IHRE DATEN ALS ROHSTOFF FÜR DIE ORGANISIERTE KRIMINALITÄT?

DR. NIELS LEPPERHOFF
BJÖRN PETERSDORF

Stand: 25. Oktober 2007

Inhaltsverzeichnis

Impressum

Herausgeber und Vertrieb
Xamit Bewertungsgesellschaft mbH
Zülpicher Str. 6
40549 Düsseldorf
www.xamit.de

Rechtliche Hinweise

1 Daten sind ein begehrter Rohstoff

Kriminelle schlachten Unternehmen aus

Seit wenigen Jahren existiert eine weltweite Schattenwirtschaft, die von Unternehmensdaten lebt (Kapitel 3). Dabei werden Unternehmen regelrecht ausgeschlachtet:

- Kunden-, Lieferanten- und Mitarbeiterdaten lassen sich an SPAM-Versender, Adresshändler und Betrüger weiterverkaufen. Ein Datensatz mit Kreditkarteninformationen besitzt einen Schwarzmarktwert von 15 bis 150 Euro.[1]
- Für Konstruktionspläne und Auftragsinformationen zahlen Wettbewerber und Geheimdienste.
- Andere Daten werden „entführt", d.h. verschlüsselt. Eine Entschlüsselung erfolgt erst nach Zahlung von Lösegeld.
- Webserver werden mit Betriebsunterbrechung bedroht, wenn kein Schutzgeld gezahlt wird.
- Firmencomputer lassen sich fernsteuern und für SPAM-Versand, Virenversand und auch für Angriffe auf Webseiten nutzen.
- Firmenserver eignen sich hervorragend, um illegale Musik- und Videokopien weltweit zu verteilen.

Schattenwirtschaft arbeitet professionell und arbeitsteilig.

Diese Schattenwirtschaft hat sich in den letzten Jahren professionalisiert und arbeitsteilig organisiert (Kapitel 4). Dank einer effizienten Arbeitsteilung brauchen Kriminelle kaum Fachwissen. Die notwendigen Softwareprogramme sind entweder frei erhältlich oder lassen sich einfach erwerben. Mit einem Baukasten für Trojaner [2] kann jeder Laie einen Trojaner mit wenigen Klicks zusammenbauen, den kein Virenscanner erkennt. Eine Sicherheitslücke kostet zwischen 20.000 und 125.000 US-Dollar.[3] Weil die Opfer selber für eine weitere Infizierung von Unternehmen bspw. durch den Versand von infizierten E-Mails sorgen, entstehen den Kriminellen kaum Kosten. Sie können sich ganz auf ihre Gewinne konzentrieren.

Keine Sicherheit trotz Virenscanner und Firewall

Einem Kriminellen stehen verschiedene Möglichkeiten offen, in ein Unternehmen einzudringen (Kapitel 5). Bereits das Internet bietet verschiedene kostengünstige und auch automatisiert nutzbare Wege an:

- Infizierte E-Mails und Webseiten
- Schwachstellen in Betriebsystemen oder Anwendungsprogrammen
- Schwachstellen in Firewalls
- Eindringen in unverschlüsselte WLAN z.B. am Flughafen
- Schwache Passwörter

[1] Heise Online (2007): Schlag gegen Internethandel mit illegal ausgespähten Kreditkarten-Daten. 29.06.2007. URL: http://www.heise.de/newsticker/meldung/91966
[2] Heise Online (2007): Trojaner-Basteln für Dummys. 20.07.2007. URL: http://www.heise.de/newsticker/meldung/93024
[3] Computer Zeitung (2007): Spione lauern auf Softwarelöcher. 10.09.2007, S. 6.

Eine persönliche Anwesenheit ist bei Internetangriffen nicht erforderlich. Dadurch besteht auch keine Gefahr erkannt und bestraft zu werden. Ein kleines Restrisiko besteht beim Notebook-Diebstahl aus dem Auto. Notebooks der Geschäftsführung enthalten meistens alle gewünschten Daten inkl. Passwörter und andere Zugangsdaten unverschlüsselt zum sofortigen Gebrauch.

Kriminelle suchen Opfer passend zum Angriff aus

Insbesondere Kriminelle suchen sich ihre Opfer passend zum Angriff aus. Wer die Opfer genau sind, ist unwichtig, da bei jedem Unternehmen „etwas zu holen ist“. Deshalb reicht bereits die Existenz einer Sicherheitslücke, um Opfer eines Angriffs zu werden. Virenscanner und Firewall sind zwar bekannte Sicherheitsprogramme versperren aber kaum einen Weg in das Unternehmen. Der Einsatz von Virenscanner und Firewall reicht deshalb nicht aus, um ein Unternehmen zu sichern. Vielmehr ist eine Gesamtstrategie notwendig.

