oder HDD-Ausfall → RAID …),
    - – Elektrische Bedrohung (z.B. Energienetz-Ausfall → USV …),
    - – Bedrohungen durch unsachgemäße Wartung (z.B. Server-Ausfall → Server-Cluster …).

  * … ein gewisses Maß an Anfälligkeit in jedem Netzwerk und IT-Gerät zu verzeichnen sind:
    - – Technologische Schwachstellen (z.B. in TCP/IP, OS, IT-Geräten),
    - – Konfigurationsschwachstellen (z.B. unsicher User Accounts etc.),
    - – Schwachstellen bei Sicherheitsrichtlinien (z.B. in Firmenpolitik, SW-/HW-Installation).
- ***Arten von Angriffen bzw. Attacken:***

  * *N*etzwerk- oder IT-Geräte-bedingten Schwachstellen im laufenden Betrieb können unterschiedlichen Angriffen
    - – durch Schadcode bzw. -software (Malware) und
    - – Netzwerkangriffe ausgesetzt sein!

  * Typische Arten von "Malware" (Schadcode bzw. Schadsoftware):
    - – "Viren": führt eine bestimmte unerwünschte und häufig schädliche Funktion auf einem Computer aus!
    - – "Würmer": führt willkürlichen Code aus und installiert weitere Kopien von sich selbst im betr. Computer-Speicher, mit dem Ziel, sich automatisch zu replizieren und zu verbreiten!
    - – "Trojaner": repliziert sich i.d.R. nicht selbst, gibt häufig vor, legitime SW zu sein, greift zumeist dann an, wenn weitere Malware heruntergeladen und geöffnet wird!

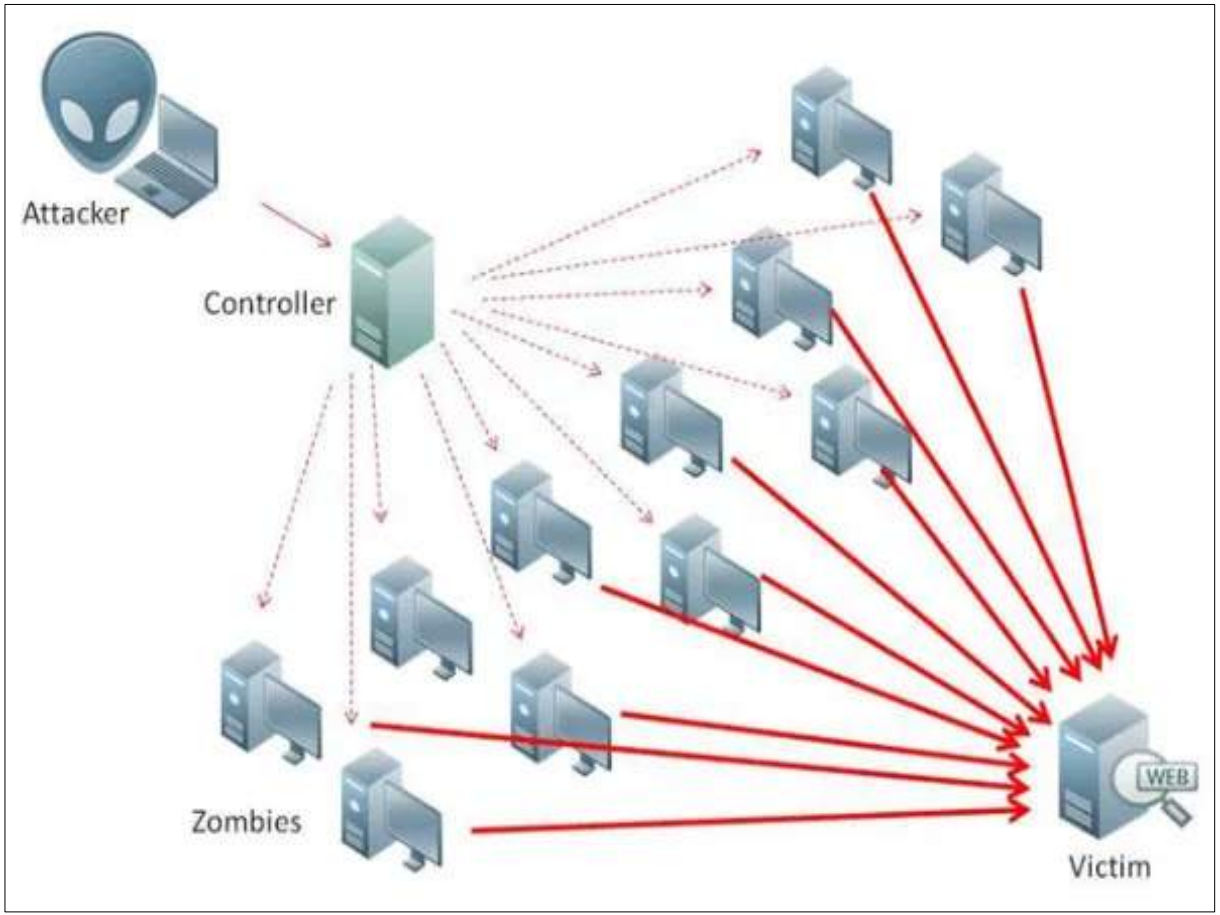
  * Typische Arten von "Angriffen" im Netzwerk:
    - – "Reconnaissance-Angriffe": Erkennen und Zuordnen von Systemen, Diensten oder Schwachstellen!
    - – "Zugriffsangriffe": Unbefugte Daten-Manipulation, unbefugter Zugriff auf Systemen oder auf Benutzerrechten!
    - – "Denial of Service" (DoS): Deaktivierung oder Beschädigung von Netzwerken, Systemen oder Diensten!

Beispiele für typische Attacken aus dem Internet

2. *DoS vs. DDoS*

(Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- Was ist ***DDoS*** (Distributed Denial of Service)?
  DDoS lässt andere Systeme die "Drecksarbeit" für sich machen bzw. arbeiten. Der Attacker als Verursacher des "Schlamassels" bzw. als "Master of Desaster" bleibt zumeist dabei unerkannt und kann zumeist nicht einmal dafür belangt werden!
- ***DoS vs. DDoS*** – Wo liegt der Unterschied?
  Wer sich umfangreich mit dem Thema beschäftigt, wird in den meisten Fällen bei der Recherche zu DDoS-Angriffen auch auf DoS-Angriffe stoßen. Der Unterschied ist hier folgender: Während der einfache DoS-Angriff i.d.R. von einem einzelnen Angreifer direkt selbst ausgeführt wird und konkret auf bestimmte Schwachstellen in der Software oder Infrastruktur zielt, handelt es sich bei DDoS-Angriffen um eine regelrechte Massenattacke. Das bedeutet auch, dass die Vorkehrungen gegen einen einfachen DoS-Angriff i.d.R. sehr viel einfacher zu handhaben sind. Wird man aber Opfer einer DDoS-Attacke, ist es i.d.R. recht schwer, passende Maßnahmen innerhalb kürzester Zeit hier gegen zu ergreifen.



Beispiele für typische Attacken aus dem Internet

3. Formen der DDoS-Attacken

(Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- Welche ***Formen der DDoS-Angriffe*** auf die Server sind typisch?
  Die Angreifer bedienen sich bei einem DDoS-Angriff verschiedener Methoden und zielen dabei nicht immer auf Schwachstellen oder Lücken im Code einer Webseite. In den meisten Fällen ist es recht einfach möglich, durch eine konzentrierte Attacke gegen bestimmte Dienste, den gewünschten Erfolg zu erreichen. In der Regel wird zwischen den folgenden drei Formen der Attacke unterschieden, wobei es wichtig ist festzustellen, dass es in den letzten Jahren noch gesonderte Arten gibt. Diese würden allerdings zu weit greifen und kommen zumindest in den meisten Wellen nicht vor. Nachfolgend drei typische Formen von DDoS-Attacken:

  Netzwerkangriffe: Bei einem einfachen Angriff auf das Netzwerk machen sich die Angreifer die Infrastruktur der meisten Server und Router zu nutze. Mit der Hilfe von fingierten und manipulierten Netzwerk-Anfragen wird binnen kürzester Zeit eine solche Belastung erreicht, dass die meisten Geräte abschalten. Eine Webseite wäre in diesem Fall nicht mehr oder nur noch sehr langsam erreichbar. Durch die Angriffsdauer schalten sich höchstwahrscheinlich einzelne Dienste aus Sicherheit zudem ab.

  HTTP-Flooding: Für normale Server erscheint das HTTP-Flooding im ersten Moment so, als hätten sich Millionen Benutzer binnen weniger Sekunden entschieden, die Webseite zu besuchen. Auf einmal überschwemmen so Millionen Anfragen den Server, die auf den ersten Blick wie normale Besuche erscheinen. Durch die Menge an Zugriffen und den Umstand inzwischen realisierter, lernfähiger Algorithmen für Attacken, erfolgt i.d.R. irgendwann eine Server-Abschaltung und die Webseite ist damit nicht mehr erreichbar.

  DNS-Angriffe: DNS-Server sind beliebte Angriffsziele, weil ein erfolgreicher Angriff binnen kürzester Zeit dazu führt, dass keine Server-Dienste mehr erreichbar sind. Zu diesem Zweck werden auch manipulierte Daten oder eine pure Masse an Anfragen genutzt, deren Beantwortung den DNS-Server überfordern.

  Der Effekt der verschiedenen DDoS-Angriffe ist i.d.R. immer gleich: Irgendwann versagen entweder Hard- oder Software und es kommt zu einem Erliegen der Webseite, des Servers oder des gesamten Netzwerkes. Je nach betroffenen Unternehmen oder Institutionen kann dies zu kritischen Situationen führen. Verschiedene Maßnahmen reduzieren zwar Auswirkungen und Risiko, lassen es aber nicht zu, dass eine solche Situation gänzlich verhindert wird.

