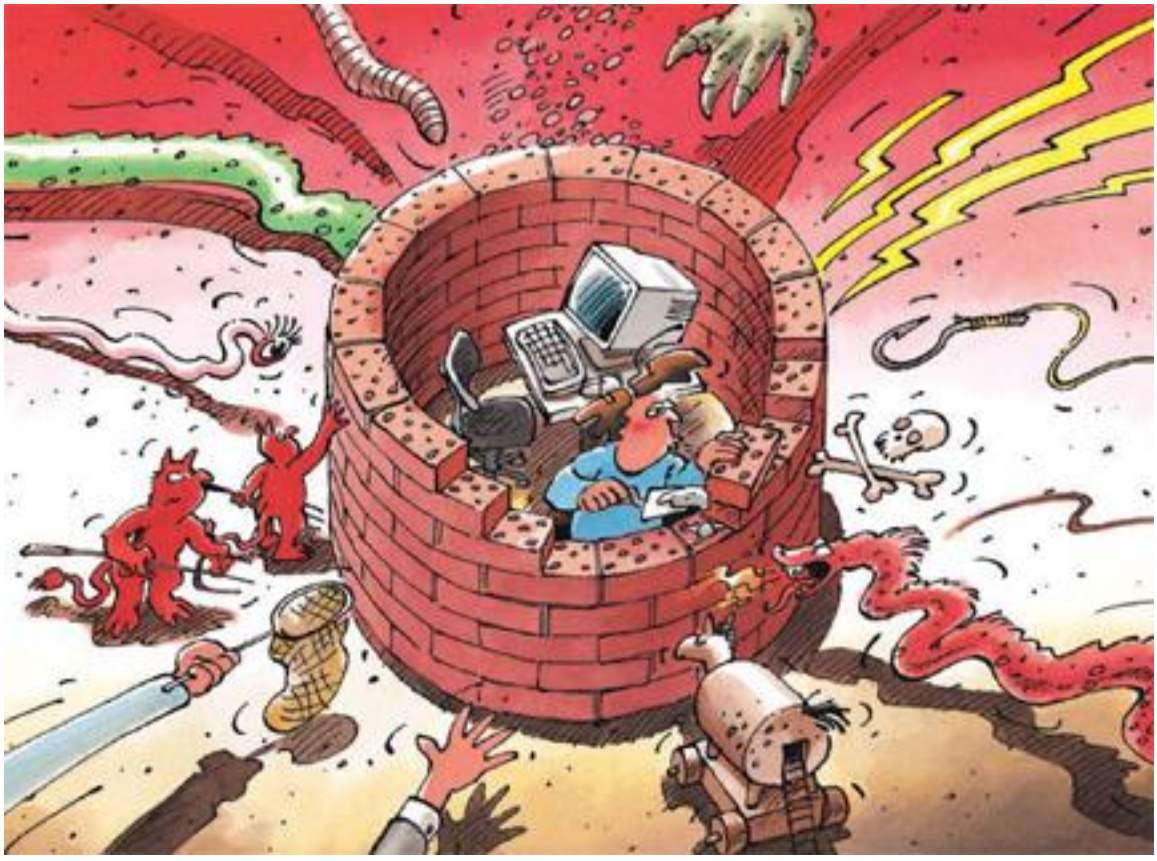
MELANI Melde- und Analysestelle Informationssicherung

INFORMATIONS-SICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

HALBJAHRESBERICHT 2005 / I



In Zusammenarbeit mit:

KOBIK SCOCI CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Ausgabe 1/2005 (Januar bis Juni 2005)

Inhaltsverzeichnis

1 Einleitung 5

2 Tendenzen / Allgemeine Entwicklungen 6

2.1 Zunehmende (organisierte) Kriminalität 6

2.2 Zunehmende Professionalität 6

2.3 Zunahme von Identitätsdiebstählen (ID Theft) 7

2.4 Gezielte Angriffe mit Spionageprogrammen: Industriespionage 8

2.5 Mangelndes Verantwortungsbewusstsein bei Internet-Benutzern 8

3 Aktuelle Gefahren und Risiken und deren technischer Hintergrund 9

3.1 Bot-Netze / DDoS-Attacken 9

3.2 Phishing und Pharming 9

3.3. Gefahren und Risiken für Benutzer von Mobiltelefonen 11

3.4 Social Engineering 11

4 Aktuelle Lage IKT Infrastruktur national 12

4.1 Pannen, Ausfälle 12

Panne auf Eisenbahnnetz 12

E-Banking-Service ausser Betrieb 13

4.2 Attacken 14

Website-Defacement: Unfug, Spass oder neue Form des sozialen Protestes? 14

Attacke auf admin.ch 15

Internet: Wurmattacke auf Grossdetaillisten 15

4.3 Kriminalität 16

Phishing in der Schweiz 16

Phishing-Seiten auf Schweizer Servern 17

Neue Betrugsformen 17

Nigerianer in Zürich wegen Betrugs verurteilt 17

Schweizer Banken im Visier eines Keyloggers 17

4.4 Terrorismus 18

Islamic-minbar.com — islamistischer Extremismus auf Schweizer Servern 18

Sunna-minbar.com — Nachfolger von islamic-minbar.com 18

Fünf verdächtige Ausländer verhaftet 18

4.5 Diverses 19

Anonymität im Telekommunikationsbereich 19

Anonymität auf dem Internet 20

5 Aktuelle Lage IKT Infrastruktur International 20

5.1 Pannen, Ausfälle 20

Pakistans Internetverbindung ins Ausland gestört. 20

5.2 Attacken 21

Fall Root-Kit 21

Gezielte Distributed Denial-of-Service (DDoS) Attacke gegen heise.de 21

DDoS-Attacke gegen Internet-Bezahldienst Worldpay 22

DoS-Attacken gegen Server der japanischen Regierung 22

Pharming-Attacken gegen Domain Name System (DNS) 23

Fussball-WM Wurm / Versand von rechtsradikaler Propaganda: Sober-Wurm 23

Gezielte Spionageangriffe gegen Kritische Infrastrukturen in Grossbritannien 24

5.3 Kriminalität 25
DDoS- und Spam-Attacken gegen Bezahlung 25
ChoicePoint Kundendaten kompromittiert: Identitätsdiebstähle drohen 25
Industriespionage: Diebstahl von Millionen von Kreditkartendaten mit Trojanischem Pferd 26
Industriespionage in Israel 27

5.4 Terrorismus 27
Cyber-Terrorismus Debatte in den USA 27
USA: IT-Sicherheitsmängel bei den Bundesbehörden 29
USA: Department of Homeland Security (DHS) vernachlässigt Cyber-Security-Pflichten 30
USA: Direktor des Secret Service fordert zu Kooperation für Cyber-Security auf 30

6 Prävention 30

6.1 Software 30
Ausweitung des Heim PC-Schutzes auf Spam, Phishing 30
Systeme zur sicheren Überprüfung des E-Mail Absenders 31

6.2 Diverses 32
Anforderungen an Online Banking Seiten 32

7 Aktivitäten / Informationen 33

7.1 Staatlich 33
Schweiz: Bundesrat will Kampf gegen Internetkriminalität verstärken 33
EU: Fortschritte bei der Anti-Spam-Politik 34
EU: Schärferes Vorgehen gegen Hacker 34
Deutschland: Anti-Spam Gesetz im Parlament diskutiert 35
Deutschland und Grossbritannien: Neue Internetsicherheits-Initiative für Bürger 36
USA: Neue Richtlinien zur Informatik-Sicherheit von Nuklearanlagen in Vernehmlassung 36
USA: „Protected Critical Infrastructure Information Program“ floppt 37
UNO-Arbeitsgruppe veröffentlicht Grundsatzpapiere zur Internet-Verwaltung 38
USA: Hacker-Crew in den US-Streitkräften 38
Deutschland: Innenminister Schily kündigt
„Nationalen Plan zum Schutz der Infrastrukturen“ an 39
USA: Senatoren legen Gesetz gegen Identitätsdiebstahl vor 39
USA: Bundesbehörden ab 2008 umgestellt auf IPv6 40
USA wollen Kontrolle über DNS-Rootzone nicht abgeben 40

7.2 Privat 40
WLAN Hot-Spots in 1. Klasse-Abteilen der SBB in Kürze zu erwarten 40
Microsoft schränkt Updates für illegale Kopien ein 41
Hersteller einigen sich auf ein „Common Vulnerability Scoring System“ (CVSS) 42
Microsoft, eBay, PayPal und Visa gründen „Phishing Report Network“ 42
Microsoft: Kooperationsprogramm mit Regierungen angekündigt 43
Microsoft richtet sich strategisch auf den IT-Sicherheitsmarkt aus 43
Cyber Incident Detection Data Analysis Center (CIDDAC) beginnt Pilotprojekt 44
Microsoft: „Windows OneCare“ angekündigt 44
Bluewin tritt Messaging Anti-Abuse Working Group (MAAWG) bei 45
Trend Micro kauft IP-Filtering-Firma 45

Schwerpunkte Ausgabe 2005/1

- *Botnetze*
  Abgesehen von den praktisch unbegrenzten (Angriffs-)Möglichkeiten, die ein grosses Botnetz seinen Besitzern ermöglicht, stellt die Involvierung tausender Heimcomputer und damit die unwissentliche Komplizenschaft ihrer Besitzer die Strafverfolgung, Nachrichtendienste und IT-Spezialisten vor ein schier unlösbares Problem. Es ist insofern auch ein Paradigmenwechsel absehbar, was die Durchführungsart von Angriffen über das Internet und den Schutz davor, respektive ihre Verfolgung, betrifft.

- *Zunehmende organisierte Kriminalität*
  Während bis vor kurzem noch Interesse als Hauptmotiv der Hackerszene galt, stehen inzwischen finanzielle Absichten hinter den Angriffen auf informationstechnologische Infrastrukturen. Vermehrt wird auch die organisierte Kriminalität, insbesondere aus Ost-Europa, mit solchen Angriffen in Verbindung gebracht.

- *Professionalisierung der Hackerszene*
  Einhergehend mit dem Fokus auf finanzielle Interessen konnte eine Professionalisierung der Angreifer beobachtet werden. Mit technisch immer raffinierteren Hybrid-Schädlingen, die Angriffsvektor und Schadpotenzial verschiedener Malware kombiniert einsetzen können, liefern sich die Hacker teilweise gar eigentliche Malware-Kriege.

- *Gezielte Spionageangriffe*
  Im ersten Halbjahr 2005 fanden verschiedene gezielte Spionageangriffen gegen Unternehmen und staatliche Systeme statt. Mit dem Einsatz gezielt gegen das jeweilige Opfer konzipierter Spionage-Malware soll eine Entdeckung des Schädlings möglichst lange vermieden werden: Bleibt der Schädling den Antiviren-Software Herstellern unbekannt, kann er über längere Zeit unerkannt eingesetzt werden.

1 Einleitung

Seit Oktober 2004 betreibt der Bund die Melde- und Analysestelle Informationssicherung (MELANI), die nun in Form des vorliegenden Texts ihren ersten halbjährlichen Bericht (Januar – Juni 2005) zur „Informationssicherung: Lage in der Schweiz und international“ vorlegt.

Der Bericht erläutert die wichtigsten Tendenzen rund um die Informations- und Kommunikationstechnologien (IKT), erklärt die technische Funktionsweise aktueller Gefahren, gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet die wichtigsten Entwicklungen im Bereich der Prävention und resümiert die wichtigsten Aktivitäten staatlicher und privater Akteure.

Kapitel zwei fasst in analytischer Form die allgemeinen Tendenzen, Gefahren und zu erwartenden Entwicklungen zusammen und können im Sinne eines Fazits verstanden werden. Kapitel drei bietet die Grundlage für das Verständnis des restlichen Textes, da es einerseits Angriffsmethoden erläutert, andererseits den technischen Hintergrund für das Verständnis der folgenden Kapitel bildet.

Kapitel vier und fünf über die nationale und internationale Lage befassen sich mit Pannen und Ausfällen, Attacken, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. In Form von Einzelbeispielen werden die wichtigsten Ereignisse der ersten sechs Monate des Jahres 2005 aufgezeigt. Einerseits kann der Leser so eine Übersicht über die wichtigsten Vorkommnisse gewinnen, andererseits findet er illustrative Beispiele für die generellen Beobachtungen in den strategisch-analytischen Kapiteln zwei und drei.

Das Kapitel sechs zur Prävention bietet nicht etwa konkrete Anweisungen und Tipps, wie Ihr Computersystem konkret vor den einzelnen Gefahren geschützt werden kann – diesbezügliche Empfehlungen sind auf der Homepage von MELANI unter http://www.melani.admin.ch publiziert. Vielmehr befasst es sich mit technologischen Entwicklungen im Bereich der Prävention bzw. der Erhöhung der Sicherheit der Informations- und Kommunikationstechnologien.

Im Kapitel sieben wird der Fokus zunächst auf staatliche, anschliessend auf privatwirtschaftliche Aktivitäten gerichtet. Einerseits soll dieser Teil eine Übersicht über die wichtigsten gesetzgeberischen Änderungen weltweit bieten, andererseits aber auch die Debatte über das komplexe Thema der Informationssicherung in anderen Ländern verfolgen. Im Unterkapitel über privatwirtschaftliche Aktivitäten werden die wichtigsten strategischen Aktionen grosser Hard- oder Software-Hersteller aufgezeigt.

2 Tendenzen / Allgemeine Entwicklungen

2.1 Zunehmende (organisierte) Kriminalität

Das Jahr 2004 stand im Zeichen einer Verschiebung der Motivation der Entwickler von Malware. Während bisher eher intellektuell motivierte Hacker mit Interesse an technischen Problemstellungen und der IT-Sicherheit im Allgemeinen als Hauptmotiv am Werk waren, findet eine Verschiebung hin zur Bereicherung als Hauptmotiv statt. Zudem kann eine immer engere Verbindung zum organisierten Verbrechen beobachtet werden: Das organisierte Verbrechen dehnt seine klassischen Betätigungsfelder wie Bestechung, Erpressung, Bedrohung und Betrug immer mehr in die virtuelle Welt aus. Die an sich unabhängigen Hacker werden entweder gut bezahlt oder regelrecht erzwungen. Computerworld berichtete Anfang Februar 2005 über den Fall eines russischen Computer-Experten, der offenbar durch Aussprechen von Drohungen gegen seine Familie zur Kooperation gezwungen worden war. Beispiele eingesetzter Mittel der Angreifer sind DDoS-Attacken, Phishing oder Pharming (siehe die techn. Erläuterungen im Kapitel 3).

MELANI geht davon aus, dass dies erst den Anfang dieser Problematik darstellt. Die nächsten Monate und Jahre werden genauer offenbaren, wohin diese Tendenz führen wird. Das Bedrohungspotenzial jedenfalls ist beachtlich: Experten gehen von weltweit mehreren zehntausend Bot-Netzen aus, teilweise mit über 100'000 Hosts pro Netz – diese Ausmasse erlauben theoretisch DDoS-Attacken mit bisher ungesehenen Bandbreiten, so dass fast jeder Dienst im Internet in die Knie zu zwingen wäre (siehe für technische Erläuterungen Kapitel 3). In Kapitel 5.3 sind einige Beispiele krimineller Aktivitäten sowie Beispiele für Preise von Hackeraktivitäten aufgeführt.

2.2 Zunehmende Professionalität

Im Jahr 2004 und der ersten Jahreshälfte 2005 konnte eine Zunahme der Professionalität der Angreifer beobachtet werden. Zunehmend werden von den Angreifern so genannte „Hybrid-Schädlinge“ entwickelt, die verschiedene Funktionen von einzelnen Malware-Arten vereinen. Unter den einzelnen Arten dieser neuartigen Malware konnte ein eigentlicher Krieg beobachtet werden. Die in diesem Jahr aufgetauchten Viren Bagle, Mydoom und Netsky versuchten nicht nur die angegriffenen Systeme zu eigenen Zwecken zu missbrauchen, sondern auf den Systemen bereits vorhandene Viren konkurrierender Angreifer zu eliminieren.

Die Viren dienen neuerdings vor allem kommerziellen Absichten: MyDoom lancierte beispielsweise verschiedene Denial of Service-Attacken (DoS, z.B. gegen SCO.com, microsoft.com, riaa.com und google.com). Inwiefern mit DoS-Attacken kommerzielle Ziele verfolgt werden, wird in Kapitel 5.3 nochmals aufgegriffen. Bagle sowie MyDoom funktionierten infizierte Systeme auch zu SMTP-Servern um, so dass auf diesem Weg Spam-Mails versandt werden konnten. Die Virengruppen von Bagle, Mydoom und Korgo dienten vor allem dem Sammeln von Login-Informationen mit Key-Loggern, die Tastatureingaben aufzeichnen. Die Absicht dieser Schädlinge ist es, an Authentifizierungs-Daten für E-Banking oder andere Finanzdienstleistungen zu kommen.

MyDoom.A öffnete nach der Infektion beispielsweise eine Hintertüre, über die sich das infizierte System fernsteuern oder zusätzlicher Schadenscode nachladen liess.

Wie der russische Antiviren-Spezialist Kaspersky in einer Einschätzung verlauten liess, zielt Malware zudem immer weniger auf eine globale Ausbreitung ab, sondern versucht, nur ein bestimmtes Netz zu befallen. Das Motiv für dieses Vorgehen liegt darin, eine Entdeckung durch Antiviren-Hersteller möglichst lange zu verhindern (was natürlich bei einer raschen globalen Ausbreitung nicht der Fall ist) und so mehr Zeit für das Sammeln von Login-Daten zu gewinnen. Zudem wurde eine vermehrte Zusammenarbeit zwischen den einzelnen Virenschreibern zwecks Optimierung des finanziellen Gewinns beobachtet, was die Qualität der Schadprogramme in den letzten 12 Monaten entscheidend ansteigen liess. Wie Kaspersky nach einer Analyse des letzten Bagle-Wurm-Ausbruchs seit Mitte Februar vermutet, arbeiten beispielsweise die Autoren von Bagle, Zafi und Netsky neuerdings zusammen. Von Relevanz für die Schweiz ist vor allem, dass die Betrüger und Malware-Autoren vermehrt den deutschen Sprachraum entdecken. Phishing- und E-Mails mit infiziertem Anhang kommen nun auch in gutem Deutsch daher. Demzufolge vergrössert sich auch die Motivation der deutsch sprechenden Internetnutzer, ein solches E-Mail zu öffnen. Mit „Sober.I“ tauchte der erste Wurm auf, der seine „Sprache“ dynamisch anpassen kann. Er schaut dabei auf die E-Mail-Adresse des Empfängers. Endet diese zum Beispiel mit .de oder .ch, wird ein deutscher Text eingeblendet. So könnten Schadprogramme in Zukunft nicht nur die Sprache feststellen, sondern den Computer auch nach anderen Präferenzen (zum Beispiel Hobbys) durchsuchen. Ein Beispiel wäre die Durchforstung der E-Mails nach den Stichwörtern Fussball, Skifahren, Tennis usw. und die anschliessende Anpassung der Betreffzeile. Dieser ganze Aufwand dient allein dem Zweck, das Vertrauen des Empfängers zu gewinnen, damit dieser die E-Mail öffnet.

