WIRTSCHAFTSUNIVERSITÄT WIEN
BAKKALAUREATSARBEIT

Titel der Bakkalaureatsarbeit:
Kriminalität im Internet

Englischer Titel der Bakkalaureatsarbeit:
Internet-crime

VerfasserIn:	Michael Pimmer
Matrikel-Nr.:	0253076
Studienrichtung:	Wirtschaftsinformatik
Kurs:	0267 Vertiefungskurs VI/Bakkalaureatsarbeit - Informationswirtschaft
Textsprache	Deutsch
BetreuerIn:	PD Dr. Edward Bernroider
Unternehmen/Betreuer:	

Ich versichere:
dass ich die Bakkalaureatsarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe. dass ich die Ausarbeitung zu dem obigen Thema bisher weder im In- noch im Ausland (einer Beurteilerin/ einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe. dass diese Arbeit mit der vom Betreuer beurteilten Arbeit übereinstimmt.

Datum _____ Unterschrift _____

Abstract

Deutsch

Diese Arbeit gibt einen Überblick über Bedrohungen und Kriminalität, denen Individuen und Firmen im Internet ausgesetzt sind. Die Eigenschaften und Motivationen der Angreifer werden vorgestellt, beispielhafte Angriffe und mögliche Gegenmaßnahmen beschrieben, sowie aktuelle Entwicklungen aufgezeigt. Nicht behandelt werden von Individuen vermeidbare Kriminalität wie Tauschbörsen oder Rassismus.

English

This paper presents an overview about the threats and crime in the internet which affects consumers and companies. The risks, attributes and the motivation of the attackers are presented, and possible countermeasures as well as current trends are diskussed. Excluded is crime which is avoidable by the consumer, as illegal file-sharing or rassism.

Keywords

Internet, Kriminalität, Cracker, Hacker, IT-Sicherheit, Datenschutz, Zensur, Anonymität, Cyber-War, Industriespionage, Schwachstellen;

Danksagung

Herzlich danken möchte ich allen Entwicklern von freier Software und offener Kryptographie, die ihre Freizeit dafür verwenden, für die Allgemeinheit nützliche Programme zu schreiben. Im Speziellen danke ich den Entwicklern von:

- Debian GNU/Linux[1] und dem Linux-Kernel[2]
- LaTeX[3], TeTex[4], Kile[5] - den Programmen, mit denen ich diese Bakkalaureatsarbeit verfasst habe

Weiters danke ich meiner Familie und meinen Freunden, die mir zwar nicht direkt bei der Verfassung der Bakkalaureatsarbeit geholfen haben, aber - was ich als wichtiger erachte - mir im Leben zur Seite stehen.

[1] Debian GNU/Linux http://www.debian.org
[2] kernel.org http://www.kernel.org
[3] LaTeX Textsatzprogramm http://www.latex-project.org
[4] TeX-Distribution für Linux http://www.tug.org/tetex/
[5] Kile LaTeX IDE für Linux http://kile.sourceforge.net/

Inhaltsverzeichnis

1. Einleitung

1.1. Kontext

Die Sicherheit in Netzwerken muss immer im Kontext betrachtet werden. Selbst wenn durch Kryptographie, Firewalls und speziell gehärtete Software die Gefahren eines Einbruchs minimiert werden können, so bleiben immer noch genügend andere unsichere Elemente. Kevin Mitnick, einer der bekanntesten Hacker, setzte vor allem auf Social Engineering[KunstDerTäuschung], dem Täuschen von gutgläubigen Mitarbeitern - und war sowohl bei Geheimdiensten als auch bei Firmen *zu* erfolgreich damit: Er verbrachte fünf Jahre seines Lebens im Gefängnis.

"Security is not a Product, it's a Process"
"Sicherheit ist eine Kette, die so stark ist wie ihr schwächstes Glied"[1]

Vorbeugende Maßnahmen sind gut, aber zu wenig. Die Erkennung von Angriffen und eine angemessene Reaktion darauf ist genauso wichtig.

Diese Arbeit beschäftigt sich mit Kriminalität und Sicherheit im Internet. Es wäre aber ein Fehler, zu glauben, dass die Beachtung der vorgestellten Gefahren für eine umfassende IT-Sicherheit ausreichend ist. Die hier vorgestellten Gefahren sind nur ein beispielhafte Auflistung bedeutender aktueller Themen. Es handelt sich nicht um eine Anleitung zur Absicherung von Client- und Firmen-PCs und Netzwerken, sondern um die Beleuchtung von Internet-Kriminalität von verschiedenen Standpunkten.

[1] Bruce Schneider, Kryptografie-Experte

1.2. Definition von Kriminalität

Unter Kriminalität ist in dieser Arbeit ein Verstoß gegen Sicherheitsziele zu verstehen.

1.2.1. Sicherheitsziele

Die drei Basis-Sicherheitsziele sind Vertraulichkeit, Integrität und Verfügbarkeit ([Netzwerksicherheit], [IT-Sicherheit]).

Vertraulichkeit bedeutet, dass nur berechtigte Subjekte auf geschützte Objekte Zugriff haben.
Integrität meint, dass Daten nur von berechtigten Personen/Programmen verändert werden dürfen.
Verfügbarkeit bedeutet, dass Daten oder Dienste zu den gewünschten Zeitpunkten auch tatsächlich abrufbar sind.

Darauf aufbauend gibt es weitere Sicherheitsziele wie Verbindlichkeit, Authentizität, Zuverlässigkeit, Überwachbarkeit, Nichtabstreitbarkeit, Anonymität oder Pseudonymisierung.

2. Schwachstellen und Angreifer

Die Anzahl von Schwachstellen und Lücken in einem System ist von der Anzahl der Funktionen, der Homogenität, dem Grad der Vernetzung und von menschlichen Fehlern abhängig[Netzwerksicherheit]. In diesem Kapitel werden Gründe und Ursachen für Schwachstellen vorgestellt. Die aktuell größten spezifischen Risiken beim Einsatz von IT sind in Appendix A.1, der SANS-Rangliste, zu finden. Nur Endbenutzer oder nur Unternehmen betreffende Angriffsmöglichkeiten sind in Kapitel 3 (Endbenutzer betreffende Kriminalität) und 4 (Unternehmen betreffende Kriminalität) beschrieben.

2.1. Buffer Overflows

Diese Art von Sicherheitslücke existiert schon lange. Es handelt sich um Fehler oder Unachtsamkeiten in der Programmierung von Software, die Benutzerangaben oder Parameter falsch oder nicht ausreichend überprüft, und so eine Ausführung von beliebigem Code auf dem Rechner des Opfers ermöglicht. Buffer Overflows sind mit großem Abstand die häufigste Ursache für Software-Schwachstellen.
Ein wirklicher Schutz ist als reiner Benutzer von Software leider nicht möglich. Nur der Programmierer hat die Möglichkeit und Verantwortung, das Auftreten von Buffer Overflows gering zu halten. Man kann als Endbenutzer folglich nur hoffen, dass die interessanten Ansätze zur Vermeidung (Kapitel 6.5.1) bald von mehr Erfolg gekrönt sind - und bis dahin qualitativ möglichst hochwertige Software verwenden, und diese am aktuellsten Stand halten.

2.2. Netzwerk-Schwachstellen

Es gibt eine Vielzahl von Netzwerk-Angriffen auf den verschiedenen Schichten. ARP-Spoofing, DDoS-Attacken (siehe Kapitel 4.3.1), DNS-Attacken wie DNS Cache Poisoning, DNS Spoofing oder DNS Hijacking, Angriffe auf Webserver (Kapitel 4.3.2) und durch Webserver (Cross Site Scripting, Kapitel 4.3.2), ICMP-Attacken und IP-Spoofing sind bei weitem noch keine vollständige Aufzählung. Auch Überwachungs- oder Spionage-Tätigkeiten lassen sich auf Netzwerkebene beispielsweise durch Packet Sniffing durchführen. Auf die technischen Details der einzelnen Angriffe wird hier aus Platzgründen nicht eingegangen, sondern nur auf übergeordnete, eine Ebene höher angesiedelten Schwachstellen und Angriffe. Detailliertere, aktuelle Informationen über die Bedrohungen durch Netzwerk-Attacken und mögliche Gegenmaßnahmen bietet das Buch [Netzwerksicherheit].

2.3. Menschen - Social Engineering

In fünf Minuten ist es durch drei Telefonate möglich, durch die Vorgabe falscher Tatsachen an die Kreditkarten-Nummer eines beliebigen Videothek-Kunden zu kommen[KunstDerTäuschung]. Gutgläubige Mitarbeiter helfen gerne einem Kollegen bei einem schweren Problem, Cracker nutzen das gerne aus.
Aber es muss nicht einmal so kompliziert sein: Heerscharen von Usern öffnen einen E-Mail-Anhang, nur weil im Betreff ”I love you“ geschrieben steht. Technisch nicht versierte, unwissende, gutgläubige Menschen, die zu schnell einem Fremden Vertrauen schenken sind die Ursache.
Diese Schwachstelle Mensch wird sich nicht so schnell ändern und verändern lassen. Die Bewusstseinsbildung für Gefahren im Internet hinkt der Realität hinterher, wie die mittlerweile schon Jahre andauernden Phishing-Wellen zeigen.

Ein gewisses Grundverständnis dieses Themas kombiniert mit einer gesunden (oder noch besser: ungesunden) Portion Paranoia ist die beste Verteidigung

gegen Social Engineering. Für Firmen bedeutet das, dass die Mitarbeiter in derartigen Themen geschult werden sollten, um ein Sicherheitsbewusstsein zu schaffen.
Die Gegenmaßnahmen sind stark von der spezifischen Situation abhängig. Anzuraten ist die Überprüfung, ob die Person am anderen Ende der Telefon- oder Internet-Leitung wirklich diejenige ist, für die sie sich ausgibt. Bei E-Mails könnte das eine elektronische Signatur sein, bei Telefonaten könnte man einfach die Person (nicht die Anrufer-Nummer) zurückrufen, für die sich der Anrufer ausgibt.

2.4. Angreifer-Typen

Angreifer weisen im Vergleich zu Opfern mindestens eine der folgenden Eigenschaften, meistens aber sogar mehrere auf: Mehr Zeit, ein besseres Fachwissen, eine höhere Risikobereitschaft, bessere (finanzielle) Ressourcen;

2.4.1. Hacker, White Hats

Sie haben meist eine fundierte Fachkenntnis. Ihre Ziele sind nicht krimineller, sondern erforschender und demonstrativer Natur. Studenten, Programmierer oder im Sicherheitsgeschäft tätige Personen sind häufig in dieser Kategorie zu finden.