Beispiele für typische Attacken aus dem Internet

4. Motive für DDoS-Attacken

(Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- Was sind die ***Motive für DDoS-Attacken***?
  Um zu verstehen, warum es in den letzten Jahren immer häufiger zu solchen Angriffen kommt, muss man nur einen Blick auf die möglichen Motive von Angreifern werfen. In den ersten Jahren war die DDoS-Attacke meistens eine Form von Vandalismus (oder "Blinder Aktivismus") gegen Webseiten. Das führte dazu, dass z.B. beliebte Browser-Games abgeschaltet worden sind, wenn sie ungeliebte Neuerungen veröffentlicht haben. Auch Zeitungen waren bei der Berichterstattung ein beliebtes Ziel. Zuletzt zeigt sich allerdings, dass die DDoS-Attacke zu einem Werkzeug der Politik und der Kriminalität im Netz geworden ist. Nachfolgend nur einige Beispiele, weswegen es bereits zu solchen DDoS-Attacken gekommen ist:

  - ***Aktivismus:*** Selbsternannte Aktivisten aus den verschiedensten politischen und gesellschaftlichen Strömen haben schon in dieser Form ihren Protest gezeigt. Während die Webseite von PETA bereits betroffen war, haben Tierschützer die Online-Shops von Fleischhändlern lahmgelegt. Meistens sind solche Attacken nicht von Dauer, richten aber dennoch Schaden an.

  - ***Erpressung:*** Immer wieder war in den letzten Jahren davon zu hören, dass mit der Hilfe von DDoS-Angriffen, beispielsweise Online-Shops oder auch Social-Media-Plattformen lahmgelegt worden sind. Die Angreifer forderten eine Summe, damit die Webseiten für den Kunden wieder erreichbar waren und nicht noch höhere Umsatz- und Imageverluste entstehen konnten.

  - ***Cyberkrieg:*** Ein sehr neues Phänomen ist die gezielte Ausschaltung von staatlichen Webseiten und Infrastrukturen im Netz. Besonders Russland und Nordkorea werden immer wieder solcher Attacken verdächtigt, wobei gesichert ist, dass auch westliche Geheimdienste sich solcher Attacken bereits bedient haben.

  - ***Vandalismus:*** Darüber hinaus gibt es noch die Beispiele des einfachen Vandalismus, in denen vorgefertigte Programme genutzt werden, um einer anderen Person zu schaden. Erst durch eine strengere Gesetzgebung sind diese Fälle seltener geworden, wobei an diesem Punkt die Cyberkriminalität dafür zugenommen hat.

Beispiele für typische Attacken aus dem Internet

5. Maßnahmen gegen DDoS-Attacken

(Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- Was sind erfolgreiche Maßnahmen gegen DDoS-Attacken?
  Generell lässt sich sagen, dass es keine „einfachen“ Schutzmethoden gegen solche Angriffe gibt. Da es sich dabei um tatsächliche organisierte Kriminalität im Netz handelt, die häufig mit entsprechenden Absichten dahinter verbunden ist, verfügen die meisten Angreifer über entsprechende Professionalität um normale Systeme auszuhebeln.

  Die meisten Maßnahmen lassen sich durch einen guten Dienstleister für das Server-Housing bzw. -Hosting erreichen. Diese Anbieter verfügen über technische und Software-basierte Lösungen für den Schutz. Dazu zählt zum Beispiel eine gute Filterung von Anfragen auf die Server und ein gutes Routing mit entsprechend verbauter Verteilung der Last. Dies ist auch durch Cluster und Virtualisierung möglich.

  Für einfache Besitzer von einem Server beginnt es aber bereits damit, nicht verwendete Dienste zu schließen und auf die Ports am eigenen Server zu achten. Der beste Schutz gegen einen Angriff ist, möglichst wenig Angriffsfläche für DDoS zu bieten. Alle Maßnahmen darüber hinaus sollten mit der Hilfe von guter Hardware und der passenden Beratung durch IT-Experten individuell für das eigene System besprochen werden.

- ***4-Punkte-Plan für einen guten Schutz des IT-Systems, z.B. Viren etc.!***

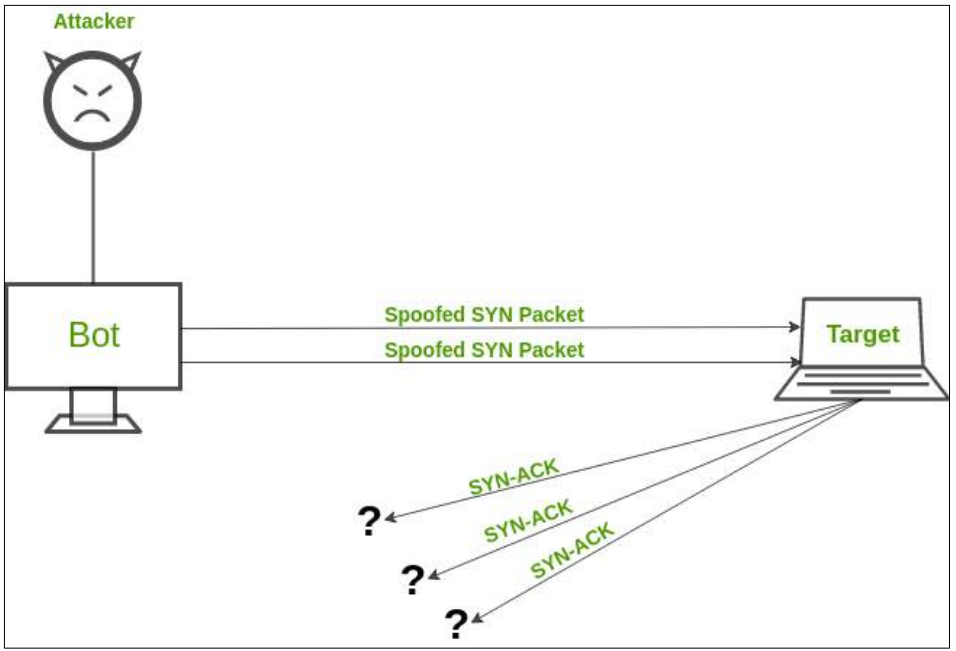
1. Halten Sie Ihre Software und Ihr Betriebssystem auf den aktuellsten Stand.
   Installieren Sie zeitnah neue Service Packs und Sicherheitsupdates.
2. Seien Sie aufmerksam beim Umgang mit E-Mails.
   Öffnen Sie keine unbekannten Datei-Anhänge
   und nehmen Sie sich in Acht vor Phishing-Mails.
3. Verwenden Sie ein aktuelles Antivirenprogramm
   und halten die Virendefinition stets aktuell.
4. Verwenden Sie eine Firewall, die den Netzwerkverkehr überwacht.

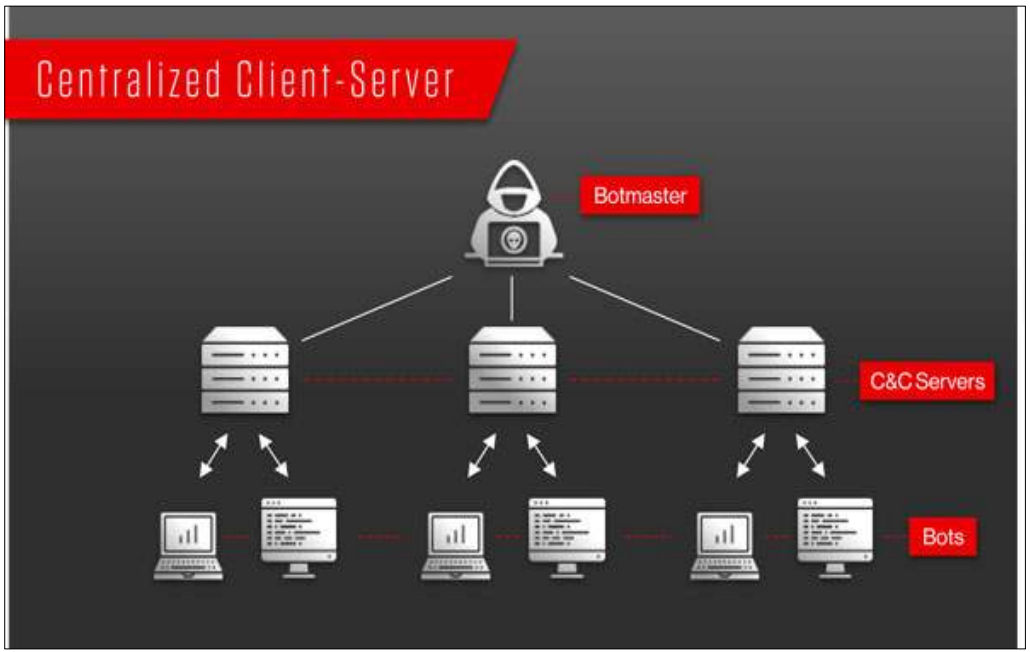
Beispiele für typische Attacken aus dem Internet

6. *DDoS & Botnets*

(Quelle: ***https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-botnet***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- DDoS-Attacken gehören heute zu den häufigsten Cyberattacken. ***Ziel der DDoS-Attacken*** sind vor allem Unternehmen aus der Industrie oder dem Finanzwesen oder politische oder öffentliche Institutionen. Das Unternehmen soll durch den Angriff unter Druck gesetzt werden. DDoS-Attacken können aber auch einfach nurAusdruck von Protest sein. Mittlerweile werden sie aber auch in der Cyberspionage eingesetzt.
- ***Botnets*** wirken wie ein gigantisches Spinnennetz und durchziehen mittlerweile das gesamte Internet. Sie verbinden Computer zu riesigen Netzwerken, ohne dass die meisten von ihnen etwas davon ahnen. (Cyber-)Kriminelle manipulieren Rechner, schließen sie zusammen und nutzen sie für ihre Zwecke. So entsteht ein Netz von infizierten PCs, die von den sogenannten Botmastern ferngesteuert werden. Botnetze gehören zu den größten illegalen Geldquellen der Cyberkriminellen. Schätzungen zufolge sind weltweit Rechner im dreistelligen Millionenbereich betroffen. Eines der größten bereits entdeckten Netze umfasste über 30 Millionen Computer. Vielleicht wurden auch wir selbst längst in ein solches Netz verstrickt.





