en
cs de
sk es

TECH
pedia

MODERNE SICHERHEITSSYSTEME

MIGUEL SORIANO

Titel der Arbeit: Moderne Sicherheitssysteme
Author: Miguel Soriano
Übersetzt (von): Alena Dvořáková
Veröffentlicht (von): České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktadresse: Technicka 2, Prague 6, Czech Republic
Tel.: +420 224352084
Drucken: (nur elektronisch)
Anzahl der Seiten: 43
Ausgabe: 1. Ausgabe, 2017

ISBN 978-80-01-06208-1

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG

	Definition(en)
	Interessantheit (Interessantes)
	Bemerkung
	Beispiel
	Zusammenfassung
	Vorteile
	Nachteile

ZUSAMMENFASSUNG

Dieses Modul gibt eine grundlegende Orientierung im Bereich der Netzwerksicherheit, einschließlich Sicherheitsdiensten, Sicherheitsmechanismen, Angreifertypen, Sicherheitslücken und Komponenten eines Netzwerksicherheitssystems.

ZIELE

Dieses Modul stellt eine Übersicht der modernen Sicherheitssysteme vor. Es ist in fünf Kapitel aufgeteilt.

Das erste Kapitel definiert die Begriffe Netzwerksicherheit, Sicherheitsdienste und Sicherheitsmechanismen. Das zweite Kapitel bietet eine Übersicht der Netzwerksicherheitslücken zusammen mit verschiedenen Angriffen (Viren, Würmer, Trojaner; Spyware, Adware; Zero-Day-Angriffe; DoS-Angriffe; Abfangen und Stehlen von Daten; Spoofing, Identitätsdiebstahl).

Im dritten Kapitel werden Komponenten des Netzwerksicherheitssystems (Antivirensoftware, Firewalls, Angrifferkennungssysteme, VPN usw.) beschrieben. Das vierte Kapitel stellt weitere Methoden der Netzwerksicherung (z. B. starke Authentifizierungsverfahren, Härten des Betriebssystems, Schutz von Webdiensten) vor.

Im fünften Kapitel wird mobile Sicherheit behandelt. Smartphones spielen eine bedeutende Rolle in der modernen Kommunikation und niemand zweifelt an ihrer Wichtigkeit im Alltagsleben. Es werden jedoch immer wieder neue Angriffsarten bekannt. In diesem Kapitel wird erwähnt, wie ein Hacker ein erfolgreich angegriffenes Smartphone nutzen kann.

LITERATUR

[1] CVE. *A dictionary of publicly known information security vulnerabilities and exposures*. Erhältlich auf: http://cve.mitre.org; 2015. [online]

[2] CHESWICK, W.; BELLOVIN, S.: *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994. ISBN: 0-201-63357-4.

[3] ZWICKY, E. D.; COOPER, S; CHAPMAN, D. B.: *Building Internet Firewalls*. O'Reilly and Associates, 2nd edition, 2000. ISBN: 978-1-565-92871-8.

[4] DE ALBUQUERQUE, J. P.; DE GEUS, P. L.: *A Framework for Network Security System Design*.

[5] BILGE, L.; DUMITRAS, T.: *Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World.* ACM Conference on Computer and Communications Security, Raleigh, NC, 2012, S. 833–844.

[6] ZETTER, K.: *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishers, 2014. ISBN: 978-0-7704-3617-9.

[7] ADEYINKA, O.: *Internet Attack Methods and Internet Security Technology*. AICMS 08. 2nd Asia International Conference on Modeling & Simulation, S.77–82, 2008. ISBN: 978-0-7695-3136-6.

[8] SHINDER, T. W.: *The Best Damn Firewall Book Period (2nd Edition)*. Syngress Publishing, Inc. 2007. ISBN: 978-1-59749-218-8.

[9] SCARFONE, K.; HOFFMAN, P.: *Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-41, 1st Revision, 09/2009.

[10] GEIER, E.: *Intro to Next Generation Firewalls*. Erhältlich auf: http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html 09/ 2011. [online]

[11] CLIFF, A.: *Password Crackers - Ensuring the Security of Your Password*. Security Focus, 02/2001. Erhältlich auf: http://online.securityfocus.com/infocus/1192. [online]

Inhaltsverzeichnis

1 1 Einleitung

Die Welt wird wegen des Internets und neuer Netzwerktechnologien immer mehr vernetzt. In den letzten Jahren haben internetbasierte Geschäfte (elektronischer Handel, E-Business) ihre Effizienz und den Umsatz drastisch gesteigert. Netzwerke bieten mehr Anwendungen und sind für immer mehr Benutzer verfügbar. Daher werden sie aber auch von einem breiteren Spektrum von Sicherheitslücken gefährdet. Um diese Lücken zu schließen und um Netzwerktransaktionen zu sichern, wird die Netzwerksicherheit wichtiger, nicht nur für Firmen und Militär, sondern auch für Organisationen und PC-Benutzer.

Früher waren Hacker hochqualifizierte Programmierer, welche alle Details der Rechnerkommunikation und Möglichkeiten der Ausnutzung von Verwundbarkeiten gut verstanden. Heutzutage kann fast jeder durch den Download der erforderlichen Werkzeuge aus dem Internet zu einem Hacker werden. Diese hochentwickelten Tools und üblicherweise offene Netzwerke haben einen erhöhten Bedarf an Netzwerksicherheit und dynamische Sicherheitsgrundsätze generiert. Die Verwundbarkeiten und ihre Auswirkungen werden von vielen Organisationen klassifiziert. Eine der bekanntesten Datenbank von solchen Vulnerabilitäten ist die **NVD** (*Nationale Verwundbarkeits-Datenbank*, *National Vulnerability Database*) der MITRE Corporation [1].

Der Bereich der Netzwerksicherheit ist riesig und befindet sich in einem sehr evolutiven Stadium, weil Sicherheitsvorfälle in alarmierendem Tempo zunehmen. Obwohl die Netzwerk- und Computersicherheit in den letzten Jahren erheblich verbessert wurden, sind Systeme immer noch verwundbarer denn je. Jeder wichtige technologische Fortschritt der Computertechnik bringt neue Sicherheitslücken, die neue Sicherheitslösungen erfordern. Die Technologie entwickelt sich jedoch schneller, als diese Lösungen gefunden werden können. Je komplexer die Gefahren sind, desto komplexer müssen die Sicherheitsmaßnahmen für den Netzwerkschutz sein.

1.1 Netzwerksicherheit

Der Begriff Netzwerksicherheit (engl. *network security*) bezieht sich auf Aktivitäten, die dem Netzwerkschutz dienen. Besonders schützen sie Verwendbarkeit, Zuverlässigkeit, Integrität und Sicherheit von Netzwerken und Daten. Die Netzwerksicherheit wurde zu einer grundlegenden Anforderung an alle Formen der Kommunikation, vor allem in Firmen, welche das Internet aktiv verwenden.

Kunden, Verkäufer und Geschäftspartner brauchen den Schutz aller geteilten Informationen, hauptsächlich der sensiblen Daten, wie Kreditkartennummern oder vertrauliche Geschäftsinformationen.

Die Netzwerksicherheit bezieht sich jedoch nicht nur auf die Sicherheit in Computern auf beiden Enden der Kommunikation. Bei der Datenübertragung soll es auch nicht möglich sein, den Kommunikationskanal leicht anzugreifen. Sonst könnte ein Hacker die Daten abfangen und entschlüsseln und eine falsche Nachricht einfügen. Die Sicherung des Netzwerkes ist daher ebenso wichtig wie die Sicherung der Rechner und die Verschlüsselung von Nachrichten. Eine effiziente Netzwerksicherheit rechnet mit verschiedenen Gefahren und verhindert ihrem Eingang oder ihrer Verbreitung im Netz.

Die Netzwerksicherheit ist eine grundlegende Voraussetzung für die problemlose Existenz einer Firma im Internet. Eine weitere wichtige Sicherheitsanforderung stellt der Schutz gegen Dienstverweigerung dar, weil Ausfallzeit des Netzwerkes für alle Geschäftstypen aufwendig ist. Eine wirksame Sicherheitspolitik erlaubt der Firma, neue Dienstleistungen und Anwendungen ohne Senkung der Netzwerkleistung hinzuzufügen. Die Datensicherung ist eine weitere proaktive Strategie, um den Ausfall der Kundendienstleistungen sogar bei ihrer Modifizierung zu verhindern.

Zu den Vorteilen eines sicheren Netzwerkes gehören für Firmen: Kundenvertrauen (geschützte Privatsphäre der Benutzer), Mobilität (sicherer Zugriff ohne Viren oder weitere Gefahren), verbesserte Produktivität (Zeitsparen bei nicht produktiven Aufgaben, wie Spam oder Umgang mit Viren) und Wirtschaftlichkeit (Ausfallzeiten stellen immer Mehrkosten für Firmen dar).

1.2 Netzwerksicherheitssystem

Ein Netzwerksicherheitssystem (engl. *network security system*) ist ein Satz von Hard- oder Softwaremitteln, der sichere Protokolle und kryptographische Algorithmen zum Schutz der Informations- und Kommunikationssysteme einer Firma verwendet.

Einige Aufgaben dieser Mittel umfassen Überwachung und Kontrolle des eingehenden und abgehenden Netzwerkverkehrs, Erkennung von Angriffen, Schutz gegen Datendiebstahl, Schutz der Netzwerkinfrastruktur einschließlich Netzwerk-Bandbreite, Sicherstellung der Dienstleistungssicherheit und -kontinuität auch bei DoS-Angriffen.

Weil die Sicherheitsanforderungen von Firmen immer komplexer werden, werden auch Netzwerksicherheitssysteme immer komplexer. Die traditionalen Strategien, wie Firewalls, müssen adaptiert werden, so dass sie verteilte Sicherheitsmechanismen, dezentralisierte Treuhandverwaltung und weitverbreitete kryptographische Verfahren, wie **IPSec** (engl. *Internet Protocol Security*) in **VPN** (*virtuelles privates Netzwerk***,** engl. *Virtual Private Network*), einschließen.

Ein Netzwerksicherheitssystem ist nur ein kleiner (aber wichtiger) Teil der Informationssicherheitsinfrastruktur einer Firma und muss zusammen mit weiteren Bereichen, wie physische und personalbezogene Sicherheit, Betriebs- und Kommunikationssicherheit und sozialen Mechanismen, betrachtet werden.