2.3 Zunahme von Identitätsdiebstählen (ID Theft)

Unter Identitätsdiebstahl versteht man den illegalen Einsatz von betrügerisch gesammelten Identitätsangaben von Opfern durch Betrüger. Identitätsdiebstahl ist ein für die betroffene Person sehr unangenehmes Problem, das viel Aufwand über lange Zeit erfordert, um den Schaden wieder zu beheben. Nach dem Sammeln von fremden Identitätsangaben (wie z.B. Kreditkartendaten, Social Security Nummern oder anderen persönlichen Daten) mittels Phishing oder anderen Methoden kaufen die Betrüger in fremdem Namen Waren, beziehen oder transferieren Geld, gründen illegitime Firmen usw. Der tatsächliche Besitzer der dazu benutzten Identität braucht oft Jahre, um alle Forderungen gegen ihn abfedern bzw. beweisen zu können, dass er nicht der Urheber war.

In den USA ereigneten sich im Verlauf der letzten Monate mehrere Datendiebstähle in grossen so genannten „Data Warehousing“-Firmen, die für die Regierung, für Versicherungen oder für Vermieter Personendaten (z.B. Kreditkartendaten, Sozialversicherungsnummern, Geburtsdaten usw.) sammeln und pflegen. Als Beispiele wären die Datenverluste bei Choice-Point, LexisNexis, CardSystems zu nennen, bei denen hunderttausende von Datensätzen in falsche Hände fielen (siehe Kapitel 5.3 für das ChoicePoint-Beispiel und den Fall bei CardSystems).

Datenverluste dieser Dimension illustrieren die Gefahren zentraler Datenhaltung eindrücklich – oft erfahren Betroffene erst nach der Fremdnutzung ihrer Identität, dass überhaupt eine Kompromittierung ihrer Daten stattgefunden hat. Angesichts der zunehmenden Zunahme von Phishing- und Datendiebstahl-Vorfällen ist künftig auch mit einer Zunahme von Idenditätsdiebstählen zu rechnen.

2.4 Gezielte Angriffe mit Spionageprogrammen: Industriespionage

Während per infiziertem E-Mailanhang nach wie vor eine grosse Infektionsgefahr mit schädlicher Software besteht, erfolgen nun häufiger gezielte, spezialisierte Angriffe auf ein bestimmtes Opfer mit spezifisch für diesen Zweck entwickelter Spionagesoftware.

Anstatt eine möglichst grosse Verbreitung zu erzielen, setzen Angreifer immer häufiger auf eine gezielte Ausbreitung allein beim auszuspionierenden Opfer. Auf diese Weise wird verhindert, dass Antiviren-Software-Hersteller den Schädling entdecken und ihre Signaturen aktualisieren können – der Angreifer kann so unter Umständen über lange Zeiträume unbemerkt Daten sammeln..

In den bekannt gewordenen Fällen (siehe die Beispiele in Kapitel 5.2, Spionage gegen Grossbritannien, und in Kapitel 5.3) wurden jeweils raffinierte Social Engineering Methoden angewandt, um Schädlinge auf einem System zu installieren. Dazu war vorgängig gezielte Recherche nötig (siehe zu Social Engineering Kapitel 3.4). Im Fall von Grossbritannien wurden beispielsweise Mitarbeiter, die vertrauliche Daten bearbeiten, direkt kontaktiert. Diese Mitarbeiter erhielten auf ihre persönlichen Interessen zugeschnittene E-Mails, welche Links auf präparierte Webseiten oder Dokumenten enthielten. Im Industriespionagefall in Israel wurde der Schädling beispielsweise mit einer CD-ROM eingeschleust, die als Marketing-CD getarnt war. Auf dem System wird, für das Opfer nicht ersichtlich, ein Programm installiert, das unter Anderem Tastatureingaben aufzeichnen oder bestimmte Daten suchen kann. Der Angreifer erhält volle Kontrolle über das infizierte System und kann gezielt und über lange Zeiträume Informationen beliebiger Art – Dateien, E-Mails, Passwörter, Account-Daten etc. – sammeln und unbemerkt aus dem Firmennetzwerk extrahieren.

Die aufgeflogenen Fälle in Grossbritannien und Israel belegen, dass diese Art der Spionage sowohl im privaten Sektor (Industriespionage, Diebstahl von geistigem Eigentum) als auch im öffentlichen Bereich (systematische Spionage gegen Betreiber Kritischer Infrastrukturen und gegen Regierungssysteme) eingesetzt wird. Der Spionagefall in Israel zog seine Spuren bis zu einer Firma im Raum Zürich, wo dasselbe Programm für eine privat motivierte Spionage eingesetzt wurde.

Da solche Spionageprogramme wie erwähnt in keiner Antiviren-Software-Signatur auftauchen, ist eine Infektion mitunter schwer festzustellen und auch in gut geschützten Netzen kaum zu verhindern. Neben einem umfassenden technischen Schutz ist eine gezielte Schulung und Sensibilisierung der Mitarbeiter im Umgang mit sensiblen Daten von grosser Bedeutung.

MELANI rechnet mit einer Zunahme dieser Bedrohung und geht davon aus, dass das Thema Industriespionage mit informationstechnologischen Mitteln auch in der Schweiz vermehrt an Bedeutung gewinnen wird.

2.5 Mangelndes Verantwortungsbewusstsein bei Internet-Benutzern

Laut einer Studie des BSI (Bundesamt für Sicherheit in der Informationstechnik)[1], die auch auf die Schweiz übertragen werden kann, weiss die Mehrheit der deutschen Computerbenutzer, was ein Virus und ein Wurm ist. Dass der eigene PC von Fremden ferngesteuert werden kann, wissen 90 Prozent. Und sieben von zehn Nutzern sind sich bewusst, dass die Absenderadressen von E-Mails gefälscht sein können. Dennoch schützen die Nutzer ihre Systeme nicht

[1] Siehe: www.bsi.de.

dementsprechend. Jeder Vierte hat keinen Virenschutz installiert. Die Studie deckt eine scheinbar paradoxe Situation auf: Man weiß zwar offensichtlich um die Gefahr, fühlt sich selbst aber nicht zum Handeln aufgefordert. Eine mögliche Erklärung dieser mangelhaften Vorsorge ist die Tatsache, dass rein privat genutzte Rechner häufig nur eine geringe Bedeutung haben. Für zwei Drittel der Befragten hat ein Computerausfall nach eigener Einschätzung auch keine schwerwiegenden Folgen.

Gerade von ungeschützten Computersystemen geht aber die Gefahr so genannter Bot-Netzwerke (siehe Kapitel 3.1) aus. Anscheinend unterschätzen viele Bürger ihre Verantwortung, wenn ihr Computer für eine Denial of Service- (DoS) beziehungsweise Spam-Attacke missbraucht wird. Die Studie liefert ein gutes Argument für den Betrieb einer Stelle zur Öffentlichkeitssensibilisierung, wie beispielsweise MELANI eine ist.

3 Aktuelle Gefahren und Risiken und deren technischer Hintergrund

3.1 Bot-Netze / DDoS-Attacken

Bot-Netze sind logische Computernetzwerke aus kompromittierten Systemen, die meist via Internet Relay Chat (IRC) kontrolliert werden, ohne dass die Besitzer dieser Systeme davon eine Ahnung hätten. Die Kompromittierung erfolgt meist durch das Ausnutzen einer ungepatchten Schwachstelle im Betriebssystem oder in einer eingesetzten Applikation (am häufigsten im Browser), schwache Passwörter sowie durch verseuchte E-Mail-Attachments. Nach der Infektion wird meist ein Programm installiert, mit dem anschliessend Tastatureingaben aufgezeichnet, Passwörter mitgelesen oder verschiedene andere unerwünschte Tätigkeiten durchgeführt werden können. Vor allem aber kann ein auf diese Art kompromittierter Rechner von einem zentralen Server aus für verschiedene Aktionen ferngesteuert werden. Im Falle eines abgestimmten Einsatzes sämtlicher einem Bot-Netz angehöriger Rechner kann ein solches Bot-Netz beispielsweise für verteilte Denial-of-Service Angriffe (DDoS) missbraucht werden. Auf diese Weise kann die Bandbreite, über die der angegriffene Server mit Datenpaketen bombardiert wird, massiv erhöht werden – gleichzeitig können auch Spuren verwischt werden, so dass die Herkunft der Attacke schwierig zu eruieren wird. Das bisher größte beobachte IRC-Botnetz hatte eine Größe von mehr als Hunderttausend Bots.

Eine der Hauptursachen für die zunehmenden DDoS-Vorfälle ist daher in der Zunahme der Bot-Netze zu orten. Solchen Bot-Netzen ist nur durch international konzertierte Aktionen beizukommen. Dabei spielt insbesondere auch die Sensibilisierung der End-Anwender eine wichtige Rolle: Erst wenn ein Grossteil der mit dem Internet verbundenen Rechner ausreichend geschützt ist, kann das Wachstum der Bot-Netze eingedämmt werden.

3.2 Phishing und Pharming

Im Verlauf der letzten Monate wurde weltweit eine massive Zunahme des so genannten Phishings verzeichnet – des Sammelns von Login-Daten insbesondere für Finanztransaktionen per betrügerischer Mail, das den User angeblich auf die Seite seines Finanzdienstleisters führt, die

tatsächlich vom Betrüger aufgesetzt worden ist. Die „Anti-Phishing Working Group“[2] stellte eine Zunahme von 28% vom Juli 2004 bis zum Januar 2005 fest. Am meisten betroffen sind Finanzdienstleister, Online-Versteigerungshäuser und Internet Provider.

Der führende Anbieter von Internet-Auktionen erlaubt es beispielsweise, Javascript auf den Auktionsseiten einzusetzen. So werden immer raffiniertere Phishingseiten ins Netz gestellt, die es auch erfahrenen Benutzern erschweren, Fälschungen auf einen Blick zu erkennen. Auch Benutzerbewertungen können so manipuliert werden.

Die meisten Phishing-Versuche betreffen zu 28% immer noch die USA[3], inzwischen finden aber auch in Europa recht häufig gezielte Attacken statt. Auch in der Schweiz kam es Anfangs Juni zu einer gezielten Phishing Attacke gegen ein Schweizer Finanzinstitut, die jedoch rasch gestoppt werden konnte.

Mögliche Gründe, weshalb die Schweiz erst jetzt von Phishing betroffen ist, liegen einerseits am hohen Sicherheitsstandard der E-Banking-Angebote der Schweizer Finanzinstitute, andererseits an der begrenzten Grösse der Schweiz und der damit verbundenen kleineren Anzahl an potenziellen Opfern.

Eine andere Methode beim Abgreifen von Daten ist das so genannte Pharming (siehe für ein Beispiel Kapitel 5.2). Pharming ist ein neuer Name für die relativ alte Angriffsmethode des DNS-Spoofing und basiert auf so genanntem „Cache Poisoning“. Das Grundprinzip funktioniert so, dass in einem DNS-Reply-Paket Extrainformation reingeschmuggelt wird, die dann vom DNS Server interpretiert wird. Dies erlaubt es dem Angreifer, falsche Informationen in den DNS Cache eines DNS-Servers zu bringen. Anders als beim Phishing landet bei einem erfolgreichen Pharming-Angriff selbst ein Benutzer, der keinem Link in einer Phishing-Mail folgt und stattdessen die URL von Hand im Browser eingibt oder die Seite über einen Bookmark aufruft, auf die gefälschte Seite. Diese Seite sieht dann zwar wie die Originalseite aus, hat auch die entsprechende URL, wird aber auf dem Server des Angreifers gehostet. Während DNS-Spoofing bei den sicher konfigurierten, grossen DNS-Servern grösserer Provider kaum droht, sind insbesondere kleinere, für die Namensauflösung in Firmennetzwerken zuständige, privat kontrollierte DNS-Server anfällig, so dass sich dieses Vorgehen insbesondere auch für Spionage-Aktivitäten (unbemerktes Umleiten der Nutzer eines Firmennetzwerks auf eine Seite, die Spionageprogramme verteilt) lohnt. In Kapitel 5.2 wird ein konkretes Beispiel eines Pharming-Angriffs aufgeführt.

Eine Untervariante von Pharming stellt das Verändern der so genannten hosts-Datei dar, die lokal auf jedem Windows-System vorhanden ist und ebenfalls der Namensauflösung dient. Bei der Eingabe einer Internet-Adresse (URL) wird ein Domain Name Server (DNS-Server) angefragt, welche IP-Nummer zu diesem Namen gehört. Windows bietet jedoch eine Funktion, zuerst auf dem lokalen Computer in der hosts-Datei nachzuschauen, ob sich dort ein entsprechender Eintrag befindet. Eine E-Mail mit vorsätzlich platziertem Scripting-Code bewirkt beim Öffnen eine Manipulation dieser lokalen hosts-Datei, so dass der Nutzer trotz der Eingabe einer korrekten URL, z.B. eines Finanzdienstleisters, auf eine Phishing-Seite umgeleitet wird. Die Internet-Dienstleistungen der Schweizer Banken umfassen jedoch diverse Sicherheitsmerkmale, die auch für diesen Fall Schutz gewähren. Insbesondere Internet-Anfänger sind im Visier der Betrüger. Es wird immer wieder versucht, das Vertrauen von Benutzern zu erlangen, indem die Webseite einer bekannten Firma imitiert wird.

[2] Siehe: www.antiphishing.org.

[3] Anti-Phishing Working Group, Bericht Januar 2005.

3.3. Gefahren und Risiken für Benutzer von Mobiltelefonen

Auch Mobiltelefone geraten vermehrt ins Visier von Malware-Autoren. Erstmals hat es ein Mobiltelefonwurm geschafft, sich über zwei Kontinente auszubreiten. Im Sommer 2004 wurde der Handywurm „Cabir“ auf den Philippinen entdeckt, inzwischen ist er auch in den Vereinigten Staaten aufgetaucht. Der Wurm kann durch ungeschützte und eingeschaltete Bluetooth Mobiltelefone übertragen werden, richtet aber keinen nennenswerten Schaden an. Im Gegensatz dazu steht der Handywurm „Skull“, der sich dadurch auszeichnet, auf dem Display statt den gewohnten Symbolen Totenköpfe anzuzeigen. Ein Entfernen dieses Virus ist mit dem Verlust von Daten verbunden. Nebst Infektion über Bluetooth können die Handywürmer aber auch den Multimedia Message Service (MMS) als Angriffsvektor nutzen, wie das Beispiel von „Commwarrior“ zeigt. Neben dem selbständigen Versenden an alle im Telefonbuch gespeicherten Adressen richtet dieser Wurm keinen Schaden an. Er befällt nur Telefone mit dem Betriebssystem Symbian 60, das unter anderen in verschiedenen Telefonmodellen der Firma Nokia eingesetzt wird.

Auf Grund dieser Meldungen stellt sich die Frage, ob mit einer ähnlichen Verbreitung der Handywürmer wie mit den Würmern im Internet zu rechnen ist. Nach Ansicht von MELANI ist eine schnelle, weltweite Verbreitung jedoch nicht zu erwarten. Dagegen sprechen verschiedene Gründe. Mobiltelefone besitzen im Moment noch nicht so viele zum Missbrauch geeignete Funktionen. Die Verbreitung der Schädlinge erfolgt zudem in den meisten Fällen über Bluetooth. Längst nicht jedes Mobiltelefon unterstützt diese Technologie und Bluetooth kann zudem bei sämtlichen Geräten deaktiviert werden. Ausserdem ist die Reichweite von Bluetooth beschränkt: Sie beträgt theoretisch etwa 300 Meter, wird aber in realen Verhältnissen, wie zum Beispiel in Städten, nur selten erreicht. Eine erhöhte Ausbreitungsgefahr besteht zum Beispiel an Grossveranstaltungen, wo sich viele Menschen auf relativ engem Raum befinden. Die effiziente Verbreitung scheitert meist auch an den verschiedenen Betriebssystemversionen, die jeweils auf die einzelnen Mobiltelefontypen zugeschnitten sind. Die Gefahr einer flächendeckenden, raschen Verbreitung wird daher momentan als eher gering eingestuft. Dies kann sich aber schnell ändern, da mit der neuen Generation von UMTS Mobiltelefonen eine Verschmelzung von Handy und Internet zu erwarten ist.

Aber auch ohne Schädlinge birgt achtlos eingesetzte Bluetooth-Technologie Gefahren: So kann zum Beispiel der Handyspeicher ausgelesen oder über das kompromittierte Mobiltelefon auf Kosten des Besitzers telefoniert, respektive Meldungen versandt werden. Ein risikobewusster Umgang mit der Bluetooth-Technologie ist daher unumgänglich.

3.4 Social Engineering

Im Informatikbereich geht die grösste Sicherheitsbedrohung für Firmen von den Angestellten aus, wie eine Studie von Gartner[4] aufzeigt. Viele Unternehmen kämpfen gegen den Missbrauch von E-Mail und Internet ihrer Mitarbeiter, der einen Zeitverlust für das Unternehmen bedeutet und zusätzliche mögliche Angriffsvektoren für schädlichen Code schafft. Die Studie bringt aber noch ein ganz anderes Ergebnis zu Tage: Über 70 Prozent der unberechtigten Zugriffe auf die Informationssysteme einer Firma werden gemäss Gartner von Angestellten begangen. 95 Prozent dieser Zugriffe enden in erheblichem finanziellem Verlust für die Firma. Die Herausforderung, die sich dadurch stellt, ist eine Balance zwischen einer freien Kommunikation zwischen den Angestellten und dem Schutz der Firma zu finden.

[4] Siehe: http://www.csoonline.com/analyst/report3317.html.

Die Problematik des Social Engineering sollte von den IT-Sicherheitsspezialisten ebenfalls auf keinen Fall vernachlässigt werden. Ein System kann noch so gut geschützt sein – wenn die Mitarbeiterinnen und Mitarbeiter nicht regelmässig auf dem Gebiet der Informationssicherheit geschult respektive informiert werden, erhöht sich das Potential eines solchen Angriffs enorm. Social Engineering Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Von allen Angriffsmöglichkeiten ist dies nach wie vor die erfolgreichste, mit höheren Erfolgsquoten als jeder Hacking-Angriff. Ein Angreifer kann mittels Social Engineering beispielsweise versuchen, an Benutzernamen und Passwörter von Mitarbeitern eines Unternehmens gelangen, indem er sich am Telefon als Systemadministrator oder Sicherheitsverantwortlicher ausgibt. Durch Vorgeben akuter Computerprobleme und Vortäuschen von Betriebskenntnissen (z.B. Namen von Vorgesetzten, Arbeitsabläufe, usw.) wird das Opfer so lange verunsichert, bis es die gewünschten Informationen preisgibt. Die Problematik des Social Engineering sollte deshalb nicht vernachlässigt werden. Es ist wichtig, das Personal regelmässig auf dem Gebiet der Informationssicherheit zu schulen und zu informieren.

Insbesondere im Bereich der gezielten Industriespionage ist Social Engineering ein wichtiger Bestandteil der Angriffe (siehe Kapitel 2.4, Kapitel 5.2: Gezielte Spionageangriffe gegen Grossbritannien und Kapitel 5.3: Spionageaffäre in Israel).

4 Aktuelle Lage IKT Infrastruktur national

4.1 Pannen, Ausfälle

In den ersten beiden Monaten des Jahres 2005 kam es zu zwei Pannen in der Schweiz. Wenngleich die Ursachen nicht dieselben waren, war das Ergebnis in beiden Fällen dasselbe: Teile der sozialen und wirtschaftlichen Aktivitäten der Schweizer Bürger waren zeitweise lahm gelegt.