2.4.2. Cracker, Black Hats

Cracker haben im Unterschied zu Hackern eine destruktive oder kriminelle Zielsetzung. Sie sind oft von Firmen beauftragt oder haben politische Motive. Cracker können auch Terroristen sein, die zwar meistens weniger Expertenwissen, dafür aber eine viel höhere Risikobereitschaft - auch zu physikalischen Angriffen - aufweisen.

2.4.3. Script Kiddies

Darunter versteht man Menschen, die kein allzu gutes Wissen im technischen Bereich aufweisen. Sie verwenden vorgefertigte Exploits, Programme und Scripts. Durch ihr massenhaftes Auftreten sind sie allerdings diejenigen, die heute am meisten Schaden verursachen[Netzwerksicherheit].

2.4.4. Mitarbeiter

70 % aller Angriffe kommen laut einer Studie des Computer Security Insitute von innen, also von Unternehmens-Mitarbeitern selbst[SecretsAndLies]. Ein verantwortungsbewusster, sozial gerechter Umgang mit den Angestellten reicht jedoch nicht zur Prävention aus: 80 Prozent der Insider-Angriffe sind auf eine finanzielle Motivation zurückzuführen, und nicht aus Rache- oder zur Schädigung des Arbeitgebers durchgeführt worden[EnterpriseSecurity]. Die Angriffe von innen sind meistens nicht besonders komplex oder technisch aufwändig.

2.5. Auffinden von Zielen und Schwachstellen aus Angreifer-Sicht

2.5.1. Auswahl des Ziels

Oft wählen Angreifer Ziele aus bestimmten (monetären, politischen oder ideologischen) Gründen aus. Hauptsächlich Script Kiddies suchen aber auch nach zufälligen neuen, leicht angreifbaren Zielen.
Das Durchführen von Port-Scans über IP-Bereiche zu diesem Zweck ist altbekannt. Dass sich Suchmaschinen - allen voran Google - ebenfalls hervorragend zum Suchen von Schwachstellen und Angriffspunkten eignen noch nicht. Man kann automatisiert und global nach bestimmten Server-Versionen,

Passwort-Dateien, vom Systemadministrator hinterlassene Nessus-Logs oder gar Datenbank-Zugangsdateien suchen [HackingExposed].

2.5.2. Footprinting & Scanning

Hat der Angreifer ein Ziel identifiziert, so gilt es nun, möglichst viele Informationen darüber zusammenzutragen. Neben den technischen Varianten wie Port-Scans (zB nmap) oder dem Einsatz von Nessus (das nach dem Scan direkt die Sicherheitslücken eines Rechners anzeigt) sind vor allem die angebotenen Dienste interessant, im Speziellen Web-Server. Auf der Internet-Präsenz lassen sich oft äußerst interessante Informationen finden, wie Mitarbeiter-Daten, manchmal auch E-Mail-Adressen oder gar Lebensläufe, was Hinweise für weitere Suchmöglichkeiten gibt. Durch eine whois-Abfrage kann man oft die geografische Lage des Opfers und persönliche Daten eruieren [HackingExposed].

2.5.3. Gegenmaßnahmen

Suchen Sie selbst Informationen über sich, scannen sie sich selbst, und überlegen Sie, welche Informationen Sie auf Ihre Internet-Präsenz stellen. Web-Server sollten nicht als Zwischenspeicher für firmeninterne Dokumente verwendet werden, was aber oft genug der Fall ist.

2.6. Anonymität der Angreifer

Anonymität für Endverbraucher ist mit Hilfe von Software (siehe Kapitel 5.1.2) mehr oder weniger gut realisierbar - diese Anonymität reicht aber vielen Angreifern noch nicht aus, oder die mit der Anonymität verbundenen Einschränkungen sind zu störend. Es ist leicht, wirklich anonyme Zugänge zum Internet zu finden: Öffentliche zugängliche WLAN-Netzwerke und Internet-Cafés; Private WLAN's, die nicht ausreichend geschützt sind - man nennt die destruktive Verwendung solcher "war-driving"[wlan-security]. Man könnte auch am

Glühweinstand vor der Universität jemanden nach seinen Login-Daten fragen, um schnell E-Mails checken zu können. Guten Angreifern ist es heute leicht möglich, einen Zugriff zum Internet zu finden, der nicht auf sie zurückzuführen ist. Durch die Zeitintensivität mancher Angriffe, durch Faulheit oder durch das freiwillige Ausplaudern können Angreifer trotzdem zurückverfolgt werden.

3. Endverbraucher betreffende Kriminalität

Über die Sicherheit von Client-PCs gibt es ausreichend Literatur (zB [Datenspionage], [HackersGuide]), und die notwendigen Maßnahmen zur Absicherung sind meist nicht allzu komplex oder technisch aufwändig. Davon abgesehen ist ein eine gesunde Skepsis und das Grundverständnis des Themas oft hilfreicher als die beste Verteidigungs-Software.

3.1. Angreifer & Motivation

Endnutzer sehen sich meistens nicht sehr spezialisierten Angriffen und Angreifern ausgesetzt, sondern generischen, automatisierten Attacken. Persönliche Motive (zB Stalking des Exfreundes) könnten spezifische, auf einen Client begrenzte Angriffe noch erklären, finanzielle Gründe jedoch nicht: Leute mit der dafür notwendigen Fachkenntnis kennen lohnendere Ziele.
Automatisierte Attacken basieren jedoch erstaunlich oft auf finanziellen Motiven: Spam-Mails sollen den Umsatz einer Firma erhöhen, Phishing die Räumung des Bankkontos ermöglichen. Root-Kits und Trojaner werden zu weiteren Angriffen auf größere Ziele benutzt, oder um Nutzer-Daten aufzeichnen und verkaufen zu können. Typische Angreifer von Endbenutzer-PCs sind Script Kiddies. Zeitungs- und Fernsehberichten zufolge wurden 2005 drei niederländische Jugendliche festgeommen, die mehr als 1,5 Millionen Rechner - das bisher größte Bot-Netz - unter ihre Kontrolle gebracht haben 1[1].

[1] http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CyberCrime2005.pdf, http://www.techweb.com/wire/security/172303160

3.2. Malware

Darunter versteht man Software, die im Hintergrund vom Nutzer nicht angeforderte und gewünschte Aktionen durchführt.
Malware benötigt meistens - aber nicht zwingend - tiefer liegende, technische Schwachstellen zur Verbreitung. Manche Viren und Spyware funktionieren aber rein durch den Einsatz von Social Engineering (siehe Kapitel 2.3).

3.2.1. Viren und Würmer

Definition

Viren sind im Gegensatz zu Würmern keine eigenständig lauffähigen Programme, sondern sie verändern bereits vorhandene Programme oder Dateien auf einem PC. Würmer breiten sich eigenständig über Netzwerke aus. Homogene Client-PC's und Standardsoftware machten es möglich, dass der 2002 in Umlauf gebrachte Virus "Klez" geschätzte 8,5 Mrd. US-Dollar an Schaden anrichtete[Datenspionage]. Während Würmer sich über Sicherheitslücken von Programmen oder Betriebssystemen selbständig und mehr oder weniger unbemerkt verbreiten, so verschicken sich Viren heutzutage meist automatisch selbst per E-Mail mit infiziertem Attachment. Sie sind also auf User-Interaktion (in diesem Fall dem Öffnen der E-Mail) angewiesen, um sich zu verbreiten.

Motivation

Die Motivation zum Schreiben von Viren und Würmern ist hauptsächlich Aufmerksamkeit: Virenattacken stossen in den Medien auf eine große Resonanz. Technisches Interesse, "Machbarkeitsstudien" im Sinne von der Demonstration von Schwachstellen, oder dem Monopolisten Microsoft schaden zu wollen - was in der Script-Kiddie-Gemeinde hohes Ansehen geniesst - sind weitere Gründe.

3.2.2. Trojanische Pferde, Backdoors und RootKits

Definition

Ein Trojanisches Pferd ist ein Programm, dessen implementierte Ist-Funktionalität nicht mit der gewünschten Soll-Funktionalität übereinstimmt [IT-Sicherheit]. Damit ist meistens die Installation von Hintertüren oder RootKits gemeint, über die der Rechner später überwacht oder ferngesteuert werden kann. Werden Daten über den Benutzer gesammelt, so handelt es sich um Spyware 3.2.3.

Motivation

Diese Hintertüren und die damit mögliche Steuerung einer Vielzahl von Client-PCs sind die Grundlage für DDoS-Angriffe 4.3.1, die neben Viren heutzutage den höchsten wirtschaftlichen Schaden verursachen. Zur Motivation von DDoS-Attacken siehe Kapitel 4.3.1. Weitere Gründe können Datenspionage und Informationsgewinnung mit dieser Art von Malware sein. Das Machtgefühl, einige tausend Rechner unter Kontrolle zu haben, ist ebenfalls nicht zu unterschätzen.

3.2.3. Spyware

Definition & Motivation

Firmen versuchen, an Informationen über das Nutzerverhalten zu kommen, um dadurch einen Informationsvorteil zu erlangen. Das geschieht leider oft auch auf illegalem Weg. Die Firma Hewlett Packard ließ sich ungefragt durch Druckertreiber diverse Informationen über das Druckverhalten der Benutzer senden, was gegen die deutschen Datenschutzbestimmungen verstieß.

Die Firma Sony BMG[2] baute in ihre CDs eine selbstinstallierende DRM-Software ein, die einige Sicherheitslücken aufwies und somit die Rechner ihrer Kunden für Attacken öffnete.

Der Windows Mediaplayer, der RealPlayer und File-Sharing-Programme wie AudioGalaxy, Kazaa und BearShare sendeten Informationen über das Nutzerverhalten wie abgespielte Mediendateien oder aufgerufene Internet-Seiten an die entsprechenden Firmen [Überwachungsmafia]. Weitere Überwachungsmöglichkeiten werden in Kapitel 5.1 angeführt.

User-Tracking

Hierbei handelt es sich um eine Identifikation eines Users über mehrere Webseiten hinweg, die meist mit Cookies realisiert wird. Somit ist es möglich, ein Benutzerprofil mit allen Daten, die der User in einer dieser Seiten in einem Formular angegeben hat, zu erstellen.
Die Firma Doubleclick[3], die Werbeeinschaltungen auf vielerlei großen Webseiten anbietet, kombiniert die Benutzerdaten der verschiedenen Seiten, und zeigt somit User-spezifische Werbung an. Den Plan, durch die Übernahme der Firma Abacus die vorhandenen Profile mit detaillierten Adress- und Personeninformationen zu kombinieren, gab Doubleclick nach öffentlicher Kritik und einem Artikel in USA Today auf. (siehe [SecretsAndLies] und [Überwachungsmafia].