1.3 Sicherheitsdienste

Ein Sicherheitsdienst (engl. *security service*) ist ein Dienst, der eine adäquate Sicherheit von Systemen oder Datenübertragungen garantiert. Sicherheitsdienste werden von Sicherheitsmechanismen nach Sicherheitsgrundsätzen implementiert.

Schon für mehr als zwanzig Jahre schafft die Grundlage der Informationssicherheit die sogenannte CIA-Triade: Vertraulichkeit (engl. *confidentiality*), Datenintegrität (engl. *data integrity*) und Verfügbarkeit (engl. *availability*). Zu diesen drei klassischen Attributen wurden später weitere Elemente hinzugefügt: Authentifizierung (engl. *authentication*), Zugriffskontrolle (engl. *access control*), Unleugbarkeit (engl. *non-repudiation*) und Datenschutz (engl. *data privacy*). Diese Klassifikation wird jedoch oft von Fachleuten in Frage gestellt. Die einzelnen Begriffe werden weiter erklärt.

- Die Vertraulichkeit bezieht sich auf den Schutz von Informationen gegen Veröffentlichung durch unbefugte Subjekte (Organisationen, Personen, Maschinen, Prozesse). Nur ein oder mehr bestimmte Subjekte dürfen auf die Daten zugreifen. Unter Informationen versteht man dabei Dateninhalt, -größe, -existenz, Kommunikationstyp usw.

- Die Datenintegrität ist der Schutz von Daten gegen Erzeugung, Änderung, Löschung, Vervielfältigung oder Umstellung durch unbefugte Subjekte (Organisationen, Personen, Maschinen, Prozesse). Eine Verletzung der Integrität wird nur von aktiven Angriffen verursacht. Die Integrität bezieht sich insbesondere auf die Vertrauenswürdigkeit der Informationsressourcen.

- Die Verfügbarkeit bedeutet einen rechtzeitigen Zugriff auf Informationen. Sie wird beispielsweise durch einen Festplattencrash oder Dienstverweigerungsangriff (**DoS**, engl. *Denial of Service*) verletzt. Jede Verzögerung, die die vorausgesetzte Dauer der gegebenen Systemdienstleistung überschreitet, kann als eine Verletzung der Verfügbarkeit betrachtet werden. Ein Informationssystem, das nicht zur Verfügung steht, wenn man es braucht, ist nicht besser als gar kein Informationssystem. Es kann sogar viel schlechter sein, wenn die Organisation von der funktionsfähigen Computer- und Kommunikationsinfrastruktur abhängig ist.

- Die Authentifizierung sorgt dafür, dass die kommunizierenden Subjekte (Personen, Maschinen, Prozesse) relevante Identitäten voneinander kennen. Sie umfasst drei unabhängige Kategorien: Wissen (engl. *knowledge*), Besitz (engl. *possession*) und Inhärenz (engl. *inherence*). Beim Wissen handelt es sich um Kenntnisse, die der Benutzer für das Einloggen wissen muss, z. B. Passwort. Der Besitz umfasst Sachen, die der Benutzer zum Einloggen haben muss, z. B. Chipkarte. Und die Inhärenz schließt biologische Merkmale ein, die der Benutzer zum Einloggen aufweisen muss, z. B. Fingerabdruck.

- Die Zugriffskontrolle bedeutet einen Schutz von Informationsressourcen oder -diensten gegen Zugriff oder Verwendung durch unbefugte Subjekte (Organisationen, Personen, Maschinen, Prozesse). Das heißt, dass Zugriffskontrolle sich auf Verhütung einer unbefugten Nutzung von

Ressourcen bezieht. Dabei wird kontrolliert, wer und unter welchen Bedingungen einen Zugriff auf spezifische Ressourcen hat und welche Aktivitäten mit den Ressourcen erlaubt sind.

- Die Unleugbarkeit ist ein Sicherheitsdienst, der zum Schutz von kommunizierenden Subjekten eine Evidenz ihrer Identifikationsdaten verwendet. Falls eines der Subjekte seine Beteiligung an der Kommunikation verweigert, kann diese Kommunikation eindeutig nachgewiesen werden, wenn er auch nur teilweise daran teilnahm.

- Der Datenschutz ist ein Sicherheitsdienst, der einer Person erlaubt, zu kontrollieren, welche Informationen über sie erfasst werden und wie und von wem sie genutzt werden.

1.4 Sicherheitsmechanismen

Ein Sicherheitsmechanismus ist ein Prozess, der Sicherheitsdienste aufgrund eines hardwarebasierten (technischen), softwarebasierten (logischen), physischen oder administrativen Verfahrens realisiert. Sicherheitsmechanismen unterstützen Sicherheitsdienste und führen spezifische Aktivitäten zum Schutz gegen Angriffe oder Auswirkungen der Angriffe aus.

Sicherheitsmechanismen werden in Mechanismen für eine spezifische Protokollschicht des **OSI**-Modells (engl. *Open System Interconnection*) und Mechanismen für alle Protokollschichten und Sicherheitsdienste aufgeteilt. Es folgen einige Beispiele der Sicherheitsmechanismen:

- Die Verschlüsselung schützt den Informationsgehalt einer Nachricht mittels mathematischer Algorithmen, die Daten in eine Form transformieren, die von unbefugten Subjekten nicht gelesen werden kann.
- Eine digitale Signatur ist ein Mechanismus, der kryptographische Transformation einer Dateneinheit zum Beweisen ihrer Quelle und Integrität und zum Schutz gegen Fälschung verwendet wird.
- Die Zugriffskontrolle bietet eine Vielfalt von Mechanismen, die Zugriffsrechte zu Ressourcen definieren, und umfasst Autorisierung des Zugriffs auf Ressourcen.
- Die Datenintegrität schließt Mechanismen ein, die Integrität einer Dateneinheit oder eines Datenstroms sicherstellen.
- Der Austausch von Authentifizierungsinformationen (engl. *authentication exchange*) ist ein Mechanismus, der die Identität eines Subjektes durch den Austausch von Informationen verifiziert.
- Traffic-Padding ist ein Mechanismus, der Bits in Lücken innerhalb eines Datenflusses ergänzt, um die Verkehrsanalyse zu verhindern.
- Die Routing-Kontrolle (engl. *routing control*) erlaubt eine Auswahl von spezifischen physisch sicheren Strecken für die Übertragung sensibler Daten und Änderung der schon ausgewählten Strecke, vor allem wenn eine Sicherheitsverletzung befürchtet wird. Dieser Mechanismus schließt auch die Perimetersicherung ein.
- Die Beglaubigung ist ein Mechanismus, der durch eine zuverlässige Dritte bestimmte Eigenschaften des Datentauschens gewährleistet.
- Die Perimetersicherung (engl. *perimeter security*) ist ein Mechanismus, der einen Empfang oder eine Ablehnung der Daten aus einer spezifischen, sich außerhalb des lokalen Netzwerkes befindenden Adresse oder Dienstleistung (oder daran) erlaubt.

1.5 Klassifikation der Angreifer

Sicherheitslücken (engl. *security threat*) werden von Angreifern ausgenutzt, die nach ihren Fähigkeiten und Aktivität aufgeteilt werden können. Nach diesen Attributen können die folgenden Charakteristiken der Angreifertypen definiert werden.

Fähigkeiten – Die Fähigkeiten eines Angreifers werden typischerweise von den folgenden Faktoren bestimmt:

- **Kosten**
    - Es handelt sich um Kosten, die vom Angreifer für einen erfolgreichen Angriff z. B. für Anlagen ausgegeben werden müssen. Diese Anlagen können extrem billig (Lötkolben und ein Paar Kabel) oder unerschwinglich (erstklassige Halbleiter-Testeinrichtung) sein.
- **Kenntnisse**
    - Allgemein handelt es sich um Wissen, das der Angreifer für einen erfolgreichen Angriff braucht. Einige Angriffe können von einem instruierten Kind realisiert werden, wobei andere Angriffe umfangreiche Kenntnisse über die konkrete Anwendung im Netzwerk oder eine Person erfordern, welche spezielle Einrichtungen verwenden kann. (Dies kann auch als Kosten betrachtet werden.)
- **Spuren**
    - Es handelt sich um Spuren, die nach dem Angriff hinterlassen wurden. Falls der Knoten nach dem Angriff in demselben Zustand wie vor dem Angriff ist, einschließlich eines unveränderten Speicherinhaltes, wird der Angriff schwieriger erkannt, im Vergleich mit einem Angriff, der die physische Zerstörung des Knotens verursacht.

Aktivität – Die Angreifer können allgemein als aktiv oder passiv klassifiziert werden:

- Passive Angriffe
    - Sie erhalten Informationen vom Netzwerk nur durch Überwachung der Kommunikation. Sie umfassen Verkehrsanalyse, Überwachung einer ungesicherten Kommunikation, Entschlüsselung von schwach verschlüsselten Informationen und Abfangen von Authentifizierungsinformationen (z. B. Passwörter).

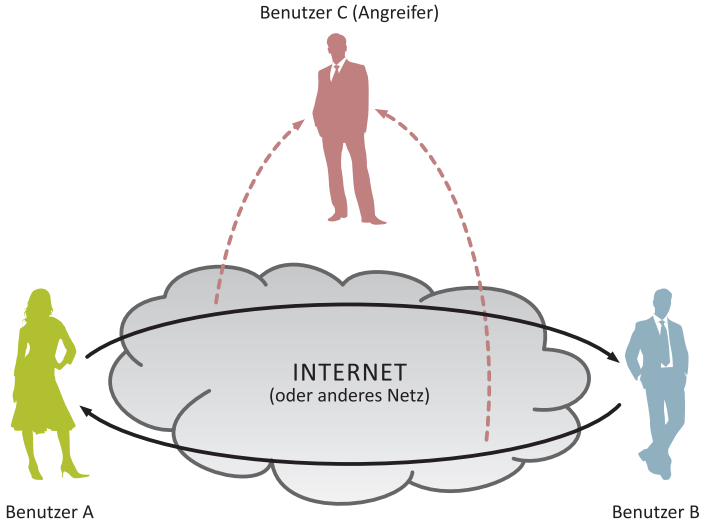

Abb. 1.1 – Passiver Angriff

- Aktive Angriffe
  - Sie zielen auf Änderung der Systemressourcen (einschließlich Daten) oder Beeinflussung ihres Betriebes. Sie umfassen Einspeisung, Modifizierung oder Sperren von Netzwerkpaketen und Manipulation mit kommunizierenden Geräten. Manchmal stellen passive Angriffe eine Vorbereitung auf aktive Angriffe dar.