Panne auf Eisenbahnnetz

Am Montag, dem 7. Februar 2005, funktionierte das Computersystem der SBB im Raum Zürich nicht mehr und konnte erst nach mehreren Stunden wieder in Betrieb genommen werden. Zunächst war nur die Zentrale in Zürich von der Blockade betroffen, dann in kürzester Zeit auch die angrenzenden Regionen. Diese Systempanne bekamen tausende von Bahnreisenden zu spüren.

Es zeigte sich, dass das Auswechseln eines falsch konfigurierten Netzwerkteils die Fernsteuerung in den Zentren Zürich HB und Zürich Altstetten lahm legte. Rund 40 ferngesteuerte Bahnhöfe im Limmattal, im Knonauer Amt und entlang der beiden Zürichseeufer liessen sich nur noch vor Ort bedienen. Dadurch erlitten Zehntausende von Bahnkunden zum Teil stundenlange Verspätungen, hunderte von Zügen fielen aus. Die Störung dauerte bis in den frühen Nachmittag, der Bahnbetrieb blieb bis in die Hauptverkehrszeit am Abend behindert.

Laut den SBB war „der Ausfall der Fernsteuerung auf eine Verkettung von unglücklichen Umständen und Missverständnissen zurückzuführen“. Bei geplanten Umschaltarbeiten im Verteiler der Güterverwaltung trennten die SBB-Dienste das Kabel

zwischen dem Stellwerk Zürich HB und dem Vorbahnhof. Da die redundante Verbindung nicht eingeschaltet war, kam es zu lokalen Störungen der Bedienplätze im Vorbahnhof. Beim Auftreten der Störungsmeldung bot das Personal im Zentralstellwerk Zürich, das über die Umschaltarbeiten nicht informiert worden war, den Pikettdienst auf. Auf der Suche nach der Störungsursache wechselte der Pikettdienst ein Netzwerkteil (Konverterbox) aus. Wenige Minuten später fiel die Bedienung der Fernsteuerung in den Zentren Zürich HB und Zürich Altstetten aus. Wie sich später herausstellte, war der ausgewechselte Netzwerkteil anders konfiguriert als der ursprüngliche. Dies führte zu Fehlermeldungen, welche die Rechner im Netzwerk nicht mehr verarbeiten konnten.

Die Ursache für diese Panne ist offenbar betriebsintern. Menschliches Versagen war der Grund, kein Angriff von aussen.

Hansjörg Hess, Verantwortlicher für die Infrastrukturen der SBB, resümierte: „Eine der wichtigsten Erkenntnisse unserer Analysen ist, dass wir die Komplexität der Anlagen reduzieren müssen." In einer Mitteilung vom 23. März 2005 informierte er, die SBB hätten folgende Schritte unternommen: Als kurzfristige Massnahme präsentierte er „die Erstellung einer provisorischen Rückfallebene für jenen der beiden betroffenen Fernsteuerbereiche, wo sich die Zugfahrten nicht manuell über eine Panoramatafel einstellen lassen. Mittel- und langfristige Massnahmen sind eine schweizweite Vereinheitlichung der Leittechnik sowie die Aufteilung der zwei Fernsteuerbereiche in fünf technisch unabhängige Sektoren. Strenge Vorgaben bei der Planung und ein doppelt gesichertes Freigabeprozedere stellen künftig sicher, dass die Wartungsarbeiten eng koordiniert ablaufen."

Hansjörg Hess führte weiter aus: „Der 7. Februar hat gezeigt, dass die Kundeninformation im Störungsfall der Schwachpunkt ist. Rechtzeitige und korrekte Kundeninformation ist entscheidend. Wir verbessern uns schrittweise hinsichtlich deren Qualität." In der Folge der Ereignisse vom 7. Februar gaben rund 600 Bahnreisende ihrem Unmut Ausdruck und stellten Entschädigungsforderungen in der Höhe von rund 1500 Franken. Toni Häne, Leiter Vertrieb und Services beim Personenverkehr SBB, fasste seine Erkenntnisse folgendermassen zusammen: „Wir haben festgestellt, dass unsere Kundenbetreuer an den Bahnhöfen während der Störung Zugriff auf aktuelle Informationen haben müssen. Dazu testen wir im Moment Taschencomputer, die dem Kundenbetreuer den drahtlosen Zugang auf aktuelle Betriebslagemeldungen und Zugsinformationen ermöglichen."

Die SBB befördern pro Jahr 250 Millionen Reisende und 55 Millionen Tonnen an Gütern. Mit Ausnahme von Herisau, Appenzell und Stans sind alle Kantonshauptorte an das Streckennetz der SBB angeschlossen. In rund 800 Bahnhöfen fahren Züge im Stunden- oder Halbstundentakt ein und aus. Zwei Drittel der alpenquerenden Transitgüter werden mit der Bahn transportiert. Die Güterwaggons können in 650 Bahnhöfen beladen und umgeladen oder empfangen und geleert werden. Rund 2450 Unternehmen haben einen direkten Anschluss an das Bahnnetz der SBB und sind so mit ganz Europa verbunden. Diese Zahlen belegen, wie bedeutend die SBB für die Schweizer Volkswirtschaft sind und illustrieren die Wichtigkeit der Sicherheit der SBB-Informatiksysteme. Und so wichtig es ist, ein System gegen aussen abzusichern, so wichtig ist es aber auch, die Schwachstelle Mensch einzukalkulieren.

E-Banking-Service ausser Betrieb

Eine wetterbedingte Panne verursachte am 18. Januar 2005 in der Westschweiz zahlreiche Probleme bei Computersystemen. Im Kanton Genf, nahe Verbois, schlug ein Blitz in eine Hochspannungsleitung ein. Die Folge: Ein mehr als einstündiger Black-out. Weil das Bahnnetz und der Flughafen Genf-Cointrin von einem unabhängigen Energienetz Strom beziehen, blieben die SBB verschont. Dafür waren die Computersysteme der Banken umso

stärker betroffen. Der Koordinator des Tradingsaals bei einer Grossbank versicherte zwar, die Bildschirme hätten funktioniert und das Licht sei nach fünf Sekunden wieder angegangen. Die E-Banking-Seite im Internet war indessen während beinahe des ganzen Tages ausser Betrieb.

4.2 Attacken

Webserver, die in der Schweiz stationiert sind, bleiben von Attacken nicht verschont. Die Zahlen sind eindeutig: Tausende Websites werden ohne Einverständnis des Systembetreuers verändert. Im Fachjargon spricht man von Defacement.

Website-Defacement: Unfug, Spass oder neue Form des sozialen Protestes?

In der Vergangenheit haben Hacker bereits Tausende Websites auf schweizerischen Servern beschädigt oder vorübergehend unbrauchbar gemacht. Defacement (engl. für "Entstellung" oder "Verunstaltung") steht bei Hackern hoch im Kurs. Man unterscheidet zwischen zwei Arten von Defacement: Homepage Defacement und Mass Defacement. Beim Homepage Defacement werden Sicherheitslücken in Webservern ausgenutzt (diese finden sich zum Beispiel in unzulänglich konfigurierten Foren), durch die schädlicher Code infiltriert wird. Ein solcher Code kann einzelne Webseiten verändern. Mass Defacement umfasst den gesamten Webserver, weshalb Hunderte von Sites gleichzeitig betroffen sind. Mass Defacement ist offenbar vor allem bei Jugendlichen, den „Script-Kiddies“, sehr beliebt. Mit diesem Begriff werden unter anderem Kinder oder Jugendliche bezeichnet, die sich einen Spass daraus machen, bei Webservern, die unzulänglich konfiguriert oder nicht mit Sicherheitspatches aktualisiert sind, Schwachpunkte zu finden, über die sie in fremde Netze eindringen können.

Eine weitere Gruppe sind die so genannten „Hacktivisten“: Hacker, die mit Webattacken auf ihre politischen oder kulturellen Anliegen aufmerksam machen wollen. Anders als Script-Kiddies missbrauchen Hacktivisten offenbar kaum schweizerische Webserver. Die wenigen Auftritte von Hacktivisten und die Art der Anliegen, die sie vorgebracht haben, lassen darauf schliessen, dass es ihnen tatsächlich um politische Inhalte geht und dass Webattacken nicht Selbstzweck, sondern ein Mittel ist, um sich Gehör zu verschaffen. Nachfolgend eine Auswahl von Hacktivisten-Gruppen, die über schweizerische Server im Web auftreten:

„Dark-Underground“, eine Gruppe von Personen oder eine Einzelperson, attackiert in der Regel nur die Websites von Regierungen, Universitäten oder öffentlichen Institutionen (NASA, Eidgenössische Bundesverwaltung, Princeton University etc.). Die gängigste Parole, die Dark-Underground aufschaltet, lautet: „Why I deface? I deface for this stupid war for all idiot terrorist in Iraq, Russia and in the rest of World. For the Beslan Victim and the victims of the future. Because the war will never have an end.“ Das fehlerhafte Englisch lässt darauf schliessen, dass wer auch immer sich hinter diesem Namen verbirgt, nicht englischsprachiger Herkunft ist. Sehr viel wahrscheinlicher ist die Vermutung, es handle sich um eine Person oder um Personen italienischer Herkunft: Immer wieder findet sich die Parole „Free Italian from Iraq“, und wiederholt werden Gruppen kritisiert, die sich auf den über die Adresse irc.azzurra.org aufgeschalteten IRC-Kanälen unterhalten. Irc.azzurra.org ist ein von der italienischen Adresse cwnet.it verwaltetes Netzwerk, über das die meisten italienischsprachigen Kanäle laufen.

Eine andere Gruppe von Hackern – „Infection Group“ – ist von Brasilien aus aktiv, einem Land, das in jüngster Zeit zahlreiche Hacker hervorgebracht hat. Die Infektion Group

hat mittlerweile Tausende Websites verändert, die auf Servern in der Schweiz liegen. Mitte Februar 2005 attackierte diese Gruppe einen Server des Hostingproviders SwissWeb und veränderte eine grosse Zahl von Websites. Auch die Infektion Group lässt sich der Gruppe der Hacktivisten zuordnen. In den Texten werden die USA und George Bush verunglimpft und der Irakkrieg kritisiert. Bislang hat diese Gruppe 23'041 Websites verändert, 2'550 einzelne Sites und 20'491 durch Mass Defacement. Die Mitglieder dieser Gruppe treten unter den folgenden Pseudonymen auf: Dominius_VIS, H4rd_L3v3l, Infektion, N1D3Z, cCkw, shellc0de. Auffallend aktiv ist seit kurzem eine Gruppe namens Core-Project, ebenfalls aus Brasilien: Ziel der Attacke waren 2005 die Server des Hostingproviders Touch Systems. Hunderte Websites waren betroffen. Ihre Aktivität ist nicht politisch motiviert. Das Thema dieser Gruppe ist offenbar die technische Entwicklung und die damit einhergehende Gefahren. Unlängst waren auch die Websites von zwei grossen Universitäten in den USA Ziel von Attacken dieser Gruppe: die Berkeley University (berkeley.edu) und die Washington University (washington.edu). Augenfällig ist das Know-how, das diese Gruppe besitzt: Die Mitglieder sind daher kaum Script-Kiddies, sondern Fachleute.

Die in der Schweiz aktiven Hackergruppen sind in den unterschiedlichsten Teilen der Welt zu Hause. Neben den in Italien oder Brasilien beheimateten Gruppen gibt es zum Beispiel die „ArCAX-ATH“. Diese Gruppe nennt sich „the Dominican defacers crew“, was den Schluss nahe legt, dass sie in der Dominkanischen Republik beheimatet sind. Eine weitere Gruppe mit der Bezeichnung „23erdem“ besteht nach eigener Aussage aus türkischen Hackern.

Der Schaden, den diese Hacker tatsächlich verursacht haben, lässt sich noch nicht beziffern. Erst eine Erhebung unter den Betroffenen würde verlässliche Aussagen erlauben. Handfeste Zahlen wären durchaus wünschenswert, würden sie doch helfen zu begreifen, wie wichtig die Sicherheitsvorkehrungen zum Schutz von Webservern sind und die Notwendigkeit der Bereitstellung von finanziellen Mitteln zum Schutz von Webservern verdeutlichen.

Attacke auf admin.ch

Am Morgen des 17. Dezembers 2004 verschaffte sich die Gruppe „Dark-Underground“ Zugang zu dem Server, der die Websites der Bundesverwaltung hostet. Neben der auf diesem Server gehostete Website swisspolice.ch wurden 17 weitere Homepages verändert. Anstelle der Homepages schaltete die Gruppe den für sie typischen Antikriegs-Slogan auf. Nachdem der Webserver unverzüglich ausser Betrieb gesetzt worden war, wurden Verbindungen hunderter Homepages mehrer Departemente der öffentlichen Verwaltung unterbrochen. Am Nachmittag desselben Tages konnte auf die Mehrzahl der Homepages wieder zugegriffen werden; die beschädigten Homepages waren jedoch erst im Laufe des Sonntags, also 48 Stunden nach der Attacke, wieder betriebsbereit.

Internet: Wurmattacke auf Grossdetaillisten

Ein Computerwurm hat zu Beginn dieses Jahres Teile der IT-Infrastruktur eines Grossdetaillisten lahm gelegt. Betroffen waren rund 2000 Computer mit einem Microsoft-Betriebssystem.

Verantwortlich für den Zwischenfall war eine Variante des Computerwurms Rbot, der das Netzwerk vollständig zusammenbrechen liess. Da die Entfernung dieses Wurms ziemlich aufwändig ist, konnten die ersten Computer erst am nächsten Tag wieder angeschlossen werden. Zwei Tage später funktionierte die Informatikinfrastruktur wieder einwandfrei.

Der Wurm RBot tritt in zahlreichen Varianten auf und abgeänderte Versionen erscheinen teilweise mehrmals täglich. Die Hauptfunktionen dieser Wurmfamilie umfassen den Zugriff von Dritten auf den Computer oder Aufzeichnen und Weitersenden von Tastatureingaben (wie zum Beispiel Passworteingaben). Der Wurm kennt verschiedene Angriffsvektoren: Beispielsweise das Ausnutzen von unsicheren Passwörtern, Ausnutzung von Betriebssystem-Schwachstellen und Benutzung von bereits bestehenden Hintertüren, welche von anderer Malware bereits installiert wurden.

Im Allgemeinen müssten Virenschutzprogramme solche Trojanischen Pferde erkennen. Dieser Vorfall illustriert jedoch deutlich, dass man sich dennoch nicht vollständig auf solche Schutzprogramme verlassen kann, sondern zusätzlich Sorgfalt walten lassen und ein sicheres Passwort einsetzen muss.

Auf Anwenderseite ist es wichtig, Mitarbeitende dahingehend zu informieren, sorgfältig mit der Informationsinfrastruktur umzugehen, sowie Regeln im Umgang mit Informatikmitteln zu erstellen und durchzusetzen. Die Internetseite der Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch) gibt für den Bürger, aber gerade auch für KMU, grundlegende Tipps im Umgang mit den Informations- und Kommunikationstechnologien.

4.3 Kriminalität

Phishing in der Schweiz

Anfang 2005 wurden vermehrt Phishing-Angriffe gegen Schweizer Finanzinstitute registriert. Nachdem Webbrowser wie etwa der Internet Explorer mit Patches ausgestattet worden sind, konnte diese Art von Trickbetrug deutlich eingeschränkt werden. In der Welt der Informatik sind der Fantasie eines findigen – und listigen – Geistes aber kaum Grenzen gesetzt. So werden mittlerweile neue Tricks und Betrügereien angewendet (siehe Kapitel 3.2). Der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) sind insgesamt an die einhundert Fälle von Phishing gemeldet worden. Die Anzeigen stammen von Internet-Benutzern, die E-Mails erhalten haben, die aussehen, als seien sie zum Beispiel von einer Bank oder einem Online-Auktionshaus versandt worden. Mit diesen gefälschten E-Mails sollten Opfer dazu gebracht werden, gefälschte Websites zu besuchen und dort persönliche Informationen wie Bankzugangsdaten, Kreditkartennummern oder Ähnliches einzugeben. Dabei handelte es sich zumeist um E-Mails, die auf ausländische Banken abzielten, wie z.B. der CitiBank oder Sun Trust. Zu bemerken ist an dieser Stelle, dass Schweizer Banken über technisch ausgereiftere Sicherheitssysteme für das E-Banking verfügen (z.B. Hardware-Tokens zur Identifizierung, Streichlisten oder Kombinationen davon), während ausländische (insbesondere US-amerikanische) Banken meist über tiefere Standards verfügen und daher für einen Phishing-Angriff attraktiver sind.

Dennoch fand am Wochenende des 5. und 6. Juni eine Phishing-Attacke gegen ein Schweizer Finanzinstitut statt, die aber rasch gestoppt werden konnte. Bei diesem Phishing-Versuch wurde wie üblich eine E-Mail mit einem Link verschickt, der nach dem Anklicken die offizielle E-Banking-Seite im Hintergrund lud und zusätzlich ein gefälschtes Popup Fenster mit einer Eingabemaske für Kundendaten öffnete. Die Phishing Seite (Popup Fenster) wurde in Russland gehostet und über verschiedene Stationen, so genannte Redirects, aufgerufen.

Phishing-Seiten auf Schweizer Servern

Am 8. Februar 2005 wurde auf einem Schweizer Server eine Phishing-Seite entdeckt. Die Seite entsprach bis ins kleinste Detail jener von eBay, dem Internet-Auktionshaus, und forderte zur Eingabe von Kundennummer und Kreditkartendaten auf. Die auf diese Weise illegal gesammelten Daten wurden an eine elektronische Adresse weitergeleitet, deren Besitzer sich wahrscheinlich in Frankreich aufhält. MELANI benachrichtigte unverzüglich den Hostingprovider der missbrauchten Webadresse. Die Seite konnte innert weniger Stunden vom Netz genommen werden. Es ist nicht bekannt, wie viele persönliche eBay- und Kreditkarten-Daten über die gefälschte Seite versandt worden sind.

Am 1. März 2005 wurde MELANI von einem Abuse Team auf eine weitere Phishing-Seite auf einem Schweizer Server hingewiesen. Das Gästebuch auf dieser Seite wies eine Schwachstelle auf, die von Dritten genutzt wurde, um eine gefälschte PayPal-Seite aufzuschalten.

Neue Betrugsformen

E-Mails, mit denen versucht wird, mit der als „Nigerian Scam“ bekannt geworden Masche an Geld zu kommen, haben während Jahren immer wieder den Weg in die elektronischen Briefkästen der Schweiz gefunden. Mittlerweile sind solche Mails seltener geworden. Dafür zeichnet sich eine neue Betrugsform ab: Über Kleinanzeigen im Internet werden für alle möglichen Artikel Käufer oder Verkäufer gesucht. Bei der klassischen Form des Nigerian Scam wird über Kleinanzeigen mit potenziellen Opfern Kontakt aufgenommen. Diesen wird dann angeboten, für eine bedeutende Provision eine grosse Geldsumme in ein afrikanisches oder asiatisches Land zu transferieren. Und dann sind da noch Betrüger, die nach Käufern Ausschau halten, die sie übers Ohr hauen können. Der Verkauf von Produkten zu deutlich niedrigeren Preisen als auf dem offiziellen Markt, beharrliche und oft aggressive Verkaufsmethoden, die diese Personen anwenden, lassen starke Zweifel an der Seriosität solcher Angebote aufkommen.