Geschäftsführung haftet persönlich für Sicherheit

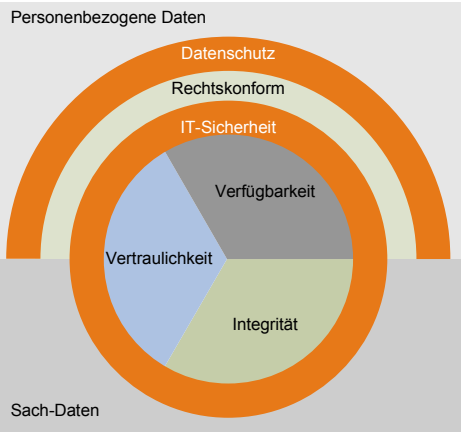
Der Gesetzgeber trägt dieser Entwicklung Rechnung, in dem er die Geschäftsführung persönlich für die IT-Sicherheit und den Datenschutz im Unternehmen verantwortlich macht. Die Geschäftsführung haftet persönlich mit Ihrem Vermögen unabhängig der Rechtsform des Unternehmens. Haftstrafen sind auch nicht ausgeschlossen.

Erst ein gut dokumentiertes und wirkungsvolles Vorgehen für die IT-Sicherheit und den Datenschutz begrenzen die persönliche Haftung. Wirkungsvolle Maßnahmen der IT-Sicherheit und des Datenschutzes umfassen sowohl die organisatorische wie auch die technische Ebene. Organisatorisch sollten bspw. Berechtigungen und Nutzungsregeln für IT-Systeme festgelegt werden. Technisch regeln dann Kontrollsysteme, dass nur berechtigte Mitarbeiter die jeweiligen Daten einsehen oder IT-Systeme nutzen können. Kurz:

IT-Sicherheit + Datenschutz = Existenz-Sicherung

Unter dem Begriff IT-Sicherheit werden alle organisatorischen und technischen Maßnahmen zusammengefasst, die die

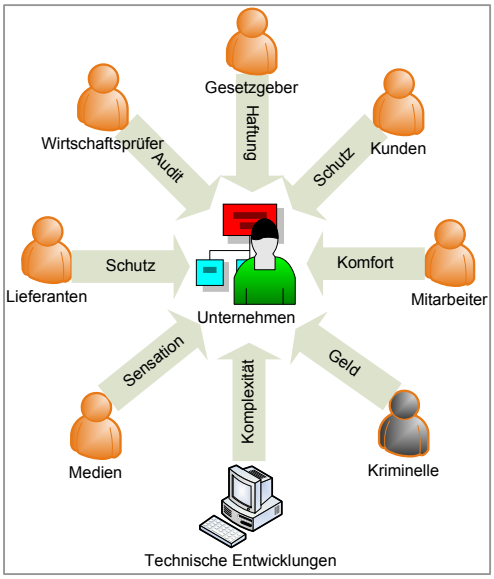
- Verfügbarkeit,
- Integrität und
- Vertraulichkeit



aller Daten und IT-Systeme im Unternehmen sicherstellen. Verfügbarkeit meint, dass die Daten und IT-Systeme genau dann zur Verfügung stehen und funktionieren, wenn diese benötigt werden. Daten und IT-Systeme sind integer, genau dann wenn sie nicht manipuliert wurden. Manipulierte Buchungssätze können bspw. zur Beanstandung der Buchführung durch das Finanzamt führen. Die Vertraulichkeit beschreibt, dass nur autorisierte Personen Zugriff auf die Daten und IT-Systeme haben.

Der Datenschutz geht für personenbezogene Daten geht über die IT-Sicherheit hinaus und berücksichtig auch die Kontrolle, dass die Datenverarbeitung rechtlich zulässig

erfolgt. Jedes Unternehmen ist gesetzlich zum Datenschutz verpflichtet.



Verschiedene Akteure beeinflussen, welche IT-Sicherheit- und Datenschutzmaßnahmen ein Unternehmen ergreifen sollte:

- Der Gesetzgeber legt Mindestanforderungen an IT-Systeme bspw. durch die Abgabenordnung, das Sozialgesetzbuch und Bundesdatenschutzgesetz fest (Kapitel 2).
- Wirtschaftsprüfer testieren IT-Systeme.
- Kunden, Mitarbeiter und Lieferanten verlangen, dass ihre Daten sicher sind.
- Mitarbeiter wollen IT-Systeme bequem und flexibel nutzen können.
- Medien interessieren sich für Sicherheitsvorfälle (Kapitel 3).
- Kriminelle dringen gezielt in die Unternehmens-IT ein, um Daten zu stehlen, zu entführen oder auszuspionieren (Kapitel 4).
- Technische Entwicklungen schaffen neue Sicherheitsrisiken (Kapitel 5).

Beauftragte für IT-Sicherheit oder Datenschutz unterstützen fachlich die Geschäftsführung.

Um ein akzeptables und wirtschaftliches Maß an IT-Sicherheit und Datenschutz zu erlagen, bedarf es umfangreichem Fachwissens in Informatik, Risikobewertung und Jura. Üblicherweise berufen deshalb Unternehmen einen IT-Sicherheitsbeauftragten oder Datenschutzbeauftragten, der

- das Sicherheitsniveau kontrolliert,
- wirtschaftlich tragfähige Verbesserungen vorschlägt,
- die Geschäftsführung berät und
- Mitarbeiter in IT-Sicherheit oder Datenschutz schult.