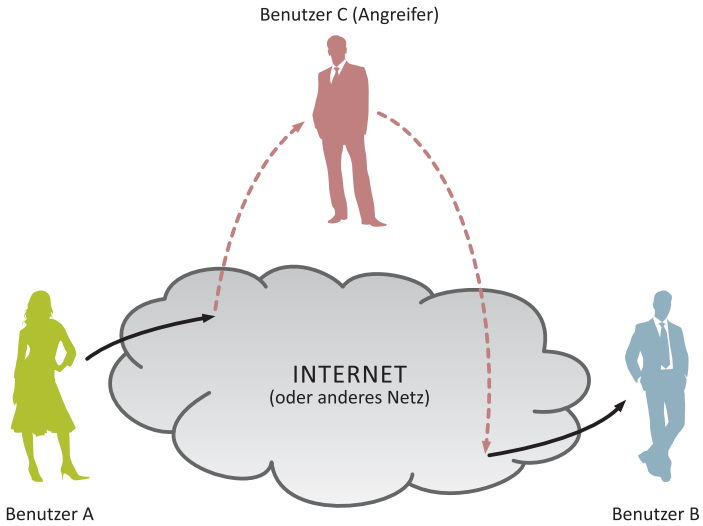

Abb. 1.2 – Aktiver Angriff

Weiter können Angriffe in nicht-invasive, semi-invasive und invasive Angriffe aufgeteilt werden:

- Nicht-invasive Angriffe manipulieren Geräte nicht.

- Semi-invasive Angriffe manipulieren die Verpackung des Gerätes, gelangen jedoch in keinen direkten elektrischen Kontakt mit der Oberfläche des Chips.
- Invasive Angriffe haben praktisch keine Begrenzungen was die Maßnahmen betrifft, die zum Erhalten der Informationen vom Gerät getroffen werden können (z. B. Teststation).

Es soll angemerkt werden, dass nicht alle semi-invasiven oder invasiven Angriffe aktive Angriffe darstellen. Beispielsweise können passive semi-invasive Angriffe versuchen, sensible Daten aus Speicherkomponenten nur zu laden, und passive invasive Angriffe können eine Teststation zum Erkennen der Signale der wertvollen Daten verwenden. Typische Beispiele der passiven Angriffe sind Verkehrsanalyse und Camouflage. Die meisten Angriffe sind jedoch aktive Angriffe, wie zum Beispiel Routing-Angriffe, Spoofing, DoS, Man-in-the-Middle, Abhören, Knotenreplikation, physische Angriffe.

Klasse. Um sowohl Fähigkeiten und Aktivität zu beurteilen, führte IBM die folgende Taxonomie der Klassen der Angreifer ein:

- Klasse I (intelligente Außenseiter - engl. *clever outsiders*) - Diese Angreifer sind oft sehr intelligent, aber besitzen eine ungenügende Kenntnis des Systems. Sie verwenden nicht so entwickelte Einrichtungen. Sie versuchen, eine bestehende Schwachstelle des Systems auszunutzen, nicht eine neue zu schaffen.
- Klasse II (kenntnisreiche Insider - engl. *knowledgeable insiders*) - Die Angreifer dieser Klasse besitzen umfangreiche spezialisierte technische Ausbildung und Erfahrung. Sie können Systemkomponenten unterschiedlich gut kennen, aber haben einen potentiellen Zugriff auf die meisten Komponenten. Oft haben sie hochentwickelte Tools und Mittel für eine detailliertere Analyse.
- Klasse III (finanzierte Organisation - engl. *funded organizations*) – Bei den Angreifern dieser Klasse handelt es sich um Teams von Spezialisten mit verwandten und komplementären Fähigkeiten, die über große finanzielle Mittel verfügen. Sie können das System gründlich analysieren und raffinierte Angriffe mittels fortgeschrittener Analyseinstrumente vorbereiten. Sie können auch Angreifer der Klasse II als ein Teil des Angriffssystems verwenden.

1.6 Terminologie

Es ist leider nicht möglich, ein komplettes sicherheitsbezogenes Wörterbuch in dieses Kapitel einzufügen. Hier werden daher nur einige grundlegende Begriffe vorgestellt, die im Bereich der Netzwerk- und Computersicherheit verwendet werden:

- Ein Angriff ist im Kontext der Computer- und Netzwerksicherheit ein Versuch, Zugriff auf Ressourcen eines Computers oder Netzwerkes ohne Autorisierung zu erlangen oder eingestellte Sicherheitsmaßnahmen zu umgehen.

- Ein Audit ist der Prozess der Überwachung der sicherheitsrelevanten Ereignisse, wie Einloggen ins System oder Netzwerk, Zugriff auf Objekte, Geltendmachung von Benutzer-/Gruppenrechten.

- Ein Aussetzen (engl. *exposure*) ist ein Ausmaß, wie ein Netzwerk oder Computer aufgrund seiner Verwundbarkeiten angreifbar ist, wie lange die Eindringlinge angreifen können und wie viel davon den Hackern bekannt ist.

- Eine Bedrohung ist eine potentielle Gefahr für Daten oder Systeme. Es kann sich um ein Virus, einen Hacker, ein Naturereignis (z. B. Tornado), einen verärgerten Mitarbeiter, einen Konkurrenten oder weiteren Gefahren handeln.

- Ein Cracker ist ein Hacker, der sich auf Knacken oder Herausfinden von Passwörtern eines Systems spezialisiert, um auf Rechnersysteme ohne Autorisierung zugreifen zu können.

- Ein DoS-Angriff ist eine vorsätzliche Aktion, die einem Rechner oder einem Netzwerk seine geplante Funktion verhindert (beispielsweise hindert sie den Benutzern am Einloggen ins Netzwerk).

- Gegenmaßnahmen sind Schritte zur Vorbeugung eines Angriffes oder schädlichen Codes oder in Reaktion darauf.

- Ein Hacker ist eine Person, die sich mit Computerprogrammierung und Betriebssystemen detailliert beschäftigt, um die Grenzen ihrer Fähigkeiten zu testen und ihre Verwundbarkeiten zu identifizieren.

- Ein Puffer (engl. *buffer*) ist ein Speicher für Zwischenlagerung von Daten.

- Ein Risiko ist die Wahrscheinlichkeit, dass eine bestimmte Sicherheitslücke durch Ausnutzung einer Systemverwundbarkeit zu Schaden, Datenverlust oder anderen unerwünschten Ergebnissen führen wird. Das bedeutet, dass ein Risiko die Summe der Lücke und der Verwundbarkeit ist.

- Das Risikomanagement ist der Prozess der Identifikation, Kontrolle und Minimierung oder kompletten Beseitigung von Ereignissen, die eine Lücke in Systemzuverlässigkeit, Datenintegrität und Datenvertraulichkeit darstellen.

- Ein schädlicher Code (Malware) ist ein Computerprogramm oder Script, das eine Aktivität ausführt, die ein System oder Daten vorsätzlich beschädigt, einen

unautorisierten Zugriff aufs System ermöglicht oder einem anderen unbefugten Zweck dient.

- Ein Sniffer ist ein Programm, das Daten im Netzwerk abfängt. Häufig wird es auch als Paketschnüffler (engl. *Packet Sniffer*) bezeichnet.

- Ein Trojaner ist ein Computerprogramm, das auf den ersten Blick erwünschte Funktion ausübt, aber enthält einen verdeckten Code, der unbefugte Erfassung, Modifizierung oder Zerstörung von Daten ermöglicht.

- Ein Überlauf des Puffers ist ein Verfahren, wie ein System zum Absturz gebracht werden kann, indem mehr Daten in den Puffer geschrieben werden, als die Kapazität es erlaubt.

- Eine Verletzung ist ein erfolgreiches Umgehen von Sicherheitsmaßnahmen mit dem Ziel, einen Zugriff auf Daten oder Ressourcen ohne Autorisierung zu erwerben, Daten oder Ressourcen für Unbefugte verfügbar zu machen oder Dateien zu löschen oder zu modifizieren.

- Eine Verwundbarkeit ist eine Schwachstelle in der Hard- oder Software oder sogar in dem Sicherheitsplan, die das System oder das Netzwerk für Bedrohungen des unbefugten Zugriffs auf Daten, ihrer Beschädigung oder Zerstörung offen lässt.

- Ein Virus ist ein Programm, das in ein System oder Netzwerk eingeführt wird, um unautorisierte Aktionen durchzuführen. Diese Aktionen können von einem Pop-up mit einer harmlosen Nachricht bis zu der Zerstörung aller Daten auf der Festplatte reichen.

- Ein Wurm ist ein selbstreplizierendes Programm, das sich von einem Gerät zu einem anderen im Netzwerk ausbreitet.

- Die Zuverlässigkeit ist die Wahrscheinlichkeit, dass ein Computersystem oder Netzwerk für eine bestimmte Zeit unter normalen Betriebsbedingungen weiter befriedigend funktioniert.

2 2 Bedrohungen der Netzwerksicherheit

Wo auch immer es ein Netzwerk gibt, gibt es auch Bedrohungen. Die Typen der potentiellen Bedrohungen der Netzwerksicherheit entwickeln sich kontinuierlich. Für alle Netzwerkadministratoren sollte eine konstante Überwachung und Sicherheit des Computernetzwerkes die oberste Priorität besitzen. Eine Beeinträchtigung der Netzwerksicherheit kann schwerwiegende Folgen haben, wie der Verlust der Privatsphäre oder ein Informationsdiebstahl.

Nicht alle Bedrohungen der Sicherheit müssen vorsätzlich sein. Nicht beabsichtigte Bedrohungen werden üblicherweise von Mitarbeitern verursacht, die im Bereich Computer ungeschult sind und Sicherheitslücken oder Verwundbarkeiten nicht kennen. Solche Fehler und Unterlassungen können Verlust, Beschädigung oder Modifizierung von wertvollen Daten hervorrufen. Nicht beabsichtigte Bedrohungen schließen auch Naturkatastrophen ein. In diesem Kapitel werden nur vorsätzliche Bedrohungen behandelt.