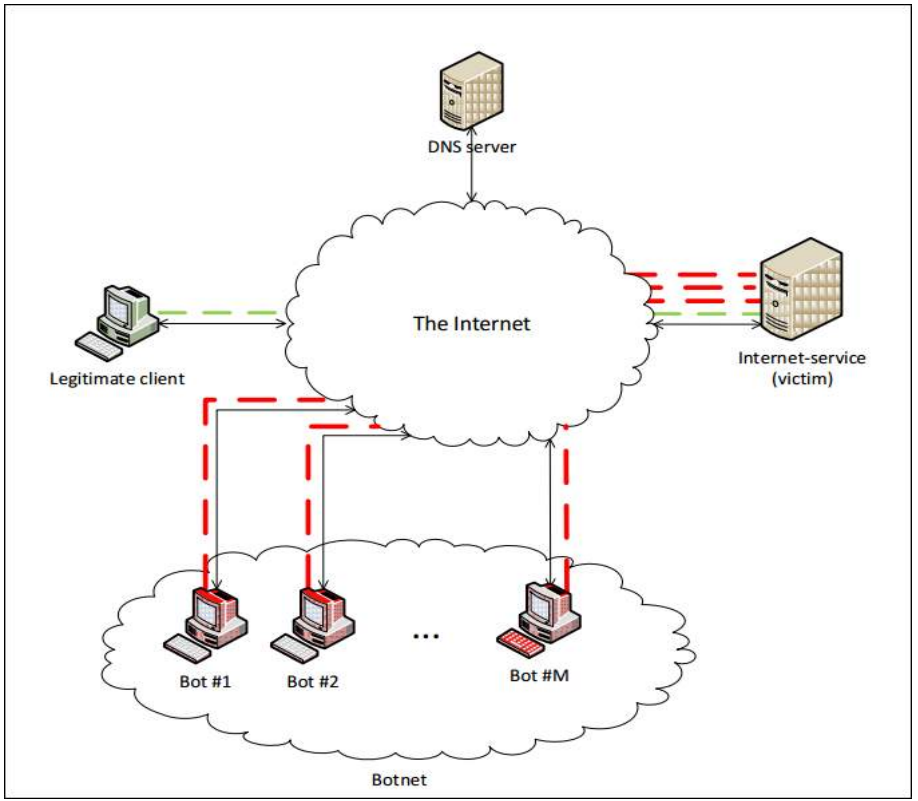
Beispiele für typische Attacken aus dem Internet

6. *DDoS & Botnets*

(Quelle: ***https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-botnet***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- Was genau ist ein ***DDoS-Angriff***?
  Der DDoS-Angriff ist eine gezielte und dezentral gesteuerte Attacke auf die Infrastruktur und die Netzwerke von Unternehmen, Webseiten und staatlichen Organisationen. Dabei zielen die Angreifer darauf ab, dass die Benutzung bestimmter Webseiten oder Dienste durch die pure Masse an Anfragen und Angriffen nicht mehr möglich ist.

  Man kann es sich so vorstellen: Ein Server bietet für Besucher einen Schalter, durch den die Anfragen bearbeitet werden. In der Regel ist der Schalter groß genug um hunderte oder vielleicht auch tausende und mehr Anfragen in der Minute zu verarbeiten. Bei einem DDoS-Angriff werden aber binnen weniger Sekunden, bis zu einer Millionen verschiedene Anfragen auf den bestimmten Server bzw. den Schalter gesteuert. Der Server kann die große Menge an Anfragen irgendwann nicht mehr abarbeiten und stellt seinen Dienst ein.



- In welchen Zusammenhang stehen ***Botnets und DDoS*** zueinander?
  Bei einem DDoS-Angriff, bedient sich der Angreifer in den meisten Fällen sogenannter "Botnetze". Dabei handelt es sich um fremde Rechner, die mit "Malware" infiziert sind und nicht einmal bemerken, dass sie für einen solchen Angriff genutzt werden. Entsprechende Netzwerke können inzwischen relativ einfach im Internet angemietet werden.

  Die Angreifer nutzen bei solchen Angriffen entweder verschiedene Sicherheitslücken auf dem Server aus oder – was klassisch für einen DDoS-Angriff ist – sie bringen die Netze zur Überlastung. Einer Belastung von mehreren tausend Anfragen pro Sekunde können nur die wenigsten Netzwerke standhalten. Die Hardware ist überfordert, das Netzwerk bricht zusammen und der Dienst oder die Webseite sind damit nicht mehr erreichbar. Das kann zu erheblichen Problemen bei der Kommunikation führen oder, im Fall von Unternehmen, zu Einbußen bei den Umsätzen.

  Die Betreiber eines Botnets schleusen Schadsoftware (Malware), sogenannte "Bots" (Kurzform: eng. „Robot“) auf fremde Computer ein. Diese Bots agieren von da an unauffällig bzw. resident im Hintergrund, ohne dass die PC-Besitzer etwas davon bemerken. So wird der Rechner für die Zwecke der Botmaster genutzt, die der User nicht bemerkt und sicherlich auch nicht unterstützen würde. Da die Computer ferngesteuert und damit wie willenlos handeln, werden die Teile des Botnetzes auch als Zombie-PCs bezeichnet.

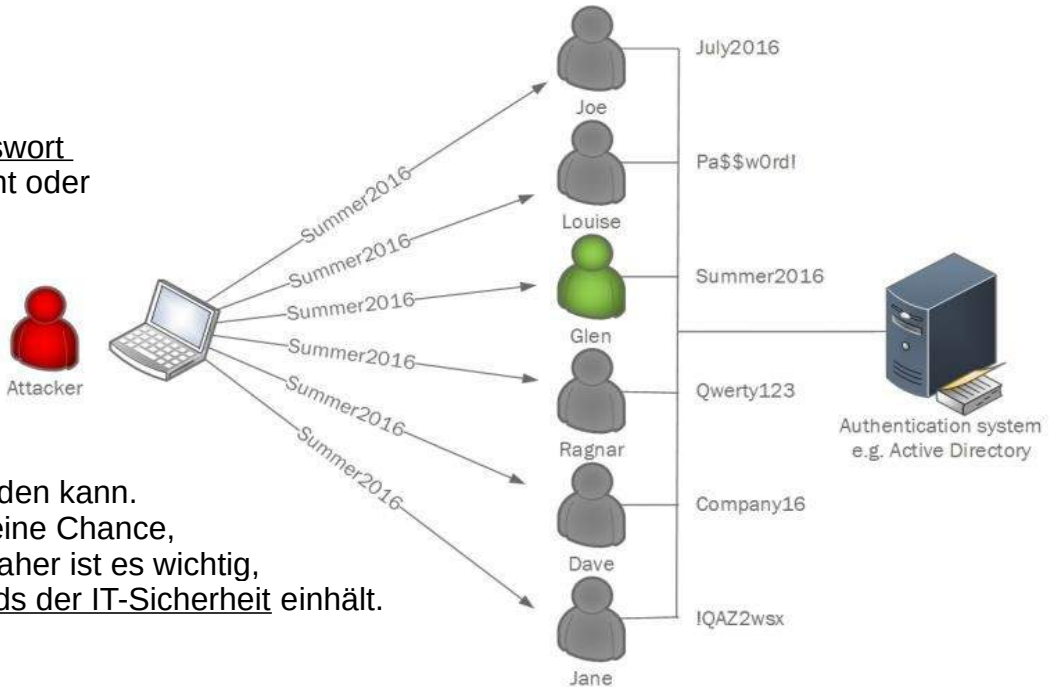
Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet (Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- ***Brute Force Attacken*** (BF-Attacken) – Begriffserklärung, Funktionsweise und Schutzmaßnahmen:

  Hacker und Kriminelle im Internet haben inzwischen ein umfangreiches Portfolio an Maßnahmen und Werkzeugen, mit denen sie versuchen, an Daten von Nutzern zu kommen oder Schaden anzurichten. Sie hören Datenleitungen ab, versuchen mittels Trojaner an Passworte zu kommen oder infizieren gleich ganze Server. Neben diesen ausgeklügelten Methoden gibt es aber auch die sogenannte BF-Attacke. Dabei handelt es sich um die Brecheisen-Methode unter den Hacks und dient in der Regel dazu, das Passwort eines Accounts herauszufinden.

  Was genau ist eine BF-Attacke ?
  Die BF-Attacke hat zum Ziel, mithilfe einfacher Gewalt an das Passwort eines Nutzers zu kommen und sich entweder Zugriff auf ein Account oder einen Server zu verschaffen. Dabei handelt es sich nicht um physische Gewalt, sondern um ein hartnäckiges Ausprobieren verschiedener Passwort-Kombinationen. Mithilfe von Programmen oder der einfachen Eingabe in Login-Masken wird versucht, die Kombination aus "Username" und "Password" entsprechend herauszufinden.

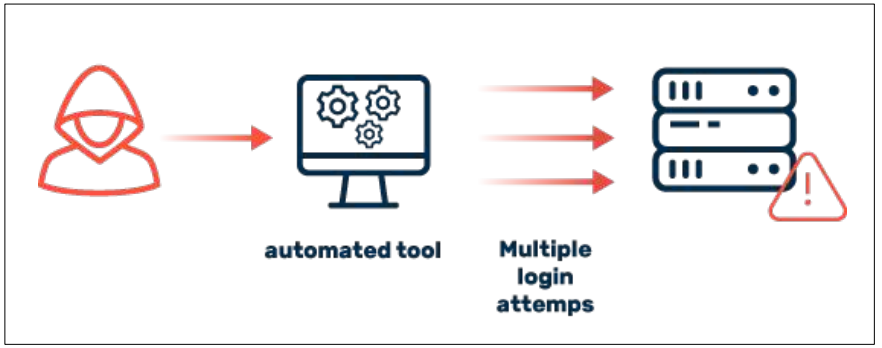
  Die Gefahr besteht darin, dass der Angreifer im Fall einer BF-Attacke am Ende tatsächlich die richtige Kombination herausfinden kann. Dadurch, dass er viele Kombinationen ausprobieren kann, gibt es eine Chance, dass bei einem unsicheren Passwort am Ende ein Erfolg gelingt. Daher ist es wichtig, dass man auf die eigenen Daten achtet und verschiedene Standards der IT-Sicherheit einhält.

Beispiele für typische Attacken aus dem Internet

7. *Weitere typische Attacken aus dem Internet*

(Quelle: ***https://www.polyas.de/blog/de/online-wahlen/sicherheit/ddos-attacken***)
(Quelle: ***http://www.was-ist-malware.de/wp-content/uploads/2017/11/ddos-destributed-denial-of-service.png***)

- ***Brute Force Attacken*** (BF-Attacken) – Begriffserklärung, Funktionsweise und Schutzmaßnahmen:



Wie genau funktioniert eine BF-Attacke?
Eine typische BF-Attacke kann in unterschiedlichen Formen ablaufen.
Die einfachste und primitivste Variante ist der simple Versuch alle Daten direkt in einem Loginfeld auszuprobieren. Der Angreifer würde in diesem Fall vor allem Kombinationen ausprobieren, die ihm logisch erscheinen oder die besonders gerne genutzt werden. Ist zum Beispiel das Passwort eines Benutzers bekannt, würde es mit solchen Daten ausprobiert werden. Allerdings ist diese Form nicht sonderlich Erfolg versprechend, da die meisten Portale inzwischen Vorkehrungen gegen solche einfachen BF-Attacken haben.