Für kleine und mittlere Unternehmen reicht ein Datenschutzbeauftragter aus

In kleinen und mittleren Unternehmen reicht oft die Berufung eines Datenschutzbeauftragten aus, der die IT-Sicherheit mit betreut. Auf einen Datenschutzbeauftragten darf nach §4f BDSG kein Unternehmen mit 10 und mehr Personen, die personenbezogene Daten mit einem Computer verarbeiten, verzichten.

Externe Datenschutzbeauftragte bringen kostengünstig Erfahrung ein

Die Rollen IT-Sicherheitsbeauftragte oder Datenschutzbeauftragte können sowohl von interne wie externe Mitarbeitern ausgefüllt werden. Externe Beauftragte bündeln Wissen und Erfahrung für verschiedene Unternehmen. Dadurch erhalten Unternehmen

- kostengünstigen Zugriff auf Spezialwissen,
- Zugang zu Branchenerfahrung,
- einen Blick von Außen und
- eine Unterstützung auf Augenhöhe.

2 Ohne IT-Sicherheit droht der Existenz-Verlust

Eine unzureichende IT-Sicherheit zieht Existenz bedrohende Konsequenzen nach sich:

Direkter Wirtschaftlicher Schaden:

- Eine US-amerikanische Studie ermittelte, dass jeder verlorene oder gestohlene Kundendatensatz dem Unternehmen 140 US-Dollar kostet.[4]
- Ein gestohlener Kreditkartendatensatz kostet 2.000 Euro.[5]
- Werden Innovationen der Konkurrenz bekannt, verringert sich der Wettbewerbsvorsprung.
- Schadensersatzansprüche von Betroffenen
- Betriebsunterbrechung wegen beschlagnahmte IT-Systeme

Wirtschaftlicher Folgeschaden:

- Negative Presseberichte schrecken potentielle Neukunden ab.
- Laut einer US-amerikanischen Studie wandern 19% der Kunden wegen des Vertrauensverlustes in Folge von Datendiebstahl oder Datenverlustdirekt ab und 40% erwägen es.[6]
- Ein Vertrauensverlust bei Mitarbeiten senkt die Produktivität.

Persönliche Haftung der Geschäftsführung:

- Eine Kapitalgesellschaft muss in Folge des AkG, KontraG, und GmbHG ein Risikomanagements einrichten und betreiben. IT-Sicherheit ist bedingt durch die Vorschriften zur Datensicherheit im BDSG ein Teil des Risikomanagements. Die Geschäftsführung hat die Beweislast, dass sie ein angemessenes Risikomanagements betreibt, um einer persönlichen Haftung zu entgehen. [7]
- Beim Betrieb eines unverschlüsselten WLAN haftet der Anschlussinhaber auch für die Taten unbefugter Eindringlinge.[8]
- Je nach Vorfall drohen auch strafrechtliche Konsequenzen bis hin zur Freiheitsstrafe und Berufsverbot.
- Wenn die private E-Mail- und Internetnutzung nicht geregelt ist, können übliche Maßnahmen wie E-Mail-Einsicht bei Krankheit eines Mitarbeiters zu strafrechtlichen Konsequenzen führen.

---

[4] Heise Online (2005): US-Studie über die Kosten durch Identitätsdiebstahl in Unternehmen. 15.11.2005. URL: http://www.heise.de/newsticker/meldung/66204

[5] Heise Online (2006): 23C3: Fahrlässiger Umgang mit Kreditkartendaten beanstandet. 30.12.2006. URL: http://www.heise.de/newsticker/meldung/83049

[6] Heise Online (2005): US-Studie über die Kosten durch Identitätsdiebstahl in Unternehmen. 15.11.2005. URL: http://www.heise.de/newsticker/meldung/66204

[7] Urteil des LG München I vom 05.04.2007, Az. 5 HK O 15964/06. Siehe auch: Handelsblatt (2007): Urteil kurz kommentiert. 12.09.2007, S. 23.

[8] Urteil des LG Hamburg, Az. 308 O 407/06. Siehe auch: Heise Online (2006): Unverschlüsseltes WLAN hat Folgen. 08.09.2006. URL: http://www.heise.de/newsticker/meldung/77921

3 Bekannte Sicherheitsvorfälle

Einige wenige Sicherheitsvorfälle wurden durch Presseberichte publik. Die folgende unvollständige Liste zeigt, dass ein sicherer Umgang mit Daten und IT-Systemen eine Aufgabe für das gesamte Unternehmen ist. Sobald ein Vorfall öffentlich bekannt wird, tritt ein unkalkulierbarer Imageschaden ein. Die folgenden Berichte kommen schwerpunktmäßig aus den USA, weil dort aufgrund von Informationspflichten Datendiebstähle und Datenverluste schneller bekannt werden. Deutsche Unternehmen sind genauso betroffen.