Vorsätzliche Bedrohungen können entweder interne Angriffe durch bösartige Mitarbeiter oder externe Angriffe durch andere Personen sein, die der Organisation schaden möchten. Die gefährlichsten Angreifer sind üblicherweise Insider (oder ehemalige Insider), weil sie viel über interne Codes und Sicherheitsmaßnahmen wissen.

Die Tools und Verfahren der Netzwerkangriffe haben sich weiterentwickelt. In der Vergangenheit brauchte ein Hacker einen guten Computer und Programmierer- und Netzwerkkenntnisse, um rudimentäre Tools für einfache Angriffe ausnutzen zu können. Heutzutage haben sich die Möglichkeiten der Hacker, ihre Verfahren und Tools ungemein verbessert und Hacker brauchen auch nicht mehr solche detaillierte Kenntnisse. Daher können zurzeit auch Leute Cyberattacken durchführen, die vorher keine Chance hatten.

Die Definition des Begriffes „Hacker“ änderte sich im Laufe der Zeit. Vorher wurde unter dem Begriff Hacker jede Person eingestuft, die Gefallen daran fand, das Meiste von ihrem System zu bekommen. Jetzt werden als Hacker Personen bezeichnet, die entweder in Systeme unbefugt einbrechen oder Grenzen der Systeme illegitim und absichtlich überschreiten. Der korrekte Begriff für eine Person, die in Systeme einbricht, ist „Cracker“. Üblicherweise wird der Zugriff auf ein System wie folgt durchgeführt: Knacken von Passwörtern, Ausnutzen der bekannten Sicherheitsschwachstellen, Netzwerk-Spoofing und Social-Engineering.

Es gibt eine Kommunikationslücke zwischen Entwicklern der Sicherheitstechnologien und Entwicklern der Netzwerke. Obwohl die Netzwerksicherheit eine entscheidende Anforderung für Netzwerke ist, sind Sicherheitsverfahren nicht leicht implementierbar. Im Unterschied zum Entwerfen der Netzwerke an sich ist die Durchsetzung der Sicherheit nicht so einfach möglich. Es gibt keine Methodologie für die komplexen Sicherheitsanforderungen.

Viele Bedrohungen der Netzwerksicherheit entstehen heutzutage im Internet. An dieser Stelle ist darauf hinzuweisen, dass Smartphone-Terminals zu integralen Bestandteil des Internets wurden. Für die Definition des Schutzes in dieser Umgebung kann eine detaillierte Analyse ihrer Eigenschaften und des menschlichen Verhaltens verwendet werden.

2.1 Malware: Viren, Würmer, Trojaner und Zombies

Bösartige Software oder Malware (vom englischen *malicious software*) ist eine Software, die zum Eindringen oder Beschädigen eines Computersystems ohne die Genehmigung des Inhabers entwickelt wurde. Sie kann Verluste oder Schäden im System verursachen. Eine breite Klasse von Malware stellen Computerviren dar, die sich auf Computern ausbreiten und schädliche Operationen ausführen.

Die Ausführung der Malware kann Störungen der Computeroperationen verursachen. Darüber hinaus kann sie auch das Erfassen von sensiblen Informationen oder den unbefugten Zugriff auf Computersysteme zur Folge haben. Malware ist keine fehlerhafte Software - eine fehlerhafte Software hat einen legitimen Zweck, aber hat schädliche Bugs, die vor dem Release nicht gemerkt wurden. Weitere Untermengen der Malware schaffen z. B. Würmer, Trojaner, Adware, Spyware und Rootkits.

Gemäß einer Analyse von PandaLabs wurden im Jahre 2014 mehr als 75 Million neuer Malware-Muster identifiziert, was 34 % der bisher bekannten Malware darstellt. Im Vergleich mit 2013 ist diese Nummer um mehr als das Zweifache gestiegen. Unten werden die bekanntesten Kategorien der Malware beschrieben.

- Viren sind selbstreplizierende Programme, die zu ihrer Verbreitung infizierte Dateien verwenden. Sobald die infizierte Datei geöffnet ist, wird das Virus im System aktiviert.

- Ein Wurm (engl. *worm*) ähnelt einem Virus, weil beide selbstreplizierend sind, der Wurm braucht jedoch keine weiteren Dateien für seine Verbreitung. Der Hauptzweck von Würmern ist ihre Replikation. Diese Programme wurden ursprünglich für legitime Zwecke im Netzwerkmanagement verwendet, aber ihre Fähigkeit der Vervielfachung wurde von Hackern schnell ausgenutzt, um schädliche Würmer zu erzeugen, die auch Schwachstellen von Betriebssystemen ausnutzen und weitere schädliche Aktionen ausüben können. Es gibt zwei Haupttypen von Würmern: Massen-Mail- und netzwerkaktive Würmer. Massen-Mail-Würmer verwenden E-Mails als ein Mittel des Infizierens weiterer Computer. Ein netzwerkaktiver Wurm wählt sich ein Ziel und sobald er diesen Zielhost erreicht, kann er ihn mittels eines Trojaners oder auf andere Art und Weise infizieren.

- Trojaner (engl. *Trojan*) sind auf den ersten Blick gutartige Programme, aber sie führen Aktionen aus, die vom Benutzer des Programms nicht beabsichtigt wurden oder denen er sich nicht bewusst war. Im Prinzip können Trojaner alles im System ausführen, was auch der Benutzer darf. Daher sind Trojaner besonders gefährlich, wenn der nichtsahnende Benutzer, der sie installiert hat, ein Administrator ist und Zugriff auf Systemdateien hat. Trojaner breiten typischerweise Ransomware aus. Es handelt sich um Malware, die ein Computersystem infiziert, den Zugriff auf den Computer beschränkt und Lösegeld für Beseitigung der Beschränkung fordert.

- Ein Zombie ist eine schädliche Software, die sich im Netzwerk ausbreitet. Nachdem er erfolgreich in ein Computersystem eingedrungen ist, kann der infizierte Computer fern gesteuert und verwaltet werden. Wenn mit dem gleichen Typ von Zombies mehrere Rechner infiziert werden, wird diese Struktur als Botnetz bezeichnet. Botnets können von einem entfernten Computer kontrolliert werden und die gleichen Befehle von den infizierten Rechnern ausüben lassen. Dadurch werden **DDoS**-Angriffe (*verteilte Dienstverweigerung*, engl. *Distributed Denial of Service*) ermöglicht.

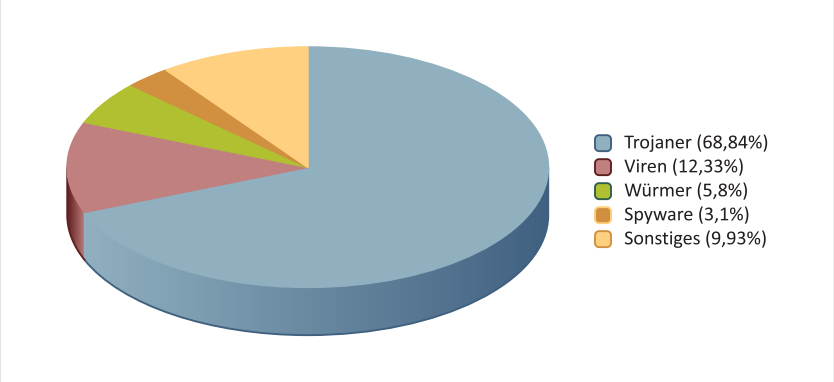

Abb. 2.1 – Typen der neuen Malware, die 2014 entwickelt wurden

2.2 Spyware, Adware

Der Begriff Adware bezieht sich auf Software, die Werbung anzeigt und in einer anderen Anwendung integriert ist.

Es handelt sich um eine legitime Alternative für Benutzer, die die lizenzierte Software nicht bezahlen möchten. Es gibt viele werbefinanzierte Programme, Spiele und Dienstprogramme, die als Adware (oder Freeware) distribuiert werden. Heutzutage steigt die Nummer der Softwareentwickler, die ihre Produkte als „gesponserte“ Freeware (Adware) anbieten.

Bei einer legitimen Adware verschwindet die Werbung, wenn der Benutzer die Software nicht mehr startet, und der Benutzer hat immer die Möglichkeit, die Werbung durch Kauf des Registrierschlüssels auszuschalten.

Spyware ist ein allgemeiner Begriff für eine Software, welche über das Internet auf einem Computer ohne eine Genehmigung des Benutzers installiert wurde und welche verschiedene Aktionen ausführt, wie Werbung, Erfassung von Surfgewohnheiten oder Änderung der Computerkonfiguration.

Die gesammelten Informationen können via Internet als eine verdeckte Nebenwirkung eines Programms an einen Server gesendet und für verschiedene Zwecke erfasst werden. Eine typische Taktik umfasst unaufgeforderte Pop-up-Werbung, Diebstahl von persönlichen Informationen (z. B. Passwörter zu online Konten, Kreditkartennummern), Überwachung des Browsens im Internet für Marketingzwecke und Weiterleitung der HTTP-Anforderungen an Werbeseiten.

Spyware kann zusammen mit weiterer Software oder als Folge einer Virusinfektion installiert werden. Bei einigen Infektionen ist die Anwesenheit der Spyware vor dem Benutzer versteckt. Spyware wird auch so entworfen, dass sie nicht nur schwierig beseitigt, sondern auch nicht erkannt werden kann. Andere Typen der Spyware ändern die Einstellung des Computers, was störend sein kann und Verzögerung oder Crash verursachen kann.

Benutzer merken dann ein unerwünschtes Verfahren und Verschlechterung der Systemleistung. Spyware kann auch eine erhöhte CPU-Aktivität, Festplattengebrauch und Netzwerkverkehr verursachen.

Anti-Spyware-Programme können einen Echtzeitschutz bieten oder regelmäßig den Computer scannen. In dem ersten Fall scannen sie alle eingehenden Netzwerkdaten und können wie Antivirensoftware Bedrohungen blockieren. Im zweiten Fall können sie nur zur Erkennung und Beseitigung der schon installierten Spyware verwendet werden.