Nigerianer in Zürich wegen Betrugs verurteilt

Am 9. Februar 2005 verurteilte das Bezirksgericht Zürich einen 39-jährigen Nigerianer zu zwanzig Monaten Gefängnis. Er war des wiederholten Betrugs und der Geldwäscherei für schuldig befunden worden. Mit seinen bislang noch unbekannten Komplizen stellte der Nigerianer seinen Opfern jeweils eine hohe Provision in Aussicht, wenn sie ihm dabei behilflich wären, grosse Geldsummen, die angeblich in Afrika blockiert seien, zu transferieren. Der erste Schritt des Geschäftes bestand darin, die Opfer von der Notwendigkeit zu überzeugen, einen gewissen Betrag für „administrative Kosten“ vorzuschiessen.

Schweizer Banken im Visier eines Keyloggers

Unlängst wurde die Malware „PWSteal.Bankash.D“ entdeckt, die Benutzernamen und Passwörter ausspionierte. Beim Einloggen in die Online-Dienste zweier Schweizer Finanzinstitute wurden die eingegeben Daten mitprotokolliert.

Der Schädling gelangte über den einer E-Mail beigefügten Anhang, über infizierte Software oder durch Ausnutzen von Sicherheitslücken im Betriebssystem auf einen Computer. Die meisten der in der Schweiz zum E-Banking verwendeten Systeme arbeiten mit einem Zweiphasen-System zur Kundenidentifikation (z. B. in Verbindung mit einer zusätzlichen Streichliste oder einem Hardware-Token). Dank dieser Sicherheitsvorkehrung

lässt sich die Gefahr, dass Benutzernamen und Passwörtern missbraucht werden, verringern, weshalb auch die Versuche von „PWSteal.Bankash.D“ erfolglos blieben.

4.4 Terrorismus

Islamic-minbar.com — islamistischer Extremismus auf Schweizer Servern

Am 8. September 2004 war in einem Forum, das auf einem schweizerischen Server gehostet wurde, eine der „Armata islamica“ in Irak zugeschriebene Mitteilung erschienen. Die Nachricht erschien im Forum der Website www.islamic-minbar.com und behauptete, es sei über das Schicksal zweier im Irak gefangener französischer Geiseln in der Gewalt von „Armata islamica“ entschieden worden. Anwender machten den in Lausanne befindlichen Hostingprovider auf den Inhalt der Website aufmerksam. Der Provider benachrichtigte unverzüglich die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) des Bundesamts für Polizei (fedpol). Auf das Forum angesprochen, wies der Besitzer der Website, ein in der Schweiz niedergelassener Tunesier, jegliche Verantwortung für den Inhalt von sich. In einem in der Zeitung „24Heures“ veröffentlichen Interview gab er zu verstehen, dass dieses Forum lediglich dazu dienen soll, sich zum Islam und zu den Geschehnissen in der Welt zu äussern. Das Forum blieb online, bis Net4all sich entschloss, die Website vom Server zu nehmen.

Sunna-minbar.com — Nachfolger von islamic-minbar.com

Kurz nachdem die Website www.islamic-minbar.com vom Web verbannt worden war, tauchte ein anderes, dem Islam und dem bewaffneten Kampf gewidmetes Forum auf. Das neue Forum unter der Adresse www.sunna-minbar.com will sich als Nachfolger von islamic-minbar.com verstanden wissen. Der Besitzer der Website ist wieder ein Nord-Afrikaner. Auch der Hostingprovider befindet sich auf Schweizer Boden. Der Besitzer der Website lebt in Tunesien. Mittlerweile ist die Website nicht mehr in Betrieb.

Laut Reuven Paz, einem israelischen Fachmann, gibt es weltweit rund einhundert Foren, über die radikale Islamisten Propaganda betreiben und Mitteilungen veröffentlichen. Dabei darf man sich nicht darüber hinweg täuschen, dass es Foren gibt, die sich ungleich grösserer Popularität erfreuen, als die beiden hier erwähnten in der Schweiz gehosteten Beispiele. Was sich in diesen Foren an Information findet, mag zum Teil korrekt, zum Teil falsch sein. Ungeachtet dessen kommen diese Foren den Terroristen jedenfalls äusserst gelegen: Sie erreichen eine grosse Zahl von Leuten, die ihre Botschaft vernehmen und sich auf diese Weise für die Sache gewinnen lassen.

Fünf verdächtige Ausländer verhaftet

Am 22. Februar 2005 verhaftete die Bundeskriminalpolizei (BKP, fedpol) fünf Personen. Sie waren verdächtigt worden, radikalen gewaltbereiten islamistischen Kreisen anzugehören. Gegen sie wurde Anklage erhoben wegen Propaganda auf dem Internet, mit der sie zu terroristischen Anschlägen aufgerufen haben. Ausserdem müssen sie sich wegen eines Videos verantworten, auf dem ein zum Tode Verurteilter hingerichtet wird und Menschen verstümmelt werden. Mindestens zwei der Angeklagten betrieben die in Frage stehende Website, www.islamic-minbar.com.

Die Verhaftung dieser Personen ist Teil der ersten Untersuchung, die die Bundesbehörden in einem Fall extremistischer Propaganda über das Internet eingeleitet haben.

In Fribourg, Düdingen und Biel wurden Hausdurchsuchungen durchgeführt. In zwei Fällen musste sich die Polizei mit Gewalt Zutritt zu den Räumen verschaffen. Die Männer, alle zwischen dreissig und vierzig Jahre alt, sind Muslime mit extremistischer Neigung. Sie kommen aus Tunesien und Belgien und halten sich legal in der Schweiz auf.

Im Zuge der Durchsuchungen wurden umfangreiche Unterlagen – hauptsächlich in Arabisch – und einschlägiges Bildmaterial sichergestellt. Das Forum auf der Website diente als Mittel zur Propaganda für die radikal-islamische Bewegung und enthielt sogar präzise Angaben darüber, wie man eine Bombe baut, Anschläge verübt und eine Entführung durchführt.

4.5 Diverses

Anonymität im Telekommunikationsbereich

Laut den Artikeln 14 und 15 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sind die Anbieter von Fernmeldediensten verpflichtet, den zuständigen Behörden bei Bedarf bestimmte Auskünfte über Fernmeldeanschlüsse zu liefern. Dazu gehören unter anderem der vollständige Name des Teilnehmers sowie Adresse und Art des Anschlusses (Art. 14 BÜPF). Nach Artikel 15, Ziffer 5^{bis}, müssen „die Anbieterinnen während mindestens zwei Jahren nach Aufnahme der Kundenbeziehung die Auskünfte nach Artikel 14 auch über Personen erteilen können, welche die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementsverhältnis aufgenommen haben." Angesichts dieser Bestimmung verlangten die Anbieterinnen von Fernmeldediensten, dass Personen, die eine im Mobilfunk verwendete Prepaid-SIM-Karten besitzen (SIM Prepaid Card), sich bis zum 31. Oktober 2004 registrieren lassen. Karte und Anschluss der Personen, die diesem Aufruf nicht nachkommen, würden gesperrt werden. Der Aufruf richtete sich indessen nur an diejenigen, die eine Prepaid-Karte nach November 2002 gekauft haben. Weshalb nur sie?

Nach dem Grund dieser Regelung gefragt, antwortete das UVEK: „Das Gesetz legt die Aufbewahrungspflicht der Anbieterinnen von Fernmeldediensten für die Daten auf mindestens 2 Jahre fest (Beschluss des Parlamentes). Die Nachregistrierung muss bis zum 31. Oktober 2004 erfolgen. Da es keinen Sinn macht Kunden nachzuregistrieren, deren Daten nicht mehr aufbewahrt werden müssen, ist die Nachregistrierung auf 2 Jahre zurück beschränkt worden."

Nach dem Gesetz muss sich also, wer eine Prepaid-SIM-Karten vor dem 31. Oktober 2002 gekauft hat, nicht registrieren lassen. Zwei Jahre nach dem Kauf einer Karte und nach der Registrierung werden die Daten in der Regel gelöscht. Auf die Frage, was es denn genau mit der Begrenzung auf zwei Jahre auf sich habe, antwortete das UVEK: „Die genauen Gründe für diesen Parlamentsbeschluss sind aus den Materialien nicht ersichtlich (Protokolle im Bundesblatt). Relevant dürften einerseits Gründe des Datenschutzes sein. Andererseits ist für die Strafverfolgungsbehörden insbesondere die Tatsache problematisch, dass viele Kriminelle ihre Karten häufig und nach kurzer Zeit wechseln."

Wegen dieser Begrenzung ist es zu einem regelrechten Handel mit SIM-Karten gekommen, die vor November 2002 gekauft worden sind. In den grossen Online-Auktionshäusern wie eBay oder ricardo.ch werden diese Karten mittlerweile sehr teuer versteigert. Sie sind sehr begehrt, zumal sie dem Besitzer gerade jene Anonymität gewähren, der man mit der

Gesetzesänderung entgegenzutreten versucht. Für eine Prepaid-SIM-Karte werden zwischen 150 bis 1200 Franken bezahlt. Mit den bestehenden Gesetzesbestimmungen lässt sich das Problem des anonymen Mobilfunkinhabers offensichtlich nicht lösen.

Anonymität auf dem Internet

Es bieten sich viele Möglichkeiten an, um im Internet anonym aufzutreten. Die vielleicht praktikabelste, weil schnelle und preisgünstige Methode besteht darin, sich eine Prepaid-Karte für einen von Swisscom Mobile bereitgestellten Hotspot zu kaufen, der sich auf Schweizer Boden befindet. Bei Computernetzen wird die Bezeichnung „Hotspot“ für einen Wireless-LAN Anschlusspunkt zum Internet verwendet. In der Schweiz sind 800 Hotspots eingerichtet. Alles, was man zu tun braucht, ist, mit einem Laptop ausgerüstet in einen Swisscom Shop zu gehen und eine Value Card zu kaufen. Auf der Rückseite dieser Karte finden sich eine UserID und ein Passwort, die den Zugang aufs Internet ermöglichen. Die MAC-Adresse der jeweiligen Netzwerkkarte ist die einzige Spur, die vom Navigieren im Internet bleibt. Es ist jedoch kaum möglich, diese Spur bis zu der betreffenden Person zurückzuverfolgen. Hinsichtlich des Internets ist die Value Card das, was die Prepaid-SIM-Karte für das Mobiltelefon ist: Eine Möglichkeit zur vollständigen Identitätsverschleierung. Zwar verpflichtet das BÜPF die Anbieterinnen von Fernmeldediensten dazu, die Personendaten ihrer Kunden zu registrieren; wer aber eine Public Wireless LAN Value Card kauft, braucht keinerlei Personendaten anzugeben.

5 Aktuelle Lage IKT Infrastruktur International

5.1 Pannen, Ausfälle

Pakistans Internetverbindung ins Ausland gestört.

Ende Juni / Anfang Juli erlitt Pakistan weit gehende Störungen in seiner Internet-Kommunikation mit dem Ausland. Gemäss der Pakistan Telecommunication Company Ltd (PTCL) liegt die Ursache dafür in einer Beschädigung eines Glasfaser-Seekabels, über das ein Grossteil der IP-Verbindungen ins Ausland geleitet wird. Während der etwa zwei Wochen dauernden Reparaturarbeiten wurde der IP-Verkehr über andere Kanäle geleitet, so dass Pakistans Internet-Adressen (.pk) zwar erreichbar waren, jedoch Wartezeiten in Kauf zu nehmen waren.

Eine mögliche Ursache liegt in einem Streik der PTCL-Mitarbeiter, die gegen eine geplante Privatisierung des Unternehmens protestierten. Erst kurze Zeit davor hatte das Militär mehrere Hundert Mitarbeiter festgenommen und die Kontrolle über die zentralen Telekommunikationsanlagen übernommen. Der Vorfall illustriert, wie wichtig eine redundante Internetanbindung für einen sicheren und störungsfreien Betrieb ist.

5.2 Attacken

Fall Root-Kit

Im Juni 2004 erlangte MELANI Kenntnis über einen bedeutenden Fall eines international durchgeführten elektronischen Angriffs. Ein System aus dem universitären Bereich in der Schweiz wurde dabei kompromittiert. Im September 2004 wurden weitere kompromittierte Universitäts-Systeme identifiziert, unter anderem waren Hosts aus Schweden, Grossbritannien, den USA, und der Schweiz betroffen. Die auf diese Weise gesammelten Passwörter wurden wiederum für Logins in weitere Systeme genutzt. In der Schweiz wurde neben der betroffenen Universität auch ein Rechner an einem Forschungszentrum kompromittiert. Die Art des Angriffs liess auf eine erfahrene Person oder Gruppe schliessen.

Anfang Oktober wurde MELANI darauf hingewiesen, dass es sich beim Angreifer um jemanden mit dem Nickname „STAKKATO“ handelt. In Schweden und den USA waren zu dieser Zeit bereits Untersuchungen gegen STAKKATO im Gange.

Im Dezember 2004 wurde MELANI über eine weitere kompromittierte Maschine in der Schweiz informiert.

Ende Dezember 2004 erhielt dann MELANI aus derselben Quelle die Information, dass die meisten beobachteten Aktivitäten im Juli und August 2004 nach Schweden zurückverfolgt werden konnten. In Schweden konnte schliesslich im Januar 2005 diese Gruppe ermittelt werden: Es handelte sich um eine Gruppe Jugendlicher, die über fundiertes Wissen verfügte.

Der Fall Root Kit wurde von der gleichen Täterschaft durchgeführt, wie der in den Medien erwähnte Einbruch in das Cisco Netzwerk im Mai 2004. Dabei wurde rund 800 MB Sourcecode der Cisco Router Software gestohlen.

Der Fall Root-Kit illustriert anschaulich, wie wichtig internationale Kooperation ist – ohne internationale Kommunikation und Zusammenarbeit hätte dieser Fall nie aufgedeckt werden können. MELANI konnte dabei seinen Teil zur Aufklärung dieses Falles beitragen. Ohne eine vertrauliche Anlaufstelle, die von einer Schweizer Firma auch dann angegangen werden kann, wenn keine Anzeige erstattet werden will, wäre die Dimension des Falles Root-Kit – und somit auch sein Bedrohungspotenzial – in der Schweiz (zumindest offiziell) gar nicht erst wahrgenommen worden.

Gezielte Distributed Denial-of-Service (DDoS) Attacke gegen heise.de

Ein illustratives Beispiel für eine DDoS-Attacke, wie sie beispielsweise mit einem Bot-Netzwerk durchgeführt werden kann, bietet ein Angriff auf die Webserver des Heise Zeitschriften Verlags in Deutschland. Dieser unterhält unter www.heise.de das meistbesuchte deutschsprachige IT-Nachrichten-Angebot im Internet.

Am Montag, 31. Januar 2005, wurde heise.de ab etwa 10 Uhr durch mehrere DDoS-Attacken bis am Dienstagabend (1. Februar 2005) stark beeinträchtigt und während fünf Stunden gar vollständig lahm gelegt. Es wurden so viele Anfragen gleichzeitig aus verschiedenen Quellen gegen den Webauftritt gerichtet, dass der Load Balancer, der sämtliche Aufrufe von www.heise.de auf rund 25 einzelne Webserver verteilt, überlastet wurde. Normalerweise verfügt dieser Load Balancer über genug Kapazität, um selbst den grössten Besucherandrang verarbeiten und auf die Webserver verteilen zu können. Im Verlaufe des Angriffs musste der Balancer aber mehrmals neu gestartet werden und auch eine Speicheraufrüstung reichte nicht aus, um den Angriffen standzuhalten.

Die Techniker des heise-Verlags und die Angreifer lieferten sich ein stundenlanges Katz-und-Maus-Spiel: Auf jede Aktion der Techniker reagierten die Angreifer mit einer Anpassung ihres Datenpaketstroms, so dass die Verteidigungsmassnahmen über lange Zeit unwirksam blieben.

Der heise-Verlag erstatte Strafanzeige und setzte für sachdienliche Hinweise ein Belohnung von 10'000 Euro aus. Am 2. Februar riefen heise Netzwerkadministratoren zur Mithilfe bei der Suche nach dem Täter auf mit dem Ziel, an eines der Schadprogramme auf einem der am Angriff beteiligten Rechner zu kommen. Über den Erfolg oder Misserfolg von heises Suche nach dem Urheber liegen MELANI keine weiteren Informationen vor.

Der DDoS-Angriff auf heise illustriert das grosse Schadenspotenzial solcher Attacken. Das Heise-Web-Portal ist eines der grössten und bedeutendsten in Deutschland, verteilt auf mehrere Server-Systeme – und dennoch schaffte es der Angreifer, den Webauftritt des Verlages stundenlang lahm zu legen. Für ein Unternehmen, das primär auf seinen Webauftritt angewiesen ist (als Paradebeispiele wären da google.com, amazon.com sowie ebay.com zu nennen), kann ein solcher Ausfall verheerende Auswirkungen haben. Neben den finanziellen Verlusten, die auf Grund der Verteidigungsmassnahmen sowie des Einnahmenausfalles entstehen, muss auch ein nicht quantifizierbarer Vertrauensverlust mit weiteren finanziellen Konsequenzen in Kauf genommen werden.

DDoS-Attacke gegen Internet-Bezahldienst Worldpay

Ein weiterer Fall einer DDoS Attacke ereignete sich Anfang Oktober 2004 gegen den amerikanischen Internet-Bezahldienst Worldpay, der den Betrieb des Online-Portals empfindlich beeinträchtigte. Durch eine Überflutung mit vielen Anfragen wurde die Transaktionsabwicklung deutlich verlangsamt, ohne dass aber eine Gefährdung der Sicherheit eingetreten wäre. Alle Transaktionen konnten dennoch verarbeitet werden.

Worldpay wurde bereits im November 2003 Opfer einer ähnlichen Attacke. Der Anbieter, dessen Eigentümer die Royal Bank of Scotland ist, zählt etwa 30'000 Online-Händler in über 70 Ländern zu seinen Kunden, unter Anderen auch Vodafone oder Sony Music Entertainment.

Bei WorldPay handelt es sich um einen grossen Finanztransaktionsanbieter im Internet, auf dessen Dienste tausende anderer Online-Dienstleister für die Abwicklung ihrer Geschäfte angewiesen sind. Man kann davon ausgehen, dass die IT-Infrastruktur von WorldPay höchsten Sicherheitskriterien genügte, die nach dem DoS-Angriff vom November 2003 wohl noch zusätzlich zur Abwehr von DDoS-Attacken optimiert worden waren. Dennoch reichte diese Infrastruktur offenbar nicht aus, um sich vollständig vor einem grossen, verteilten DoS-Angriff zu schützen.

DoS-Attacken gegen Server der japanischen Regierung

Nicht nur private Unternehmen wurden Opfer von DoS-Attacken: In der dritten Februar-Woche 2005 waren mehrere japanische Regierungs-Webseiten solchen Angriffen ausgesetzt. Ein permanenter Schaden wurde an den Systemen nicht angerichtet – der Angriff war aber auch nicht auf die Erzielung eines solchen ausgerichtet. Die japanische Regierung prüft nun ihr IT-Sicherheitskonzept.