Beschreibung	Umfang	Unternehmen
Virus ab Werk Notebook enthält ab Werk den Virus „Stoned.Angelina“, der zuletzt 1994 aktiv war.[9]		Aldi als Verkäufer Medion als Hersteller
Spionieren mit Anonymisierungsnetz Tor Das Anonymisierungsnetz Tor wird auch von Geheimdiensten und Kriminellen genutzt um den durch das Netzwerk gehenden Datenverkehr inkl. Zugangsdaten, Passworte und geheime Daten mitzulesen.[10]		Anonymisierungsnetz Tor
Virus durch Hersteller-Webseite Infizierte Webseiten von Asus installieren beim Ansehen unbemerkt einen Virus. Die Webseiten stellen Treiber für Computer bereit und gelten deshalb als besonders vertrauenswürdig.[11]		Asus
Kundendaten aus Webshop gestohlen[12]	19.000 Datensätze	AT&T
Behörde als Datenschleuder Die Behörde versteigerte 41 Datenbänder und einige Blackberries ohne die vorhandenen Daten über ihre Bürger zu löschen. Wegen fehlender Verschlüsselung kann der Käufer die Daten problemlos einsehen und nutzen.[13]		Behörden von British Columbia, Kanada
Behörden-PC verteilen Pornos und Raubkopien Mindestens 2 Monate lang verteilen Behörden-PC unbemerkt Pornos und Raubkopien.[14]	78 PC	Behörden von British Columbia, Kanada
Unverschlüsselte Datenbänder vermisst Citigroup vermisst Datenbänder, auf denen unverschlüsselt Namen, Adressen, Sozialversicherungsnummern, Kontonummern, Kontobewegungen und Kreditinformationen gespeichert sind.[15]	3,9 Mio. Datensätze	Citigroup

[9] Heise Online (2007): Aldi-Notebook mit Virus an Bord [Update]. 12.09.2007. URL: http://www.heise.de/newsticker/meldung/95886
[10] Heise Online (2007): Anonymisierungsnetz Tor „abgephisht“. 10.09.2007. URL: http://www.heise.de/newsticker/meldung/95770
[11] Heise Online (2006): Asus-Server als Virenschleuder. 15.12.2006. URL: http://www.heise.de/newsticker/meldung/82637
[12] Heise Online (2006): Massiver Diebstahl von Kundendaten bei AT&T. 30.08.2006. URL: http://www.heise.de/newsticker/meldung/77455
[13] Heise Online (2006): Kanadische Provinzbehörden als Datenschleudern. 29.03.2006. URL: http://www.heise.de/newsticker/meldung/71444
[14] Heise Online (2006): Kanadische Provinzbehörden als Datenschleudern. 29.03.2006. URL: http://www.heise.de/newsticker/meldung/71444
[15] Heise Online (2005): 3,9 Millionen Citigroup-Kundendatensätze verschwunden. 07.06.2005. URL: http://www.heise.de/newsticker/meldung/60365

Beschreibung	Umfang	Unternehmen
Chinesische Hacker dringen in Regierungscomputer ein Angeblich sollen chinesische Hacker in Regierungscomputer eingedrungen sein. Die chinesische Regierung weist die Vorwürfe zurück.[16]		Deutsche Regierung, Pentagon, britisches Außenministerium, französische Regierung
Betrug durch Datenleck Eine Lücke bei PayPal erlaubt das missbräuchliche Auslesen von eBay-Kundendaten. Betrüger nutzten die so erlangten Kundendaten, um gezielt eBay-Kunden zu betrügen. Rechtliche Konsequenzen sind bisher unklar, da eBay besitzt eine Banklizenz.[17]		eBay und Tochter Paypal
Passwortliste auf Mailingliste veröffentlicht Eine Liste mit Passwörtern wurde auf einer Sicherheitsmailingliste veröffentlicht. Wie die Liste entwendet werden konnte, ist unbekannt.[18]	100.000 Nutzer	Flirtlife.de
Kreditkartendaten gestohlen Kreditkartennummern und Rechnungsanschriften von Kunden, die Tickets über die Webseite Kartenhaus.de mit Kreditkarten gekauft haben, wurden gestohlen.[19]	66.000 Kunden	Kartenhaus
Trojaner auf MP3-Player verteilt Auf MP3-Playern mit Firmen-Brand war der Trojaner QQPass installiert, der Passwörter ausspioniert. Die MP3-Player wurden im Rahmen eines Preisspiels verteilt.[20]	10.000 Kunden	McDonalds Japan
Trojaner stiehlt Daten von Arbeitssuchenden Ein über E-Mail, Werbung und präparierten Webseiten verbreiteter Trojaner nutzt die Arbeitgeberzugänge von Monster.com, um die Daten von Arbeitssuchenden zu sammeln.[21]	Mind. 1,6 Mio. datensätze	Monster.com
MySpace informiert Opfer nicht Nachdem 50.000 Adressen und Passwörter von MySpace-Nutzern im internet veröffentlich wurden, informierte MySpace die betroffenen Nutzer laut Umfrage nicht.[22]	50.000 Adressen und Passwörter	MySpace
Phishing-Seite sammelt Login-Daten in öffentlich zugänglicher Datei E-Mails machten die Phishing-Seite, die täuschend echt aussah, bekannt. Die gesammelten Login-Daten lagen öffentlich zugänglich auf einem Server.[23]	57.000 Login-Daten	MySpace