User-Tracking nimmt mittlerweile ab: Von 2000 bis 2002 ist die Zahl der kommerziellen Web-Sites, die persönliche Angaben sammeln, von 96 auf 84 Prozent zurückgegangen. Die Anzahl von Seiten, die Cookies zur Verfolgung und Identifikation verwenden, ist von 79 auf 48 Prozent gefallen [Überwachungsmafia].

[2] http://www.sonybmg.com/
[3] http://www.doubleclick.com

3.2.4. Gegenmaßnahmen zu Malware

Die Eigenschaften der Angriffe erleichtern die Verteidigung: Abgrenzung von der Masse ist ein guter Weg. Selbst wenn die alternativ verwendete Software nicht weniger Fehler aufweist: Das Hauptziel von Angreifern ist der Massenmarkt. Die wenigsten Cracker werden sich die Mühe machen, für einen Browser mit 3 % Marktanteil eine Schadensroutine in eine Web-Seite zu integrieren. Linux bzw. Open Source Software ist nicht per Definition sicher vor Viren - es gibt auch dort genügend Sicherheitslücken - mir ist aber kein einziger Linux-, BSD- oder OSX-Benutzer bekannt der jemals einen Virus hatte, im Gegensatz aber kein Windows-Benutzer der noch nie mit Viren in Kontakt gekommen ist. Hauptziel von Malware sind folglich Windows-Rechner von Firmen und Endbenutzern in der Standard-Installation. Schutz bietet alternative Software[4], ein aktuelles Betriebssystem, ein aktueller Virenscanner und eine Firewall, die am Besten auf einem separaten Router und nicht auf dem Client-PC läuft.
Firmen haben einige weitere Möglichkeiten. Gefährlich erscheinende E-Mail Attachments können auf dem Mailserver gefiltert werden. Ausgeklügelte Firewalls, Anwendungs-Gateways und Proxy-Server können den Internet-Verkehr ebenfalls kontrollieren, sind aber bei weitem nicht ausreichend für eine umfassende Unternehmens-Sicherheit (siehe Kapitel 4).

Gegenmaßnahmen zu Spyware

Keine Software wie Bildschirmschoner, Scherzprogrammen, lustige PowerPoint-Präsentationen oder File-Sharing-Software von unbekannten oder dubiosen Herstellern zu verwenden ist ein guter Anfang. Programme wie Ad-Aware[5] helfen ebenfalls, den PC möglichst frei von unerwünschten Datensammlern und Werbung zu halten. Weiterführende, aktuelle Informationen zu diesem und ähnlichen Themen bietet die Electronic Frontier Foundation[6] (EFF).

[4] OSS-Verzeichnisse: `http://sourceforge.net`, `http://www.webi.org` für Endbenutzer
[5] `http://www.lavasoftusa.com/`
[6] `http://www.eff.org/`

User-Tracking kann durch ein paar Browser-Einstellungen, die heutzutage jeder Browser bieten sollte, stark eingeschränkt werden:

- Cookies nur von angeforderten Seiten akzeptieren, bzw. bei jedem Cookie nachfragen
- Cookies beim Beenden des Browsers löschen
- Das Senden des Referrers (der zuletzt aufgerufenen Seite) verbieten

3.3. Spam

3.3.1. Definition & Motivation

Spam sind unerwünschte Nachrichten - meist Werbung, die Motivation ist also fast durchwegs kommerzieller Natur. Benutzer sollen meistens auf bestimmte Web-Seiten gelockt werden, um Produkte zu kaufen, oder den PC mit Malware zu infizieren.

In diesem Kapitel wird nur Spam per E-Mails behandelt - Informationen zu Spam in Verbindung mit Web-Servern sind in Kapitel 4.3.2 zu finden.
Schätzungen zufolge ist Mail-Spam für über 40 % aller E-Mails verantwortlich, und verursacht erhebliche Kosten durch verlorene Arbeitszeit und Präventionsmaßnahmen [Netzwerksicherheit].

3.3.2. Phishing & Pharming

Phishing bedeutet, per E-Mail-Spam Leute dazu zu bringen, ihre Online-Banking Login-Daten und TAN's bei gefälschten Seiten einzugeben.
Sogar auf die anfänglich äußerst plumpen, mit Rechtschreibfehlern gespickten Phishing-Mails fielen genügend Leute herein, was interessanterweise weitere Spam-Wellen zur Suche nach "Finanzmanagern" zur Geldwäsche (siehe Appendix A.2) nach sich zog.

Die Angriffe sind mittlerweile viel ausgefeilter und schwerer zu erkennen. Denk- und realisierbar wären sogar Man-in-the-middle Seiten, die die von dem Nutzer eingegebenen Daten an die Bank weiterleiten - und die Internet-Seiten der Bank an den Kunden zurückgeben, und nur bei der Durchführung von Transaktionen eine eigene, gefälschte Seite einfügen. Dieser beispielsweise mit PHP's socket-Funktionalität Angriff ist bisher noch nicht aufgetreten.

Pharming basiert auf Netzwerk-Angriffen auf DNS-Server oder DNS-Informationen von Client-PCs. Dadurch sollen User auf falsche Web-Server geleitet werden, um dort deren Konten-Informationen und TAN's auszuspähen. Pharming ist deutlich schwieriger zu erkennen als Phishing - und kann sogar bei einer manuellen Eingabe der Internet-Adresse auftreten.

3.3.3. Gegenmaßnahmen zu Spam

Man sollte sich mindestens zwei E-Mail-Adressen zulegen: Eine möglichst anonyme für Allfälliges im Internet, die andere für wichtigere, geschäftliche Dinge. Vor allem letztere sollte man nicht unüberlegt freigeben.
Aktuelle E-Mail-Clients wie Thunderbird[7] bieten eine individuelle, konfigurierbare und lernfähige Filterung. Firmen haben die Möglichkeit, die Filterung direkt auf dem Mail-Server vorzunehmen [Netzwerksicherheit], was durch die Vielzahl der E-Mails meistens zu besseren Ergebnissen führt. Open-Source-Filter sind zum Beispiel Spam Assassin[8], SpamBayes[9], SpamProbe[10] oder DSPAM[11] [Netzwerksicherheit].

[7] http://www.mozilla.com/en-US/thunderbird/
[8] http://spamassassin.apache.org/
[9] http://spambayes.sourceforge.net/
[10] http://spamprobe.sourceforge.net/
[11] http://dspam.nuclearelephant.com/

OpenDNS[12] nutzt die auf der Seite http://www.phishtank.com gesammelten Informationen über Phishing-Seiten, und sperrt den Zugriff auf diese. Es gibt noch weitere ähnliche Software-Projekte, wie zB ScamBlock[13].
Der sicherste Weg, um Phishing (auch Man-in-the-Middle-Phishing) und Pharming zu vermeiden, ist aber eine manuelle Überprüfung der Gültigkeit des SSL-Zertifikates der Bank-Seite. Dieses sollte selbstverständlich auf die Bank ausgestellt sein, und von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority, CA) wie VeriSign[14] stammen. Das Vorhandensein einer SSL-Verschlüsselung alleine sagt noch rein gar nichts über die Authentizität der Web-Seite aus.

3.4. Kreditkartendiebstahl

3.4.1. Definition & Motivation

Hier handelt es sich um eine Gefahr, die Endbenutzer meistens nur indirekt trifft. Wiederholt wurden und werden tausende von Kreditkartennummern von Online-Händlern gestohlen, die unzureichende Sicherheitsvorkehrungen getroffen hatten. Selbst Bill Gates' Kreditkartennummer wurde inzwischen zweimal gestohlen. Mit Hilfe von Kreditkartennummern kann man vergleichsweise anonym an Geld oder Waren kommen, was den Diebstahl lohnend macht.

3.4.2. Gegenmaßnahmen

Das System der Zahlung mit Kreditkarten im Internet ist in der aktuellen Implementierung per se unsicher. Wenn möglich sollte man auf Online-Zahlungen

[12] http://www.opendns.com/
[13] http://www.scamblocker.com/
[14] http://www.verisign.com/

mit der Kreditkarte verzichten und auf alternative Zahlungsmethoden ausweichen. Das Ansehen des Zahlungsempfängers ist kein Schutz, auch Unternehmen mit guter Reputation werden erfolgreich angegriffen. Spätestens ab dem Zeitpunkt eines Online-Kaufes mit Kreditkarte und der damit verbundenen Weitergabe der Nummer sollte man regelmäßig die Abrechnungen prüfen. Die Kreditkartenfirmen sind hier kulant um das Online-Zahlungsmittel Kreditkarte nicht in Verruf zu bringen, und erstatten den Betrag in so gut wie jedem Fall zurück - beziehungsweise wälzen den Schaden auf den Online-Händler ab.

4. Unternehmen betreffende Kriminalität

Zugangsdaten für Web-Server werden ohne Bedenken oder Überüfung der anfragenden Person unverschlüsselt per E-Mail verschickt. Durch die Vorgabe, Mitarbeiter der EDV-Abteilung zu sein, werden bereitwillig Login-Daten oder Informationen über das Netzwerk herausgegeben. Wie gut sind die Backup-Daten vor Fremdzugriffen geschützt? Die wenigsten Firmen schulen Ihre Mitarbeiter in Themen wie diesen.

Angreifern ist es nicht zu mühsam, den Müll von Firmen nach interessanten Daten zu durchwühlen. Selbst wenn keine Passwort-Listen darunter sind, so lassen sich durch die gefundenen Informationen zumindest Social Engineering-Attacken (Kapitel 2.3) glaubhafter und effektiver durchführen.

Grundsätzlich gelten alle Gefahren für End-Verbraucher in gleichem Maße auch für Firmen, bzw. für Client-PCs von Firmen.
Zusätzlich dazu sind Firmen im Gegensatz zu Endnutzern oft gezwungen, Dienste nach außen bereitzustellen: Web- oder Applikationsserver, Zugänge für Lieferanten, VPN-Zugriff auf das interne Firmennetzwerk für Mitarbeiter. Kombiniert man dies mit der Vielzahl der involvierten Rechner, Menschen und Plattformen, so wird man schnell verstehen wieso es keinen hundertprozentigen Schutz gibt: Das System ist schlicht zu komplex, um alle Eventualitäten berücksichtigen zu können. Unerwünschte, unerwartete Effekte beim Zusammenspiel vom Software oder einfach nur eine noch nicht geschlossene Sicherheitlücke reicht aus, um in das System eindringen zu können, sei es in den Client-PC's, der Firewall, einem Server - oder über den kompromittierten Geschäftspartner, der Zugang zum internen Netz hat.