Die angegriffenen Webseiten gehörten zum Büro des Premierministers sowie zum Kabinettsbüro. Der Angriff führte zu einem Versagen der Online-Dienste auf Grund der massiven Datenanfragen. Die Seiten standen mehrmals nicht zur Verfügung. Kurz nach den Angrif-

fen erbrachten die Server ihre Dienste wieder wie gewohnt. Die japanische Regierung untersucht den Vorfall, tappt aber bisher im Dunkeln.

Zusätzlich zu den Einschätzungen der vorangehenden Attacken lässt sich zu diesem Vorfall bemerken, dass offensichtlich auch Regierungsdienste im Internet nicht vor Angriffen dieser Art gefeit sind. Als asymmetrische Waffe zur Erregung politischer Aufmerksamkeit ist künftig vermutlich vermehrt mit solchen Angriffen zu rechnen. Damit sind DoS-Attacken neben Sabotage- und Bereicherungs-Absichten ein zusätzliches Motiv zuzuschreiben: Politische Propaganda und Einflussnahme. DoS-Attacken könnten in Zukunft als Mittel des so genannten „Information Warfare" vermehrt auftauchen – schliesslich stehen solche Attacken nicht nur Kriminellen, sondern auch Terroristen, Staaten oder Interessensgemeinschaften offen.

Pharming-Attacken gegen Domain Name System (DNS)

Wie das Internet Storm Center (ISC) im April bekannt gab, fanden im März und April mehrere gezielte Pharming-Attacken gegen den Internet-Dienst DNS statt.

Der DNS-Dienst ist zuständig für die Namensauflösung von Domain-Namen: Wer beispielsweise nach www.melani.admin.ch sucht, schickt eine Anfrage an den für die Schweizer Domain (.ch) zuständigen DNS-Server und erhält von diesem die IP-Adresse der URL zurück, so dass die Seite im Browser angezeigt werden kann. Bei einem Pharming-Angriff kompromittiert der Angreifer die Datenbank des DNS-Servers, so dass der DNS-Server – vom anfragenden User unbemerkt – eine falsche IP-Adresse als Antwort auf Anfragen schickt. So ist es möglich, sämtliche Nutzer eines bestimmten DNS-Servers auf eine bestimmte Website zu führen, über die dann meistens schädlicher Code verteilt wird (siehe für genauere Erläuterungen Kapitel 3.2).

Insbesondere in Nord- und Südamerika waren schätzungsweise bis zu 1000 Firmen betroffen. Sämtliche Angestellten wurden so auf Websites geleitet, über die Spyware installiert werden konnte. Auch wenn in den beschriebenen Fällen keine Spionage betrieben wurde, könnte auf diese Weise schädlicher Code in ein Firmennetz eingeschleust werden, mit dem Daten, E-Mail-Verkehr, Passwörter und anderes mehr abgehört, gesammelt und anschliessend an den Angreifer weitergeschickt werden können (siehe dazu weiter unten: Angriff auf Kritische Infrastrukturen in Grossbritannien, und in Kapitel 5.3 CardSystems Datenverlust und Spionageaffäre in Israel).

Fussball-WM Wurm / Versand von rechtsradikaler Propaganda: Sober-Wurm

Anfang Mai verbreitete sich ein neuer Wurm (Sober, in verschiedenen Versionen) dank einer raffinierten Social Engineering Technik rasant im Internet. Nur zwei Wochen nach dem Ende der ersten Bewerbungsrunde für Fussball-WM-Tickets kündigte ein gefälschtes E-Mail an, worauf Millionen gewartet haben – dass man ein WM-Ticket erhalten habe. Wer den Anhang anklickte, wurde infiziert.

Sober sammelte alle auf dem Rechner gespeicherten Mail-Adressen, versandte sich selbst weiter, deaktivierte Antiviren-Produkte und die Windows-Firewall und wurde innert kürzester Zeit zum bisher erfolgreichsten Massmailing-„Wurm" – bis zu 77% des weltweiten Malwareverkehrs wurde kurzfristig von Sober produziert.

Nur wenige Tage später wurde Deutschland von einer Welle von Propaganda-Spam mit rechtsradikalen Sprüchen überflutet: „Ausländer bevorzugt", „massenhafter Steuerbetrug durch ausländische Arbeitnehmer" oder „Deutsche werden künftig beim Arzt abgezockt"

lauteten die Betreffzeilen beispielsweise. Wie sich bald herausstellte, war der WM-Wurm Sober verantwortlich für den Spam-Versand. Mit ihm infizierte Rechner luden aus dem Internet eine neue Sober-Variante (Sober.Q) nach, die zu einem festgelegten Zeitpunkt mit dem Versand der Spam-Nachrichten begann.

Bei Sober.Q handelt es sich um den zweiten grösseren Vorfall von Propaganda-Spam. Bereits im April und Mai 2004 sorgten die Vorgänger, „Sober.G“ und „Sober.H“, für Aufsehen. Just während der Europaratswahlen in der EU verschickten sie rechtsradikale Texte und erreichten eine beträchtliche Verbreitung. Der hier thematisierte Versand der rechtsextremen Nachrichten von Sober.Q ist vor dem Hintergrund der Jubiläumsfeiern zum 60. Jahrestag des Kriegsendes zu sehen. Zudem fanden im Bundesland Nordrhein-Westfahlen kurz nach dem Versand Wahlen statt, in denen die NPD ihre Erfolge von Sachsen bestätigen wollte. Sober.Q verteilte allerdings kein juristisch verwertbares Material (z.B. im Sinne des Anti-Rassismus-Gesetzes): Die Mail enthielt lediglich eine Linksammlung zu URLs im Internet (NPD-Seiten, Spiegel, TAZ, Heise-Online u.a.), die entweder der rechtsextremen Szene zuzuordnen sind oder aber Artikel enthalten, die der Sober-Autor offenbar rechtsextrem interpretiert. Das Motto in der Mail-Nachricht lautete: „Sehe selbst“. Beim Autor dürfte es sich um dieselbe Person handeln, die bereits im letzten Jahr politische Spampropaganda betrieb. In nächster Zeit ist mit einer Zunahme dieser Form der politischen Einflussnahme zu rechnen.

Gezielte Spionageangriffe gegen Kritische Infrastrukturen in Grossbritannien

Wie im Juni 2005 durch das britische NISCC (National Infrastructure Security Coordination Centre) bekannt wurde, erfolgte seit Mitte 2003 eine Serie von gezielten Angriffen gegen Regierungsstellen und Betreiber von Kritischen Infrastrukturen in Grossbritannien.

Die Angreifer hatten dabei in erster Linie Mitarbeiterinnen und Mitarbeiter mit Zugang zu sensiblen Daten im Visier. Angesprochen wurden diese mit raffinierten Methoden des Social Engineering: Die Betreffzeile der E-Mail, mit der Trojanische Pferde eingeschleust wurden, enthielt oft Informationen, die für den Mitarbeiter von Interesse waren und bereits im Vorfeld aus seinem engsten Umfeld vom Angreifer recherchiert wurden. Das Mail selbst enthielt Links auf unscheinbare News-Webseiten oder Attachments, die nach News-Berichten aussahen.

Die zum Einsatz gekommenen Trojanischen Pferde waren z.B. in der Lage, Passwörter zu sammeln, Screenshots anzufertigen, das Netzwerk zu scannen, die vollständige Kontrolle über das kompromittierte System zu übernehmen oder Dokumente ins Internet zu verschicken. Ziel der Angriffe war es, vertrauliche Informationen mit strategischem oder kommerziellem Wert zu sammeln.

Bemerkenswert ist insbesondere, dass die eingesetzten Trojanischen Pferde sonst nirgends auftauchten und daher keiner Antiviren-Software-Firma bekannt waren. So konnten die Schädlinge über Monate hinweg unbemerkt agieren. Dennoch, so hiess es von offizieller Seite, sei keine vertrauliche Information gestohlen worden.

Die Herkunft der Angriffe ist unklar, auch wenn sie ihren Ursprung im Fernen Osten haben dürfte, wie NISCC bekannt gab. Die raffinierte und gezielte Vorgehensweise legt einen grösseren, finanzkräftigen Akteur nahe.

Im ersten Halbjahr 2005 konnten vermehrt gezielte Angriffe mit massgeschneiderten Spionageprogrammen beobachtet werden (siehe z.B. „Industriespionage in Israel“ oder „Diebstahl von Millionen von Kreditkartendaten“ im nächsten Kapitel sowie die allgemeinen Ausführungen in Kapitel 2.4). MELANI geht davon aus, dass dieser Trend in nächster Zeit zunehmen wird.

5.3 Kriminalität

DDoS- und Spam-Attacken gegen Bezahlung

Wie in den Kapiteln 2 und 3.2 mehrfach angedeutet, verfolgen die Besitzer von Bot-Netzen und Entwickler von Malware inzwischen in erster Linie kommerzielle Ziele. In Grossbritannien beispielsweise wurde im 4. Quartal 2004 der Fall des so genannten „Randex" Bot-Nets bekannt, das von vier noch Minderjährigen betrieben wurde (teils kanadischer, teils britischer Staatsangehörigkeit). Die Gruppe infizierte mit ihrem Computervirus „Randex" tausende von Rechnern und installierte auf diesen ein Programm, welches über einen IRC-Channel Kontakt zu seinem Master aufnahm. Das Programm konnte nach CD-Keys von Spielen suchen, DDoS-Attacken gegen bestimmte Server starten oder unbemerkt beliebig weitere schädliche Software nachladen. Beispielsweise wurde ein SOCKS-Proxyserver auf die infizierten Maschinen nachgeladen, der den Einsatz des infizierten Systems zur Weiterleitung von Spam-Mails ermöglichte. Wie das amerikanische FBI ermitteln konnte, vermietete die Randex-Gruppe ihr Bot-Netz auch kommerziell. Offenbar bezahlte der CEO einer amerikanischen Firma, spezialisiert auf den Verkauf von Satelliten-Empfängern, der Gruppe Geld für einen DDoS-Angriff auf die Webseiten seiner Konkurrenz (z.B. rapidsatellite.com, weakness.com). Des Weiteren wurde bekannt, dass die Randex-Gruppe offenbar Hilfe des 21-jährigen Axel G. aus Deutschland erhielt – seines Zeichens der Entwickler von „Agobot" und „Phatbot". Die Gruppe Randex setzte offenbar eines seiner Tools für die Durchführung ihrer http-Flood-Attacke ein.

Wie in Kapitel 2.1 ausgeführt, fand im Jahr 2004 eine Verschiebung der Motive der Angreifer weg von intellektueller Neugier hin zu Bereicherung statt. Das hier beschriebene Beispiel illustriert gut, wie mit DDoS- und Spam-Angriffen Geld verdient werden kann.

Doch nicht nur mit DDoS- und Spam-Aktivitäten lässt sich als Hacker Geld verdienen. Auf einschlägigen Seiten oder Foren ist beispielsweise Exploit-Code für eine bekannte Sicherheitslücke für $100 – $500 zu kaufen, für eine bisher unbekannte Lücke steigt der Preis auf $1000 – $5000. Listen mit IP-Adressen infizierter Systeme, die beispielsweise für den Versand von Spam missbraucht werden können, sind bereits für $150 - $550 zu haben. Die Daten von etwa 1000 noch gültigen Kreditkarten können für einen Preis zwischen $500 und $5500 bezogen werden. Ein professioneller Hacker mit Erfahrung, der seine Dienste beispielsweise an Spammer oder zu Phishing-Zwecken verkauft, kommt durchaus auf ein Jahresgehalt von gegen $200'000.

Ebenfalls bekannt geworden sind Vorfälle von Erpressung: Ein kurzer DDoS-Angriff, der die Infrastruktur des Opfers noch nicht vollständig zum Erliegen bringt, wird gefahren, um sich anschliessend mit finanziellen Forderungen an das Unternehmen zu wenden. Andernfalls würde ein grösserer, verheerender Angriff stattfinden. Die Dunkelziffer solcher Vorfälle dürfte beträchtlich sein, zumal ein betroffenes Unternehmen aus Image-Gründen damit kaum an die Öffentlichkeit oder die Behörden gelangt.

ChoicePoint Kundendaten kompromittiert: Identitätsdiebstähle drohen

Wie im Februar 2005 bekannt wurde, hatten Kriminelle mehr als ein Jahr lang ungehinderten Zugriff auf persönliche Daten von mindestens 35'000 Personen. Die betroffene Firma, ChoicePoint Inc. (Georgia, USA), ist der grösste US-Spezialist für die Überprüfung von Stellenbewerbern. ChoicePoint stellt seine Informationen sowohl der Regierung, als auch privaten Unternehmen (z.B. Versicherungsunternehmen) oder Hausbesitzern zwecks Risikoeinschätzung eines neuen Kunden oder baldigen Mieters zur Verfügung. ChoicePoint

verfügt nach eigenen Angaben über den Zugriff auf mehr als 17 Milliarden amtliche Datensätze.

Verschiedene Experten gehen aber von einer Kompromittierung von den persönlichen Daten (Social Security Number, Kreditkarten- und Konto-Daten etc.) von mehr als 100'000 Personen aus. Die Daten könnten von Betrügern beispielsweise für Identitätsdiebstahl verwendet werden. Der Polizei von Los Angeles und dem FBI, welche gemeinsam die Ermittlungen führen, ist mindestens ein Fall von Identitätsdiebstahl mit einer bei ChoicePoint erschlichenen Identität bekannt. Es sieht aber danach aus, als seien bereits mehr als 750 der erschlichenen Datensätze betrügerisch eingesetzt worden.

Die Betrüger erhielten Zugriff auf die Daten, indem sie sich als legitime Firma ausgaben, die Zugriff auf die Informationen wünschte. Auf diese Weise ergatterten sie sich etwa 50 Standard Kunden-Accounts, mit denen sie normalen Zugriff auf die Daten erhielten – mit anderen Worten: Es fand kein Eindringen in das System statt. Die illegitimen Firmen wurden von den Betrügern mit vorgetäuschten Identitäten gegründet. Aufgeflogen ist der Fall bereits im Oktober 2004, als ein gefaxter Antrag einer illegitimen Firma für einen Account bei ChoicePoint Misstrauen erweckte.

Bemerkenswert ist der Umstand, dass ChoicePoint von der Entdeckung bis zur Meldung des Vorfalls über vier Monate verstreichen liess – ob der Vorfall überhaupt bekannt geworden wäre ohne ein kalifornisches Gesetz, das die Verwalter solcher Daten bei einem Vorfall zu einer Meldung zwingt, ist höchst fraglich. Allgemein ist beim Verlust solch heikler Daten mit einer grossen Dunkelziffer zu rechnen. Zu betonen ist an dieser Stelle auch, dass neben ChoicePoint verschiedene andere amerikanische Data-Warehousing-Unternehmen Datendiebstähle zu verzeichnen hatten (wie z.B. LexisNexis), die aber an dieser Stelle nicht alle näher erläutert werden können.

Industriespionage: Diebstahl von Millionen von Kreditkartendaten mit Trojanischem Pferd

Dem US-Unternehmen CardSystems Solutions wurden im Mai mehrere Millionen Kreditkarten-Datensätze entwendet. Die betroffenen Kunden müssen damit rechnen, dass auf ihre Rechnung Waren oder Dienstleistungen bezogen werden. Auch mehrere Hundert Schweizer Kreditkartenbesitzer sind vom Zwischenfall betroffen. Das Ausmass des Schadens ist nach wie vor unklar.

CardSystems wickelt jährlich Transaktionen von mehr als 25 Milliarden US-Dollar zwischen Einzelhandel, Kunden und Kreditkartenunternehmen ab. Die Betrüger entwendeten Datensätze von MasterCard und Visa, vermutlich auch von American Express und Discover. Mindestens 200'000 der entwendeten Datensätze sind komplett, so dass mit ihnen Online-Transaktionen getätigt werden könnten.

Der Fehler für diesen bisher grössten ID-Theft-Zwischenfall (siehe Kapitel 2.3) ist bei CardSystems selbst zu suchen: Mitarbeiter hatten regelwidrig Transaktionsdaten lokal im Firmennetz zwischengespeichert. Diese Daten konnten mittels eines Spionageprogramms (Trojanisches Pferd) ausgelesen und an die Angreifer weitergeleitet werden. Das Spionageprogramm war zuvor über eine Sicherheitslücke im Computersystem von CardSystems gezielt eingeschleust worden.

Wie auch im Industriespionagefall in Israel (siehe nächsten Punkt) sowie im Fall der gezielten Spionageaktivitäten gegen Grossbritannien (siehe Kapitel 5.2) wurde auch im hier beschriebenen Fall ein Spionageprogramm gezielt und ausschliesslich beim Opfer eingesetzt. Aus Sicht von MELANI ist dieses Vorgehen beunruhigend: Durch den gezielten und begrenzten Einsatz des Schädlings bleibt dieser sämtlichen Antivirenprogrammen unbekannt, so

dass dem Angreifer genügend Zeit für eine langfristige, weitgehende Spionagetätigkeit gegen das betroffene Unternehmen bleibt (siehe Kapitel 2.4).

Industriespionage in Israel

Ende Mai wurde in Israel ein bedeutender Fall von Industriespionage aufgedeckt. Mit einem gezielt entwickelten und eingesetzten Trojanischen Pferd wurden mehrere grössere Unternehmen monatelang von Konkurrenten ausspioniert. Zu den Auftraggebern gehörten beispielsweise Mobilfunkprovider, Satelliten-TV-Anbieter und Auto-Importeure.

18 Personen wurden in Israel und Grossbritannien in diesem Zusammenhang festgenommen, darunter auch der Entwickler des Spionageprogramms und dessen Auftraggeber. Diese hatten über israelische Privatdetekteien den Computerspezialisten M. Haephrati angeheuert, der das schadhafte Programm schrieb und auch in Umlauf brachte. Gegen eine monatliche „Gebühr“ von 1'500 britischen Pfund verschickte Haephrati eine verseuchte CD-ROM an ausgewählte Firmen. Das Trojanische Pferd wurde dabei jeweils den Bedürfnissen der Auftraggeber angepasst.

Aufgeflogen ist der Fall, weil Haephrati das Programm auch für einen persönlichen Rachefeldzug gegen den Stiefvater seiner Ex-Frau einsetzte. Man geht davon aus, dass das Spionageprogramm teilweise über zwei Jahre im Einsatz war.

Die involvierten Detekteien genossen einen tadellosen Ruf und waren vom israelischen Justizministerium lizenziert. Auch in der Schweiz war ein Unternehmen betroffen – dieses wurde aber nur aus persönlichen Gründen involviert, ohne dass systematische Industriespionage betrieben worden wäre.

Auch im vorliegenden Fall wurde nicht auf eine rasante, sondern vielmehr auf eine gezielte, langsame und unauffällige Verbreitung unterhalb des Radars der Antiviren-Software-Hersteller gesetzt, was das Auffinden des Trojanischen Pferdes fast unmöglich machte. Das Spionageprogramm erlaubte es dem Angreifer, die volle Kontrolle über das kompromittierte System zu übernehmen und so auf Dateien, Mail-Verkehr und andere vertrauliche Firmendaten zuzugreifen.

MELANI geht – wie bereits in Kapitel 2.4 ausgeführt – davon aus, dass diese Form der Wirtschafsspionage erst im Anfangsstadium steht und daher künftig vermehrt mit solchen Vorfällen zu rechnen ist.