[16] Heise Online (2007): Auch Frankreichs Regierungscomputer sollen Ziel chinesischer Angriffe gewesen sein. 09.09.2007. URL: http://www.heise.de/newsticker/meldung/95693
[17] Heise Online (2007): Bericht: Ursache für eBay-Datenleck war Lücke bei PayPal. 13.09.2007. URL: http://www.heise.de/newsticker/meldung/95916
[18] Heise Online (2006): Passwortdaten von Flirtlife.de kompromittiert. 22.05.2006. URL: http://www.heise.de/newsticker/meldung/73396
[19] Heise Online (2007): Zehntausende Kartenhaus-Kunden von Kreditkartendaten-Diebstahl betroffen. 04.10.2007. URL: http://www.heise.de/newsticker/meldung/96953
[20] Heise Online (2006): McDonalds Japan verteilte infizierte MP3-Player [Update]. 16.10.2006. URL: http://www.heise.de/newsticker/meldung/79544
[21] Heise Online (2007): Monster-Trojaner stiehlt Daten von Arbeitssuchenden. 20.08.2007. URL: http://www.heise.de/newsticker/meldung/94570
[22] Heise Online (2007): MySpace vernachlässigt Kundenschutz. 09.03.2007. URL: http://www.heise.de/newsticker/meldung/86488
[23] Heise Online (2007): Phishing-Seite sammelte 57.000 Login-Daten von MySpace-Nutzern. 16.01.2007. URL: http://www.heise.de/newsticker/meldung/83752

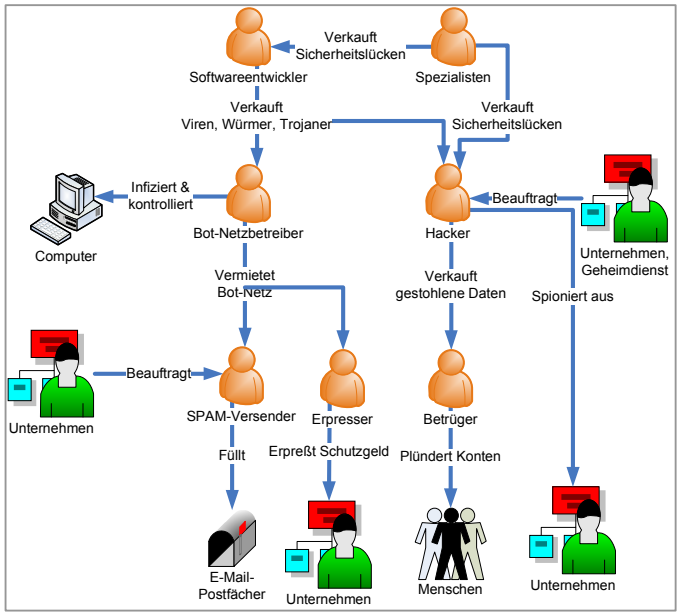
Beschreibung	Umfang	Unternehmen
Sicherheitslücken von Bank-Webseiten veröffentlicht Heise Security veröffentlicht eine detaillierte Sicherheitsanalyse der Webseiten von der SEB-Bank. Der Bericht listet zahlreiche Sicherheitslücken auf, obwohl die Webseiten u.a. für ihre Sicherheit ausgezeichnet worden waren.[24]		SEB-Bank
Nutzerdatenbank ausgelesen Mailadressen, Zugangsdaten und Freundschaftsverbindungen der Nutzer wurden ausgelesen.[25]		StudiVZ
Mehrere Sicherheitslücken bei StudiVZ Verschiedene Sicherheitslücken ermöglichten Nutzerdaten auszuspähen und fremde Konten einzusehen. Zusätzlich wurden Daten von 32 Nutzern mittels Phishing-Angriff gestohlen.[26]	32 Nutzer	StudiVZ
Kreditkartennummern über 18 Monate gestohlen Kreditkartennummern von Transaktionen seit 2002 wurden in UK und USA durch einen Einbruch in das Computersystem entwendet. Die Diebe hatten 18 Monate lang Zugriff.[27]	47,7 Mio. Kredit- und Debit-Kartennummern	TJX Companies
Geheime Unterlagen öffentlich zugänglich Geheime Millitärdokumente lagen auf öffentlich zugänglichen FTP-Servern. Sie waren mehrere Wochen frei zugänglich.[28]		US-Armee
Festplatte gestohlen – Soldaten enttarnt Eine externe Festplatte des US-Ministeriums für Kriegsveteranen wurde aus einem Privathaus gestohlen. Veteranenverbände fordern bis 26,5 Mrd. US-Dollar Schadensersatz.[29]	Mehrere Millionen Datensätze	US-Ministeriums für Kriegsveteranen
Unbefugter Zugriff auf E-Mails Wegen einer Fehlkonfiguration waren Teile der Mailserverinfrastruktur und der abgelegten E-Mails öffentlich zugänglich.[30]		Versatel
Sensible Daten bei eBay zu kaufen Gebrauchte Datenträger bei eBay enthalten persönliche oder geheime Daten. Nur 33% der Datenträger (Festplatten, USB-Sticks, Digitalkameras, Speicherkarten) waren sicher gelöscht[31]		Verschiedene Privatpersonen, Unternehmen, Regierungsbehörden
US-Stromnetz gehackt Während eines Sicherheitstests gelangt der Sicherheitsdienstleister Internet Security Systems in die Steuerungsanlagen im US-Stromnetz. Die Trennung von Office- und Produktionsnetze entpuppte sich als Mythos.[32]		Verschiedene US-Stromnetzbetreiber