4.1. Angreifer & Motivation

Als Angreifer kommen leider alle in Kapitel 2.4 erwähnten Charaktere in Frage. Die Vielseitigkeit und die speziellen Eigenheiten der möglichen Gegner sollte im Sicherheitskonzept berücksichtigt werden.

Politisch motivierte Angriffe, die natürlich auch für Unternehmen relevant sind, werden im Kapitel 5.2 vorgestellt.

4.2. Sicherheitsgrundsätze

Hier finden Sie eine generelle Auflistung von Aspekten, die man bei der Implementierung von Software oder einer Unternehmens-Sicherheitsstrategie beachten sollte. Eine Rangliste des SANS-Institutes[1] über die größten Risiken in der IT-Sicherheit ist in Appendix A.1 zu finden.

- **All incoming data is evil** Vertraue keinen Daten, die von außen - aus dem Internet - kommen, sondern überprüfe, ob die Daten den Erwartungen entsprechen
- **Security by Obscurity does not work** Gehen Sie offen mit auftretenden Sicherheitslücken um. Verwenden Sie veröffentlichte, getestete Kryptographie-Algorithmen. Das heißt nicht, dass Sie ihre Netzwerk-Infrastruktur jedem erklären sollen, der Interesse daran zeigt.
- **Default Deny** Verbieten Sie standardmässig alles, und erlauben Sie nur was Sie wirklich benötigen.
- **Awareness** Schaffung eines Sicherheitsbewusstseins der Mitarbeiter und des Managements
- **Secure by Design** Machen Sie sich bereits bei der Konzeption von Software oder der Planung ihres Netzwerkes Gedanken über die Sicherheit. Nur später aufzutretende Sicherheitslücken zu beheben reicht nicht aus,

[1] http://www.sans.org/

wie beispielsweise die fortwährend hohe Anzahl der Sicherheitslücken des Internet Explorer beweist.

4.3. Beispiele für Attacken

Jedes Glied des Unternehmensnetzwerks ist gefährdet und angreifbar. Beispiele für Angriffspunkte sind Drucker-Server, Firewalls, VPN-Verbindungen, angebotene Dienste, Client-PCs und das WLAN.

4.3.1. Denial of Service - DoS-Attacken

Definition

Denial of Service (DoS) bedeutet, einen angebotenen Dienst nicht mehr verfügbar zu machen. Das kann erreicht werden, indem man beispielsweise den Dienst (oder das Betriebssystem) zum Absturz bringt, oder es durch eine Vielzahl von Anfragen für normale Anfragen unerreichbar macht.
Bei den meisten heutigen DoS-Attacken handelt es sich um DDoS, also Distributed DoS-Angriffe. Dabei wird die Kontrolle einer Vielzahl von Rechnern mit Trojanern oder RootKits ausgenutzt, um ein Angriffsziel mit Anfragen zu überschütten.

Motivation

Die häufigsten Gründe für DoS-Attacken sind Machtdemonstration bzw. Erpressung, Ausschalten / Schädigen der Konkurrenz oder politische Faktoren. Je nach Geschäftsmodell kann die Nicht-Erreichbarkeit von Diensten eine durchaus existenzielle Bedrohung darstellen.

Gegenmaßnahmen

Es gibt nur Vorkehrungen gegen DDoS-Attacken, aber keinen Schutz. Ein guter, auf einer breiten Basis an kontrollierten PCs beruhender Angriff ist mit herkömmmlichen Mitteln kaum abwehrbar. Angriffs-Anfragen können auf Netzwerk-Ebene nur schwer identifiziert werden, weil sie genauso wie normale Anfragen aussehen. Attacken müssten außerdem bereits im Internet an Knotenpunkten ausgefiltert werden, weil die Filterung durch das Opfer zu spät kommt: An diesem Punkt ist die Kapazität der Leitungen oder der Rechner meistens schon überschritten, und das Opfer für normale Anfragen nicht mehr zugänglich.
Um den regulären Unternehmenszugang zum Internet nicht zu behindern ist das Auslagern von Diensten sinnvoll. Weiters ist das Erhöhen der Ressourcen (vor allem der Bandbreite) eine sinnvolle, aber meist kostspielige Möglichkeit, die aber nur Wirkung zeigt, wenn der Angriff nicht zu heftig ist.

4.3.2. Angriffe auf Server am Beispiel Web-Server

Attacken auf Webserver gehören zu den am häufigsten auftretenden. Der Angriff kann auf vielen Ebenen geschehen: Das Betriebssystem muss geschützt sein, die Server-Software und die verwendete Skriptsprache müssen sicher sein, die Web-Seite bzw. Web-Applikation selbst, und schlussendlich kann der Angriff auch noch auf der Netzwerk-Ebene, also der Verbindung des Clients zum PC erfolgen. Es ist nicht verwunderlich dass erfolgreiche Angriffe auf einen scheinbar so einfachen Dienst wie Web-Server alltäglich sind. Eine ausführliche Anleitung zum Absichern stellt das Buch [ApacheSecurity] dar.
Hat man keine Sicherheitsexperten mit ausreichendem Know-How und genügend Zeit im Unternehmen, so ist es am Besten, den Web-Server an andere Firmen auszulagern. Die Kosten hierfür sind vergleichweise niedrig, und die Überwachung der Server kann dort effizienter stattfinden.
Open-Source-Programme wie Nikto[2] oder Whisker[3], die Web-Server nach ver-

[2] http://cirt.net/code/nikto.shtml
[3] http://sourceforge.net/project/showfiles.php?group_id=8057

schiedenen Schwachstellen scannen, erleichtern und unterstützen - aber ersetzen nicht - die Suche nach Sicherheitslücken.

Sicherheit des Betriebssystems

Auf dem Rechner, der den Web-Server anbietet, sollte wenn möglich nur dieser eine Dienst zur Verfügung stehen. So hat ein Angreifer bei einer erfolgreichen Attacke noch nicht Zugriff auf die komplette Datenbank, Nutzer-Verwaltung oder ähnliches.
Die Anzahl der Dienste sollte also genauso wie die Anzahl der Personen mit Zugriffsberechtigung minimiert werden. Nicht benötigte Ports sind zu schließen. Die Wahl eines geeigneten Betriebssystems ist selbstverständlich von großer Bedeutung. BSD-Betriebssysteme sind mit viel Rücksicht auf Sicherheit entwickelt worden und bieten einige sehr interessante Ansätze (zB Secure Levels oder Immutable Files), sind aber trotzdem nur soweit sicher soweit sie gut administriert werden.

Sicherheit des Web-Servers und der angebotenen Skript-Sprachen

Die Konfiguration eines Web-Servers und den Skript-Sprachen ist nicht trivial, und sollte von einem Fachmann durchgeführt werden. Web-Server und Skript-Sprachen werden in der Praxis zu selten upgedated, weil Veränderungen der Standard-Installation in der Vergangenheit zu nicht funktionierenden Web-Seiten und Applikationen führten. Ein Fehler an dieser Stelle reicht meistens aus, um in den Server einzudringen.
Sicherheitsgrundsätze für Web-Server sind: SSL (Verschlüsselung) aktivieren, Zugriff soweit wie möglich limitieren (zB mittels .htaccess), nicht benötigte Skriptsprachen (CGI) und Server-Module deaktivieren, jegliche Software am neusten Stand halten, Log-Dateien kontrollieren.
Alleine die POST-Anfragen auf die Login-Seite oder andere Formulare, und

weitere von dieser IP-Adresse ausgehende Aktivitäten (nicht nur im Webserver- sondern auch im Firewall-Log!) können durch wenige Kommandozeilen-Befehle angezeigt werden, und sind äußerst interessant.

Sicherheit der Web-Applikation

Schlussendlich muss auch die Web-Seite / Applikation selbst den Sicherheitsansprüchen genügen. Die Skriptsprache PHP erlaubt in der Standardinstallation (register_globals aktiviert) unsichere Implementierungen, und ermöglichte dadurch eine Vielzahl von Angriffen. Durch ungenügende Variablen-Überprüfung oder unsichere, direkt übernommene oder unzureichend geprüfte Pfadangaben kann man beispielsweise Passwort-Dateien auslesen, auf die Datenbank zugreifen (SQL Injection) und für andere Clients schädlichen Code in der Seite hinterlassen (XSS).

Und letztendlich sind auf Web-Seiten veröffentlichte E-Mail-Adressen ein Garant für Spam. Im Moment stark im Kommen ist Werbe / Malware / Google-Ranking verbessernder Spam durch Bots in Foren, Gästebüchern und Kontaktformularen.

Sicherheit der Verbindung

Die Verbindung vom Client zum Server ist eine weitere Schwachstelle. Durch Man-in-the-Middle-Attacken oder Packet Sniffing kann die Verbindung abgehört und manipuliert werden. Mögliche Abwehrmaßnahmen sind Verschlüsselung, am besten in Kombination mit einer Überprüfung des Server-Zertifikates durch den User (siehe auch Kapitel 3.3.3, Gegenmaßnahmen zu Phishing & Pharming).

Weiterführende Überlegungen

Ist der anfragende Client mit Malware infiziert, so ist zumindest eine Überwachung - und damit zB das Erlangen der Zugangsdaten - auch an dieser Stel-

le möglich. Zugangsdaten werden erstaunlich oft unverschlüsselt per E-Mail versandt. Die Authentifikation des FTP-Protokolls erfolgt ebenfalls nicht verschlüsselt.

Benutzer verwenden durch die Vielzahl der benötigten Zugangsdaten oft die gleichen Passwörter für verschiedene Dienste, was weitere Angriffsmöglichkeiten bietet.

4.4. Gegenmaßnahmen

Neben präventiven Maßnahmen wie einer umfassenden Sicherheitsstrategie, Firewall und Zugriffskontrolle sind vor allem Intrusion Detection Systeme (IDS) und ähnliche Maßnahmen empfehlenswert. Das regelmäßige Kontrollieren von Log-Dateien oder das Installieren von Honey-Pots kann aufschlussreiche Hinweise zu Einbruchs-Versuchen und -Methoden sowie Schwachstellen im System liefern. Wichtig ist die fortlaufende Kontrolle dieser Maßnahmen: Hat der Eindringling einmal Vollzugriff auf die internen Rechner, so ist es auch ein Kinderspiel, Log-Dateien zu verändern oder ein IDS auszuhebeln.
Falls die im Firmennetz befindlichen Vermögenswerte von großer Bedeutung und hohem Wert sind sollte die Durchführung von Sicherheits-Audits durch externe Firmen überlegt werden. Die Kosten dafür sind in etwa gleich wie die der Erarbeitung und Implementierung einer Sicherheits-Strategie [SecretsAndLies]. Ein umfassendes Kompendium zu für Firmen relevanten Sicherheitsthemen wie Authentifizierung bzw. Zugriffskontrolle, Sicherheitsstrategien und -modellen und weiteren zur Absicherung von Firmennetzwerken relevanten Aspekten bietet das Buch [IT-Sicherheit].