Viel eher z.B. in professionellen Hacker-Kreisen wird ein SW-Programm genutzt, um dies bei der BF-Attacke einzusetzen. In diesem Fall würde das SW-Programm automatisch verschiedenste Kombinationen nach Listen ausprobieren. In solchem Fall läuft das Programm bei der BF-Attacke nicht nur verschiedenste Kombinationen nach Zufall ab. Es gibt Listen im Internet, in denen die beliebtesten und am häufigsten genutzten Passwörter eingetragen sind. Diese Kombinationen werden probiert. Auf diese Weise können in einer Minute ohne entsprechender Gegenmaßnahme mehrere hunderte Kombinationen ausprobiert werden. Sollte es dem Angreifer per BF-Attacke gelingen, am Ende die nötigen Daten zu erfahren, erhält er einen Zugriff auf einen Server, ein Account oder etwa das Online Banking.

Was sind wirksame Maßnahmen gegen eine BF-Attacke?
Bei Maßnahmen gegen BF-Attacken gibt es zwei Ebenen: User sollten zunächst selbst dafür sorgen, dass ihre Passwörter nicht einfach per BF-Attacke geknackt werden können. Sichere Passworte mit Sonderzeichen, Groß- und Kleinschreibung sowie Zahlen sind in heutiger Zeit Standard, der zum Datenschutz eingehalten werden sollte. Weiterhin müssen Service- und Internetprovider Maßnahmen ergreifen, z.B. technisch verbieten, für ein Account mehr als 5 nicht erfolgreiche Login-Versuche zuzulassen. So können zumindest BF-Angriffe per automatisiertem Programm größtenteils unterbunden werden. Zudem können sie die Nutzer auffordern, Passworte zu nutzen, die eben nicht in solchen Listen vorkommen. Das reduziert die Möglichkeit einer erfolgreichen BF-Attacke drastisch und dürfte die meisten Scripte vor eine kaum zu lösende Herausforderung stellen.

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)
(Quelle: ***https://www.ionos.de/digitalguide/server/knowhow/was-ist-mac-spoofing/***)

- Was ist ein ***Spoofing***-Angriff?

In der Netzwerk-Terminologie bezeichnet "Spoofing" (eng. „Verschleierung“) verschiedene Methoden, die der Manipulation grundlegender Adressierungssysteme in Computernetzen dienen. Hacker nutzen dieses Angriffsmuster, um die eigene Identität zu verbergen oder eine andere zu imitieren. Beliebte Ziele für Spoofing-Attacken sind neben der MAC-Adresse das Internetprotokoll (IP), das Domain-Name-System (DNS) und die Adressauflösung via ARP. Grundsätzlich bzw. normalerweise lässt sich Spoofing als Lösungsstrategie zur Fehlerbehebung einsetzen (Legale Spoofing-Anwendung). Meist steht jedoch die Infiltration fremder Systeme im Rahmen illegaler Netzaktivitäten im Vordergrund, d.h. die heutzutage gängige und sich schnell ausbreitende "Cyberkriminalität"!

"Spoofing" ist der Akt der Verschleierung einer Kommunikation oder einer Identität, damit sie mit einer vertrauten, autorisierten Quelle in Verbindung gesetzt wird. Spoofing-Angriffe treten in unterschiedlicher Form auf, angefangen bei gängigen eMail-Spoofing-Angriffen in Phishing-Kampagnen bis hin zum Spoofing von Rufnummern-Anzeigen, das häufig mit dem Ziel des Betrugs eingesetzt wird. Angreifer nehmen mitunter im Rahmen ihres Spoofing-Angriffs auch die technischen Elemente des Unternehmensnetzwerks in den Fokus, wie die IP-Adresse, DNS oder das Adress Resolution Protocol (ARP).

Spoofing-Angriffe missbrauchen in der Regel Vertrauensbeziehungen, indem sie sich als eine Person oder Organisation ausgeben, die dem Opfer bekannt ist. In einigen Fällen – z. B. Whale-Phishing-Angriffen, zu denen E-Mail- oder Website-Spoofing zählen – werden diese Nachrichten so auf das Opfer personalisiert, dass diese Person von der Legitimiät der Kommunikation überzeugt ist. Wenn der Benutzer nicht weiß, dass die Internetkommunikation gefälscht werden kann, ist es um so wahrscheinlicher, dass er oder sie auf den Spoofing-Angriff eingeht.

Konsequenzen bei erfolgreichem Spoofing-Angriff:
Ein erfolgreicher Spoofing-Angriff kann schwerwiegende Konsequenzen (Folgen) haben. Ein Angreifer kann möglicherweise vertrauliche personenbezogene Daten oder Unternehmensdaten stehlen, Anmeldeinformationen für die Verwendung in zukünftigen Angriffs- oder Betrugsversuchen abrufen, Malware über bösartige Links oder Dateianlagen verbreiten und unerlaubten Netzwerkzugriff erlangen, indem Vertrauensbeziehungen missbraucht oder die Zugriffskontrollen umgangen werden. Möglicherweise startet der Angreifer sogar einen Denial-of-Service-Angriff (DoS) oder einen Man-in-the-Middle-Angriff (MITM).

Was bedeutet das für das jeweilige Geschäft? Sobald es einem Spoofing-Angriff gelungen ist, das Opfer hinters Licht zu führen, könnte das Unternehmen einem Ransomware-Angriff ausgesetzt sein oder einen kostspieligen und geschäftsschädigenden Datenverstoß erleben. Business Email Compromise (BEC), bei dem ein Angreifer sich als firmeneigener Manager ausgibt und den Mitarbeiter auffordert, Geld auf ein Konto zu überweisen, das tatsächlich dem Hacker gehört, ist ein weiterer häufig auftretender Spoofing-Angriff. Auch könnte das Unternehmen feststellen, dass seine Website Malware verbreitet oder vertrauliche Daten stiehlt. Letztlich könnte das Unternehmen sich gerichtlich verantworten müssen, seine Reputation einbüßen und das Vertrauen der Kunden verlieren.

Spoofing-Arten/-Typen: Aus o.a. Gründen ist es ratsam, sich über aktuell kursierende Arten/Typen von Spoofing-Angriffen zu informieren und wie man diese erkennen und verhindern kann: → *s. Fortsetzung, next page!*

Beispiele für typische Attacken aus dem Internet

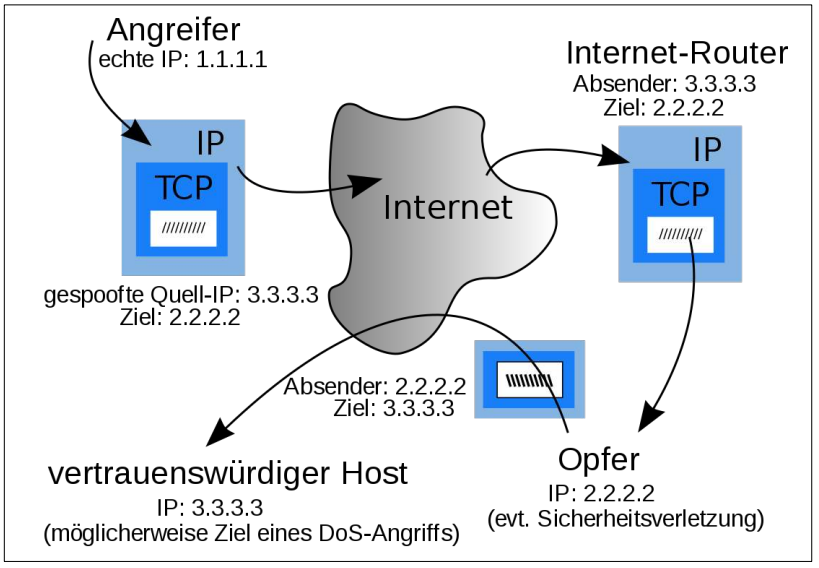
7. *Weitere typische Attacken aus dem Internet*

(Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)

IP-Adress-Spoofing-Angriffe (kurz "IP-Spoofing"): Beim IP-Spoofing werden IP-Pakete mit manipulierter Quelladresse erzeugt, um entweder die Identität des Absenders zu verbergen, sich für ein anderes Computersystem auszugeben oder gar beides. Diese Technik wird oft von böswilligen Akteuren für DDoS-Angriffe gegen ein Zielgerät oder eine umgebende Infrastruktur eingesetzt.

Das Senden und Empfangen von IP-Paketen ist eine der wichtigsten Kommunikationsmethoden für vernetzte Computer und andere Geräte und damit die Grundlage für das moderne Internet. Alle IP-Pakete enthalten den eigentlichen Paket-Inhalt ("Body") und einen "Header" mit wichtigen Routing-Informationen wie z.B. IP-Quell- und -Sende-Adresse. Bei einem normalen IP-Paket ist die Quell-IP-Adresse die IP-Paket-Absender-Adresse. Wenn das Paket manipuliert wurde, ist die Quell-Adresse wahrscheinlich gefälscht.

IP-Spoofing ist damit vergleichbar, dass ein Angreifer ein IP-Paket an jemanden sendet und dabei eine falsche IP-Absender-Adresse angibt. Wenn der Empfänger des Pakets verhindern möchte, dass der Absender ihm weitere Pakete sendet, nützt es wenig, alle Pakete zu blockieren, die von der falschen Adresse stammen. Die Absenderadresse kann leicht geändert werden. Wenn der Empfänger eine Antwort an die Absenderadresse schickt, wird sein Antwortpaket nicht an den tatsächlichen Absender gesendet, sondern irgendwo anders hin.



Die Möglichkeit, Adressen von Paketen zu fälschen, ist eine zentrale Schwachstelle, die bei vielen DDoS-Angriffen ausgenutzt wird. Beim IP-Spoofing-Angriff sendet ein Angreifer so IP-Pakete von einer verschleierten IP-Adresse, um seine wahre Identität zu verbergen. Angreifer nutzen die IP-Adress-Spoofing-Angriffe so am häufigsten bei DoS-Angriffen, die ihr Ziel mit Netzwerkverkehr überwältigen. Bei einem solchen Angriff setzt ein bösartiger Akteur eine verschleierte IP-Adresse ein, um Pakete an mehrere Netzwerkempfänger zu senden. Der Inhaber der realen IP-Adresse wird dann von allen Reaktionen überflutet, was möglicherweise eine Störung des Netzwerkdienstes bewirkt. Ein Angreifer kann auch die IP-Adresse eines Computers oder Geräts verschleiern, um sich Zugriff auf ein Netzwerk zu beschaffen, das Benutzer oder Geräte auf der Grundlage ihrer IP-Adresse authentifiziert.