[24] Heise Online (2007): Online Banking fatal. Vom ausgezeichneten Webauftritt zum Security-Desaster. 23.08.2007. URL: http://www.heise.de/security/artikel/print/94451
[25] Heise Online (2007): StudiVZ-Nutzerdaten ausgespäht. 27.02.2007. URL: http://www.heise.de/newsticker/meldung/85970
[26] Heise Online (2006): StudiVZ unter Beschuss [Update]. 27.11.2006. URL: http://www.heise.de/newsticker/meldung/81639
[27] Heise Online (2007): Massiver Kreditkartennummern-Klau beim US-Einzelhändler TJX. 29.03.2007. URL: http://www.heise.de/newsticker/meldung/87611
[28] Heise Online (2007): Unterlagen des US-Militärs öffentlich zugänglich. 13.07.2007. URL: http://www.heise.de/newsticker/meldung/92666
[29] Heise Online (2006): Datenklau könnte US-Regierung 26,5 Milliarden US-Dollar kosten. 08.06.2006. URL: http://www.heise.de/newsticker/meldung/74017
[30] Heise Online (2007): Anonymisierungsnetz Tor „abgephisht". 21.09.2007. URL: http://www.heise.de/newsticker/meldung/96322
[31] Heise Online (2007): Gebrauchte Festplatten als Fundgrube für brisante und intime Daten. 03.09.2007. URL: http://www.heise.de/newsticker/meldung/95380
[32] Heise Online (2006): Dienstleister hackt sich in Anlagen des US-Stromnetzes. 31.01.2006. URL: http://www.heise.de/newsticker/meldung/69063

4 Die organisierte Kriminalität übernimmt

Kriminelle setzen Mrd. Euro ein – reichen 100 € für Verteidigung?

Die weltweite Vernetzung durch das Internet und die gleichzeitige technologische Entwicklung von mobilen Geräten, Speichermedien und Computern ermöglichen neue Dienstleistungen, eine weltweite Arbeitsteilung und mehr Automatisierung. Unternehmen können ohne funktionierende IT, d.h. ohne E-Mail, Office-Programme, elektronische Kundenkarteien und Buchhaltung, Maschinensteuerung, nicht mehr existieren. 2006 hat das organisierte Verbrechen die Vorteile des Internet erkannt und damit eine neue Bedrohung geschaffen. Das Internet erlaubt es, mit relativ wenig Aufwand weltweit Verbrechen zu begehen. Das Risiko, erwischt zu werden, ist verschwindend gering. Die Szene geht hoch professionell und arbeitsteilig vor.



Softwareentwickler stellen legal die notwendigen Werkzeuge für Viren, Würmer und Trojaner her und verkaufen diese. Es gibt mittlerweile komplette Baukästen für Trojaner[33], Schwachstellen[34] und Phishing-Seiten[35] und Passwortknacker[36], auch als Bezahldienst[37]. Spyware für Handys[38] wird auch angeboten. Dazu kommen noch Spezialanfertigungen von Viren und Würmer, die von Virenscannern nicht erkannt werden.

Schwachstellen in Betriebsystemen und Anwendungsprogrammen erlauben das Eindringen in Computern. Spezialisten suchen deshalb Schwachstellen in populären Programmen wie Microsoft Windows oder Office und verkaufen diese für bis zu 125.000 US-Dollar[39] an Hacker und Softwareentwickler.

Bot-Netzbetreiber kaufen Baukästen oder Spezialanfertigungen ein, um Bots herzustellen. Weiterhin beschaffen sie sich Viren, die Bots auf den Computern der ahnungslosen Opfer platzieren. Bots sind ferngesteuerte Programme, die sich unbemerkt in Computern einnisten und dem Bot-Netzbetreiber alle Handlungen ermöglichen, als ob

[33] Heise Online (2007): Trojaner-Basteln für Dummys. 20.07.2007. URL: http://www.heise.de/newsticker/meldung/93024
[34] Heise Online (2007): Exploits für alle: Metasploit 3.0 in finaler Fassung erschienen. 27.03.2007. URL: http://www.heise.de/newsticker/meldung/87430
[35] Heise Online (2006): Phishing-Seiten aus dem Baukasten. 25.02.2006. URL: http://www.heise.de/newsticker/meldung/70061
[36] Heise Online (2006): Passwortknacker lernt Teamwork. 17.02.2006. URL: http://www.heise.de/newsticker/meldung/69759
[37] Heise Online (2005): Passwort-Cracker als Bezahldienst. 11.11.2005. URL: http://www.heise.de/newsticker/meldung/66039
[38] Heise Online (2006): Spyware für Handys überwacht Anwender. 30.03.2006. URL: http://www.heise.de/newsticker/meldung/71460
[39] Computer Zeitung (2007): Spione lauern auf Softwarelöcher. 10.09.2007, S. 6.

er an dem Computer säße. Er kontrolliert zwischen 1.000 und 100.000 Computer gleichzeitig.