4.4.1. Kryptographie

Auf die Details kryptographischer Algorithmen und Implementierungen soll hier nicht eingegangen werden. Nur so viel: Es ist aus kryptographischer Sicht

möglich, Daten oder Verbindungen nur mit unrealistisch und unwirtschaftlich hohem Aufwand knackbar zu machen. In den allermeisten Fällen ist es aus Sicht des Angreifers nicht notwendig, sich die Mühe zu machen, Daten zu entschlüsseln, weil es viele einfachere Angriffsmöglichkeiten gibt. Das soll nicht heissen, dass Kryptographie nutzlos ist - im Gegenteil. Aber sie ist meistens noch das stärkste Glied der Sicherheits-Kette, solange sie gut ausgewählt und implementiert wurde.

5. Politische Entwicklungen

Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren. (Benjamin Franklin)

Die zunehmende Verbreitung und Wichtigkeit des Internets schuf Platz und Notwendigkeit für die Politik. Die Versuche, aus den anfänglich anarchisch anmutenden Strukturen ein regulier- und kontrollierbares System zu schaffen sind zwar häufig von nicht allzu viel Erfolg gekrönt gewesen, werden aber zunehmend vehementer forciert und sind in großer Bewegung. Ob Maßnahmen wie beispielsweise die Speicherung von Verbindungsdaten (siehe Kapitel 5.1) gerechtfertigt, notwendig und zielführend sind ist äußerst fragwürdig. Sogar das Gegenteil könnte der Fall sein: Die dadurch zusätzlich entstehende Datenflut schafft Raum für weitere, die Privatsphäre von Bürgern verletzende Aktivitäten - und wie die Geschichte zeigt: Was missbraucht werden kann, das wird missbraucht. Wer garantiert die Integrität der gesammelten Daten, die ja in Folge zu Verhaftungen führen können? Im Rahmen von diversen Anti-Terror-Maßnahmen, Kinderpornographie-Verfolgungen und auf Drängen der Film- und Musikindustrie wird somit die Grundlage für eine mögliche Gesamtüberwachung der Gesellschaft aufgebaut.

Die notwendigen Änderungen der Gesetzgebung durch Kriminalität im Internet werden grundsätzlich überschätzt: Gesetze für Einbrüche, Sachbeschädigung oder Diebstahl sind bereits vorhanden. Der entstehende Schaden ist bei Vergehen im virtuellen Raum durchaus real, und es spricht wenig dagegen, diese Gesetze auch auf das Medium Internet anzuwenden. Ein Hindernis ist eher die fehlende internationale Kooperation und Koordination bei der Grenzüberschreitung von Straffällen.

5.1. Überwachung, User-Kontrolle und Zensur

Die EU hat ihre Mitgliedsländer dazu verpflichtet, ab spätestens 2009 alle Verbindungsdaten für mindestens 6 und maximal 24 Monate aufzeichnen zu lassen[1], wobei die Rechtmässigkeit dieser Maßnahme noch nicht vollends geklärt ist. Auf das Internet bezogen heißt das, dass vom Kunden besuchte Internet-Seiten sowie Absender und Empfänger von E-Mails mit jeweiligem Datum und Uhrzeit abgespeichert werden[Überwachungsmafia]. Weiters werden Absender und Empfänger von SMS-Nachrichten, Telefon-, Handy- und Fax-Kommunikation und im Falle von Mobilfunk auch die Standortangaben aufgezeichnet. Die direkte Gefahr für Bürger mag nicht offensichtlich sein - aber die Menge an Daten erlaubt vielerlei Analysen und Rückschlüsse. Verdächtige oder ungewöhnliche Kommunikationsmuster könnten durch Netzwerkanalysen eruiert werden. Selbst wenn der Inhalt einer Nachricht nicht bekannt ist, so können auch die Dauer (bzw. im Falle einer E-Mail die Grösse) einer Kommunikation, der Zeitpunkt, die Wiederholungen bzw. durch die Kommunikation ausgelöste weitere Kommunikationen nützliche Informationen liefern [SecretsAndLies]. Der behördliche Zugriff auf diese Daten ist nicht geregelt, was deren Missbrauch vorprogrammiert.

In Artikel 8, Punkt 1 der europäischen Menschenrechtskonventionen heißt es:
'*Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.*
Ob damit gemeint ist, dass diese Daten aufgezeichnet werden sollen, ist zweifelhaft.

Prekär ist auch die Tatsache, dass die EU bereit ist, diese Daten in "specific and well defined cases" an die USA weiterzuleiten[2] - die ja selbst lange Zeit internationale Carrier und Backbone-Leitungen illegal überwacht hat[3].

[1] http://register.consilium.eu.int/pdf/de/05/st03/st03677.de05.pdf
[2] http://www.europarl.eu.int/registre/questions/reponses_qe/2006/2846/P6_RE(2006)2846_EN.doc
[3] http://www.heise.de/newsticker/meldung/73767

Da manche Regierungen nicht allzu zimperlich mit *potentiellen* Kritikern, Terroristen oder Mördern umgehen (illegale Entführungen durch die CIA[4], mögliche Verhaftung/Therapierung von Personen die ein ähnliches Persönlichkeitsprofil wie Mörder[5] aufweisen) sind derartige Maßnahmen kritisch zu betrachten.

5.1.1. Google

Das Ungleichgewicht zwischen Konzernen und Regierungen spiegelt sich auch in der Überwachung wider, bei der große Unternehmen eine bedeutende Rolle spielen. Neben "kleineren" Vergehen die als Spyware klassifiziert werden (Kapitel 3.2.3) ist die Fülle an Daten, die Google nicht nur durch seine Suchmaschine, sondern vor allem durch die Verknüpfung von Daten aus den Diensten wie GMail, Google Calendar, Google Earth oder Google Analytics erhält bzw. erhalten könnte, durchaus bereits von politischer Relevanz, da sie bisher ungeahnte Möglichkeiten der Kontrolle, Überwachung und Zurückverfolgung ermöglicht. Das Privacy Statement von GMail besagt, dass Google keine personenbezogenen Informationen weitergeben oder verkaufen wird. Im Falle einer Übernahmen bleiben diese Rechte jedoch nicht gesichert: "We reserve the right to transfer your personal information in the event of a transfer of ownership of Google, such as acquisition by or merger with another company"[GMail].

Länder könnten Google gesetzlich zur Herausgabe der Daten zwingen, was jedoch bisher scheiterte[6]. Die Firma selbst ist als Aktiengesellschaft dem Profit verpflichtet. Der Firmengrundsatz "Do No Evil" ist veränderbar (GMail-User werden beispielsweise über von Google als signifikant erachtete Änderungen bei der Login-Seite informiert), und die Weitergabe bzw. der Verkauf von personenbezogenen Daten ist in den USA im Gegensatz zu Europa sehr

[4] http://www.zeit.de/2005/52/Kurnaz
[5] http://www.heise.de/newsticker/meldung/81606
[6] http://www.heise.de/newsticker/meldung/71000

wohl erlaubt[SecretsAndLies]. Die Zusammenarbeit mit der chinesischen Regierung zur Zensur von Suchergebnissen - siehe auch Kapitel 5.1.2 - ist daher alles andere als beruhigend. Die drohende Rufschädigung und der daraus entstehende Schaden und Machtverlust dürfte wohl derzeit hauptverantwortlich für die Beibehaltung des Firmenmottos sein. Das negative Potential dieser Menge an personenbezogenen Daten ist mehr als alarmierend.

5.1.2. Zensur

Zensur ist in den westlichen Ländern kein großes Thema mehr, in den westlichen Konzernen leider sehr wohl. Diese helfen pflicht- und profitbewusst mit, kritische Bürger autoritärer Staaten oder Diktaturen zu überwachen[7] oder gar zu verhaften[8].

Das Internet bietet glücklicherweise einige gute Gegenmaßnahmen: Anonyme Proxies (deren Log-Dateien verbindlich gelöscht werden sollten) und sich noch in der Entwicklung befindende Ansätze wie psiphon[9], das rein Browserbasiert ist und eine verschlüsselte Kommunikation vom Client zum ”Proxy“ bietet sind nur sinnvoll, solange man dem vermittelnden Rechner vertrauen kann (und kein Opfer einer Man-in-the-middle-Attacke ist). Für Remailer (Webseiten, über die man anonym E-Mails versenden kann) gilt das Selbe. Den besten Schutz bieten auf Peer-to-Peer-Technologie aufbauende Onion-Routing[10] Programme wie TOR[11]. Dadurch lassen sich Bewegungen und Aktionen im Internet sehr gut verbergen. Letzteres bietet sogar Schutz vor Netzwerkanalysen (siehe Kapitel 5.1), der Nachteil liegt in dem deutlich höheren Traffic und einer signifikanten Verzögerung jeder Kommunikation: Alle Datenpakete werden über mehrere, zufällig ausgewählte TOR-Rechner geroutet. Man selbst fungiert auch als Zwischenknoten für andere Nutzer.

[7] http://www.heise.de/newsticker/meldung/75703
[8] http://www.heise.de/newsticker/meldung/75479
[9] http://psiphon.civisec.org/
[10] http://chacs.nrl.navy.mil/projects/onion-routing/inet97/index.htm
[11] http://tor.eff.org/

TOR und SSH-Tunnels funktionieren sogar dann noch, wenn - wie beispielsweise in Singapur, dem westlichsten und reichsten aller asiatischen Länder - der gesamte Internet-Traffic über staatlich kontrollierte Proxies mit Filterregeln geroutet wird. Ein Problem wäre allerdings, wenn gesetzlich gegen Umgehungsmaßnahmen der Zensur vorgegangen wird, wie es in China der Fall ist. Die verschlüsselten Pakete müssten trotzdem über den Proxy geroutet werden, und können dort geloggt und identifiziert werden - somit ist natürlich auch die Ahndung des Verstoßes kein Problem mehr.

Die ”Great FireWall“ Chinas scannt den Inhalt von TCP-Paketen nach unerwünschten Schlüsselwörtern, und sendet gegebenenfalls RESET-Messages an beide Enden der Verbindung. Die auf dem ”Privacy Enhancing Technologies“ Workshop[PET] vorgestellte Methode, durch Änderungen im TCP-Stack diese RESET-Messages zu ignorieren ist zwar eine Möglichkeit zur Umgehung, aber sicher nicht der Weisheit letzter Schluss. Der Umstellungsaufwand wäre gigantisch, da er auf *beiden* Seiten notwendig wäre, weiters könnte das Deaktivieren von RST-Flags andere technische negative Auswirkungen mit sich bringen.