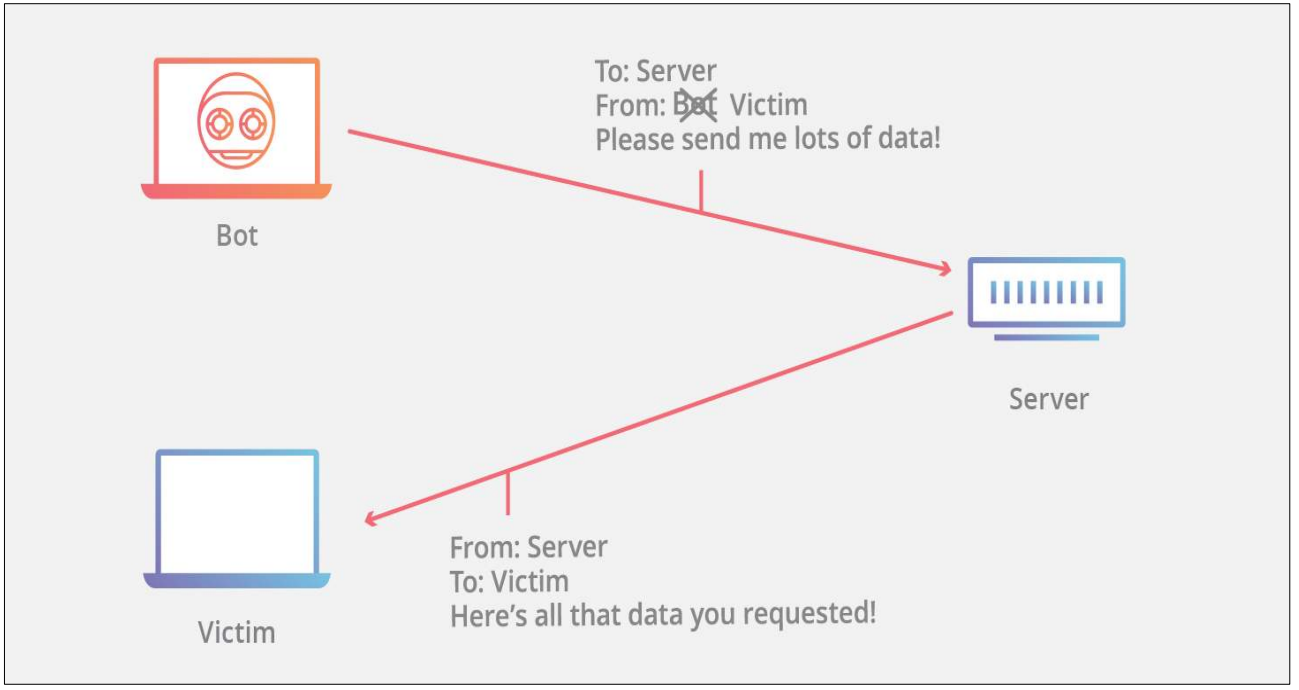
Paketfilter sind eine mögliche Gegenmaßnahme gegen IP-Spoofing! Das Gateway (Proxy) zu einem Netzwerk sollte dabei eine eingehende Filterung vornehmen: Von außen kommende Pakete, die IP-Quelladressen von innen liegenden Rechnern haben, werden z.B. verworfen. Dies verhindert, dass ein externer Angreifer die Adresse einer internen Maschine fälschen und sich dieser bedienen kann. Als weiteres Beispiel für "IP-Spoofing zum Zweck eines DDoS-Angriffs": s. Bild, next page!

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.cloudflare.com/de-de/learning/ddos/glossary/ip-spoofing/***)

IP-Spoofing zum Zweck eines ***DDoS-Angriffs***:



Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)
(Quelle: ***https://de.wikipedia.org/wiki/ARP-Spoofing***)

ARP-Spoofing*-Angriffe alias "****ARP-Poisoning****":* ARP-Spoofing (eng. "to spoof" – dt. "täuschen, reinlegen") bzw. ARP-Poisoning (dt. "Anfrageverfälschung") bezeichnet das Senden gefälschter ARP-Pakete. Dieser Angriff wird dazu benutzt, um ARP-Tabellen in einem Netzwerk so zu verändern bzw. zu manipulieren, dass anschließend der Datenverkehr zwischen zwei (oder mehr) IT-Systemen in einem Rechnernetz abgehört oder weiter manipuliert werden kann. Dies ist eine gängige Möglichkeit, einen MITM-Angriff im lokalen Netz durchzuführen.

"ARP" löst eine IP-Adresse auf eine physische MAC-Adresse auf, um Daten über ein LAN zu übermitteln. Beim ARP-Poisoning sendet ein bösartiger Akteur verschleierte ARP-Nachrichten über ein lokales Netzwerk mit dem Ziel, seine eigene MAC-Adresse mit einer legitimen IP-Adresse zu verknüpfen. Auf diese Weise kann der Angreifer Daten stehlen oder modifizieren, die an den Inhaber der betreffenden IP-Adresse gerichtet waren. Ein Angreifer, der als legitimer Host auftreten will, kann so auch auf Anfragen eingehen, auf die er mithilfe der eigenen MAC-Adresse nicht reagieren hätte können.

Mit wenigen gezielt platzierten ARP-Paketen kann ein Angreifer den privaten Datenverkehr zwischen zwei Hosts aufspüren, woraus er wertvolle Daten extrahieren kann, z.B. den Austausch von Sitzungs-Tokens, die den vollständigen Zugriff auf Anwendungskonten gewährleisten, auf die ein Angreifer niemals Zugriff haben sollte.

ARP-Spoofing (ARP-Poisoning) wird oft in MITM-, DoS-Angriffen und bei Sitzungs-Hijacking eingesetzt. ARP-Spoofing sind MITM-Angriffe auf ARP-Tabellen lokaler Netzwerke. Bei dieser Angriffsform senden Hacker gefälschte ARP-Pakete, um sich unbemerkt zwischen zwei kommunizierende Systeme zu schalten und deren Datenverkehr abzuhören oder zu manipulieren.

Fazit: Nicht alle Attacken erfolgen von außen. Das schwächste Glied in der IT-Sicherheitskette ist nun mal das LAN. Befindet sich ein ARP-Angreifer bereits im internen Netzwerk, stehen ihm so i.d.R. alle Wege offen, den Datenverkehr zu belauschen und nach Belieben zu manipulieren. Solche "Täter von innen" nutzen dazu die Angreifbarkeit des ARP-Protokolls aus. Dieses kommt in IPv4-basierten Ethernet-Netzwerken zum Einsatz, um IP-Adressen in MAC-Adressen aufzulösen, und stellt Administratoren bis heute vor ein Sicherheitsproblem.

Funktionsweise: Um den Datenverkehr zwischen Host A und Host B im LAN abzuhören, sendet der Angreifer an Host A eine manipulierte ARP-Nachricht zur Zuordnung einer bestimmten IP-Adresse. In dieser Nachricht ist seine eigene MAC-Adresse anstelle der von Host B enthalten, so dass Host A zukünftig die eigentlich für Host B bestimmten Pakete an den Angreifer sendet. Dasselbe erfolgt mit Host B, so dass dieser Pakete, anstatt direkt an Host A zu senden, nun ungewollt zum Angreifer sendet. Der Angreifer muss nun die von A und B erhaltenen Pakete an den eigentlichen Empfänger weiterleiten, damit eine abhörbare Verbindung zustande kommen kann. Wenn dies erfolgt ist, arbeitet der Angreifer unbemerkt als "***Proxy***" bzw. als "***Man-in-the-Middle***" ("MITM"), was also einen typischen MITM—Angriff darstellt. Der Angreifer hat nun freie Hand, ob er die Pakete tatsächlich weiterleitet: Er kann so selbstverständlich auch den Netzwerkverkehr verwerfen, um eine Kommunikation zwischen bestimmten Hosts unmöglich zu machen oder aber den Datenverkehr verändern bzw. manipulieren, um andere Ziele zu verfolgen.

ARP-Spoofing erkennen und verhindern: Dies ist nicht einfach. Eine Möglichkeit wäre es z.B., ARP zu deaktivieren und mit statischen ARP-Tabellen zu arbeiten. Das ist aber nicht sehr effizient, da ARP-Tabellen ständig aktualisiert werden müssen. Da jede ARP-Antwort von fast allen OS akzeptiert werden, ist es z.B. besser einem "***IDS***"-Programm mit größerer Intelligenz zu überlassen, zu überwachen, wer ARP-Antworten wann und mit welchem Inhalt verschickt. Gefälschte ARP-Pakete lassen sich so erkennen und verwerfen, und zudem kann ein IDS entsprechende Warnungen an den Systemverwalter ausgeben. → Fortsetzung, s. next page!

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)

ARP-Spoofing erkennen und verhindern: ARP-Spoofing lässt sich zumeist auch gut durch eine entsprechende ***Analyse der ARP-Tabellen*** erkennen. Im nachfolgenden ersten Beispiel führt der Rechner mit der MAC-Adresse c5:cb:df:56:b5:f2 ein ARP-Spoofing durch, bei dem er allen Hosts im Netzwerk sagt, er sei jeder andere, d,.h. er gibt seine MAC-Adresse für jede IP an, so dass ihn der Netzwerkverkehr an alle Hosts erreicht. Er leitet den Traffic allerdings transparent weiter, so dass die Attacke für alle anderen Hosts eigentlich unbemerkbar bleibt. Natürlich könnte auch jeglicher Traffic verworfen werden, wodurch eine vollständige Blockade jeglichen Traffics entstehen würde. Gezeigt wird die ARP-Tabelle eines der Opfer-PC im Netzwerk. Es ist nicht erkennbar, wer der Angreifer ist. Hierfür müsste der Administrator alle MAC-Adressen absuchen, was allerdings durch ein ***MAC-Spoofing*** verhindert werden könnte.