SPAM-Versender mieten Botnetze an, um SPAM zu versenden. SPAM bewirbt Produkte, Phising-Seiten oder verteilt Viren mit neuen Bots. Der Versand von 20 Mio. E-Mails ist bereits für 350 Euro zu haben.[40]

Erpresser mieten Botnetze, um Schutzgeld zu erpressen, weil sonst die Webseiten eines Unternehmens mit einem verteilten DoS-Angriff durch das Botnetz tagelang lahm gelegt werden. Das betroffene Unternehmen verliert seinen Online-Umsatz. Bot-Netzbetreiber bieten verteilte DoS-Angriffe für 14 Euro pro Stunde an.[41]

Hacker kaufen Schwachstellen, um unerkannt in fremde IT-Systeme zu eindringen. Sie spionieren im Auftrag von Wettbewerbern oder Geheimdiensten Unternehmen gezielt aus und verkaufen auch gefundene Adressen weiter. Kundendaten sind pro Datensatz je 15 bis 150 Euro wert.[42]

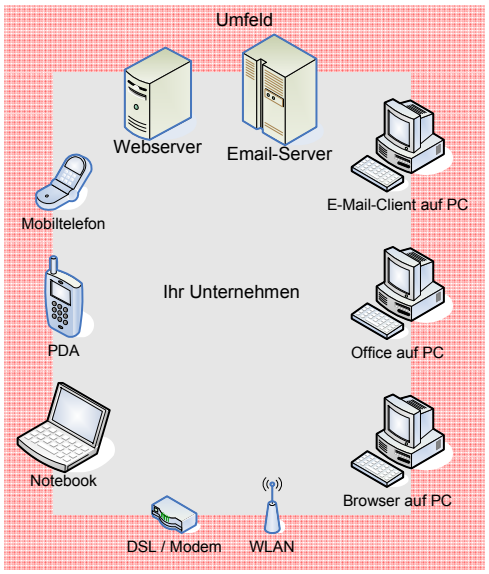
Betrüger kaufen Kreditkartendaten und Bankdaten, um Konten zu plündern oder sehr überzeugende Phishing-E-Mails zu versenden. Mit Hilfe von Phishing-E-Mails lassen sich fehlende Informationen wie z.B. TAN-Nummern im Online-Banking beschaffen. Der Kontoräumung steht dann nichts mehr im Weg.

[40] Heise Online (2007): Spam zum Schnäppchenpreis. 23.10.2007. URL: http://www.heise.de/newsticker/meldung/97780
[41] Heise Online (2007): Spam zum Schnäppchenpreis. 23.10.2007. URL: http://www.heise.de/newsticker/meldung/97780
[42] Heise Online (2007): Schlag gegen Internethandel mit illegal ausgespähten Kreditkarten-Daten. 29.06.2007. URL: http://www.heise.de/newsticker/meldung/91966

5 Wege in ein Unternehmen

In jedem Unternehmen ist etwas zu „holen“

Kriminelle greifen Unternehmen auf zwei Weisen an: zielgerichtet oder wahllos. Ein zielgerichteter Angriff ist aufwendiger, weil der Angreifer die Sicherheitslücken seines Opfers erkennen muss. Je nach Sicherheitsniveau muss dazu einiger Aufwand getrieben werden. Ein wahlloser Angriff sucht sich seine Opfer passend zum Angriff aus. Wer die Opfer genau sind, ist unwichtig, da bei jedem Unternehmen „etwas zu holen ist“. Deshalb reicht bereits die Existenz einer Sicherheitslücke, um Opfer eines Angriffs zu werden. Beide Angriffsarten verursachen den gleichen Schaden.



Jedes Gerät und jedes Programm, das Kontakt mit dem Internet hat, eignet sich als Einfallstor:

- Webserver
- E-Mail-Server
- Browser am PC
- E-Mail-Client am PC
- Office-Anwendungen am PC
- Handys
- PDA
- WLAN
- DSL-Modem
- usw.