2.3 Zero-Day-Verwundbarkeiten, Zero-Day-Angriffe

Es gibt einige bekannte, jedoch leicht unterschiedliche Definitionen der Zero-Day-Verwundbarkeiten. Gemäß einer Definition können unter diesem Begriff Softwarefehler verstanden werden, welche offen für Cyberangriffe ist, bevor ein Patch verfügbar oder eine Zwischenlösung veröffentlicht wird. Dabei ist die Verwundbarkeit nicht bekannt, mit der Ausnahme des Angreifers (oder Verkäufers der Zero-Day-Möglichkeiten auf dem Schwarzmarkt). Eine andere Definition sieht sie als Sicherheitsverwundbarkeiten, die am sog. nullten Tag öffentlich und damit bekannt werden. Der Softwarehersteller kennt die Lücke, hat aber noch keinen Bugfix herausgegeben.

Diese Angriffe werden selten entdeckt - es kann Tage, Monate oder Jahre dauern, bis der Entwickler die Verwundbarkeit findet, die den Angriff ermöglichte.

Auf jedem Fall werden Benutzer dabei dem Angriff ausgesetzt. Als L. Bilge und T. Dumitras in [5] konstatieren: „Solange die Verwundbarkeit unbekannt ist, kann die gegebene Software nicht korrigiert werden und Antivirensoftware kann den Angriff mittels Scanning der Signaturen nicht erkennen.“ Diese Verwundbarkeiten können von Crackern, Sicherheitsfirmen, Forschern, Softwareherstellern oder von Benutzern entdeckt werden. Wenn sie von Crackern entdeckt werden, wird die Ausnutzung so lange wie möglich geheim gehalten und nur unter Crackern/Hackern verteilt, bis die Software- oder Sicherheitsfirmen diese Angriffe erkennen bzw. entdecken.

Abb. 2.2 – Verwundbarkeitsintervall eines Zero-Day-Angriffes

Die Zero-Day-Angriffe gehören zu den destruktivsten und berühmtesten Angriffen der letzten Jahre. Zum Beispiel die Operation Aurora (2009) nutzte die Verwundbarkeit des Internet Explorer mit mehr als 20 Zielen einschließlich Morgan Stanley, Google, Yahoo, Dow Chemical, Adobe Systems, Juniper Networks und sogar Software für Sicherheitsfirma wie Symantec aus.

Vielleicht der berühmteste Zero-Day-Angriff war Stuxnet (2010). Tatsächlich verwendete der Stuxnet-Wurm vier unabhängige Zero-Day-Möglichkeiten, um Industrieregler zu beschädigen und Urananreicherungsanlagen im iranischen Natanz zu zerstören. Stuxnet wurde für die Manipulation der industriellen speicherprogrammierbaren Steuerung der deutschen Firma Siemens entworfen, welche die Geschwindigkeit der Zentrifugen regeln und überwachen. Die Angreifer

konnten die Geräte nicht fernsteuern, weil die Computer nicht ans Internet angeschlossen waren. Daher basierte die Attacke auf infizierten USB-Massenspeichern. Zuerst infizierten sie Computer von fünf externen Firmen, die irgendwie mit dem nuklearen Programm verbunden sein sollten. Die Ausnutzung von vier Zero-Day-Verwundbarkeiten ist außergewöhnlich und unikal für diese Bedrohung. Darüber hinaus verwendet Stuxnet auch eine Reihe weiterer Verwundbarkeiten, womit eine große Erfahrung in Methodik und Planung dieses Angriffes bewiesen wurde.

2.4 Scanning, Spoofing, Identitätsdiebstahl

Im Kontext dieses Moduls bezieht sich der Begriff Scanner auf ein Hacker-Softwareprogramm, das eventuelle Verwundbarkeiten eines Systems von einer entfernten Stelle bestimmt.

Auch Administratoren verwenden Scanner, um Verwundbarkeiten ihrer Systeme zu erkennen und zu korrigieren, bevor ein Eindringling sie findet. Viele Scanner sind als Freeware im Internet verfügbar.

Ein guter Scanner kann einen (für Angriff offenen) Computer im Internet finden, seine TCP/IP-Dienste ermitteln und sie auf Sicherheitsschwachstellen testen.

Unter einem Spoofing-Angriff versteht man eine Handlung, bei der sich ein Angreifer als ein anderes Gerät oder Benutzer im Netzwerk ausgibt.

Es gibt einige Typen von Spoofing-Angriffen: E-Mail-Spoofing, IP-Spoofing, ARP-Spoofing, DNS-Spoofing usw.

Ein E-Mail-Spoofing umfasst das Absenden von Nachrichten von einer gefälschten E-Mail-Adresse oder Fälschen der E-Mail-Adresse eines anderen Benutzers. Die meisten E-Mail-Server haben integrierte Sicherheitselemente, die Senden von unautorisierten Benutzern verhindern. Man kann trotzdem eine E-Mail von einer Adresse bekommen, die keine tatsächliche Adresse der Person ist, die die Nachricht geschickt hat.

Bei einem IP-Spoofing sendet der Angreifer IP-Pakete von einer falschen („gespooften") Quellenadresse, um seine Identität zu maskieren. Die Nachricht kommt von einem Computer, aber als Quellenadresse wird eine andere Adresse eines zuverlässigen Computers verwendet.

Es stehen viele Tools und Verfahren zur Verfügung, mit denen die Firmen die Bedrohung der Spoofing-Angriffe mindern können. Zur Vermeidung von Spoofing-Angriffen werden Paketfilter, Software zur Erkennung von Spoofing und kryptographische Netzwerkprotokolle eingesetzt.

2.5 DoS- und DDoS-Angriffe

Wie in [8] detailliert behandelt wird: „**DoS**-Angriffe stellen eine der beliebtesten Angriffsarten der Internethacker dar, um Netzwerkoperationen zu stören. Obwohl sie im Gegenteil zu anderen Angriffsarten Daten weder zerstören noch stehlen, ihr Ziel ist es, den Absturz des Netzwerkes zu veranlassen und Dienstleistungen den legitimen Benutzern zu blockieren. DoS-Angriffe können leicht gestartet werden - auf Hacker-Webseiten ist die Software verfügbar, die es jedem ermöglicht, einen DoS-Angriff mit geringen technischen Kenntnissen zu starten.“

Bei diesen Angriffen empfängt das System so viele Anfragen, dass es nicht imstande ist, auf die Kommunikation gemäß den Anforderungen zu antworten. Das System verbraucht dann Ressourcen für das Warten auf den sog. Handshake. Schließlich kann das System auf keine weiteren Anfragen antworten und hört auf, zu funktionieren.

DDoS-Angriffe verwenden vermittelnde Computer (Agenten), die häufig mit Trojanern infiziert wurden. Diese Systeme schaffen ein Botnetz, das zum DoS-Angriff auf ein anderes System eingesetzt wird.

Der Unterschied zwischen einem klassischen DoS-Angriff und einem DDoS-Angriff liegt in der Verwendung von Botnetzen mit vielen Computern (einigen hundert oder sogar tausend) und vielen Internetanschlüssen, die häufig in DDoS global verteilt werden.

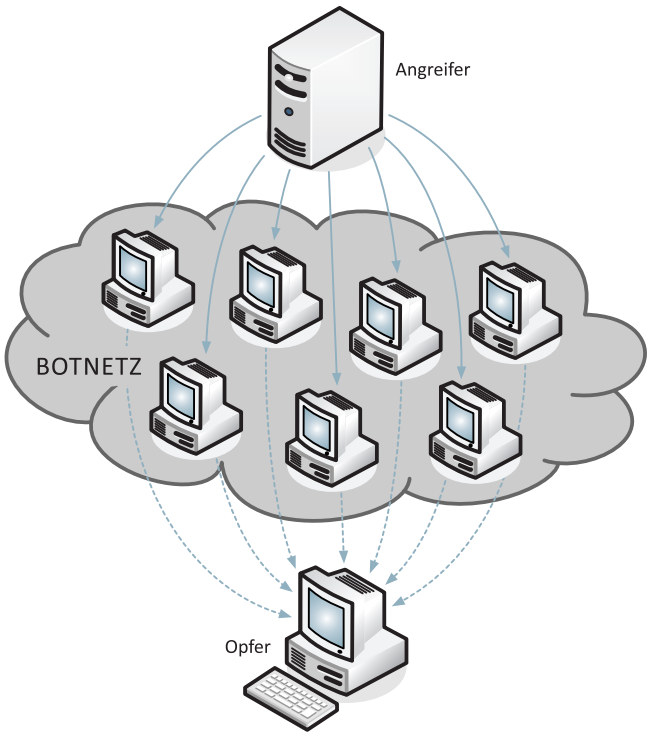

Abb. 2.3 – Schema eines DDoS-Angriffes

Der Angreifer aktiviert diese Trojaner von einem entfernten Standort und veranlasst einen gleichzeitigen Angriff der vermittelnden Computer. Wegen dieses Mechanismus ist es unmöglich, sich gegen den Angriff durch Blockieren einer einzigen IP-Adresse zu verteidigen, weil der Angriff von Computern stammt, die in Netzwerken der ganzen Welt verteilt sein können. Außerdem ist es sehr schwierig, den legitimen Benutzerverkehr vom angreifenden Verkehr zu unterscheiden, wenn er über so viele Quellen verbreitet wird.

Man soll sich bewusst sein, dass DDoS-Angriffe eine Bedrohung in zwei Schichten darstellen. Einerseits kann ein Netzwerk ein Ziel des DoS-Angriffes sein, welcher seine Server abstürzen lässt und jeden ein- und abgehenden Verkehr verhindert, und andererseits können seine Computer als Vermittler des DoS-Angriffes gegen andere Netzwerke zum Einsatz kommen.

DDoS-Angriffe können in volumengesteuerte Angriffe, Protokollangriffe und Anwendungsschicht-Angriffe gemäß dem Ziel des Angriffes aufgeteilt werden. In dem ersten Fall soll die Bandbreite des Netzwerkes saturiert werden, in dem zweiten die Ressourcen des Servers oder der vermittelnden Kommunikationsgeräte verbraucht werden und in dem dritten der Anwendungsserver zum Absturz gebracht werden.

2.6 Social-Engineering-Angriffe

Unter Social Engineering versteht man das Sammeln von vertraulichen Informationen durch menschliche Interaktion.

Die Typen der Informationen, welche Hacker erlangen möchten, können unterschiedlich sein, wenn aber Einzelpersonen angegriffen werden, möchten Hacker üblicherweise ihre Passwörter, ihre Bankinformationen oder Zugriff auf ihren Computer, um dort Malware zu installieren.