5.4 Terrorismus

Cyber-Terrorismus Debatte in den USA

Eine Rede des ehemaligen CIA-Direktors Robert Gates an einer Terrorismuskonferenz Anfang Dezember 2004 lancierte in den USA eine Debatte zum Thema Cyber-Terrorismus. Gates bezeichnete in seiner Rede Cyber-Terrorismus als möglicherweise verheerendste Massenvernichtungswaffe bisher, die die amerikanische Wirtschaft verkrüppeln könnte (Wortwahl stammt von Gates!): „When a teenage hacker in the Philippines overnight can wreak $10 billion in damage to the U.S. economy by implanting a virus, imagine what a sophisticated, well-funded effort to attack the computer base of our economy could accomplish.“

Die CIA und die National Security Agency (NSA) hätten bereits vor sechs Jahren anlässlich einer Übung mit 50 Computerspezialisten herausgefunden, dass bloss wenige Tage

Vorbereitungszeit nötig seien, um beispielsweise die nationale Energieversorgung anzugreifen. Gates verwies als Beispiel auf den Stromausfall im Nord-Osten der USA aus dem Jahr 2003: „What I am talking about is bringing the U.S. economy to its knees."

Angesichts des Kampfes gegen den Terrorismus, der gemäss Gates ebenso langfristig zu werden drohe wie die Konfrontation mit dem Kommunismus, sei früher oder später mit einem verheerenden Angriff zu rechnen. Eine Umfrage des „Pew Internet & American Life Project" unter 1286 Computer-Sicherheits-Experten in den USA bestätigte diese Ansicht bloss wenige Wochen später: 66% meinten, dass in den nächsten zehn Jahren mit mindestens einem verheerenden Angriff auf die vernetzte Informationsinfrastruktur oder das Stromnetz der USA zu rechnen sei. Nur 18% halten ein solches Szenario für unrealistisch.

In einer Stellungnahme vor dem Senat beschäftigten sich die Direktoren der CIA sowie des FBI mit demselben Thema. Auch sie schätzen die Bedrohung als real ein und konstatieren eine andauernde Zunahme von Akteuren mit den Fähigkeiten und den nötigen Absichten für den Einsatz von Computern für illegale Aktionen. Die Gefahr droht ihrer Meinung nach einerseits von fremden Staaten, die mit grossen Ressourcen Technologien für einen Angriff auf die Informationssysteme der USA vorbereiten könnten, andererseits von nicht-staatlichen Akteuren wie Terroristengruppen und Hackern. Staatliche Akteure seien dabei gefährlicher, da sie die technischen und finanziellen Mittel für einen Angriff auf die US-Wirtschaft oder die Nationale Sicherheit der USA hätten. Terroristen seien zwar noch nicht soweit, hätten aber die Bedeutung der Informationssysteme für den US-Wirtschaftsalltag und die Nationale Sicherheit erkannt und seien dabei, Mathematik-, Informatik- oder Ingenieur-Studenten anzuwerben.

Hauptgrund für die Zunahme der Befürchtungen in den USA ist die zunehmende Ausrichtung der Hacker auf finanziellen Gewinn: Wenn dieser Pool von Spezialisten erst einmal von Terroristen, Regierungen oder kriminellen Organisation angeheuert werde, nehme das Potenzial für einen erfolgreichen Cyber-Angriff auf kritische Infrastrukturen massiv zu.

Auch wenn die Aussagen der erwähnten Experten richtig sind, müssen sie dennoch relativiert werden. In der Tat ist eine zunehmende Einflussnahme auf die Wirtschaft durch Hackerangriffe anzunehmen – viele Experten sind aber der festen Überzeugung, dass damit keine Menschenleben direkt gefährdet würden und daher kein direkter Vergleich zu herkömmlichen, physischen Terrorangriffen gezogen werden könne.

Sicherheitsexperten für kritische Infrastrukturen betonen ausserdem, dass ein erfolgreicher Cyber-Angriff auf solche Systeme ohne detailliertes Insiderwissen unrealistisch sei. Auch wenn es zwar möglich sei, in Computersysteme beispielsweise der Wasserversorgung einzudringen, sei es fast unmöglich, dramatische Effekte auf die Steuerung zu erzielen. Sollte dies doch gelingen, könnte zudem die automatische Steuerung rasch deaktiviert und die Versorgung manuell sichergestellt werden. Daher ist davon auszugehen, dass ein physischer Angriff auf absehbare Zeit hinaus viel grösseren Erfolg verspricht.

Wahrscheinlicher wäre eine Kombination eines physischen mit einem Cyber-Angriff: Wird beispielsweise nach einem physischen Angriff im Stil des 11.9.2001 mit cyberterroristischen Mitteln die Organisation der Rettungseinheiten, die Kommunikation der Regierung oder die Versorgung der Bevölkerung mit Informationen beeinträchtigt, kann das Ausmass des physischen Angriffs massiv ausgeweitet werden.

Es ist zwar mit einer Zunahme von aus E-Mail herrührenden oder über Netzwerke direkt verteilten Schädlingen, von Identitätsdiebstählen, DDoS-Attacken und Daten-Manipulation zu rechnen – erfolgsversprechende Angriffe auf kritische Infrastrukturen sind aber auf Grund des mangelnden Insider-Wissens der Angreifer in den nächsten Jahren (noch) nicht zu erwarten. Wie sich die Lage weiter entwickelt, ist jedoch noch offen – schliesslich werden

immer mehr Staaten von Informationsinfrastruktur abhängig, die nicht unbedingt die gleichen Sicherheitsvorkehrungen implementieren können wie europäische Staaten oder die USA.

Um Volkswirtschaften aber vor den zunehmenden digitalen Bedrohungen schützen zu können, wird in den nächsten Jahren ein Ausbau von nationalen Notfall-Teams nötig sein – eine Einschätzung, die von vielen Sicherheitsexperten weltweit geteilt wird. Allein im Oktober 2004 entstand weltweit etwa $15 Milliarden Schaden durch offene oder versteckte digitale Angriffe. Insbesondere kleinere und mittlere Unternehmen werden sich künftig kaum eigenständig gegen grössere Angriffe verteidigen können, weshalb eine nationale Anlaufstelle für solche Probleme immer nötiger wird.

Die Schweiz befindet sich nach der Etablierung von MELANI und SONIA[5] auf einem guten Weg dahin – schliesslich bietet MELANI nicht nur für die Betreiber kritischer Infrastrukturen, sondern auch für die Öffentlichkeit und KMUs eine Anlaufstelle im Problemfall.

Momentan beschränkt sich der Einsatz digitaler Mittel in terroristischen Kreisen ausschliesslich auf Propaganda, Rekrutierung und die Beschaffung finanzieller Mittel. Auf dem Laptop des Verantwortlichen für die Terroranschläge in Bali im Jahr 2002 wurden beispielsweise Beweise gefunden, dass er seine Aktivitäten mit Cyber-Betrug finanzieren wollte. In den nächsten Jahren ist es aber durchaus möglich, dass sich auch terroristische Angriffe vermehrt auf digitale Weise ereignen.

USA: IT-Sicherheitsmängel bei den Bundesbehörden

Wie die New York Times Anfang Juni 2005 berichtete, stellte der Inspector General des US-amerikanischen Department of Homeland Security (DHS) in einem Bericht fest, dass die Computersysteme des Departements oft gravierende Sicherheitsmängel aufweisen. So hätten beispielsweise die Transportation Security Administration, die Customs and Border Protection und die Küstenwache nicht einmal Backup-Systeme installiert.

Selbst die Federal Emergency Management Agency weise grosse Nachlässigkeiten auf und sei auf einen Notfall nicht vorbereitet. Offenbar sind 80 Prozent der IT-Systeme des DHS im Notfall nicht in der Lage, wichtige Daten zur Verfügung stellen zu können. Besonders fatal, monierte der Bericht, könne sich dies beispielsweise auf die Überwachung von Flugpassagieren auswirken.

Nur wenige Tage später liess zudem das Government Accountability Office (GAO) in einem Bericht verlauten, die US-amerikanischen Bundesbehörden seien generell nicht ausreichend gegen Internet-Gefahren wie Spam, Spyware und Phishing gewappnet. Die im Federal Information Security Management Act of 2002 (FISMA) definierten Vorschläge und Vorschriften würden zumeist nicht angewendet.

Zudem melden offenbar selbst US-Behörden keine die Cyber-Sicherheit betreffende Vorfälle, obwohl sie dazu verpflichtet wären und obwohl gleichzeitig Werbung für eine diesbezügliche Meldebereitschaft der Privatwirtschaft betrieben wird. Der Bericht betont, dass die Bundesbehörden ohne wirksame Koordination nicht in der Lage seien, Cyber-Attacken zu identifizieren und zu bekämpfen.

---

[5] SONIA: Der Schweizer „Sonderstab Information Assurance“. MELANI fungiert als ständiges Lagezentrum für SONIA und alarmiert diesen im Notfall. Der „Sonderstab Information Assurance“ soll bei schwerwiegenden Störungen den Bundesrat beraten und diesen bei seinen Entscheidungen unterstützen. Geleitet wird SONIA vom Informatikstrategieorgan Bund (ISB). Die WL (Bundesamt für Wirtschaftliche Landesversorgung) ist in diesem Sonderstab durch Fachleute aus dem Milizkader vertreten. Siehe: http://www.bwl.admin.ch/deutsch/themen-infra-ict-assurance.asp (Stand: 8.6.05) sowie http://www.isb.admin.ch/intranet/sicherheit/00791/index.html?lang=de (Stand: dito).

USA: Department of Homeland Security (DHS) vernachlässigt Cyber-Security-Pflichten

Das Government Accountability Office (GAO) hat dem DHS im Mai schwerwiegende Mängel beim Aufbau von Schutzmechanismen gegen Cyber-Terror-Attacken vorgeworfen. Seit Anfang 2003 werden die IT-Sicherheitskompetenzen des FBI, des Verteidigungs-, des Handels- und des Energieministeriums der USA im DHS konzentriert.

Unter anderem sei versäumt worden, einen Notfallplan zur Wiederherstellung von Internet-Infrastrukturen nach einem Cyber-Angriff zu entwickeln. Auch sei kein Worst-Case-Szenario entworfen worden, das eine Identifizierung möglicher Schwachstellen im nationalen IT-Sicherheitskonzept der USA erlaubt hätte. Obwohl die Gefahr von Angriffen aus dem Internet (Terroristen, ausländische Geheimdienste, Kriminelle, Spammer, Spyware-Autoren, Botnet-Betreiber) immer weiter zunehme, habe das DHS keine seiner dreizehn Cybersecurity-Verantwortlichkeiten ausreichend erfüllt.

USA: Direktor des Secret Service fordert zu Kooperation für Cyber-Security auf

Ralph Basham, der Direktor des US-amerikanischen Secret Service, rief an einer Konferenz Mitte Mai Unternehmen dazu auf, vermehrt Zwischenfälle aus dem Bereich der IT-Sicherheit an die Behörden zu melden. Ohne die Hilfe aus der Privatwirtschaft sei der Kampf gegen Bedrohungen der Cyber-Security nicht zu gewinnen.

Als Grund gab er an, dass immer weniger Vorfälle bloss eine Firma beträfen: „An intrusion for one represents a collective threat for us all." Der Informationsaustausch zwischen Strafverfolgungsbehörden und der Privatwirtschaft müsse daher massiv verbessert werden.

Im Rahmen der Melde- und Analysestelle Informationssicherung Schweiz (MELANI) wird innerhalb des so genannten „Geschlossenen Kundenkreises" ein solcher Informationsaustausch zwischen Betreibern Kritischer Infrastrukturen und den Behörden unter geregelten Bedingungen betrieben und laufend ausgebaut.

6 Prävention

6.1 Software

Ausweitung des Heim PC-Schutzes auf Spam, Phishing

Bis anhin beschränkte sich der Schutz eines Heimcomputers normalerweise auf einen Virenscanner und eine Firewall. Das wird sich in naher Zukunft ändern. Wie es heute für jedermann selbstverständlich sein sollte, ein Antiviren-Programm installiert zu haben, wird in naher Zukunft auch ein Schutz vor Phishing und Spam unverzichtbar sein. Der Trend geht dabei zu Komplettlösungen, so genannten Security Packs. Trendmicro hat mit PCillin eine solche Komplettlösung vorgestellt. Diese beinhaltet neben Viren- und Spamschutz auch einen Schutz vor Phishing-Attacken. Dabei greift das Tool aber noch nicht auf eine zentrale Datenbank mit gespeicherten Phishing-Seiten zurück, sondern es wird nach der Eingabe eines Teils der Kreditkartennummer gescannt, der dem Programm bei der Installation angegeben werden muss.

Auch im Bereich der Programme, die „nur" gegen Phishing agieren, hat sich einiges getan. Gegen einfaches URL-Spoofing kann ein so genannter „Spoofstick" installiert, werden der jeweils die Adresse, auf der man wirklich ist, angibt und somit ein Adressen-Spoofing

vereiteln kann. Von Netcraft gibt es ein technisch ausgeklügelteres Programm. Hierbei wird für jede aufgerufene Seite in einer Datenbank nachgeschaut, wo die Seite gehostet wird, wie lange sie bereits aufgeschaltet ist und ob sie als dubiose Phishing-Seite gemeldet wurde. Damit können die Benutzer die Echtheit einer Seite in etwa abschätzen. Auch können mit diesem Tool Phishing-Seiten direkt gemeldet werden. Eine Initiative, die in die gleiche Richtung zielt, kommt vom US-amerikanischen Sicherheitsspezialisten Wholesecurity, der ein Meldesystem namens „Phishing Report Network“ für betrügerische Websites initiieren will. Erste Unternehmen, die sich beteiligen wollen, sind Microsoft, eBay, PayPal und Visa. Die Datenbank soll möglichst viele Phishing-Attacken registrieren und diese Meldungen in einer zentralen Datenbank speichern, auf die andere Firmen Zugriff bekommen, damit sie den Zugang zu den betrügerischen Seiten sperren können.

Es ist zudem anzunehmen, dass Microsoft einen grossen Teil des Schutzes in die nächste Version seines Betriebssystems integrieren wird oder im Vorfeld diese Programme schon zum Download anbieten wird. So verteilt Microsoft neuerdings zum Beispiel via Auto-Update an jedem „Patch Tuesday“ (jedem zweiten Dienstag im Monat) ein Viren-Erkennungs- und Entfernungs-Tool, das jeweils 30 aktuelle Viren erkennen und entfernen können soll. Ausserdem hat Microsoft mit der Betaversion ihres AntiSpyware Programms (MS AntiSpyware Beta) einen ersten Schritt in diese Richtung getan. Dieses wird voraussichtlich in einer Basisversion nach der vollständigen Fertigstellung gratis vertrieben werden. Auch Mozilla arbeitet an einer Thunderbird-Version, die bei Phishing-Mails Alarm schlägt. Dies deutet darauf hin, dass Computer zukünftig schon beim Kauf einen guten Grundschutz aufweisen werden. Fehlmanipulationen durch Benutzer können so vermindert, jedoch nicht vollständig verhindert werden.

Systeme zur sicheren Überprüfung des E-Mail Absenders

Etwa drei Viertel aller versendeten E-Mails sind mittlerweile entweder Spam (unerwünschte Werbung), Malware oder beides. Die zuverlässige Identifizierung solcher Mails ist nach wie vor nicht einfach. Spam lohnt sich, da bis zu 60% der e-Mailuser auf solche Nachrichten reagieren.

Malware wird relativ zuverlässig von Virenscannern entdeckt. Wichtig ist hier vor allem die Zeit zwischen der ersten Sichtung einer Malware und ihrer Erkennung durch Virenschutzprogramme. Die Unterschiede zwischen den verschiedenen Herstellern sind signifikant. Zudem zeigt es sich, dass im kommerziellen Umfeld ein einzelnes Produkt nicht zuverlässig genug arbeitet. MELANI empfiehlt daher die Benutzung von zwei oder mehr Produkten in Serie.

Das Erkennen von Spam ist bedeutend schwieriger. Um eine zuverlässige Erkennung zu gewährleisten, muss auf eine grosse Anzahl verschiedener Tests zurückgegriffen werden. Einerseits wird der Mailtext auf Phrasen und Eigenschaften, welche für Spam typisch sind, resp. häufiger vorkommen, getestet. Andererseits wird versucht, die Herkunft der Mails zu ermitteln. Dazu gibt es verschieden Vorschläge, wie z.B. das Sender Policy Framework (SPF) oder das von Microsoft entwickelte Sender ID System. Eine geplante gemeinsame Entwicklung dieser Systeme kam leider nicht zustande. Zudem ist das korrekte Implementieren dieser Systeme schwierig. Zur Zeit ist nicht klar, welche Zukunft diese Technologien haben. Einige populäre Spamfilter setzen diese Technologie bereits ein.

Schliesslich gibt es Dienste, welche die Auftretenshäufigkeit einer Mail zu ermitteln probieren. Je öfter dieselbe oder eine ähnliche Mail gesehen wird, desto wahrscheinlicher handelt es sich um eine Spam-Mail. Solche Systeme sind zum Beispiel das Distributed

Checksum Clearinghouse (DCC), Spamcop, Spamhouse, Razor und Andere mehr. Da sich diese Systeme schnell an neue Gegebenheiten anpassen, sind sie relativ erfolgreich.

Die meisten Spam/Malware-Mails werden heutzutage über Bot-Netze versandt. Die Bekämpfung von Bot-Netzen ist daher einer der wichtigsten Massnahme zur Spam-Bekämpfung, da auf diese Weise das Übel bei der Wurzel gepackt werden kann. Spamfilter dagegen bekämpfen nur die Symptome.

6.2 Diverses

Anforderungen an Online Banking Seiten

Das deutsche Fraunhofer-Institut SIT (Sichere Informations-Technologie) testete letztes Jahr 12 deutsche Online Banken. Obschon das Ergebnis nicht direkt auf die Schweiz übertragbar ist, ist es dennoch interessant, die Bewertungskriterien kurz aufzulisten. Unter anderem wurden folgende Kriterien in der Bewertung einbezogen:

Eine konsistente Adressierung über das gesamte Web-Angebot hinweg erleichtert die Bildung einfacher, handhabbarer Regeln. Das Online-Banking-Angebot soll unter derselben 2nd-Level-Domain geführt werden wie die öffentliche Website der Bank.

Damit der Nutzer die Adresse prüfen kann, muss sie sichtbar sein. Die URL muss während der ganzen Online Sitzung sichtbar sein. Es dürfen sich keine Fenster öffnen, schon gar nicht ohne URL- und Menüzeile.

Alle Banken setzen für ihre Online-Banking-Angebote das SSL-Protokoll ein. Die dabei übermittelten Sicherheitszertifikate sind die zuverlässigste Form der Echtheitsprüfung. Die Zertifizierungsstelle bescheinigt den Zusammenhang zwischen der besuchten Adresse und der Betreiberorganisation. Das Sicherheitszertifikat muss gültig und auf den Namen der Bank ausgestellt sein.

Damit der Nutzer das Zertifikat rechtzeitig prüfen kann, bevor er Daten eingibt, muss bereits die Login-Seite über eine gesicherte Verbindung geladen werden.

Die Kunden müssen über das Problem Phishing und die Schutzmöglichkeiten informiert werden.