1. Beispiel (Der Angreifer führt hier mit MAC-Adresse "c5:cb:df:56:b5:f2" ein ARP-Spoofing durch):

* ARP-Tabelle auflisten:

```
Address         HWtype   HWaddress           Flags Mask  Iface
192.168.1.6     ether    c5:cb:df:56:b5:f2   C           eth0
192.168.1.8     ether    c5:cb:df:56:b5:f2   C           eth0        → Der Angreifer!
192.168.1.1     ether    c5:cb:df:56:b5:f2   C           eth0
192.168.1.9     ether    c5:cb:df:56:b5:f2   C           eth0
```

* Ein "traceroute" auf dem Opferhost zum Nachbarrechner sähe wie folgt aus:

```
traceroute to 192.168.1.9 (192.168.1.9), 30 hops max, 60 byte packets
 1  192.168.1.8 (192.168.1.8)  2.629 ms  2.615 ms  2.604 ms      Der Angreifer, der alle Pakete weiterleitet!
 2  192.168.1.9 (192.168.1.9)  77.776 ms  78.261 ms  79.246 ms   Der Zielrechner
```

* Ohne ARP-Spoofing müsste die Ausgabe so aussehen:

```
traceroute to 192.168.1.9 (192.168.1.9), 30 hops max, 60 byte packets
 1  192.168.1.9 (192.168.1.9)  134.356 ms  134.824 ms  135.314 ms
```

Die obige Prüfung mit der Traceroute-Methode ist natürlich nutzlos, wenn der Angreifer den Verkehr nicht weiterleitet, sondern ihn verwirft, und damit der gesamte Netzwerkverkehr unterbunden wird. Die Methode, die ARP-Tabelle zu prüfen, ist daher zumeist effektiver als das prüfen per "traceroute", da es eigentlich nicht vorkommen sollte, dass sich mehrere IP-Adressen eine MAC-Adresse teilen. Die ARP-Tabelle in Windows ist wie folgt zu überprüfen bzw. anzuzeigen: "`arp -a`"!

2. Beispiel (Der Angreifer fängt hier den Internet-Verkehr mithilfe der IP-Adresse "192.168.1.1" der Standard-Gateway bzw. dem Router ab):

```
Address         HWtype   HWaddress           Flags Mask  Iface
192.168.1.6     ether    00:15:af:43:90:de   C           eth0
192.168.1.8     ether    c5:cb:df:56:b5:f2   C           eth0        → Der Angreifer!
192.168.1.1     ether    c5:cb:df:56:b5:f2   C           eth0        → Der eigentliche Router, der aber durch eine gefälschte MAC-Adresse zum Angreifer geleitet wird!
192.168.1.9     ether    a8:7b:39:dc:78:a3   C           eth0
```

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet (Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)

ARP-Spoofing – Beispiel

(Aufruf einer "ARP-Tabelle ("ARP Cache"), z.B. per "arp -a" unter Windows):

```
Address                  HWtype     HWaddress           Flags Mask            Iface
192.168.1.6              ether      c5:cb:df:56:b5:f2   C                     eth0
192.168.1.8              ether      c5:cb:df:56:b5:f2   C                     eth0
192.168.1.1              ether      c5:cb:df:56:b5:f2   C                     eth0
192.168.1.9              ether      c5:cb:df:56:b5:f2   C                     eth0
```

ARP-Spoofing – Erklärung:

*(Quelle: "**https://de.wikipedia.org/wiki/ARP-Spoofing**")*

ARP-Spoofing (eng. "to spoof", dt. "täuschen", "reinlegen") bzw. alias "***ARP-Request-Poisoning***" (zu dt. in etwa "Anfrage-Verfälschung") bezeichnet das ***Senden von gefälschten ARP-Paketen***. Es wird benutzt, um die ***ARP-Tabellen*** ("ARP Cache") in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei (oder mehr) Systemen in einem Rechnernetz abgehört oder manipuliert werden kann. Dies ist eine Möglichkeit, einen "***Man-in-the-Middle***"-Angriff im lokalen Netz durchzuführen. Ziel eines derartigen Angriffes kann auch IP-Telefonie sein, um Telefonate abzuhören. Trotz der Bekanntheit und des Alters des Angriffes bieten gängige Betriebssysteme i.d.R. keinen Schutz vor ARP-Spoofing an. Dieser muss in der Regel nachgerüstet werden.

ARP-Spoofing – "Gefährliche Schlupflöcher (Schwachstellen)":

… z.B. per "IP-Broadcasts", die in unzähligen Situationen beispielsweise im Zusammenhang mit dem "ARP-/RARP-", "DHCP-", "SMB-" und "Wake-On-LAN-"Mechanismus und auch teils mit Netzwerk-fähigen Computerspielen auf Basis von "IPv4" stets auftreten!

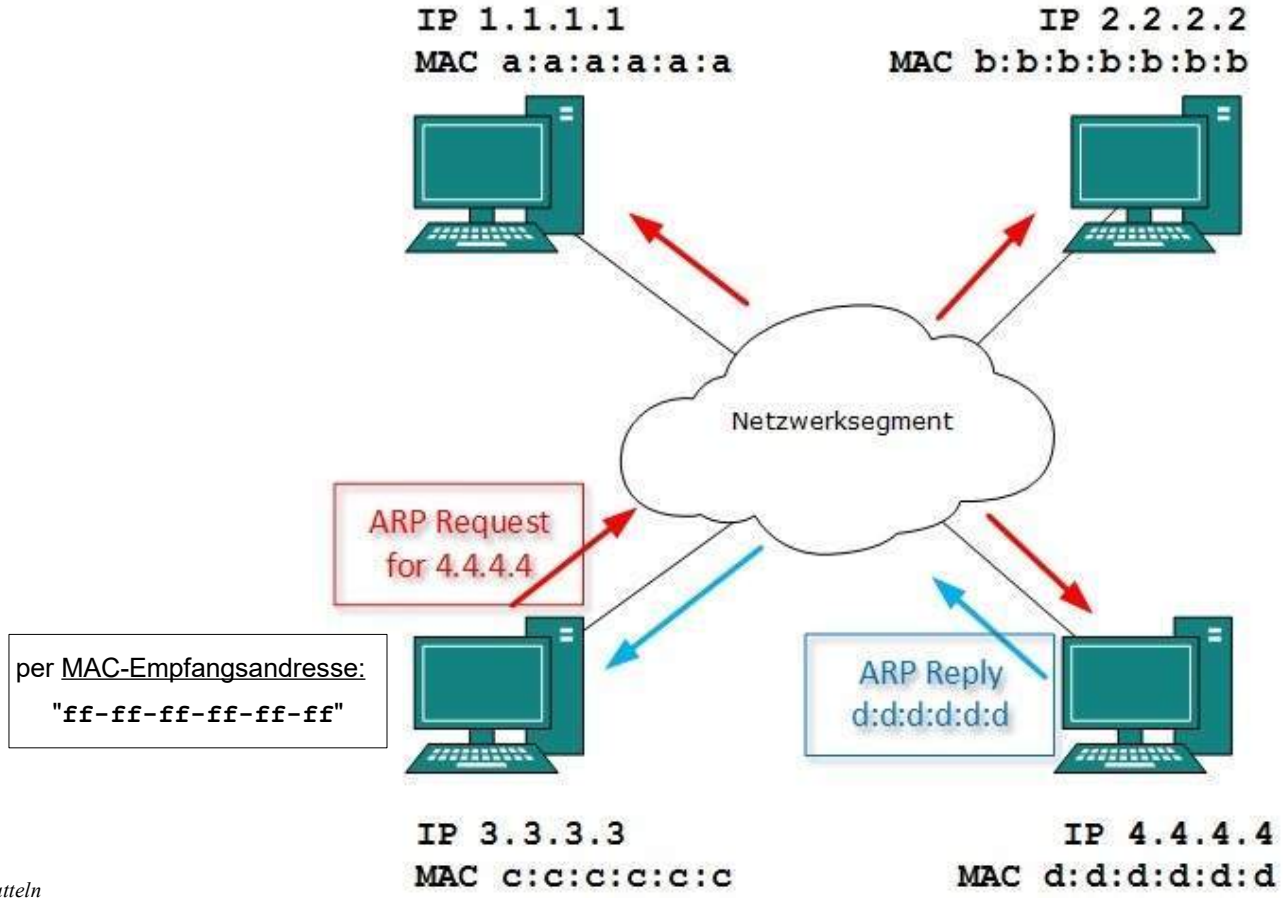
… z.B. per "ICMP", das von "ping" und "traceroute" (IPv4) verwendet wird und das u.U. aus Sicherheitsgründen auf bestimmten Rechnern/Netzknoten deaktiviert sein kann! ICMP-Pakete sind i.d.R. ungesichert und oft versuchen Angreifer aus dem Internet per "ping" die Existenz und Erreichbarkeit von Rechnern zu prüfen, um sie anschließend anzugreifen. Es ist daher in vielen Bereichen üblich, dass Netzwerkschnittstellen von Endgeräten oder Servern im öffentlichen Internet nicht auf "Echo-Requests" antworten.

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet (Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)

ARP-Spoofing – ARP-Mechanismus:

(Quelle: ***https://www.tutorialspoint.com/de/data_communication_computer_network/network_layer_protocols.htm***)



Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.rapid7.com/de/cybersecurity-grundlagen/spoofing-attacks/***)

Anrufer-ID Spoofing-Angriffe: Spoofing-Angriffe können auch als Telefonanrufe eingehen. Bei einem Anrufer-ID-Spoofing-Angriff gibt der Betrüger vor, der Aufruf ginge von einer dem Empfänger bekannten und vertrauenswürdigen Nummer ein, oder alternativ einer Nummer, die mit einem bestimmten geografischen Standort verbunden ist. Ein Anrufer-ID Spoofer kann sogar eine Nummer einsetzen, die die gleiche Vorwahl und die gleichen Anfangsziffern der Telefonnummer des Opfers hat, in der Hoffnung, dass dieses den Anruf in der Annahme annimmt, dass es sich um eine vertraute Nummer handelt. Diese Praxis wird als „Neighbor Spoofing“ bezeichnet. Wenn ein Opfer des Anrufer-ID-Spoofing den Anruf entgegennimmt, kann der Betrüger u. U. sich als Darlehensbeauftragten oder einen anderen Vertreter einer offiziellen Einrichtung ausgeben. Der vermeintliche Vertreter wird dann versuchen, das Opfer zu überzeugen, vertrauliche Informationen zu übermitteln, die zum Betrug oder zur Ausführung anderer Angriffe eingesetzt werden.