Im Unterschied zu weiteren Angriffstypen beziehen sich Social-Engineering-Angriffe nicht auf eine technologische Manipulation mit Verwundbarkeiten der Computerhardware oder -software und benötigen keine tiefen technischen Kenntnisse. Stattdessen werden dabei menschliche Schwachstellen ausgenutzt, wie Fahrlässigkeit oder Kollegialität, um Zugriff auf legitime Anmeldedaten des Netzwerkes zu erhalten. Die für einen solchen Eindringling nützlichste Eigenschaft ist Geschick im Umgang mit Menschen, wie eine charmante oder überzeugende Persönlichkeit oder dominierendes, autoritatives Auftreten.

Als das schwächste Glied in der Sicherheitskette wird von vielen Sicherheitsanalytikern der Faktor Menschen betrachtet. Ein üblicher Social-Engineering-Angriff umfasst eine E-Mail von einem „Freund“ mit einem Link oder einer herunterladbaren Datei (mit integrierter Malware) oder Bitte um Hilfe, Phishing oder Baiting.

3 3 Komponenten des Netzwerksicherheitssystems

Zur Senkung der Verwundbarkeit eines Computers stehen viele Produkte zur Verfügung. Um alle Bereiche des Netzwerkes zu schützen, können sich Firmen aus vielen Technologien wählen, die von Antivirensoftware zu einer spezialisierten Netzwerksicherheitshardware reichen, wie z. B. Firewalls und Angrifferkennungssysteme (**IDS**, engl. *Intrusion Detection System*).

Keine Lösung schützt jedoch das System gegen alle Bedrohungen. Ein Netzwerksicherheitssystem besteht üblicherweise aus vielen Komponenten. Idealerweise arbeiten alle Komponenten zusammen und wenn eine ausfällt, erhalten andere Komponenten die Sicherheit aufrecht. Diese Komponenten können mittels Hard- und/oder Software realisiert werden. Die Software muss ständig aktualisiert werden, so dass neue Bedrohungen auch abgewehrt werden.

Firmen verwenden heutzutage eine Kombination von Firewalls, IDS, Verschlüsselung und Authentifizierungsmechanismen, um „Intranets“ zu erzeugen, die ans Internet angeschlossen sind, aber zugleich geschützt werden. Intranet ist ein privates Computernetzwerk, das Internetprotokolle verwendet. Intranets begrenzen sich in der Regel auf die Computer einer Firma, wobei über Extranets auch Kunden, Lieferanten oder weitere freigegebene Subjekte Zugriff bekommen können.

3.1 Antiviren- und Antispyware-Software

Viren, Würmer und Trojaner sind Beispiele von Malware. Dagegen gibt es spezielle Anti-Malware-Tools, die zur Vorbeugung, Erkennung und Beseitigung von Malware dienen. Sie werden fast mit allen Rechnern mitgeliefert und können den meisten Virenbedrohungen entgegenwirken, unter der Voraussetzung, dass sie regelmäßig aktualisiert und ordnungsgemäß gewartet werden, andernfalls können sie den Schutz gegen neue Viren nicht leisten.

Die Antiviren-Branche baut auf ein riesiges Netzwerk von Benutzern, die über neue Viren früh berichten, so dass Antidote schnell vorbereitet und verteilt werden können. Weil einige tausend neue Viren jeden Monat erzeugt werden, muss die Virendatenbank ständig aktualisiert werden. Sie hilft bei der Identifikation der bekannten Viren, wenn sie versuchen anzugreifen. Namhafte Hersteller der Antivirensoftware veröffentlichen die neuesten Antidote auf ihren Webseiten und die Software selbst weist die Benutzer auf periodische Aktualisierung hin. Die Grundsätze der Netzwerksicherheit sollen festlegen, dass alle Computer im Netzwerk regelmäßig aktualisiert werden und idealerweise von der gleichen Antivirensoftware geschützt werden. So werden Wartungs- und Aktualisierungskosten minimiert. Auch die Antivirensoftware an sich muss aktualisiert werden.

Ohne Hinsicht auf die Nützlichkeit der Antivirensoftware hat sie auch einige Nachteile. Eine Antivirensoftware kann beispielsweise die Computerleistung senken. Für unerfahrene Benutzer können die Aufforderungen und Entscheidungen kompliziert sein. Und eine falsche Entscheidung kann zu einer Sicherheitsverletzung führen.

Wenn ein Computer von Viren gereinigt wird, werden Viren auf unterschiedlichste Art ausgerottet: Beseitigung des Codes in der infizierten Datei, der dem Virus entspricht; Beseitigung der ganzen infizierten Datei oder Stellen der infizierten Datei unter Quarantäne (ihr Verschieben auf eine Stelle, wo sie nicht gestartet werden kann).

Für die oben genannten Verfahren werden üblicherweise verschiedene Methoden verwendet.

Es gibt zum Beispiel die signaturbasierte Erkennung, welche bekannte Muster von Daten in dem ausführbaren Code sucht. Viren vervielfältigen sich durch Infizieren von Hostanwendungen - sie kopieren einen Teil des ausführbaren Codes in ein bestehendes Programm. Sie werden daher so programmiert, dass sie die gleiche Datei nicht mehrmals infizieren. Dafür fügen sie eine Folge von Bytes in die infizierte Anwendung ein und später können sie kontrollieren, ob die gegebene Datei schon infiziert wurde - dieser Prozess wird als Virensignatur bezeichnet. Antivirensoftware erkennt an Hand dieser Signatur das Virus. Diese signaturbasierte Erkennung ist die älteste Methode der Antivirensoftware.

Diese Methode kann keine Viren erkennen, die noch nicht in der Virendatenbank gespeichert sind. Darüber hinaus maskierten die Programmierer von Viren sie häufig, so dass ihre Signatur schwer oder gar nicht erkannt werden kann. Um solchen Bedrohungen entgegenzuwirken, wird Heuristik eingesetzt.

Eins der heuristischen Verfahren verwendet generische Signaturen und kann damit neue Viren oder Varianten der bestehenden Viren identifizieren, durch Suchen der bekannten Malware oder ihrer unbedeutenden Variationen in Dateien. Dieses Verfahren umfasst die Analyse des Verhaltens der Anwendungen, um eine ähnliche Aktivität zu erkennen, die bei einem bekannten Virus auftritt.

Diese Antivirensoftware kann daher Viren erkennen, selbst wenn die Virendatenbank noch nicht aktualisiert wurde.

Andererseits löst sie oft einen falschen Alarm aus.

3.2 Firewall

Eine Firewall ist ein typischer Mechanismus zur Grenzkontrolle oder Verteidigung am Perimeter. Der Zweck einer Firewall besteht in der Vorbeugung eines unbefugten Zugriffs auf das Netzwerk oder vom Netzwerk durch Sperren des unerwünschten Uplink- und Downlink-Verkehrs.

Alle Daten, die ins Netzwerk eingehen oder davon abgehen, werden durch die Firewall geprüft. Darin wird jedes Paket überprüft und diejenigen werden gesperrt, die die eingestellten Sicherheitskriterien nicht bestanden haben. Firewalls können sowohl in Hard- als auch Software, oder in einer Kombination der beiden implementiert werden [8].

Firewalls setzen die Sicherheitsgrundsätze einer Firma durch Begrenzung des Zugriffs auf spezifische Netzwerkressourcen durch. In einer Analogie der physischen Sicherheit kann man sich eine Firewall als Äquivalent des Schlosses an der Außen- oder Innentür eines Gebäudes vorstellen - sie ermöglicht einen Zugang nur den autorisierten Benutzern, d. h. Benutzern mit dem entsprechenden Schlüssel oder Zugangskarte. Firewalls sind auch in Varianten für Heimeinsatz erhältlich. Die Firewall schafft eine schützende Schicht zwischen dem Netzwerk und der Außenwelt. Eigentlich repliziert die Firewall das Netzwerk gleich bei seinem Eingang, so dass sie autorisierte Daten ohne eine erhebliche Verzögerung empfangen und senden kann. Es hat aber integrierte Filter, um das Eindringen von unautorisierten oder möglicherweise gefährlichen Daten in das reale System nicht zu gestatten. Firewalls bieten auch eine wichtige Funktion des Einloggens und Audits. So können Netzwerkadministratoren einen guten Überblick über den Typ/Umfang des Verkehrs, einschließlich der Einbruchversuche, haben.

Das Nationale Institut für Standards und Technologie (**NIST**, *National Institute of Standards and Technology*) 800-41, [9] teilt Firewalls in drei grundlegende Typen auf: Paketfilter, zustandsorientierte Paketüberprüfung und Proxy-Firewall. Diese drei Kategorien sind jedoch nicht voneinander unabhängig und die meisten modernen Firewalls haben Eigenschaften, dank deren sie in mehr als eine der oben angeführten Kategorien angeordnet werden können.

Die Paketfilter-Firewalls sind im Prinzip Routing-Geräte, die Zugriffrechte für Systemadressen und Kommunikationssitzungen verwalten können. Sie können daher auch den Netzwerkverkehr filtern, je nach Charakteristik des Verkehrs. Sie werden normalerweise in den **TCP/IP**-Netzwerkinfrastrukturen eingesetzt. Ihre Stärke stellen Geschwindigkeit und Flexibilität dar und ihre Schwachstelle ist, dass sie nicht fähig sind, Angriffe auf spezifische Verwundbarkeiten der Anwendungen vorzubeugen (weil sie Daten auf oberen Schichten nicht untersuchen).