Die Beschlagnahmung mehrerer frei zugänglicher TOR-Knoten durch die deutsche Polizei im Rahmen einer Razzia gegen Kinderpornografische Internet-Foren[12] ist nur durch absolutes Unverständnis von TOR - die dort vorhandenen Log-Dateien sind völlig wertlos - oder aber durch eine Aversion gegen TOR zu erklären. Die Beeinflussung der öffentlichen Meinung durch die Assoziation von Anonymisierungswerkzeugen mit Kinderpornografie und Terrorismus durch Aktionen wie dieser sollte nicht unterschätzt werden, insbesondere bei der kommenden Ratspräsidentschaft Deutschlands, deren primäres Ziel die Kontrolle des Internet - ”einer Fernuniversität und Trainingscamp für Terroristen“[13] - sein wird.

[12] http://www.heise.de/newsticker/meldung/77915
[13] http://www.heise.de/newsticker/meldung/82283

5.1.3. Trusted Computing Group - TCG

Das Ziel von Trusted Computing ist es, die Ausführung von Software auf Rechnern besser kontrollieren zu können, um Malware zu vermeiden und Datendiebstahl zu verhindern (offiziell) und Urheberrechts-Verletzungen zu verringern (inoffiziell) - und somit eine vertrauenswürdige Rechner-Landschaft herzustellen.

Die TCG ist der Nachfolger der Trusted Computing Platform Alliance (TCPA). TC-Implementationen bestehen aus zwei Hardware-Teilen: Dem Trusted Platform Module - TPM, für die Verschlüsselungs-, Hash- und Speicher-Funktionalität zuständig, und dem Root of Trust for Measuring Integrity Metrics - RTM, für die Zur-Verfügung-Stellung von darauf basierenden Funktionen. Dazu gehört noch ein Software-Teil (Trusted Software Stack - TSS), die API für Zugriffe auf von TPM und RTM.

Diese Module stellen dem Betriebssystem Sicherheits- und Integritätskontroll-Funktionen zur Verfügung, die jedoch entgegen der verbreiteten Meinung keinen absoluten Kontrollverlust des eigenen Rechners mit sich bringen: Die Spezifikation sieht vor, dass das TPM standardmässig deaktiviert ist, und dass im Falle einer Aktivierung (die übrigens einen - hoffentlich - nur dem Anwender bekannten Schlüssel voraussetzt) jederzeit manuell deaktiviert werden kann. Derzeit ist diese Deaktivierung durch Jumper gelöst. Das Starten des Betriebssystems ist auch im Falle von Veränderungen der Soft- oder Hardware explizit möglich. Die Aktionen, die das Betriebssystem in solch einem Fall tätigt, sind durch die TCG nicht festgelegt, und hängen von der jeweiligen Implementation im Betriebssystem ab. Die Bewahrung der Anonymität ist durch die Einführung von Attestation Identity Keys (AIK) berücksichtigt worden.

Erste Hardware-Implementierungen sind seit 2003 vorhanden. Windows Vista wird voraussichtlich erstmals für die Unterstützung auf Betriebssystem-Ebene sorgen. Das reicht aber nicht aus: Alle kritischen Komponenten eines Rechners - dazu gehören auch Elemente wie die Grafikkarte oder der Direct Memory Access-Controller - müssen TC unterstützen. Ohne umfassende Hardware-Unterstützung ist kein sicherer und kontrollierbarer Bootprozess möglich, der

aber eine Voraussetzung ist, um das darauf aufbauende Betriebssystem auch als sicher klassifizieren zu können.

Der Hauptgrund für das Vorantreiben dürfte die Durchsetzung von Digital Rights Management (DRM), der Abspiel-Kontrolle von Mediendateien, sein, das nicht zu Unrecht auch ”Digital Restriction Management“ genannt wird. Weitere Einsatzmöglichkeiten sind die unternehmensweite Umsetzung von Sicherheits-Policies, also die Kontrolle und Restriktion von Zugriffen auf Dokumente.

Es gibt aber noch viele ungeklärte Probleme und Fragen beim Einsatz von TC: Es können nur sehr schwer alle Software-Komponenten jeglicher Rechner überprüft und signiert werden, das wäre bei der heutigen Software-Landschaft ein gigantischer Aufwand. Deshalb trennt Microsoft in seiner NGSBC-Implementierung zwischen kritischer und unkritischer Software. Unkritische Software benötigt keine Signierung. Der Wurm Lovesan verwendete zwei Kommandos: tftp.exe und cmd.exe. Beide Befehle sind als unkritisch definiert, und unterliegen nicht der Überprüfung einer Integritätskontrolle. Eine vollständige Implementation von TC wäre also gegen einen *alten* Virus nutzlos [IT-Sicherheit], wodurch sich sehr leicht auf die Wirksamkeit gegen *neue* Malware schließen lässt. Die Umsetzung von Sicherheits-Policies scheint derzeit aus Benutzer-Sicht die einzig sinnvolle Anwendung von TC zu sein. Die Effektivität hängt stark von den jeweiligen Betriebssystem-Implementierungen und der Definition und Exaktheit der jeweiligen Policies ab.

Ein weiteres , bisher ungeklärtes Problem ist der Zugriff auf Backups bei einem Defekt des TPM-Chips. Die Anfertigung von Ersatz-Chips würde den Datenschutz aushebeln, und viele Sicherheitskonzepte nutzlos machen.

Laut dem Kryptoforscher Rüdiger Weis gilt der dem TMP zugrunde liegende SHA-1 mittlerweile als geknackt. Dadurch könnte man Software so manipulieren, dass sie wieder den gleichen Hash-Wert ergibt, wodurch die Verifizierung umgangen werden könnte. SHA-1 ist bei TC in Hardware implementiert, und daher nicht veränderbar[14].

[14] http://www.heise.de/newsticker/meldung/67809

Weiters muss das Lizenzieren und Verifizieren (und die damit verbundenen Kosten) von Open-Source-Software, die mittlerweile vor allem im Server-Bereich eine wichtige Rolle spielt, oder anderer sich häufig ändernder Software noch geklärt werden.

Das Betriebssystem sollte eine möglichst kleine, sichere Schicht (zB Micro-Kernel) zwischen den Applikationen und der Hardware sein [ossTC], das die Ausführung der Applikationen und Einhaltung der Policies kontrolliert.
Bei herkömmlichen, monolithischen Betriebssystem-Kernen kann diese Sicherheit aufgrund der Komplexität nicht garantiert werden. Das Betriebssystem könnte manipuliert werden, sodass die - nur passiv angebotenen - TPM-Funktionen einfach nicht mehr abgefragt werden, was ja rein Aufgabe des Betriebssystems ist, so wie manche Viren Anti-Viren-Software einfach deaktivieren. Ähnlich wie Virtual Machines muss die Kontrollinstanz eine Ebene tiefer angesiedelt sein.

Angenommen, es wird die Integrität jeglicher für Client-PCs vorhandenen Software überprüft. So könnten die Entwickler-Firmen sich durch die Unmöglichkeit von dauerhaften Betriebssystem-oder Programm-Infektionen (bei einer unerwünschten Veränderung wird der letzte attestierte Zustand wiederhergestellt) wesentlich mehr Zeit bei der Anfertigung von Patches zu Sicherheitslücken lassen. Benutzer spielen aus ebendiesem Grund die Updates später oder gar nicht ein. So ist zwar kein Rechner dauerhaft infiziert. Durch eventuelle, sich aufschaukelnde Wurm-Infektionen und den dadurch entstehenden Traffic könnte das Internet allerdings an die Grenzen seiner Kapazität gelangen.
Ein ähnliches Problem würde übrigens die dauerhafte, vermehrte Benutzung von nicht oder nur schwer veränder- und aktualisierbaren Live-Systemen mit sich bringen, die oft fälschlich als unverwundbar hingestellt werden. Davon abgesehen ist eine temporäre Verwundbarkeit auch nicht der Weisheit letzter Schluss, damit würden genügend Sicherheits-Probleme weiter bestehen bleiben.

Fazit und eigene Meinung
In der derzeitigen Form wird TC auf Rechnern durch die Vielzahl der offenen

Fragen und noch nicht vollständigen Hardware-Unterstützung in den kommenden Jahren keine wichtige Rolle spielen. Der Grundgedanke und die Motivation hinter TC werden jedoch bleiben. Sollten die Design-Probleme ausgemerzt werden, und TC hardware-seitig voll unterstützt sein, so wäre eine durchgängige TC-Landschaft denkbar, was eine Revolution der PC- und Sicherheitslandschaft bedeutet. Bis dahin sind aber noch viele Probleme zu lösen, vor allem muss die Privatsphäre, Anonymität und die Kontrolle über den eigenen PC gewährleistet bleiben.

5.2. Länderübergreifende, politisch motivierte Kriminalität

Um Firmen oder Regierungen anzugreifen ist meist ein deutlich größeres Fachwissen nötig, als bei Einbrüchen in die Rechner von Endbenutzer. Diese hängen aber stark miteinander zusammen - siehe Kapitel 3.1. Hacker bzw. Cracker haben ein sehr gutes Fachwissen und sehr viel Zeit, Terroristen schrecken weder vor hohen Strafen noch vor physischen Angriffen zurück.

5.2.1. Terrorismus

Terrorismus wird als wichtiges Thema der letzten Jahre natürlich auch mit dem Internet in Verbindung gebracht. Selbstverständlich nutzen Terroristen genauso die Vorteile des Internets. Laut [cyberterrorismus] benutzen Terroristen das Internet hauptsächlich für fünf Punkte: Informationsbereitstellung, Finanzierung, Kommunikation/Koordination, Mitgliedergewinnung/Werbung und Informationsgewinnung. Diese Aktivitäten können nicht ohne massive Einschränkung der Bürger- und Datenschutz-Rechte kontrolliert werden. Und selbst wenn beispielsweise alle Anleitungen zum Bau von Bomben aus dem Internet entfernt werden (was so gut wie unmöglich ist), wäre diese Informati-

on noch durch viele Zeitschriften, Bücher[15] oder bereits auf PC's heruntergeladenen Anleitungen verfügbar.

Angriffe gegen das Internet selbst - beispielsweise in der Form von physischen Attacken gegen die Hauptknoten - sind zwar unwahrscheinlich, aber möglich. Solche Angriffe können durch die Routing-Eigenschaft von TCP/IP korrigiert werden, solange sie nicht massiv sind. 80 % des inner-amerikanischen Datenverkehrs wird über 12 Knotenpunkte geroutet[HackersGuide].
Angriffe durch Software könnten das Internet zumindest für einen begrenzten Zeitraum stark beeinträchtigen[SecretsAndLies]. Dazu wäre viel Know-How notwendig, das man sich widerum nur über das Internet aneignen kann, wobei man wahrscheinlich schnell die eigenen Einsatzmöglichkeiten und Vorteile erkennen würde, und damit der Angriff unwahrscheinlicher wird.