Die Bank sollte auf der Webseite konkrete Parameter angeben, an denen Kunden die Echtheit der Website prüfen können: die URL der Banking-Website und Parameter des Sicherheitszertifikats.

Im Verdachtsfall sollten Kunden zunächst bei ihrer Bank nachfragen, ob eine Aufforderung zur Dateneingabe legitim ist. Dazu sollte jede Bank Kontaktinformationen (z.B. Telefonnummern und E-Mail-Adresse) angeben.

Banken weisen im Zusammenhang mit Phishing immer wieder darauf hin, dass sie keine Aufforderungen zur Eingabe sensibler Daten per E-Mail versenden. Für den Kunden am transparentesten wäre jedoch, wenn der E-Mail-Verkehr – zumindest auf Wunsch – gänzlich unterlassen würde. Kunden sollten daher nicht zur Angabe der E-Mail-Adresse gezwungen werden.

In der Schweiz ist die Sensibilität bezüglich elektronischen Bankgeschäften sehr gross. Dementsprechend verhält es sich auch mit der Qualität der E-Banking-Angebote.

In diesem Zusammenhang ist interessant, dass die Banken ihrerseits für die Kreditvergabe in Erwägung ziehen, die IT-Sicherheit einer Firma als Bewertungskriterium mit zu

berücksichtigen. Laut einem Bericht des Computermagazins iX[6] werden unter der Eigenkapitalvereinbarung „Basel II“ Regeln zur Minimierung des Risikos bei der Kreditvergabe bis 2007 EU-weit verbindlich. Je mehr der Geschäftsbetrieb auf die technische Infrastruktur angewiesen ist, je mehr hängt letztlich auch die Kreditentscheidung von einem aktiven IT-Risiko Management ab. Wer bei der IT spart, verschlechtert sein Rating und muss höhere Zinssätze in Kauf nehmen. Im schlimmsten Fall kann ein Kredit sogar abgelehnt werden.

Um eine gute Bewertung der IT-Sicherheit bei Kreditevaluationen zu erzielen, sollten Systemverantwortliche sowohl geeignete Früherkennungs- als auch Abwehrmassnahmen definieren und ein Notfallprogramm für das Worst-Case-Szenario eines Systemausfalls ausgearbeitet haben (Incident Response). Auch Schulungen und eine schriftlich fixierte Sicherheitspolicy gehören dazu. Vor allen Dingen sind aber die Systeme auf dem neuesten Stand zu halten. Das Problem ist allerdings, dass die IT-Vorschriften des Basler Komitees relativ unkonkret sind.

7 Aktivitäten / Informationen

7.1 Staatlich

Schweiz: Bundesrat will Kampf gegen Internetkriminalität verstärken

Der Bundesrat hat Mitte Dezember 2004 zwei Gesetzesentwürfe in die Vernehmlassung geschickt, die die Rechtslage von Content Providern, Service Providern und Access Providern klären sollen. Die Gesetze sollen festlegen, unter welchen Voraussetzungen Provider belangt werden können und zudem in einer ersten Ermittlungsphase die Bundeskompetenzen stärken.

Der erste Entwurf sieht vor, dass Content Provider (die Inhalte anbieten) wie bisher voll verantwortlich für von ihnen ausgehende illegale Inhalte bleiben, während sich der Hosting Provider (Anbieter von Speicherplatz) nur dann als Mittäter, Anstifter oder Gehilfe strafbar macht, wenn er vorsätzlich illegale Informationen auf seine Rechner aufschalten lässt. Erfährt er jedoch im Nachhinein von solchen Inhalten, macht er sich neu dann strafbar, wenn er entweder die Nutzung nicht verhindert oder aber keine Hinweise an die Strafverfolgungsbehörden weiterleitet (bisher konnten die illegalen Inhalte ungemeldet belassen werden). Die gleiche Regelung soll für Anbieter von Internet-Suchmaschinen gelten. Access Provider (Zugangsvermittler zum Internet) sollen hingegen nicht zur Rechenschaft gezogen werden können, da sich ihre Dienstleistung allein auf technische und automatisierte Vorgänge (die Einwahl ins Internet) begrenzt.

Der zweite Gesetzesentwurf regelt die Ermittlungskompetenzen bei Internetkriminalität neu. In einer ersten Phase der Ermittlungen sollen dem Bund mehr Kompetenzen zukommen. Bundesanwaltschaft und Bundeskriminalpolizei sollen in Fällen, die Internetkriminalität betreffen und bei denen der Ursprungskanton noch unbekannt ist, erste und dringende Ermittlungen durchführen, ohne dass dadurch eine Bundesgerichtsbarkeit begründet werden soll.

Die beiden Gesetzesentwürfe aus dem EJPD beruhen auf den Erkenntnissen aus der Operation „Genesis“ gegen Pädophilie im Internet und auf einem Bericht der Expertenkom-

[6] Siehe: iX Ausgabe 12/04.

mission „Netzwerkkriminalität“ und lehnen sich an die entsprechenden Regelungen der EU an.

Das Vernehmlassungsverfahren läuft noch bis Herbst 2005. Es ist allerdings mit teilweise ablehnenden Reaktionen seitens betroffener Interessengruppen zu rechnen. Eine ausführliche Analyse der Vernehmlassungsresultate folgt im zweiten Halbjahresbericht 2005, der etwa im Januar / Februar 2006 erwartet werden kann.

EU: Fortschritte bei der Anti-Spam-Politik

Die EU ist dabei, von ihren Mitgliedstaaten ein neues Dokument unterzeichnen zu lassen, das den grenzübergreifenden Austausch von Spam-Beschwerden innerhalb der EU regeln soll. Das Protokoll trägt den umfangreichen Titel „Vorgehen zur Kooperation bei der Übermittlung von Beschwerden und Erkenntnissen hinsichtlich der Durchsetzung des Artikels 13 der Richtlinie über den Datenschutz in elektronischen Kommunikationsnetzen 2002/58/EC und anderer nationaler Gesetze gegen unerwünschte elektronische Kommunikation“. Es wurde bisher aber erst von Italien, den Niederlanden, Österreich, Litauen, Tschechien, Belgien, Dänemark, Frankreich, Griechenland, Malta, Spanien, Zypern und Irland unterschrieben.

Ziel der Regelung soll eine bessere Zusammenarbeit innerhalb der EU zwischen Behörden sein, die in der Spam-Bekämpfung tätig sind. So soll jedes EU-Mitglied im Ursprungsland (einem anderen EU-Mitglied) eine Beschwerde absetzen können, die vom Ursprungsland verfolgt werden muss, als wäre die Beschwerde nationaler Herkunft. Das meldende Land muss dabei auf dem Laufenden gehalten werden.

Noch ist unklar, wie viel von der neuen EU-Regelung erwartet werden kann. Kritiker bemängeln, es gebe noch nicht einmal in allen Mitgliedsstaaten entsprechende Stellen, die sich mit der Spam-Problematik befassten. Noch immer sei daher viel mehr Koordination nötig, als vom neuen Papier vorgesehen. Bisher ist das Papier ausserdem noch nicht einmal offiziell empfohlen worden. Die Unterzeichnung des Protokolls beruht gar auf Freiwilligkeit.

Grundsätzlich muss jedoch jede Bemühung zur Reduktion des unerwünschten Mail-Verkehrs begrüsst werden. Dass die Bekämpfung dieser Problematik nur international erfolgreich sein kann, liegt auf der Hand – eine Umsetzung von Richtlinien dagegen kann schlicht nicht von heute auf morgen erwartet werden.

EU: Schärferes Vorgehen gegen Hacker

Der EU-Rat hat am 24. Februar 2005 einen umstrittenen Rahmenbeschluss verabschiedet, der die Strafverfolgung von Angriffen auf Informationssysteme neu regeln soll. Erstmals werden für die Mitgliedsstaaten verbindliche Richtlinien bezüglich Cyberkriminalität geschaffen.

Die Richtlinie sieht vor, dass Handlungen wie das unerlaubte Eindringen in Computersysteme („Hacking“), Viren-Verbreitung oder Denial-of-Service Angriffe verboten werden. Unter Strafe gestellt wird „der vorsätzliche oder unbefugte Zugang zu einem Informationssystem“ oder Teilen davon, die „unbefugte vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems“ oder das „unbefugte vorsätzliche Löschen, Beschädigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten“. Auch Anstiftung oder Beihilfe dazu soll verboten werden. Vorgesehen sind Freiheitsstrafen bis zu drei, im Falle einer Verbindung zur organisierten Kriminalität bis zu fünf Jahren. Zudem wurde ein verbesserter Informationsaustausch über solche Straftaten beschlossen. „Leichte Fälle“ sind von der Strafverfolgung ausgenommen, nicht aber ein ursprünglich vorgesehenes Privileg für Security-Experten im Rahmen der Durchführung von Sicherheitstests.

Die neue EU-Richtlinie lehnt sich, vor allem bei der Angleichung des materiellen Rechts, eng an die Cybercrime Convention des Europarates, die seit dem Juli 2004 in Kraft ist und richtet somit das EU-Recht auf die Vorgaben der Cybercrime Convention aus. Kritiker bemängeln, das Gesetz schiesse über das Ziel hinaus, insbesondere darum, weil ihrer Meinung nach auch legitime Sicherheitstester kriminalisiert werden könnten. Tatsächlich gilt jedoch ein Zugang oder Eingriff als unbefugt, wenn er „vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde oder nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist".

Die EU-Minister erläuterten abschliessend, warum sie das Gesetz trotz der grossen Kritik verabschiedeten: Auf Grund einer wachsenden Besorgnis über das Potenzial möglicher Terroranschläge gegen Informationssysteme und der wachsenden Betätigung der Organisierten Kriminalität in diesem Gebiet

In Deutschland beispielsweise muss somit neu auch der blosse Zugang zu einem Datenverarbeitungssystem oder die Datensabotage bei Privatpersonen strafbar werden, wie dies in der Schweiz bereits der Fall ist. Schweizer Gesetzestexte beinhalten z.B. jedoch im Gegensatz zur neuen EU-Richtlinie nicht explizit die Tathandlungen „Verstümmeln" oder „Unterdrücken" von Daten. Während die EU-Richtlinie, ausser bei einem „leichten" Fall, Strafbarkeit verlangt, definieren die entsprechenden Artikel des Schweizer Strafgesetzbuches (Art. 143bis, Art. 144bis) Delikte dieser Art zum Teil als Antrags-, nicht als Offizial-Delikte. Das Schweizer Gesetz sieht zudem beim Strafmass zum Teil lediglich Bussen vor und liegt damit bei gewissen Tatbeständen unter dem von der EU-Richtlinie geforderten Mindestmass. Im Schweizer Recht nicht explizit erwähnt ist die Verbindung und Verschärfung der Tatbestände bei Vorliegen von kriminellen Vereinigungen (Art. 7 EU-Richtlinie), wobei zu bedenken ist, dass in der Schweiz eine Vereinigung zur Begehung von Straftaten an sich bereits strafbar ist (Art. 260ter StGB).

Deutschland: Anti-Spam Gesetz im Parlament diskutiert

Die SPD und die Grünen brachten Mitte Februar 2005 ein Anti-Spam-Gesetz in den Bundestag ein, das die Rechtsmittel gegen Spam-Mails verschärft. Neu sollen den Absendern Bussen von bis zu 50'000 Euro drohen, sofern sie ihre Identität zu verschleiern versuchen. Bereits in der Betreffzeile soll klar deklariert sein müssen, dass es sich bei der Mail um eine Werbesendung handele. Somit wird ein ähnlicher Ansatz wie in den USA angewendet.

Sowohl von Seiten der Politik als auch von Experten wurde der Gesetzesentwurf inzwischen massiv kritisiert. Die Internet-Beauftragte der CDU/CSU monierte etwa, der Entwurf sei gar nicht geeignet, die Spam-Flut zu bekämpfen. Spamming in Gästebüchern oder Foren würde gar nicht erst berücksichtigt. Von Experten-Seite wurde bemängelt, das Gesetz sei kontraproduktiv: Statt generell gegen Spam vorzugehen, würde vielmehr die Rahmenbedingung geschaffen, zwischen „gutem" und „bösem" Spam zu unterscheiden – und somit würde Spam unter gewissen Bedingungen gar legalisiert. Zu sehr sei vom Gesetzgeber auf die Wünsche der Wirtschaftsverbände eingegangen worden, die sich die Möglichkeit „legitimer" Werbezusendungen erhalten möchten. Gar nicht erst geregelt wurden beispielsweise auch die Kompetenzen der Provider im Spam-Filtering.

Die Expertenanhörung zum Gesetzesentwurf vor dem Bundestagsausschuss für Wirtschaft und Arbeit, fand am 18. April 2005 statt und zeigte ebenfalls die Schwachstellen des Entwurfs auf. Eine Überarbeitung des Entwurfs ist deshalb zu erwarten.

Deutschland und Grossbritannien: Neue Internetsicherheits-Initiative für Bürger

Neben dem bereits bestehenden Portal zur Internetsicherheit für Bürger (www.bsi-fuer-buerger.de) ist am 12. März 2005 auf der URL www.sicher-im-netz.de unter der Schirmherrschaft des Bundeswirtschaftsministeriums ein zweiter Internetauftritt zur Sensibilisierung für Computer-Sicherheits-Probleme ins Leben gerufen worden. An der Initiative sind unter anderem Microsoft, eBay, T-Online sowie einige Verbände beteiligt. Als Ziel bezeichneten die Verantwortlichen, innert wenigen Monaten bis zu 10 Millionen Haushalte zu erreichen und diese so auf Sicherheitsprobleme und Internet-Kriminalität aufmerksam zu machen. Bei Computer-Händlern können die Bürger auch kostenlose CD-ROMs mit einem „Basis-Sicherheitscheck" beziehen.

Nur wenige Wochen zuvor, am 23. Februar 2005, wurde vom britischen „Home Office" ein Webauftritt zum selben Thema ins Leben gerufen. Auf der URL www.itsafe.gov.uk sollen Heimanwender und KMUs mit Informationen über Virus-Gefahren und mit Ratschlägen zur sicheren Internet-Nutzung versorgt werden. ITSafe wird dazu Daten des National Infrastructure Security Co-Ordination Centre (NISCC) verwerten und bietet auch eine E-Mail-Warnliste an.

Vielerorts werden momentan Regierungsstellen geschaffen, die sich mit der Sensibilisierung der Bürger zum Thema Internet-Kriminalität beschäftigen. Beide hier erwähnten Portale wollen mit fachjargon-freier, klarer Sprache und einfachen Konfigurationsanleitungen den technisch weniger bewanderten Heimanwender ansprechen – den gleichen Ansatz verfolgt auch die vom Bund betriebene Schweizer „Melde- und Analysestelle Informationssicherheit" (MELANI) mit ihrem „Offenen Kundenkreis".

Unter Experten wird dieser Ansatz mehrheitlich begrüsst, auch wenn einige Kritiker monieren, Sicherheit im Internet sei nicht durch eine Sensibilisierung der Nutzer, sondern allein durch die Einführung sicherer Standards zu gewährleisten. Es sei niemals möglich, jeden Internetnutzer zu „erziehen" und zu sensibilisieren – vielmehr müsse endlich der Fokus auf die Erarbeitung einer sicheren Technologie gerichtet werden.

USA: Neue Richtlinien zur Informatik-Sicherheit von Nuklearanlagen in Vernehmlassung

Die U.S. Nuclear Regulatory Commission (NRC) lancierte Ende Januar 2005 eine öffentliche Kommentierungs-Phase für eine 15-seitige Aktualisierung ihrer Weisung „Criteria for Use of Computers in Safety Systems of Nuclear Power Plants". Die momentan gültige, dreiseitige Version stammt aus dem Jahr 1996 und soll nun ersetzt werden. Die Vernehmlassungsphase ist seit dem 14. März 2005 abgeschlossen.

Die Grundidee der neuen Weisung ist es, für jeden Schritt von der Entwicklung bis zur Stilllegung eines Atomkraftwerks die Computer-Sicherheit systematisch zu berücksichtigen. Zudem wird geraten, keine Verbindungen zu Vertragspartnern oder zu öffentlichen Netzen zu implementieren. Kraftwerkbetreiber werden zudem angehalten, den Effekt jedes neuen Systems auf die Sicherheit der Anlage zu prüfen und Reaktionspläne für Computervorfälle zu entwerfen. Hersteller erhalten Weisungen, wie sie das Risiko von Saboteuren vermeiden können, die so genannte „Backdoors" oder „logische Bomben" bereits in der Entwicklungsphase eines solches Sicherheitssystems einzubauen drohen.

Den grössten und wichtigsten Kritikpunkt an der neuen Regelung provoziert die Tatsache, dass die Regelung nur unverbindlichen Status bekommen soll und daher keinen verpflichtenden Charakter erhält.

Die MELANI bekannten Reaktionen von der Seite der Hersteller solcher Informations-Systeme für AKWs sind bisher durchwegs negativ. Die kalifornische Capri Technology,

Herstellerin spezialisierter Systeme und Software für die Nuklearindustrie, bemängelte, die Weisung sei „frühreif“: Sie schrecke Kraftwerkbetreiber eher von einer Reorganisation ihrer IT-Infrastrukturen ab, statt sie zu einer Modernisierung und Härtung solcher Systeme zu motivieren. Bevor die NRC und Industrieexperten eindeutigere Weisungen erarbeiten könnten, sei es kontraproduktiv, eine Weisung zu erlassen.

Framatone, eine französische Firma, die Kraftwerke von Beginn weg entwickelt und baut, übt ähnliche Kritik. Der Ansatz der NRC sei zu breit, wenn sie beispielsweise dieselben Vorschriften für eine Software auf einem generell einsetzbaren PC ansetze wie für die Firmware eines Chips für die Steuerung. Sicherheit in diesem Feld sei zu komplex, um auf 16 Seiten umrissen zu werden.

Dominion, eine im selben Sektor tätige Firma in Virginia (USA), kritisiert den Ansatz gegen Saboteure bei den Entwicklern: Wie soll eine Firma eine Software entwickeln können, auf die die eigenen Programmierer nicht vollen Zugriff haben? Zudem wurde kritisiert, dass die Anbindung beispielsweise an ein Web-Interface nicht zwingend Sicherheitsrisiken schaffen müsse.

Die Hauptprobleme in der Sicherheit der so genannten SCADA-Systeme in Kraftwerken (Supervisory Control and Data Acquisition) ist in den Bereichen der bisher weitgehend unverschlüsselten Daten- und Kommando-Transmissionen, der Anbindung an öffentliche Netzwerke und in der fehlenden Standardisierung der Technologien zu suchen. Die neue NRC-Weisung beschränkt sich hingegen bloss auf die Anbindung an öffentliche Netze – die anderen Themen werden weitgehend ausgespart.

USA: „Protected Critical Infrastructure Information Program“ floppt

Das „Information Analysis and Infrastructure Protection Directorate“ des amerikanischen „Department of Homeland Security“ (DHS) unterhält seit einem Jahr das so genannte „Protected Critical Infrastructure Information Program“ (PCII). Es soll Unternehmen, die Schlüsselfunktionen in der amerikanischen Infrastruktur wahrnehmen, die Möglichkeit bieten, Details über ihre physischen und digitalen Verwundbarkeiten zu melden. Das Programm basiert auf einem Gesetz aus dem Jahr 2002, das damals nicht zuletzt auf Grund massiver Lobby-Arbeit der Informationstechnologie- und Telekommunikations-Industrie zustande gekommen ist.