Die Tabelle 1 zeigt Beispiele des Regelwerks der Paketfilter-Firewall, übernommen von [9]

	Quellenadresse	Quellenport	Zieladresse	Zielport	Aktion	Beschreibung
1	beliebig	beliebig	192.168.1.0	> 1023	erlauben	Erlauben der Rückkehr von TCP-Anschlüssen ins interne Subnetz
2	192.168.1.1	beliebig	beliebig	beliebig	verboten	Verhindern des direkten Anschlusses der Firewall
3	beliebig	beliebig	192.168.1.1	beliebig	verboten	Verhindern des direkten Zugriffs der externen Benutzer auf das Firewallsystem
4	192.168.1.0	beliebig	beliebig	beliebig	erlauben	Erlauben des Zugriffs der internen Benutzer auf externe Server
5	beliebig	beliebig	192.168.1.2	SMTP	erlauben	Erlauben des Sendens der E-Mails von externen Benutzern
6	beliebig	beliebig	192.168.1.3	HTTP	erlauben	Erlauben des Zugriffs der externen Benutzer auf WWW-Server
7	beliebig	beliebig	beliebig	beliebig	verboten	Alles, was vorher nicht erlaubt wurde, wird explizit verboten

Die Firewalls mit der zustandsorientierten Paketüberprüfung, die auch als dynamische Paketfilterung bezeichnet werden, überwachen den Zustand der aktiven Anschlüsse und verwenden diese Information, um zu bestimmen, welche Netzwerkpakete durch die Firewall durchgehen können. Diese Firewalls analysieren die Pakete bis zur Anwendungsschicht. Durch Aufzeichnung der Sitzungsinformationen, wie IP-Adressen und Portnummern, kann die dynamische Paketfilterung ein viel strengeres Sicherheitsausmaß implementieren und durch Überprüfen bestimmter Werte in den Protokollheadern den Zustand jedes Anschlusses für eine gegebene Zeitdauer verfolgen. Die abgehenden Pakete, welche spezifische Typen der eingehenden Pakete erwarten, werden von der Firewall verfolgt und nur den eingehenden Paketen, die eine richtige Antwort darstellen, wird eine Übertragung durch die Firewall erlaubt. Jedes neue Paket wird mit der Zustandstabelle der Firewall verglichen, um einen eventuellen Widerspruch des Paketzustandes mit dem erwarteten Zustand festzustellen. Die traditionellen Firewalls mit einer zustandsorientierten Paketüberprüfung prüfen die Nützlichkeit der Daten der Netzwerkpakete nicht. Sie haben nicht einmal eine ausreichende Intelligenz zum Unterscheiden eines Typs des Webverkehrs von dem anderen (legitime Anwendungen von Angriffen).

Proxy-Firewalls oder Anwendungsgateway-Firewalls stellen eine ziemlich neue Ergänzung der etablierten Sicherheitsumgebung dar. Sie kombinieren die zustandsorientierte Paketüberprüfung mit tiefen Anwendungskontrollen. So wird eine Analyse der Anwendungsschicht-Protokolle, wie HTTP und FTP, und Verfolgung des Verkehrs ermöglicht, um das Verhalten der gutartigen Protokollaktivität mit den beobachteten Ereignissen zu vergleichen und damit Abweichungen (Zeichen eines möglichen Angriffes) zu identifizieren. Dies

ermöglicht der Firewall, den Zugriff aufgrund des Verhaltens der Anwendung im Netzwerk zu erlauben oder zu verbieten.

NGFW (*Next-Generation Firewall*) ist eine integrierte Netzwerkplattform, die eine traditionelle Firewall mit weiteren Netzwerkgeräten mit der Filterfunktionalität, wie Proxy-Firewall, kombiniert. Sie verwendet **DPI** (engl. *Deep Packet Inspection*), Systeme zur Vorbeugung der möglichen Angriffe **IPS** (engl. *Intrusion Prevention System*) und/oder weitere Techniken, wie **SSL**- (engl. *Secure Socket Layer*) und **SSH**-Abhören (engl. *Secure Shell*), Filterung von Webseiten, Management der Dienstgüte (**QoS**, engl. *Quality of Service*) und Bandbreite, Antivirenkontrolle und Integration von Produkten der Dritten (z. B. *Active Directory*) [10]. Diese Techniken stellen eigentlich eine Form der vereinigten Bedrohungsabwehr **UTM** (engl. *Unified Threat Management*) dar. Der Hauptnachteil der NGFW ist, dass sie üblicherweise selbstständige interne Module zur Sicherstellung der einzelnen Sicherheitsfunktionen verwenden. Dann kann ein Paket mehrmals von unterschiedlichen Modulen überprüft werden, bevor es schließlich ins Netzwerk eingehen kann. Diese mehrfache Verarbeitung erhöht die Verzögerung, welche die Netzwerkleistung beeinflussen kann.

3.3 Angrifferkennungssysteme (IDS)

Ein Angrifferkennungssystem (**IDS**, engl. *Intrusion Detection System*) ist eine zusätzliche Schutzmaßnahme, die bei der Abwehr von Computerangriffen hilft, und zwar durch Überwachung des Netzwerkverkehrs, Verwendung von Signaturdatenbanken und durch heuristische Analyse. So werden verdächtige Muster des Einbrechens in ein System oder seiner Beeinträchtigung identifiziert, die einen Angriff andeuten.

IDS-Systeme können Soft- und Hardwaregeräte darstellen. IDS-Produkte dienen zur Überwachung des Anschlusses, um eventuelle Angriffe zu erkennen. Einige IDS-Systeme dienen nur der Überwachung und warnen vor einer Attacke, wobei andere versuchen, sie zu sperren. In der physischen Analogie ähnelt IDS einer Videokamera und einem Bewegungssensor - sie erkennen eine unbefugte oder verdächtige Aktivität und können Wachmänner automatisch warnen, so dass die Aktivität unterbunden wird.

Der Unterschied zwischen IDS und Firewalls besteht darin, dass die Firewall Eindringen sucht, um sie zu stoppen. Die Firewall begrenzt den Zugriff aufs Netzwerk, um das Eindringen zu vermeiden, aber signalisiert einen Angriff auf das Netzwerk von Innen nicht. IDS wertet ein vermutetes Eindringen aus und erst wenn es geschieht, signalisiert es einen Alarm. Das IDS kann auch Angriffe aufnehmen, die im System an sich entstehen.

IDS verwendet die Analyse der Verwundbarkeiten (manchmal als Scanning bezeichnet). Es handelt sich um eine Technologie, die zur Bewertung der Sicherheit eines Computersystems oder Netzwerkes dient. IDS-Funktionen umfassen Überwachung und Analyse der Aktivitäten sowohl der Benutzer als auch des Systems, Analyse der Systemkonfigurationen und -verwundbarkeiten, Bewerten der System- und Dateiintegrität, Analyse abnormaler Aktivitätsmuster und Verfolgung der Verletzungen der Benutzerregeln. IDS können nach einigen Kriterien klassifiziert werden:

- Erkennung eines Missbrauchs (engl. *misuse detection*) vs. Erkennung einer Abweichung (engl. *anomaly detection*)
    - Bei der Erkennung eines Missbrauchs analysiert das IDS die erfassten Informationen und vergleicht sie mit einer umfangreichen Datenbank der Angriffssignaturen. Im Prinzip sucht das IDS einen spezifischen Angriff, der schon dokumentiert wurde. Die signaturbasierte Erkennung eines Eindringens bedeutet eine Suche der Signaturen (typischer Zeichenfolgen eines Angriffes) in der Kommunikation im Netzwerk. So kann sie Angriffe auf der Anwendungsschicht erkennen, selbst wenn sie den Standards der Protokolle zwischen Anwendungen entsprechen, weil sie um eine Entschlüsselung dieser Kommunikation ergänzt wird. Wie ein System der Virenerkennung ist die Erkennung des Missbrauchs so gut wie die Datenbank der Angriffssignaturen, mit der die Pakete verglichen werden. Daher muss diese Datenbank aktualisiert werden, so dass diese Technik relevant sein kann.

- Bei der Erkennung einer Abweichung definiert der Systemadministrator den normalen Zustand der üblichen Belastung des Netzwerkes, seine Gliederung, Protokolle und typische Paketgrößen. Dann werden Netzwerksegmente überwacht, um ihren Zustand mit dem normalen Zustand zu vergleichen und eventuelle Abweichungen zu finden.

- Netzwerkbasierte vs. hostbasierte Systeme

  - Die netzwerkbasierten Systeme (NIDS) analysieren die einzelnen Pakete, die durch das Netzwerk fließen. Ein NIDS kann schädliche Pakete erkennen, die so entworfen werden, dass einfache Filter der Firewall sie übersehen.

  - Die hostbasierten Systeme (HIDS) prüfen alle Aktivitäten jedes Computers oder Hosts.

3.4 Virtuelle private Netzwerke (VPN)

VPN ist die Abkürzung für das englische „*Virtual Private Network*“. VPN ist eine Netzwerktechnologie, welche die Verwendung eines öffentlichen Netzwerkes wie Internet für eine private Kommunikation durch Erzeugung eines sicheren (verschlüsselten) Anschlusses erlaubt.

VPNs werden häufig eingesetzt, um entfernte Benutzer an ein privates Netzwerk sicher anzuschließen und so Intranets weltweit zu erweitern. Mit anderen Worten, VPN ermöglicht das Senden von Daten zwischen zwei Rechnern mittels einer Routing-Infrastruktur eines geteilten oder öffentlichen Netzwerkes (wie Internet) durch Emulieren der Eigenschaften des privaten Point-to-Point-Anschlusses. Der sichere Anschluss scheint dem Benutzer als Kommunikation über ein privates Netzwerk, obwohl diese Kommunikation über ein öffentliches Netzwerk realisiert wird. Daher werden solche Netzwerke als virtuelle private Netzwerke bezeichnet.

Es gibt verschiedene Gründe des Aufbaus von VPNs, aber gemeinsam für alle ist die Anforderung an Virtualisierung eines Teils der Kommunikation der Firma, d. h., dass ein Teil der Kommunikation (oder die ganze Kommunikation) für externe Bobachter praktisch „unsichtbar“ wird und gleichzeitig Vorteile einer üblichen Kommunikationsinfrastruktur ausnutzen werden können. Üblicherweise werden VPNs für einen sicheren entfernten Zugriff auf Firmenressourcen via Internet und Anschluss von Netzwerken via Internet verwendet. VPNs sollen vor allem die folgenden Sicherheitsdienste anbieten:

- Benutzerauthentifizierung - VPNs erlauben den Zugriff nur den befugten Benutzern und daher muss ihre Identität verifiziert werden. Darüber hinaus sollen VPNs Auditprotokolle speichern.
- Verschlüsselung von Daten - Die Daten, die via ein öffentliches Netzwerk übertragen werden, müssen für unbefugte Benutzer unlesbar gemacht werden.
- Schlüsselverwaltung - Vor der Verschlüsselung müssen Benutzer die kryptographischen Parameter definieren und einstellen (Algorithmen, Schlüssel, ...).