Bereits 1997 wurde von einem Jugendlichen das Netzwerk eines Flughafens geknackt. Der Kontrollturm, die Flughafenfeuerwehr und die Kommunikationseinrichtungen waren sechs Stunden lang ausser Gefecht gesetzt.
2002 wurden in Santiago de Chile 17 Computer gestohlen, die für die Steuerung des lokalen Verkehrsnetzes dienten. Der Verkehr der Stadt stand für drei Tage lang still. [HackersGuide]

Eine Kombination derartiger Attacken könnte physische Angriffe um vieles verheerender und effektiver machen.
Ende Oktober 2006 einigten sich die Innenminister von England, Frankreich, Deutschland, Italien und Spanien, die Zusammenarbeit bei der Überwachung und Analyse von terroristischen Bewegungen im Internet zu intensivieren[16], bzw. Deutschlands "check the web"-Initiative zu unterstützen.

5.2.2. Cyber-Wars

Cyber-Wars im eigentlichen Sinne sind noch nicht existent, sondern derzeit nur eine - von Bürgern durchgeführte - Begleiterscheinung von realen Attacken,

[15] The Anarchist Cookbook, William Powell
[16] http://www.press.homeoffice.gov.uk/press-releases/g6-meeting-conclusions

die übrigens selbst in die Kategorie Terrorismus fällt.
Als Antwort auf die Terroranschläge des 9. Septembers begannen Hacker-Gruppen, diverse Ziele in Afghanistan oder Iran über das Internet anzugreifen. Hunderte Web-Seiten wurden defaced, und DDoS-Attacken durchgeführt. Der CCC[17] rief dazu auf, die Angriffe einzustellen und auf Kommunikation zur Konfliktlösung zu setzen.[cyberterrorismus]
2001 wurden aufgrund eines chinesischen Spionageflugzeugs etwa 2.500 chinesische Web-Sites defaced, und im Gegenzug dazu 1.200 amerikanische Seiten.

Verschiedene Regierungen, allen voran die USA, haben aber schon längst begonnen, Teams für den "network warfare" aufzubauen[18]. Genauere Informationen zu diesem Thema sind verständlicherweise so gut wie nicht erhältlich, Geheimdienste lassen sich nur ungern in die Karten sehen.

Auch wenn ein Cyber-War alleine derzeit noch vergleichsweise geringen Schaden anrichtet: Mit der zunehmenden Bedeutung und Durchdringung des Internets nimmt auch das Gefahrenpotential und damit die Wahrscheinlichkeit von Cyber-Wars zu.
In den kommenden Jahren ist eher eine Ausweitung bereits durchgeführter Angriffe wie Industriespionage5.3, (militärische) Informationsgewinnung durch Einbrüche, oder eine (vom Staat ausgehende) Kombination von physischen Angriffen und Netzwerk-Attacken wahrscheinlicher als reine Cyber-Wars.

5.3. Industriespionage

Bei dem ersten dokumentierten Computer-Einbruch [Kuckucksei] wurden 1986 die gestohlenen Daten westlicher Firmen oder Geheimdienste an den KGB verkauft. Die Einbrüche hätten ohne den KGB nie dieses Ausmaß erreicht.
Industriespionage über das Internet ist keine Science-Fiction, sondern schon

[17] Chaos Computing Club http://www.ccc.de/
[18] http://armed-services.senate.gov/statemnt/2005/March/Cartwright%2003-16-05.pdf

lange tägliche Realität [KunstDerTäuschung]. Russland entwendete umfangreiche Daten über das amerikanische Raumfahrtsprogramm, und konnte damit auf viele kostspielige Eigenentwicklungen, Forschungen und Tests verzichten. Die NSA stahl Daten und Pläne für eine neue 500-Megawatt-Windkraftanlage der Firma Enercon in Austrich. Dazu gehörte nicht nur das Abhören der Telefonate und E-Mails, sondern weiters das Anzapfen der Datenleitung zwischen dem Forschungslabor und dem Firmen-Hauptsitz, sowie der physische Einbruch in eine Windkraftanlage. Die NSA leitete die Daten an die amerikanische Firma Kenetech weiter, die die entsprechenden Patente in Amerika einreichte [Wirtschaftskriminalität]. Auch ohne das Zutun von Regierungen passiert Industriespionage. Der Wandel westlicher Länder zu einer Informations- bzw. Wissensgesellschaft, und der zunehmende Wert immaterieller Güter und Daten werden zu einer weiteren Zunahme von Industriespionage führen. Länder, deren Geheimdienste und Firmen haben erhebliche finanzielle Ressourcen und oft ein sehr gutes Fachwissen - beziehungsweise die finanziellen Möglichkeiten, das nötige Fachwissen zu erwerben [SecretsAndLies].

6. Aktuelle Tendenzen und mögliche zukünftige Entwicklungen

Während im Jahre 1999 der Schaden durch Kriminalität im Internet noch auf 10 Mrd. Euro geschätzt wurde[Wirtschaftskriminalität], so schätzt die Sicherheitsfirma mi2g[1] den Schaden im Jahr 2006 auf 220 bis 260 Mrd. Dollar - was beinahe dem österreichischem BIP entspricht, und eine jährliche Steigerung von knappen 60 % bedeutet. Genaue Zahlen sind mit großer Vorsicht zu genießen. Viele Unternehmen oder Länder verschweigen erfolgreiche Angriffe aus Angst vor Rufschädigung.

6.1. CERT-Statistik

Laut dem Computer Emergency Response Team (CERT) der Carnegie Mellon Universität (CMU) ist die Anzahl der Sicherheitslücken, vor allem aber die Anzahl der Angriffe stark steigend [Netzwerksicherheit]:

2001	2002	2003	2004	2005	2006
100	2.200	4.100	3.900	3.900	6.000

Tabelle 6.1: CERT Schwachstellen-Statistik

1999	2000	2001	2002	2003
10.000	20.000	52.000	82.000	137.000

Tabelle 6.2: CERT Zwischenfall-Statistik

[1] http://www.mi2g.com/

Diese Zahlen sollen nur die Tendenz darstellen: Wie bereits erwähnt werden nicht alle Zwischenfälle und Schwachstellen dem CMU CERT gemeldet, außerdem gibt es seit 2002 in vielen anderen Ländern weitere CERT's, was die Schwachstellen-Stagnation zwischen 2002 und 2005 erklären könnte.

6.2. Kommerzialisierung der Kriminalität

Wurden in den Anfängen des Internets Computer-Einbrüche hauptsächlich aus Interesse oder zum Aufzeigen von Schwachstellen durchgeführt, so ist davon - und von der vom CCC definierten Hacker-Ethik (Appendix A.3) leider nicht mehr viel bemerkbar. Cracker, Kriminelle Banden, Netzwerke und Firmen sind involviert, und es fließt zusehens mehr Geld. Ein Windows Vista-Exploit dürfte bei Untergrund-Auktionen aktuell etwa 20.000 US-$ bis 50.000 US-$ kosten[2], während ein WMF-Exploit am Jahresanfang noch für 4.000 US-Dollar zu haben war[3].

6.3. Überwachungs-Problematik

Regierungen und Firmen sind gerade dabei, die Basis für einen elektronischen Überwachungsstaat aufzubauen. Noch vor wenigen Jahren wurde man als Verschwörungstheoretiker belächelt, wenn man behauptete, was heute nachgewiesen ist - die USA überwacht(e) das Internet, die CIA entführt(e) illegal Menschen auf europäischem Boden, und spioniert Firmen aus (siehe 5.1).
Noch immer erscheint ein Überwachungsstaat unwahrscheinlich - trotzdem sind die technischen Möglichkeiten und Voraussetzungen gegeben, und die aktuellen und möglichen Übergriffe von Staaten auf Privatpersonen sollten genau beobachtet werden. Dass etwa Maßnahmen wie der Fernzugriff durch

[2] http://www.heise.de/newsticker/meldung/82679
[3] http://www.heise.de/security/news/meldung/69207

Regierungen auf Privat-PCs in Deutschland ernsthaft vorgeschlagen und diskutiert werden[4] ist einerseits absolut lächerlich, andererseits sehr bedenklich. Genannt "Programm zur Stärkung der inneren Sicherheit" erinnert es belesene Bürger an "Krieg bedeutet Frieden, Freiheit ist Sklaverei und Unwissenheit ist Stärke"[5].

6.4. Ausweitung der Angriffe

Vermehrt werden kritische Infrastrukturen wie Banken und Börsen oder Kommunikation an das Internet angeschlossen, und bieten dadurch weitere Angriffsmöglichkeiten, vor allem in Verbindung mit Terrorismus oder Cyber-Wars. Auch Handys, Handhelds, digitale TV-Geräte mit Rückkanal und die Verbindung von Haushaltsgeräten oder ganzen Häusern mit dem Internet werden noch für viele Schlagzeilen sorgen.

6.4.1. VoIP-Sicherheit

Voice over IP (VoIP) liegt im Trend, birgt aber viele Risiken. Es kann an zahlreichen Stellen (VoIP Gateway, DoS-Attacken, Schwachstellen in der Protokoll-Implementierung oder in einem Server-Betriebssystem, "herkömmliche" Netzwerkattacken uvm.) angegriffen werden [voip-sicherheit]. Der durchgehende Einsatz von VoIP und die damit verbundenen Risiken sollten in Unternehmen gut überlegt werden. Die immer beliebter werdenden DDoS-Angriffe würden beim Einsatz von VoIP noch mehr Schaden verursachen, und Gegenmaßnahmen erschweren.

[4] http://www.heise.de/newsticker/meldung/82154, http://www.im.nrw.de/pm/280806_947.html

[5] George Orwell, Roman "1984"

6.4.2. Survivability

Zusätzlich zur Vorbeugung von Angriffen sollten sich Firmen auch Gedanken machen, wie sie im Falle eines Angriffes oder eines Teil- bzw. Komplettausfalles der IT-Infrastruktur reagieren, um den normalen Geschäftsbetrieb möglichst ungestört aufrecht zu erhalten. Das Stichwort heißt Survivability - also die Überlebenskraft eines Netzwerkes bzw. einer Firma im Falle von Angriffen und Ausfällen - die verständlicherweise eine immer wichtigere Rolle spielt [BeyondSecurity]. Laut diesem Artikel ist der Einsatz von Managed Security Service Provider (MSSP), also die Beauftragung einer Fremdfirma zur Gewährleistung bzw. Maximierung der Sicherheit, für die meisten Firmen vorteilhafter als der Einsatz von eigenem Personal. Fremdfirmen haben in diesem Bereich oft ein besseres, differenzierteres Know-How und mehr Erfahrung, wodurch sich der Zukauf lohnt, um sich auf die Kernkompetenzen konzentrieren zu können.

