

Glossar - Sicherheit im Netzwerk

Ein kleines Lexikon der „Hacker“-Sprache

Um die potentiellen Gefahren erkennen zu können, die heute Ihrem Netzwerk durch Angriffe von Außen und von Innen (!) drohen, sollten Sie die folgenden Begriffe kennen!

Broadcast-Stürme

Mittels eines ARP-Angriffes (Adress Resolution Protocol) werden ARP-Pakete an nicht existierende IP-Adressen eines Netzwerkes versendet. Diese Anfragen werden über die Gateways an die angeschlossenen Netzwerke weitergeleitet (Broadcast). Dies führt zu einer erheblichen Einschränkung der Bandbreite im lokalen Netzwerk.

Brute-Force-Attack

Eine Passwortheingabe wird solange mit Buchstaben- Zeichen- und Zahlenkombinationen beschickt, bis das Passwort gefunden wurde. Als Hilfe gibt es Wortlisten (Dictionaries) mit häufig genutzten Wörtern.

Denial-of-Service oder Distributed Denial-of-Service

Auch IP-Bombing genannt. Der „Opferrechner“ wird mit einer Vielzahl von IP-Paketen bombardiert und stellt seinen Dienst wegen Überlastung ein (Denial-of-Service). Wird dies nicht von einem einzelnen Rechner, sondern zeitgleich von vielen Rechnern aus durchgeführt, spricht man von einem Distributed Denial-of-Service.

Fingerprinting

Es werden ungebräuchliche TCP-Flags an den Zielrechner gesendet. Die Antworten erlauben einen Rückschluss auf das System.

Flooding

Genau: SYN-Flooding. Es werden sehr schnell Verbindungsaufforderungen an die TCP-Verbindung gesendet, ohne die vorherige Verbindung zu beenden.

Joiner

Ein Programm, mit dem sich zwei Dateien zusammenfügen lassen. Hilfreich zum Erstellen eigener Trojaner.

Keylogger

Einmal in ein System eingeschleust (z. B. über einen Trojaner) werden alle Tastatureingaben aufgezeichnet und per Mail verschickt. Benutzernamen und Passwörter erscheinen im Klartext. Diese Vorgehensweise wird auch als „Monitoring“ bezeichnet.

Link-Listing

Eine Form des Mail-Bombing. Die Zielperson wird mit der Mail-Adresse in unzählige Newsgroups eingetragen. Die Flut an E-Mails kann man sich ja vorstellen. Eine Austragung ist nur manuell bei jeder Newsgroup einzeln möglich.

Mail-Bombing

Das Postfach der Zielperson wird mit einer Unzahl von Mails beschickt. Nicht selten bricht der Mail-Server unter der Belastung zusammen. T-Online hat das 1996 schon einmal schmerzlich erfahren müssen. Im Idealfall wird als Gegenmaßnahme einfach das Postfach des betroffenen Users abgeschaltet.

Nuken

Ist die IP-Adresse eines Rechners bekannt, wird diese mit unzähligen Pings überschüttet. Dies führt bei Windows-Rechnern zu dem gefürchteten „blauen Bildschirm: einem Systemabsturz. Eigene Nuker-Tools (z.B. Winnuke) übernehmen diese Aufgabe.

Ping of Death

Es wird ein unzulässig langes Datenpaket in fragmentierter Form gesendet. Nach der Zusammensetzung der Bestandteile kann ein Systemabsturz die Folge sein. Benutzt wird dafür ein ICMP Echo Request.

Port-Scan

Systematische Ausspähung von sog. offenen Ports einer Ziel-IP-Adresse, als Vorbereitung auf einen Angriff. Die Rückmeldung des Ports gibt Auskunft über den jeweiligen Status. Offene, d.h. ungeschützte Ports sind ein willkommenes Einfallstor für Angriffe von Außen.

**Kostengünstige
Komplettprodukte
für Ihr Netzwerk**

Portstrobe

Hierbei wird die Ausspähung nicht systematisch betrieben, sondern zeitlich versetzt und nur auf die „weil-known“ Ports begrenzt. Die Gefahr einer Erkennung ist niedriger.

Retro-Viren

Viren, die gezielt Applikationen, besonders Anti-Viren-Programme, befallen.

Spoofing

Vortäuschen von falschen Angaben. Bei dem IP-Spoofing z.B. wird dem Zielrechner als Absender eines Datenpaketes eine IP-Adresse einer internen Workstation oder eine nicht existierende IP vorgegaukelt.

Trojaner

Programme die bei der Ausführung unerkannt für den Benutzer ein zweites Programm installieren (sogenannte Backdoors), z.B. zur Ausspähung von Passwörtern. Die Verbreitung erfolgt in der Regel über E-Mails.

Viren oder Computerviren

Die Idee zu Computerviren leitete sich von dem biologischen Vorbild der Viren ab und gab ihnen ihren Namen. Durch Computerviren kommt es auf einem Computer häufig zur Veränderung oder zum Verlust von Daten und Programmen sowie zu Störungen des regulären Betriebs. Viren werden oft per Email oder durch Download von Dateien aus dem Internet auf den eigenen Computer gebracht. Viren werden meist erst durch das Öffnen einer ausführbaren Datei aktiviert. Durch sog. Viren-Scanner können sie unschädlich gemacht werden. Jedoch können Viren-Scanner nur bekannte Viren erkennen, weshalb das regelmäßige und oftmalige Aktualisieren der sog. Viren-Signaturen dringend anzuraten ist, um immer einen aktuellen Schutz auf seinem Computer zu haben.

Zeit-Server-Angriff

Einmalpasswörter, z.B. TAN-Nummern bei Banktransaktionen, werden ausgespäht, und es wird versucht, sie erneut einzusetzen. Dazu wird der Zeit-Server des Systems manipuliert, d.h. die Systemzeit zurückgestellt.

Weitere Informationsquellen - Virenschutz und Netzwerksicherheit

Definitionen und Erklärungen:

<http://de.wikipedia.org/wiki/Computervirus>

Informationen des Bundesamtes für Sicherheit in der Informationstechnik:

www.bsi.de/av/virbro/index.htm

Heise Verlag – Links zu Virenschutzprogrammen und Informationsseiten:

www.heise.de/security/dienste/antivirus/links.shtml

Virenlexikon und Whitepaper rund um Computerviren:

www.sophos.de/virusinfo

Umfassender Viren- und Spam-Schutz bei unseren coXervern

Zwei (!) unabhängige integrierte Virens Scanner prüfen nicht nur jede ein- und ausgehende Email sondern überwachen permanent alle Dateiablagen auf Viren. Virenverseuchte Dateien können nicht mehr geöffnet werden und der Download von virenverseuchten Dateien wird verhindert.

Die Viren-Signaturen werden automatisch stündlich aktualisiert, um Ihr Netzwerk optimal zu schützen!

Zusätzlich sorgt ein Spam-Filter dafür, dass unerwünschte Emails gar nicht erst bei Ihnen ankommen.

***Wir kümmern uns um den Schutz
Ihres Netzwerks,
Sie kümmern sich um Ihr Business!***

coXerver ist ein Produkt der coXorange networXservice Bendig und Dohrmann GbR, Cottbus, im Vertrieb der Web4you NetworX GmbH, Berlin.