E-Mail-Adressen-Spoofing-Angriffe: E-Mail-Spoofing beinhaltet den Versand von E-Mails unter Verwendung von falschen Absenderadressen. Angreifer nutzen E-Mail-Adressen-Spoofing häufig in sozial orchestrierten Phishing-Angriffen in der Hoffnung, die Empfänger davon zu überzeugen, dass diese E-Mail legitim ist, da sie von einer vertraulichen Quelle stammt. Wenn der Angreifer in der Lage ist, die Opfer dazu zu bewegen, einen bösartigen Link in der E-Mail anzuklicken, kann er die Anmeldedaten, finanziellen Angaben oder Firmendaten stehlen. Phishing-Angriffe über E-Mail-Spoofing können den Computer des Opfers auch mit Malware infizieren, oder in Fällen wie dem Business Email Compromise (BEC) die Opfer anweisen, Geld zu überweisen. Phishing-Varianten wie Spear-Phishing oder Whaling sind möglicherweise sorgfältig auf bestimmte Einzelpersonen im Unternehmen zugeschnitten und sind tendenziell sogar erfolgreicher.

Website-Spoofing-Angriffe: Bei einem Website-Spoofing-Angriff wird der Betrüger versuchen, eine bösartige Website genau wie ein legitimes Modell zu gestalten, das das Opfer kennt und dem es vertraut. Website-Spoofing ist häufig mit Phishing-Angriffen verbunden. Wenn Opfer auf einen Link in einer Phishing-E-Mail klicken, gelangen sie über den Link auf eine Website, die so aussieht wie eine von ihnen genutzte Website – z. B. die Login-Seite ihrer Bank. Dort sehen die Opfer genau das gleiche Logo, das Branding und die von ihnen erwartete Benutzeroberfläche. Wenn sie dann ihre Anmeldedaten oder andere personenbezogene Daten eingeben, wird die Website diese Informationen jedoch für Angriffe oder Betrugsversuche abspeichern.

DNS-Server-Spoofing-Angriffe: "DNS" löst Domänennamen in IP-Adressen auf ähnliche Weise auf, wie ARP IP-Adressen in MAC-Adressen auflöst. Bei der Durchführung eines DNS-Spoofing-Angriffs versucht ein Angreifer korrupte DNS-Cachedaten in einen Host einzuführen, um den Domänennamen des Hosts zu imitieren, z.B. www.onlinebanking.com. Sobald dieser Domänenname erfolgreich verschleiert wurde, kann der Angreifer ihn einsetzen, um ein Opfer zu täuschen oder unbefugten Zugriff auf einen anderen Host zu erhalten. DNS-Spoofing kann bei einem MITM-Angriff zum Einsatz kommen, bei dem ein Opfer unbeabsichtigt vertrauliche Informationen an einen bösartigen Host versendet, in der vermeintlichen Annahme, dass es sich um eine vertrauenswürdige Quelle handelt. Auch kann das Opfer auf eine Website umgeleitet werden, die Malware enthält. Ein Angreifer, der bereits erfolgreich eine IP-Adresse verschleiert hat, könnte die IP-Adresse eines DNS ganz leicht auflösen, indem er die IP-Adresse eines DNS-Servers in seine eigene IP-Adresse auflöst.

MAC-Spoofing: Jedes IT-System im Netzwerk besitzt eine weltweit einmalige physikalische ID, die MAC-Adresse. Sie wird vom Hersteller in die HW bzw. NIC fest "eingebrannt" (burned-in-address). User haben i.d.R. keine Möglichkeit, diese MAC-Adresse umzuschreiben, um z.B. unerkannt zu bleiben. Möglich ist jedoch eine SW-seitige Maskierung ("Mascerading"). Man spricht in diesem Fall dann auch von "MAC-Spoofing".

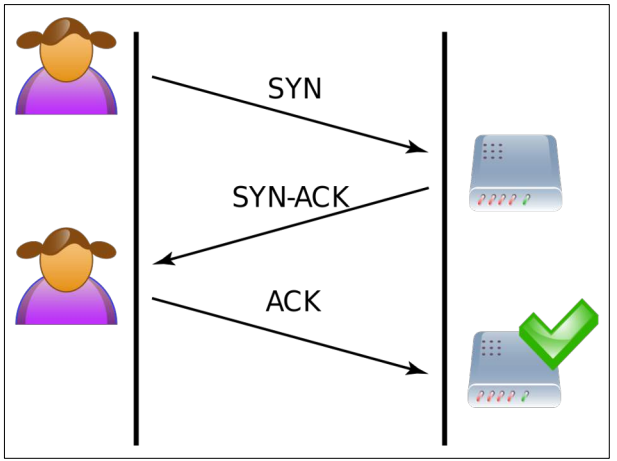
Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

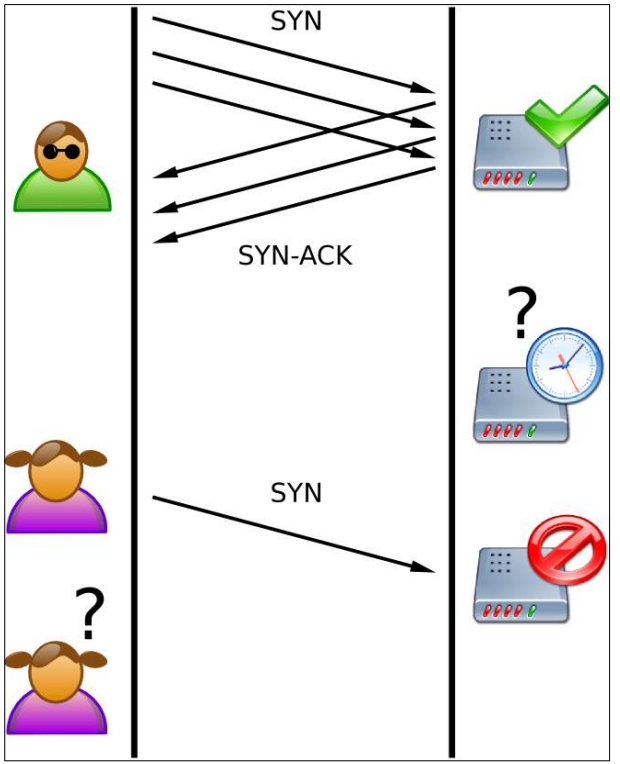
(Quelle: ***Wikipedia***)

- ***SYN-Flooding:*** Dies ist eine DoS-Form auf Computersysteme. Der Angreifer verwendet den Verbindungsaufbau des Transportprotokolls "TCP" dazu, um einzelne Dienste oder ganze Computer aus dem Netzwerk unerreichbar zu machen.

Normaler, erfolgreicher TCP-Handshake!



Der Angreifer (grün) sendet viele SYN-Pakete, jedoch keine ACK-Pakete. Durch die halboffenen Verbindungen wird der Server so sehr ausgelastet, dass die Anfrage eines normalen Benutzers (lila) nicht bearbeitet werden kann!

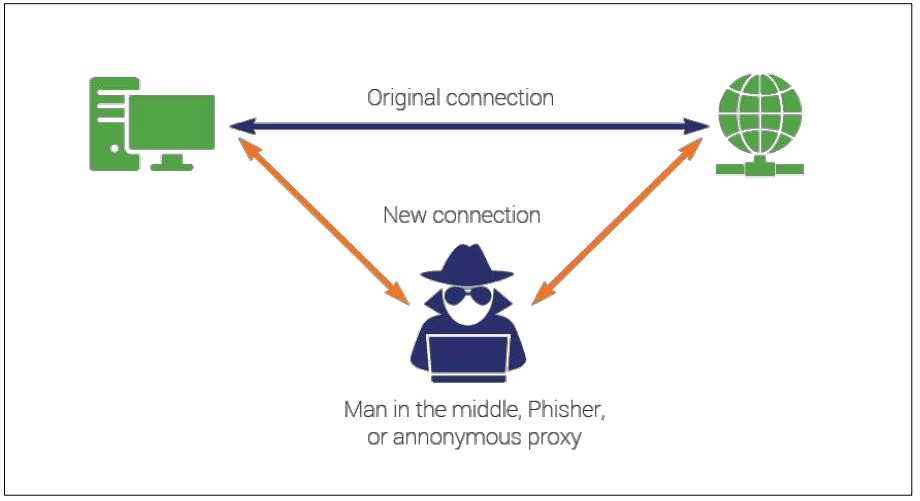


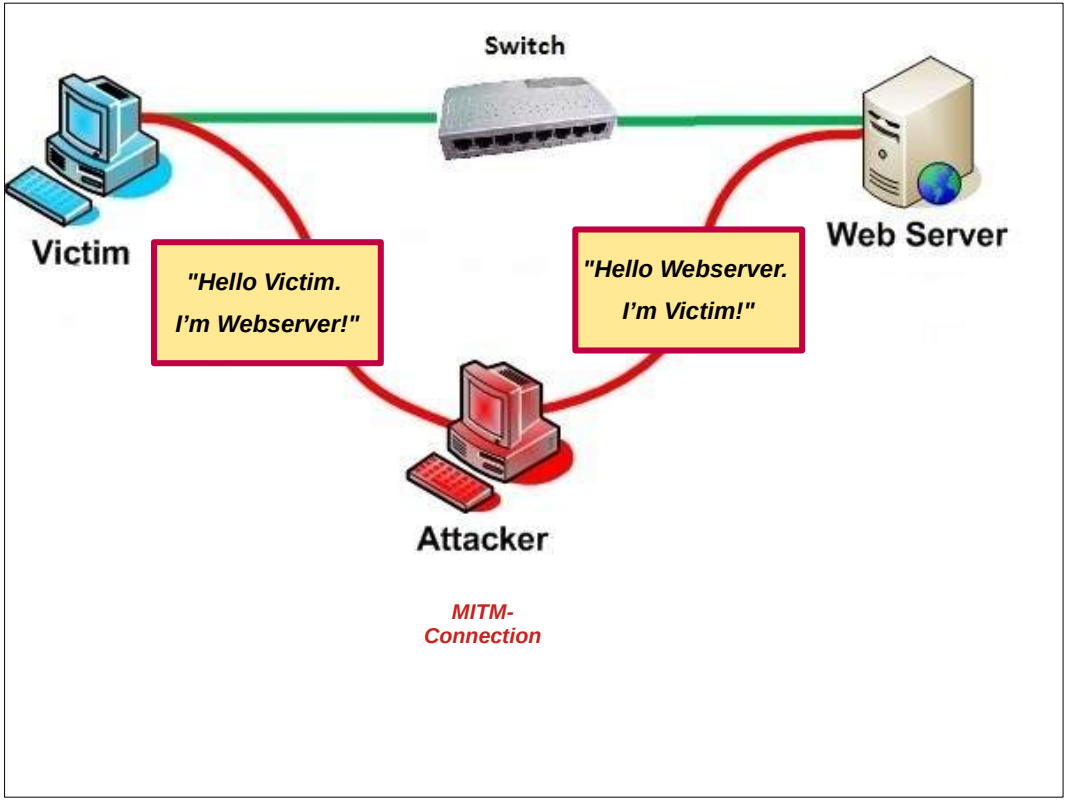
Beispiele für typische Attacken aus dem Internet

7. *Weitere typische Attacken aus dem Internet*

(Quelle: ***https://www.cloudflare.com/de-de/learning/ddos/glossary/ip-spoofing/***)

- "***Man-in-the-Middle-Attacken***" (MITM):





Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.avast.com/de-de/c-spoofing#topic-3***)

Spoofing & ***Phishing*** – Was ist der Unterschied?