6.5. Technische Änderungen

Laut [SecretsAndLies] sollte man folgende Entwicklungen im Auge behalten:

- Kryptographische Durchbrüche, Faktorisierungsdurchbrüche
- Quanten-Computer
- Künstliche Intelligenz
- Sichere Netzwerkinfrastrukturen, Gewährleistung - siehe auch Trusted Computing (TC), Kapitel 5.1.3
- Datenverkehrsanalyse

Am wahrscheinlichsten erscheint derzeit eine signifikante Änderung ausgehend vom dem Einsatz von TC.

6.5.1. Vermeidung von Buffer Overflows

Die Zahl der Buffer Overflow-Sicherheitslücken (Kapitel 2.1), derzeit die am häufigsten auftretenden und ausgenützten Lücken, könnte in den kommenden Jahren abnehmen. Höhere Programmiersprachen wie Java oder Python sind per Design gegen Buffer Overflows geschützt. Für systemnahe Programmiersprachen wie C stehen abgesicherte Bibliotheken (libsafe) zur Verfügung, außerdem gibt es Programme, die den Quellcode nach fehlerhaften Implementierungen durchforsten. Und schlussendlich wird auf Hardware-Ebene - im Prozessor - und auf Betriebssystem-Ebene versucht, strikter zwischen Programm-Speicherplatz und Daten-Speicherplatz zu trennen: AMD hat eine Buffer Overflow-Protection in Prozessoren integriert (NX-Flag), genauso wie Intel (Execute Disable-XD). Beide benötigen auch eine Unterstützung auf Betriebssystem-Ebene, die in den meisten aktuellen Versionen bereits integriert ist. Seit 2003 sind sowohl für Linux (Exec Shield) als auch für BSD (PROT_* purity, WX̂, .rdata, propolice) verschiedene Lösungsansätze vorhanden, die aber noch keinen hundertprozentigen Schutz bieten.

6.6. Fazit

Die politischen Entwicklungen sind äußerst besorgniserregend. Sicherlich verwenden Terroristen das Internet, sehr wahrscheinlich sind Konsumenten von Kinderpornografie eher als normale Bürger darauf bedacht, anonym zu bleiben. Die getroffenen Maßnahmen sind aber teilweise deutlich überzogen, und betreffen vor allem Normalverbraucher.

Obwohl heute auf den meisten Client-PCs rudimentäre Sicherheitsmaßnahmen wie Viren-Scanner und Firewalls installiert sind hat die Sicherheit nicht zugenommen. Das Sicherheits-Bewusstsein und -Verständnis ist noch zu niedrig, und die angewandten Techniken werden immer raffinierter.

Firmen sind sich zwar meistens der Gefahr bewusst, aber die Wahrscheinlichkeit wird als zu gering erachtet. Das Absichern der IT eines Unternehmens ist komplex und kompliziert, ein hundertprozentiger Schutz kann niemals gewährleistet werden - deshalb sollten Aspekte wie die Survivability beachtet werden.

Internet-Kriminalität ist den Kinderschuhen entwachsen, und hat sich von einer Handvoll technisch begabter, interessierter Freaks zu einer ernstzuehmdenden Bedrohung für viele Firmen gewandelt. Die geschätzten Schadenssummen sind erschreckend hoch - und steigen weiter. Dieser Trend wird sich auch in den kommenden Jahren fortsetzen, weil immer mehr Lebensbereiche und Geschäfte mit dem Internet verknüpft werden, sowie immer mehr Leute und Länder an das Internet angeschlossen werden.

Literaturverzeichnis

[ApacheSecurity] Ivan Ristic. *Apache Security*. O'Reilly Media, 2005.

[BeyondSecurity] Ramanan Ramanathan. Thinking beyond security, 2006. Information Systems Security.

[Datenspionage] Hagen Graf. *Datenspione stoppen.* Markt und Technik, 2003.

[EnterpriseSecurity] Walter Fumy and Jörg Sauerbrey. *Enterprise Security: IT Security Solutions: Concepts, Practical Experiences, Technologies*. Publicis Corporate Publishing, 2006.

[GMail] Edward H Freeman. Gmail and privacy issues, October 2006. Zeitschrift Information Systems Security.

URL `http://www.infosectoday.com`

[HackersGuide] Anonymous. *Hacker's Guide. Sicherheit im Internet und im lokalen Netz.* Markt+Technik, 2003.

[HackingExposed] George Kurtz Stuart McClure, Joel Scambray. *Hacking Exposed 5th Edition*. McGraw-Hill Osborne Media, 2005.

[IT-Sicherheit] Claudia Eckert. *IT-Sicherheit. Konzepte - Verfahren - Protokolle*. Oldenbourg, 2006.

[Kuckucksei] Clifford Stoll. *Kuckucksei*. Fischer (Tb.), Frankfurt, 1998.

[KunstDerTäuschung] Kevin D. Mitnick and William L. Simon. *Die Kunst der Täuschung. Risikofaktor Mensch*. Mitp-Verlag, 2006.

[Netzwerksicherheit] Michael Alexander. *Netzwerke und Netzwerksicherheit - Das Lehrbuch*. Hüthig Telekommunikation, 2006.

[PET] Carl E. Landwehr Stephen A. Weis. Privacy-enhancing technologies, June 2006. IEEE Conference Report.

[SecretsAndLies] Bruce Schneier. *Secrets and Lies. IT-Sicherheit in einer vernetzten Welt*. Wiley-VCH, 2004.

[Wirtschaftskriminalität] Frank Hartmann. *Wirtschaftskriminalität im Internet. Geschäftsrisiken durch Computermissbrauch und Datenspionage*. Deutscher Wirtschaftsdienst, 2001.

[cyberterrorismus] Maura Conway. Terrorist 'use' of the internet and fighting back, 2006. Information and Security, Vol. 19.

[ossTC] Christian Stüble Ahmad-Reza Sadeghi. Towards multilaterally secure computing platforms with open source and trusted computing, 2005. Information Security Technical Report.

[voip-sicherheit] Darrell Epps; Scott Tanner; Carl Silva. Can voip secure itself for the next technology wave?, 2006. Information Systems Security.

[wlan-security] Phil Cracknell. Why phish when you can trawl?, 2005. Information Security Technical Report.

[Überwachungsmafia] Pär Ström. *Die Überwachungsmafia. Das gute Geschäft mit unseren Daten*. Hanser Wirtschaft, 2005.

Appendix

A. Appendix

A.1. SANS Rangliste der IT-Risiken 2006

Die aktuelle Liste mit Erklärungen ist unter http://www.sans.org/top20 abrufbar.

Operating Systems

- Internet Explorer
- Windows Libraries
- Microsoft Office
- Windows Services
- Windows Configuration Weaknesses
- Mac OS X
- UNIX Configuration Weaknesses

Cross-Platform Applications

- Web Applications
- Database Software
- P2P File Sharing Applications
- Instant Messaging
- Media Players
- DNS Servers

- Backup Software
- Security, Enterprise, and Directory Management Servers

Network Devices

- VoIP Servers and Phones
- Network and Other Devices Common Configuration Weaknesses

Security Policy and Personnel

- Excessive User Rights and Unauthorized Devices
- Users (Phishing/Spear Phishing)

Special Section

- Zero Day Attacks and Prevention Strategies

A.2. Spam-Mail zur Suche nach Geldwäschern

Guten Tag,

EJF ist ein führendes Unternehmen, das hochwertige Online-Finanzdienstleistungen für Kunden auf 6 Kontinenten bereitstellt. Zurzeit planen wir die Ausweitung unseres Marketings und die Gewinnung neuer Kunden aus neuen Ländern.

Anfang des Jahres richteten wir neue Stellen für Finanzmanager ein und beschlossen, dass die vielversprechendsten Kandidaten direkt über das Internet angeworben werden sollten.

Versuchen Sie Ihre Glück mit EJF!

Arbeiten Sie als Finanzmanager, auch wenn Sie keine Erfahrung in diesem Vertriebs- und Marketingbereich haben. Sie müssen nur den richtigen Schwung, Ehrlichkeit und Fleiß mitbringen.

Bewerben Sie sich für die Position eines Finanzmanagers mit oder ohne Erfahrung im Bereich Finanz-Support und Abwicklung.

Ihre Vorteile:

1. Sie werden zunächst unser Vertreter und Mittelsmann zwischen uns und unseren Kunden in Ihrem Land.

2. Sie gewinnen Autorität bei Menschen aus aller Welt, die volles Vertrauen in Ihre Dienste setzen.

3. Sie zahlen keine Gebühren und müssen vor Arbeitsantritt nichts investieren (vergessen Sie betrügerische Stellenangebote, bei denen Sie erst zur Kasse gebeten werden).

4. Sie senken die Bereitstellungsfrist für Geldmittel und gewinnen das Vertrauen und die Hochachtung unserer Stabsmanager und unserer treuen Kunden.

5. Sie nehmen an der Anti-Betrugs-Kampagne des Unternehmens teil. Sie erhalten nur Überweisungen und kennen den Status einer jeden Transaktion, die von der Bank selbst geprüft wird.

6. Sie beschleunigen den Prozess von Zahlungsmethoden rund um die Welt und können dann rasch zu einem motivierten und unabhängigen Vertreter für EJF aufsteigen.

7. Sie kombinieren Ihre Routinearbeit mit Ihrem Service bei EJF.

8. Sie verwenden darauf rund 12 Stunden pro Woche und verdienen zwischen 500 und 800 Dollar pro Woche.

9. Sie erhalten Zahlungen von unseren Kunden, bearbeiten diese und leiten sie dann an unser Hauptbüro oder an eine unserer regionalen Zweigstellen weiter.

10. Sie können Karriere machen.

Wenn Sie daran interessiert sind, fordern Sie weitere Unterlagen über dieses Stellenangebot an.

E-Mail: careers@ejg-careers.com <mailto:careers@ejg-careers.com> (Ihre E-Mails bitte nur auf Englisch abfassen!)

Vielen Dank für Ihre Aufmerksamkeit.

Mit freundlichen Grüßen

Andrew Kaprinski

EJF Stabsmanager

A.3. CCC Hacker-Ethik

Quelle: Chaos Computing Club (CCC), http://www.ccc.de/hackerethics

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten - fördere Dezentralisierung
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern
- Mülle nicht in den Daten anderer Leute
- Öffentliche Daten nützen, private Daten schützen