4 4 Methoden der Netzwerksicherung

Ein Netzwerk ist nur so sicher wie sein schwächstes Glied. Neben dem Einsatz der in dem vorigen Kapitel beschriebenen Komponenten werden weiter Aktionen aufgeführt, die von Benutzern und/oder Netzwerkadministratoren implementiert werden sollten, um die Systemsicherheit zu unterstützen.

4.1 Einsatz von sicheren Authentifizierungsverfahren

Viele Firmen bestehen darauf, dass starke Authentifizierungsverfahren vor allem in online Transaktionen verwendet werden, die Zahlungsdienste einschließen. Dabei hat jedoch die starke Authentifizierung verschiedene Definitionen. Gemäß einigen Autoren bezieht sich dieser Begriff auf die Multi-Faktor-Authentifizierung, die zwei oder mehr der drei Faktorkategorien verwenden: Wissen, Besitz und Inhärenz, die schon im Kapitel 1.3 angeführt wurden. Andere Autoren (A. J. Menezes, P. C. van Oorschot und S. A. Vanstone) glauben, dass solche Authentifizierung kryptographische Challenge-Response-Verfahren erfordern, mehr dazu in [11]. Auf jedem Fall kann ein starkes Authentifizierungsprotokoll mit der Übertragung von Passwörtern nicht erreicht werden.

Man soll sich dabei bewusst sein, dass die Zuverlässigkeit der Authentifizierung nicht nur von der Anzahl der eingesetzten Faktoren, sondern auch von der Art ihrer Implementierung abhängt. Die Wahl der Authentifizierungsregeln bestimmt die Sicherheit jedes Faktors. Beispielsweise, schwache oder keine Regeln für Passwörter können die Verwendung von Passwörtern wie „Gast“ erlauben und dann wird der Beitrag der Passwörter ganz annulliert. Bewährte Verfahren fordern inhärent starke Passwörter, die regelmäßig aktualisiert werden. Laxe Regeln und Implementierung führt zu einer schwachen Sicherheit, andererseits stellen bessere Regeln eine höhere Sicherheit der einzelnen Faktoren und eine bessere gesamte Sicherheit für Multi-Faktor-Authentifizierungssysteme sicher.

Wenn Passwörter benutzt werden, sollen hochwertige Passwortgrundsätze durchgesetzt werden, um Erraten und Cracken von Passwörtern vorzubeugen. Die Entwicklung des Passwortknackens vereinfachte es den Hackern, die Passwörter zu „erraten“. Es stehen auch zahlreiche Tools dafür zur Verfügung, dass jede Person verwenden kann. Leider verwenden durchschnittliche Benutzer eher Passwörter, an die man sich einfach erinnert, als die, die schwierig zu erraten sind.

Das Knacken von Passwörtern ist ein Prozess zum Herausfinden oder Entschlüsseln der Passwörter, um einen unautorisierten Zugriff auf ein System oder Konto zu erwerben. Passwörter können auf verschiedene Weisen geknackt werden. Die einfachste ist die Brute-Force-Methode mit dem Einsatz einer Liste von Wörtern oder eines Wörterbuchprogramms. Diese Programme vergleichen Listen von Wörtern oder Zeichenkombinationen mit dem Passwort, bis sie eine Übereinstimmung finden. Daraus folgt, dass Passwörter keine Wörter aus Wörterbüchern, keine Eigennamen oder keine Fremdwörter sein können.

Das Passwortknacken kann auch zur Sicherstellung verwendet werden, dass die Benutzer starke Passwörter haben. Systemadministratoren können damit die Stärke der Benutzerpasswörter testen und die Benutzer warnen, welche unsichere Passwörter haben.

Darüber hinaus können Passwörter durch Social Engineering herausgefunden werden. Viele Benutzer erstellen Passwörter mit persönlichen Information. Solche

Passwörter können erraten werden, wenn man nur ein wenig über den Benutzer weiß. Daher sollen Passwörter keine persönlichen Informationen enthalten.

Viele Benutzer speichern ihre Passwörter in Dateien. Dann sollen diese Dateien verschlüsselt werden, um die Auswirkung von Passwort-Sniffing zu mildern. Diese Empfehlung gilt jedoch nicht nur für Passwortdateien, sondern auch für alle Dateien mit sensiblen Informationen.

4.2 Härten eines Betriebssystems

Das Härten des Betriebssystems bedeutet eine sichere Konfiguration des Betriebssystems, seine Aktualisierung, Definition von Regeln und Grundsätzen seiner sicheren Verwaltung und Beseitigung unnötiger Anwendungen und Dienste.

Das Härten des Betriebssystems erhöht seine Sicherheit. Das umfasst üblicherweise die Beseitigung aller unnötigen Dienstprogramme und Tools vom Rechner, Anwenden von aktuellen Patches, Löschen unbenutzter Dateien und alter Benutzerkonten. Obwohl diese Programme dem Benutzer nützliche Eigenschaften anbieten können, sie müssen deaktiviert werden, wenn sie eine „Hintertür“ für den Zugriff auf das System darstellen.

Obwohl es wichtig ist, Anwendungen zu löschen, Dienste auszuschalten, Patches und Hotfixes anzuwenden und Servicepacks zu installieren, ist es nicht die einzige Methode zum Härten des Betriebssystems. Administrative Rechte sollen sinnvoll verliehen werden und Grundsätze sollten eingehalten werden, um die Regeln der Firma durchzusetzen.

Dem Administrator stehen viele Checklisten für das Härten der meistverwendeten Betriebssysteme zur Verfügung. Das Härten kann für Betriebssysteme sowohl von Macintosh als auch von Windows durchgeführt werden, aber wird häufiger in Windows realisiert, weil deren Sicherheit wahrscheinlicher bedroht wird.

4.3 Physische Sicherheit

Um eine physisch sichere Netzwerkumgebung zu garantieren, muss zuerst der Zugriff auf sensible Daten und Systemdateien kontrolliert werden, was aber nur einen Teil eines guten Sicherheitsplans darstellt. Heutzutage ist dieser Schritt noch wichtiger denn je, weil Netzwerke jetzt mehr „Eingänge“ haben. Ein mittleres oder großes Netzwerk hat einige Zugriffspunkte, VPN-Server und einen reservierten zeitunbegrenzten Internetanschluss. Sogar kleine Netzwerke sind ans Internet mindestens für eine gewisse Zeitdauer angeschlossen.

Virtuelle Eindringlinge treten in keinen physischen Kontakt mit den Computern oder dem Netzwerk an sich ein. Sie können aufs Netzwerk von einer Stelle auf derselben Straße oder auf der anderen Erdhalbkugel zugreifen. Sie können ähnliche Schäden wie ein Dieb verursachen, der in den Hauptsitz der Firma einbricht und Daten stiehlt oder zerstört - aber sie können schwieriger gefasst werden. Die Sicherstellung der physischen Zugriffskontrolle auf dem sogenannten Außenperimeter umfasst das folgende:

a) Kontrolle des physischen Zugriffs auf Servern

b) Kontrolle des physischen Zugriffs auf Arbeitsplatzrechner im Netzwerk

c) Kontrolle des physischen Zugriffs auf Netzwerkgeräte

d) Kontrolle des physischen Zugriffs auf Verkabelung

e) Sicherung auf der Ebene der drahtlosen Medien

f) Sicherung auf der Ebene der Mobilrechner

g) Behandeln der Sicherheitsrisiken der Freigabe des Datendrucks

h) Behandeln der Sicherheitsrisiken der USB-Sticks, externen Platten, CDs und weiterer Wechseldatenträger

5 5 Mobile Sicherheit

Mobilgeräte ersetzen oder ergänzen immer öfter PCs für Haushalte und Firmen. Die schnelle Zunahme der Verwendung von Smartphones und Tablets in der letzten zwei Jahren führte zu einem unausbleiblichen Zuwachs der Cyberangriffe, die sich auf diese Geräte konzentrieren. Außerdem vermehren ungeregelte Anwendungsmärkte Probleme, die mit Malware in diesen Geräten zusammenhängen. Die Autoren der mobilen Malware wissen, dass sie möglichst viele Geräte infizieren können, wenn sie die zentralen Anwendungsmärkte angreifen.

Hacker können dann von erfolgreich angegriffenen Mobilgeräten auf verschiedene Arten profitieren. Einige sind schon vom Bereich der traditionellen PCs bekannt, wie Ransomware, Botnetze und Datendiebstahl. Mobilgeräte sind jedoch auch für neue Angriffstypen wegen ihrer Eigenschaften offen. Ihr Risiko liegt vor allem in ihrer Tragbarkeit - wenn sie physisch verloren werden, können ihre Daten auch verloren werden, wenn das Gerät nicht verschlüsselt oder auf eine geeignete Weise gesichert ist.

Die Entwicklung von Anwendungen für die persönliche und geschäftliche Kommunikation schafft Möglichkeiten für neue Angriffsarten, vor allem im Bereich der Social Engineering und Daten-Exfiltration. Ein Adressbuch mit sozialen Kontakten stellt dann einen Schatz für Cyberangreifer aller Typen dar. Kontrolle über mobile und webbasierte Anwendungen für Firmen wird bei der Minderung dieses Risikos helfen.

Die moderne Entwicklung der Mobile-Banking bringt noch größere Risiken für Benutzer. Leistungsfähige Mobilgeräte werden schon von Malware aktiv angegriffen, um nicht nur Daten, sondern auch Geld zu stehlen, weil diese Geräte die Realisierung der finanziellen Transaktionen auch unterwegs ermöglichen. Um sichere Mobile-Banking zu garantieren, sollten Smartphones vor Malware und Keylogger geschützt werden.

Sicherheitsspezialisten warnen schon jahrelang vor Risiken der mobilen Malware. Weil noch keine größeren Angriffe organisiert wurden, wird die Glaubwürdigkeit dieser Alarme untergraben und viele Benutzer betrachten diese Risiken als nicht gewichtig und sind weniger vorsichtig. Die ungeheure Anzahl der Mobilgeräte und das Übergewicht der neuen mobilen Malware steigern die Wahrscheinlichkeit, dass ein solcher großer Angriff durch mobile Malware auftreten wird.

M. Bermingham von Kaspersky sagt: „Wenn Verbraucher und Firmen Mobilgeräte für einen steigenden Anteil ihrer alltäglichen Tätigkeiten verwenden, werden Cyberangreifer einen größeren Wert auf Angriffe dieser Plattformen legen, vor allem Android und der mit dem Jailbreak versehenen iOS-Geräte.“