Der Unterschied zwischen Spoofing und Phishing besteht darin, dass beim Spoofing eine andere Identität vorgetäuscht wird, während bei Phishing-Angriffen versucht wird, an sensible Informationen zu gelangen. Typisch bei Phishing-Angriffen ist, dass Opfer unter anderem mit Ködern wie gefälschten E-Mails „angelockt“ und dazu gebracht werden, vertrauliche personenbezogene Daten preiszugeben, die dann für Identitätsdiebstahl verwendet werden können.

Spoofing-Angriffe erwecken den Anschein, dass die Kommunikation vertrauenswürdig ist, da die Absender vertrauenswürdigen Absendern täuschend ähnlich sind. Viele Phisher verwenden Spoofing, um ihren Opfern vorzugaukeln, dass die E-Mail seriös ist. Mit dieser Art von manipulativem Social Engineering bringen Phishing-Betrüger Sie dazu, persönliche Informationen preiszugeben.

Wie bereits erwähnt, gibt es verschiedene Arten von Spoofing. Spoofing auf DNS- oder IP-Ebene unterscheidet sich vom Phishing, da technische Mittel verwendet werden, um einen Computer oder ein Netzwerk auszutricksen. Typosquatting ist z.B. eine Art Spoofing-Angriff, bei dem häufige Fehler bei der Eingabe von URLs ausgenutzt werden, um die Nutzer glauben zu machen, sie würden die gewünschte Website besuchen.

Aber E-Mail-Spoofing und Phishing sind sehr ähnlich und werden häufig zusammen angewendet. Clevere Hacker nutzen Spoofing, um ihre Phishing-E-Mails oder SMS-Nachrichten glaubwürdiger zu machen und so die Erfolgsaussichten zu erhöhen. Schauen wir uns mal an, wie sie das machen.

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://www.cloudflare.com/de-de/learning/ddos/glossary/ip-spoofing/***)

- "***Botnets***":

  Was ist ein Botnet? So bezeichnet man den Zusammenschluss mehrerer autonom tätiger SW-Programme (Bots) zu einem großen Netzwerk. Botnetze sind beliebte Angriffswerkzeuge von Cyberkriminellen. Sie bestehen in der Regel aus tausender miteinander vernetzter "Bots". Bots ist die Kurzform von eng. “Robot” und deutet auf die primäre Funktionalität der Tools hin, d.h. sie erledigen selbständig und automatisch vordefinierte Aufgaben. Als Schadsoftware operieren Bots meist ohne Kenntnis des Anwenders auf gekaperten PCs, Netzwerkservern und allen anderen vernetzten IT-Geräten aus dem Internet der Dinge ("IoT"), die zusammengeschaltet das Botnetz ergeben. Auch IP-Kameras, Netzwerkdrucker, Smart-TVs und ähnliche Geräte können Teil eines Botnetzes werden. Im Zusammenschluss bilden die Bots als kollektives Botnetz eine mächtige Waffe, um schädliche Aktionen gegen Unter-nehmen oder Organisationen durchzuführen.

  Wie funkjtionieren Botnetze? Sie funktionieren als "Distributed Computing Networks", d.h. die als zusammengeschlossene Computer zwar miteinander kommunizieren, allerdings unabhängig voneinander arbeiten. Die Aufgaben des Botnets erfüllt der Computer im Hintergrund, zumeist ohne dass sein User etwas davon mitbekommt. Damit der Bot agieren kann, muss der Rechner eingeschaltet und mit dem Internet verbunden sein.

  Wie entstehen Notnetze? Ihre Entstehung erfolgt zumeist in mehreren bzw. zumindest in den drei folgenden Stufen:

  1. Das Infizieren von ungeschützten Computern: Dies kann auf unterschiedlichen Arten erfolgen, z.B. per infizierter Website, welche Schadsoftware unterschiebt. Auch das Infizieren über eMails kommt häufig vor, entweder über Anhänge, welche den Schadcode enthalten oder über Links, die wiederum auf eine infizierte Website führen. Es kommt auch vor, dass Nutzer ein ganz anderes Programm installieren, welches einen Trojaner enthält – auch so wird die Tür für das Botnet geöffnet.
  2. Die Eingliederung bzw. Einordnung in das Botnet: Die infizierten Computer werden Teil einer automatisierten Gruppe von Computern, welche sich durch das gesamte Internet spannt und zahlreiche Computer zu riesigen Botnetzen miteinander verbindet. Zumeist setzen Cyberkriminelle Botnetze für Angriffe über das Internet ein. Zur Steuerung der Bots nutzen die Betrüger sogenannte ***Command-and-Control-Server (C&C)***, über diese läuft die Kommunikation und die Datenübertragung zu den einzelnen Bot-Programmen im Netzwerk.
  3. Die Ver- bzw. Anwendung des Botnets: Legal finden Botnets z.B. beim Data Mining für Kryptowährungen ihren Einsatz. Doch Botnets, welche ohne das Wissen der Computernutzer aufgebaut werden, kommen vor allem für folgende kriminelle Zwecke zum Einsatz:
     - ***DDoS:*** Bei Botnet-getätigten Angriffen kann es sich etwa um DDoS-Attacken handeln, bei denen die Angreifer auf eine Überlastung des anvisierten Ziels im Internet abzielen. Die im Botnet verbundenen IT-Systeme senden hierzu unzählige sinnfreie Anfragen z.B. an einen spezifischen Webserver, bis dieser aufgrund der schieren Masse an Requests in die Knie geht.
     - ***Spam:*** Eine der gängigsten Verwendungsarten von Botnets ist der massenhafte Versand von Spam-E-Mails.
     - ***Phishing:*** Auch der unbemerkte Versand von Phishing-E-Mails von betroffenen Computern aus ist ein häufiger Zweck von Botnets.
     - ***Datenraub:*** Über Botnets können Kriminelle an sensible Nutzerdaten gelangen, welche sie entweder selbst verwenden oder verkaufen können.
     - ***Proxy:*** Per Bot-Computer ist auch die Verbindung zu einem dritten Computer herstellbar. Die eigentliche Ursprungsadresse wird dabei verborgen.
     - ***Zielgerichtete Werbeanzeigen:*** Der Bot-Computer-User findet im Browser z.B. spezielle Banner-Werbeanzeigen, worüber ihm gefälschte Antispyware-SW angeboten wird.

Beispiele für typische Attacken aus dem Internet

7. Weitere typische Attacken aus dem Internet

(Quelle: ***https://de.wikipedia.org/wiki/Ransomware***)

- Was ist "***Ransomware***"?

Ransomware (eng. "ransom" für „Lösegeld“) wird auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner genannt. Dies sind Schadsoftware-Programme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Die Bezeichnung setzt sich zusammen aus "ransom", dem englischen Wort für Lösegeld, und "ware", entsprechend dem für verschiedene Arten von Computerprogrammen üblichen Benennungsschema (Software, Malware etc.).

Die Cyberkriminalität entwickelt immer neue Ansätze. Dazu gehört auch Ransomware, die Benutzer vor ein sehr spezielles Problem stellt. "Ransom" bedeutet "Lösegeld" und genau das ist es, was Ransomware von einem betroffenen User verlangt:

- Ransomware versperrt eine IT-System mit einem "Lockscreen", der nicht einfach zu beseitigen ist.
- Auf dem Lockscreen steht zumeist die Info zum Lösegeld, d.h. dass der User eine Zahlung leisten muss, damit er seinen Computer wieder entsperrt bekommt.
- Dabei wird oft eine falsche Quelle angegeben. Bekannt ist z.B. der "Bundespolizei-Trojaner", bei dem Opfern vorgetäuscht wurde, dass sie eine Zahlung an die Polizei leisten müssten.
- Bei heutiger Ransomware wird als Zahlungsmittel oft eine Kryptowährung wie z.B. Bitcoin verlangt, da hier der Geldfluss viel schwieriger zu verfolgen ist.

Möglichkeit zur Problemlösung, nachdem der Worstcase eingetreten ist: Einmal mit Ransomware infiziert, ist es nicht ganz einfach, das IT-System wieder zu entsperren. Es ist ratsam, den Computer direkt auszuschalten, um eine weitere Verschlimmerung zu verhindern. Anschließend sollten der Inhalt der Festplatte auf einem anderen Datenträger gesichert werden, so dass die Festplatte formatiert und neu aufgesetzt werden könnte.

Präventivmaßnahmen: Im Idealfall beugt der User entsprechend vor. Es gibt spezielle SW-Tools wie "Anti-Ransomware" von "Malwarebytes" als effektiver Schutz gegen die Infizierung. Grundsätzlich sollte man sich außerdem von riskanten Webseiten fernhalten und keine unbekannten Dateien öffnen. Regelmäßige Datensicherungen schützen nur dann vor Ransomware, wenn diese nicht im direkten Zugriff von Benutzern oder Administratoren stehen. Eine Datensicherungsstrategie mit auswechselbaren Medien sollte die Regel sein. Selbst dann können „Schläfer“ auf den Backup-Sets nach wie vor vorhanden sein, sodass ein Großvater – Vater – Sohn – Prinzip (Generationenprinzip) überdacht werden sollte. Zudem hilft eine eMail-Archivierung.