Lücken in den jeweiligen Programmen erlauben, dass Unbefugte eindringen und teilweise auch die Kontrolle über die Geräte übernehmen können. Sobald mobile Geräte wie Notebooks, Handys oder PDA das schützende Firmengelände verlassen, sind sie zusätzlichen gefahren ausgesetzt:

- Diebstahl
- Verlust
- Eindringen bei Nutzung öffentlicher WLAN-Netze in Hotels oder Flughäfen
- Eindringen im Vorbeigehen durch Sicherheitslücken

Datenträger vor Verkauf sicher löschen

Datenträger wie Sicherungsbänder, Festplatten oder USB-Sticks transportieren oft sensible Daten. Neben Diebstahl und Verlust stellt hier der Verkauf ein Sicherheitsrisiko dar. Meistens werden die Daten nicht oder nicht fachgerecht gelöscht, so dass der Käufer sie einfach wiederherstellen kann. Forscher berichten, dass nur 8% der bei eBay verkauften gebrauchten Festplatten fachgerecht gelöscht worden waren.[43]

USB-Sticks sind die Trojanischen Pferde der Neuzeit

Werden fremde Geräte wie Notebooks oder USB-Sticks in das Firmennetzwerk eingesteckt, können diese ebenfalls Daten saugen oder

[43] Heise Online (2003): Datenschützer warnen vor Fallstricken beim Verkauf ausgemusterter PCs. 24.03.2003. URL: http://www.heise.de/newsticker/meldung/35598

Schadsoftware installieren. Eine bekannte Masche sind „verlorene“ USB-Sticks im Umfeld eines Unternehmens. Sobald der Finder sie neugierig in einen PC steckt, installiert sich ein Trojaner, der fortan das Unternehmen ausspioniert.[44]

Internetdienste als Spionagewerkzeuge für Jedermann

Eine ähnliche fatale Funktion wie USB-Sticks können Internet-Dienste entfalten. Das bekannte Anonymisierungsnetzwerk, das auch von Regierungen benutzt wird, lässt sich für Jedermann in ein Spionagewerkzeug verwandeln.[45] Wer eine bestimmte Serverart („Exit-Notes“) in dem Netzwerk betreibt, kann den Datenverkehr unverschlüsselt mitlesen. Zugangsdaten und anderen Daten enthüllen schnell den eigentlichen Absender der Daten, so dass auch die Anonymität aufgehoben ist. Mit diesem Trick konnten die Zugangsdaten zu 100 E-Mail-Postfächern internationalen Regierungsinstitutionen erspäht werden.[46] Internetdienste wie z.B. Online-Virenscanner, die Zugriff auf Dokumenten von der Festplatte erhalten, bergen ein ähnliches Sicherheitsrisiko.

Wirkungsvolle Sicherheit braucht ein technisches und organisatorisches Gesamtkonzept

Virenscanner und Firewalls werden gerne als Allheilmittel in der IT-Sicherheit dargestellt. Leider funktionieren alle der oben genannten Wege auch mit aktuellen Virenscannern und Firewalls. Virenscanner und Firewalls als einzige Maßnahme zur IT-Sicherheit sind nutzlos und Geldverschwendung. Erst ein Gesamtkonzept, das neben technischen Maßnahmen auch den notwendigen organisatorischen Rahmen schafft, sichert die Existenz eines Unternehmens.

[44] Heise Online (2006): USB-Sticks als Trojanische Pferde der Neuzeit. 12.06.2006. URL: http://www.heise.de/newsticker/meldung/74135
[45] Heise Online (2007): Anonymisierungsnetz Tor „abgephisht“. 10.09.2007. URL: http://www.heise.de/newsticker/meldung/95770
[46] Heise Online (2007): Zugangsdaten für Regierungs-Mail-Accounts veröffentlicht. 31.08.2007. URL: http://www.heise.de/security/news/meldung/95262

Xamit Bewertungsgesellschaft mbH

Die Xamit Bewertungsgesellschaft mbH wurde im Februar 2006 von Björn Petersdorf und Dr. Niels Lepperhoff gegründet. Kernkompetenz des in Düsseldorf ansässigen Unternehmens ist die IT-Revision und das IT-Controlling. Xamit untersucht die unter Zuhilfenahme fundierter Methodiken den Leistungsumfang sowie die Effizienz und Gesetzeskonformität von IT-Projekten, Software und IT-Systemen.

Als innovativer Dienstleister hat Xamit daher für Sie die Leistungen in den folgenden vier Produkten zusammengefasst:

- Projekt Check
- Produkt Check
- Firmen Check
- Web Check

Mit seiner Arbeit schafft Xamit Investitions- und Planungssicherheit. Xamit unterstützt Sie damit insbesondere bei

- ganzheitlicher IT-Bewertung
- Aufwandschätzungen für Eigenentwicklungen
- Produktivitätsmessungen in Ihrem IT-Umfeld
- nutzenorientierter und nutzenfokussierter Softwareauswahl
- Erfolgsanalysen von Webpräsenzen
- dem betrieblichen Datenschutz als TÜV-zertifizierter Datenschutzbeauftragter

Ihre Vorteile mit Xamit

- Neutrale Bewertung,
- Unabhängige Beratung und
- Verständliche Gutachten

Treten Sie mit uns in Kontakt. Wir freuen uns, Sie zu unterstützen. Ein erstes Beratungsgespräch ist für Sie selbstverständlich kostenlos.

Xamit Bewertungsgesellschaft mbH

Zülpicher Str. 6
40549 Düsseldorf

Tel.: 0211 / 58 300 330
Fax: 0211 / 58 300 331

E-Mail: info@xamit.de
WWW: www.xamit.de