Nach einem Jahr muss ein schlechtes Fazit gezogen werden: Insbesondere von der informations-technologischen Industrie wurde das Programm bisher nie genutzt, wie der Präsident der „Information Technology Industry Association“ (ITAA) erklärte – dabei war gerade die ITAA 2002 einer der aktivsten Lobbyisten. Auch das „IT Information Sharing and Analysis Center“, eine Industrie-Sicherheits-Initiative bestehend aus Microsoft, Oracle, Intel und anderen, hat bisher keine einzige Meldung an das PCII abgesetzt. Auch die Elektronik-Industrie konnte sich bisher wenig für das Programm erwärmen.

Die Kritiken der dem Programm angeschlossenen Unternehmen fallen hart aus und bemängeln vor allem zwei Punkte: Erstens erachtet insbesondere die Elektronik-Industrie die Meldungsformalitäten des PCII für zu umständlich – die Meldungen sollen jeweils in Papierform übermittelt werden, obwohl die Beteiligten ein elektronisches System vorziehen würden. Zweitens wird von allen Beteiligten der unklare weitere Verwendungszweck einer Information nach dem Meldungseingang bemängelt. Während sich das DHS zwar dazu verpflichtet, die Informationen nicht nach Aussen weiterzuleiten und nicht gegen die Interessen der angeschlossenen Unternehmen zu verwenden, ist unklar, welche weiteren Ämter innerhalb der Regierung über die Meldung in Kenntnis gesetzt werden.

Wie der Präsident der ITAA bemerkte, meldeten die Unternehmen nicht Werbe- oder Marketing-Informationen, sondern müssten ihre tiefsten, bestgehütetsten Geheimnisse preisgeben. Während der Informationsfluss innerhalb des PCII selbst zwar klar geregelt ist, wird die Information auch an verschiedene weitere Stellen innerhalb der Regierung und gar zu Gliedstaaten der USA weitergeleitet – und dies ohne Kontrolle des Meldenden. Der Melder weiss nicht einmal, wohin die Information überall verteilt wird.

MELANI ist gerade dabei, die Aktivitäten mit ihrem geschlossenen Kundenkreis aufzunehmen. Für das Schweizer Konzept droht die hier geschilderte Gefahr aber nicht: Während einerseits ein sicheres Kommunikationssystem implementiert werden wird, untersteht andererseits der Informationsfluss der strikten Kontrolle des Melders.

UNO-Arbeitsgruppe veröffentlicht Grundsatzpapiere zur Internet-Verwaltung

Die UNO-Arbeitsgruppe „Internet Governance“ veröffentlichte Anfang Februar 2005 mehrere Grundsatzpapiere zum Thema Internet-Verwaltung. Die Papiere befassen sich mit Themen wie DNS-Verwaltung, Telekommunikation und Konvergenz, Spam, Sicherheit und Cybercrime und sollen das Dreiecksverhältnis zwischen Privatsektor, Zivilgesellschaft und Regierungen im Bereich der Netzverwaltung klarer festlegen. Auf Basis dieser Papiere sollen bis im Juni 2005 Empfehlungen zur Zukunft der globalen Netzverwaltung an den Generalsekretär und die Staatengemeinschaft erarbeitet werden.

Um einer drohenden Entwertung des Internets vorzubeugen sei es dringend notwendig, gemeinsame Verwaltungsanstrengungen zu unternehmen und Forschung, Zwischenfall-Abwicklung, Informationsaustausch, Technologie-Standards und Gesetzgebung international abzustimmen. In gemeinsamen Anstrengungen soll die Öffentlichkeit weltweit für die Problematik sensibilisiert werden. Als Hauptgefahren wurden DNS-Kompromittierung (DNS-Poisoning), Denial-of-Service Angriffe, Schwächen des Routing-Protokolls BGP und vor allem die Verwundbarkeit der eingesetzten Netzwerksoftware identifiziert.

Am heftigsten dürften die Papiere zur Namens- und Nummernverwaltung sowie zur Organisation der DNS-Root-Server-Systeme debattiert werden. Darin wird nämlich die mächtige Rolle des US-Handelsministeriums beziehungsweise der „National Telecommunications and Information Administration“ (NTIA), welche die Root-Zone des Internets kontrolliert, in Frage gestellt. Ob die auf 2006 terminierte Unabhängig der NTIA wirklich umgesetzt werden wird, bleibt unsicher.

Die Grenzen in der Vernetzung der Informations- und Kommunikationstechnologie stimmen nicht mit den Staatsgrenzen überein. Eine effektive Erhöhung der Sicherheit ist daher nur unter weitgehender internationaler Kooperation zu erreichen. Die UNO-Arbeitsgruppe „Internet Governance“ hat die wichtigsten Probleme erkannt – inwiefern sie aber mit ihren Empfehlungen einen nachhaltigen Einfluss auf die Entwicklung der Politik der einzelnen Mitgliedstaaten haben wird, bleibt noch ungewiss.

USA: Hacker-Crew in den US-Streitkräften

Ein sich seit längerer Zeit haltendes Gerücht wurde im Verlauf des Monats April 2005 zur Gewissheit: Die US-Streitkräfte verfügen über ein hochspezialisiertes Team von Experten, die in der Lage sind, einen so genannten „Cyberwar“ gegen gegnerische Informationsnetzwerke zu führen.

Dabei, so das Technologiemagazin „Wired“, handelt es sich um „the world’s most formidable hacker posse: a super-secret, multimillion-dollar weapons program that may be

ready to launch bloodless cyberwar against enemy networks – from electronic grids to telephone nets.“ Die Einheit trägt den Namen “Joint Functional Component Command for Network Warfare” (JFCCNW).

Die zentrale Aufgabe des Teams ist der Schutz der Netzwerke des US-Verteidigungsministeriums. Eine weitere Zuständigkeit, „Computer Network Attack“, wird jedoch streng geheim gehalten. Vermutet wird, dass die Truppe aus Experten aus der CIA, der National Security Agency (NSA), dem FBI, den vier Bereichen der US-Armee (Navy, Army, Air Force, Marines), Zivilisten und möglicherweise gar militärischen Vertretern von Alliierten besteht. Ein ehemaliger Nachrichtendienstmitarbeiter der Marines schreibt der Truppe weitgehende Angriffskapazitäten – auch gegen gegnerische militärische Informationssysteme – zu. Vermutet wird beispielsweise die Fähigkeit, in kürzester Zeit islamistische Propaganda-Webseiten vom Netz nehmen zu können.

Deutschland: Innenminister Schily kündigt „Nationalen Plan zum Schutz der Infrastrukturen“ an

Der Deutsche Innenminister, Otto Schily, kündigte Mitte Mai anlässlich des 9. Deutschen IT-Sicherheitskongresses in Bonn einen „Nationalen Plan zum Schutz der Informationsinfrastrukturen in Deutschland“ an. Bis zum Ende der Redaktionsfrist des vorliegenden Berichts war das Bundesinnenministerium gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) noch mit der Ausarbeitung desselben beschäftigt.

Für Behörden, Unternehmen und private Nutzer sollen „neue Strategien zur Bekämpfung von Angriffen von Hackern und Viren“ entwickelt werden. Nach der Sommerpause soll der Plan im Bundeskabinett vorgestellt werden. Vorgesehen ist, dass dem BSI neuerdings auch operative Aufgaben übertragen werden sollen, welche weit über die derzeitig beratenden Funktionen hinausgehen sollen. Neben dem Verfassungsschutz, dem Bundesgrenzschutz und dem Bundeskriminalamt soll das BSI zur vierten Säule der inneren Sicherheitsarchitektur in Deutschland ausgebaut werden.

Mit ein Grund für diesen Schritt, führte Schily aus, sei auch die zumindest theoretische Möglichkeit eines Terrorangriffs mit Cybermitteln, gegen den man sich rechtzeitig wappnen müsse. Der Inhalt des Nationalen Plans wurde bisher lediglich angedeutet: Vorgesehen sind unter Anderem „klare Vereinbarungen für die hierfür notwendige Aufgabenbewältigung“ sowie „Massnahmen zur wirkungsvollen Reaktion“ nach einem IT-Sicherheitsvorfall. Das BSI soll ein Krisenreaktionszentrum des Bundes aufbauen und eng mit den privaten Betreibern Kritischer Infrastrukturen (in Deutschland die Sektoren Energie, Finanz- und Versicherungswesen, Transport und Versorgung, Notfall- und Rettungswesen, Gesundheitswesen und öffentliche Verwaltung) zusammenarbeiten. Dazu sollen belastbare und verbindliche Vereinbarungen getroffen werden, eine Gesetzesänderung zu diesem Zweck wurde von Schily nicht ausgeschlossen.

USA: Senatoren legen Gesetz gegen Identitätsdiebstahl vor

Angesichts der zahlreichen ID-Theft-Zwischenfälle in den USA der letzten Monate (siehe Kapitel 2.3 und 5.3) schlug der demokratische Senator Patrick Leahy einen neuen Gesetzesentwurf vor, der Unternehmen betreffen würde, die sensible Daten verarbeiten. Für seinen „Personal Data Privacy and Security Act of 2005“ konnte Leahy bereits Hilfe von republikanischer Seite – den Vorsitzenden des Justizausschuss im Senat, Arlen Specter – gewinnen, was die Chancen des Entwurfs erhöht. Senator Leahy ist seinerseits persönlich von einem Identitätsdiebstahl betroffen.

Das Gesetz sieht verschiedene Massnahmen zur Verbesserung der Datensicherheit vor: Unternehmen sollen künftig nur noch unter bestimmten Bedingungen an sensible (Bürger-)Daten gelangen, beispielsweise bei der Erteilung von Krediten, und nur unter dem Einverständnis der Betroffenen. Diese sollen auch darüber Bescheid wissen, welche Firma Daten über sie gespeichert hat. Personen, die von Identitätsdiebstahl oder Missbrauch betroffen sind, müssten zudem künftig viel schneller informiert werden.

Firmen, die über mehr als 10'000 Datensätze dieser Art verfügten, sollten künftig unter besonderer Beobachtung stehen und verschärfte Sicherheitsstandards erfüllen müssen.

USA: Bundesbehörden ab 2008 umgestellt auf IPv6

Wie Ende Juni bekannt wurde, wird das US-amerikanische Office of Management and Budget demnächst alle Bundesbehörden anweisen, bis 2006 Inventarlisten der IPv6-fähigen Systeme zu erstellen und bis 2008 ihre Netzwerke auf das neue IPv6-Protokoll umzustellen. Hauptgrund für die Forcierung der Umstellung sind einerseits die verbesserten Sicherheitsfunktionen, andererseits die Möglichkeit zur besseren Integration von mobilen Überwachungssensoren. Das einzige Departement, das bisher einen vollständigen Migrationsplan ausgearbeitet hat, ist das Verteidigungsministerium.

Die wichtigsten Neuerungen im neuen Internetprotokoll IPv6 bestehen in zusätzlichen Sicherheitsfeatures (z.B. inhärente Verschlüsselungsoptionen) oder auch im wesentlich grösseren Adressraum dank der 128-Bit-Adressen.

USA wollen Kontrolle über DNS-Rootzone nicht abgeben

Kurz vor Veröffentlichung des abschliessenden Berichts der UNO Working Group on Internet Governance (WGIG) zur Internet-Administration kündete die US-Regierung überraschend an, dass sie ihre Aufsicht über das Domain Name System (DNS) und über die Internet Corporation for Assigned Names and Numbers (ICANN) nicht aufgeben will.

Der Assistant Secretary der US-amerikanischen National Information and Telecommunication Administration (NTIA) legte dabei die vier Kernpunkte der US-DNS-Politik dar. Die US-Regierung würde nichts unternehmen, was einen erfolgreichen und effizienten Betrieb des DNS gefährden könnte „und wird daher ihre historische Rolle bei der Autorisierung von Änderungen oder Anpassungen des massgeblichen Rootzone-Files beibehalten." Auch die Aufsicht über die ICANN will man behalten.

Bis vor kurzem erklärte die ICANN-Spitze noch ihr Interesse, das DNS-Management dem privaten Sektor zu übergeben und bestätigte diese Ansicht auch im aktuellsten Strategieplan.

7.2 Privat

WLAN Hot-Spots in 1. Klasse-Abteilen der SBB in Kürze zu erwarten

Bereits seit der zweiten Jahreshälfte 2004 ist es in grösseren SBB-Bahnhöfen (Basel, Bern, Genf, Lausanne, Luzern, Winterthur und Zürich) für Reisende möglich, mit ihren eigenen Laptops über Wireless Local Area Network (WLAN) auf dem Internet zu surfen. Bis zum September 2005 soll es dank einer Zusammenarbeit zwischen den SBB und Swisscom Mobile zudem auch in einigen Zügen möglich sein, auf das Internet zuzugreifen. Vorläufig wird der

Dienst aber nur in 1.-Klasse-Wagen hauptsächlich auf der Ost-West-Achse eingesetzt. Vorgesehen sind Bandbreiten von bis zu zwei Megabit pro Sekunde. Sollte sich der Betrieb bewähren, wollen die SBB das Angebot bis Ende 2007 auf weitere 1.-Klasse-Wagen anderer Linien ausdehnen.

Die erweiterten Möglichkeiten für Zugreisende sind grundsätzlich zu begrüssen. Dennoch bestehen aber gewisse Bedenken im Bereich der Sicherheit.

Jeder Internet-Service-Provider in der Schweiz ist gesetzlich dazu verpflichtet, die Verbindungsdaten seiner Nutzer während sechs Monaten aufzubewahren und im Falle einer illegalen Aktivität den Strafverfolgungsbehörden zur Verfügung zu stellen (BÜPF, Artikel 3 und 15, Abs. 3). Inwiefern die Swisscom dieser Verpflichtung im Rahmen ihrer Kooperation mit den SBB nachkommt, ist MELANI leider unbekannt – die zuständige Person bei den SBB konnte während mehrerer Tage nicht erreicht werden. Sollte aber ein anonymer Zugriff auf das Internet in Wagen der SBB möglich sein, könnte Jedermann während der Zugfahrt alle beliebigen illegalen Inhalte erstellen, anschauen und herunterladen oder aber anderen illegalen Aktivitäten im Internet nachgehen.

Die Deutsche Bahn beispielsweise, die auf den Herbst 2005 zwischen Köln und Düsseldorf einen ähnlichen Pilotversuch starten möchte, plant nur eindeutig identifizierte Personen auf das Internet zugreifen zu lassen: Kunden des involvierten Providers (D1) können ihre gewohnten Zugangsdaten nutzen, andere Personen erhalten per SMS ihre Login-Daten. Auf diese Weise ist die Identität des Surfenden immer feststellbar.

Zudem besteht möglicherweise die Gefahr eines so genannten „Evil Twin“. Der Rechner eines Hackers, der fälschlicherweise vorgibt, Hotspot für kabelloses Surfen zu sein, wird als Evil Twin bezeichnet. Dabei droht für den Surfer die Gefahr, sich unbemerkt gar nicht beim legitimen Hotspot anzumelden, sondern am Gerät des Hackers – der anschliessend den gesamten Datenverkehr aufzeichnen kann. Auf der Strecke Zürich – Bern beispielsweise, die morgens und abends von arbeitenden Pendlern befahren wird, entstünde so ein beträchtliches Potenzial zur Wirtschaftsspionage.

Inwiefern die hier angedeuteten Gefahren Realität werden könnten, hängt jedoch von der bisher noch unbekannten technischen Detailkonfiguration des Angebots ab und kann daher zu diesem Zeitpunkt noch nicht definitiv beurteilt werden.

Microsoft schränkt Updates für illegale Kopien ein

Ende Januar 2005 gab Microsoft bekannt, die Updates für Betriebssysteme und Applikationen bereits in wenigen Monaten von einer Überprüfung der Lizenz abhängig zu machen. Bevor künftig Software- oder Sicherheits-Updates von der Homepage „http://www.windowsupdate.com“ oder per Auto-Update-Funktion des Betriebssystems bezogen werden können, muss der Benutzer zuerst den Nachweis einer gültigen Lizenz erbringen.

Kann kein Lizenzbeweis erbracht werden, können nur noch als „kritisch“ eingestufte Updates bezogen werden. Das mit „Windows Genuine Advantage“ betitelte Programm verfolgt das Ziel, härter gegen Raubkopierer vorgehen zu können – keine andere Software ist weltweit so oft raubkopiert und illegal vertrieben worden, wie die Betriebssysteme von Microsoft. Microsoft gibt an, in den vergangenen zehn Jahren mehrere Milliarden Dollar wegen Raubkopien verloren zu haben.

Microsofts Betriebssysteme geniessen einen weltweiten Marktanteil im Endanwender-Bereich von über 95% – eine beeindruckende Zahl, die nicht zuletzt auch deshalb erreicht wurde, weil die Systeme dank Raubkopien auch in weniger zahlungskräftigen Weltregionen

Fuss fassen konnten. Immerhin muss mit einer Quote von etwa 30% unlizenzierter Microsoft-Software gerechnet werden. Microsoft stellt den Update-Bezug für illegitime Betriebssysteme zwar nicht ganz ein und verteilt kritische Updates weiterhin, da unsichere Windows-Systeme auch die Sicherheit anderer Windows-Nutzer gefährden und das Internet generell unsicherer machen. Experten kritisieren dennoch, dass viele wichtige Updates künftig von einem grossen Teil der Microsoft-Nutzer nicht mehr installiert werden können, was schliesslich in einer Verschlechterung der Sicherheitslage im Internet resultieren müsse – denn ein infizierter Windows-Computer kann für den Angriff auf weitere Systeme unbemerkt eingesetzt werden.

Hersteller einigen sich auf ein „Common Vulnerability Scoring System" (CVSS)

Führende Informations- und Kommunikations-Technologie Hersteller, darunter Cisco Systems, Microsoft, Qualys und Symantec, haben sich Ende Februar anlässlich der RSA-Sicherheitskonferenz in San Francisco darauf geeinigt, eine gemeinsame Kategorisierung für Sicherheitslücken zu etablieren. Das neue „Common Vulnerability Scoring System" (CVSS) soll die bisher herstellerspezifischen Bezeichnungen durch ein System ersetzen, das eine eindeutige Terminologisierung erlaubt und somit die Linderungsmassnahmen bei einem Zwischenfall vereinheitlichen und vereinfachen soll.

Das CVSS ist Teil eines Projekts des „US National Infrastructure Advisory Council", einer Abteilung des „Department of Homeland Security", mit dem Ziel, Rahmenbedingungen für die Identifizierung von Sicherheitslücken zu schaffen. Die Dringlichkeit und Kritikalität von Sicherheitslücken soll unter dem CVSS künftig anhand standardisierter Kriterien eindeutig definiert werden.

Dazu werden unter anderen die folgenden Kriterien berücksichtigt: Zugangsmöglichkeit des Hackers zu vertraulichen Informationen, Möglichkeit des Hackers zur Manipulation von Daten oder Möglichkeit eines Angreifers zur Lancierung eines Denial-of-Service-Angriffs, der Umstand, ob eine Sicherheitslücke an sich den Zugang ermöglicht, oder ob dazu noch Passwörter nötig sind und die verstrichene Zeit seit der Entdeckung der Lücke.

Wie im Bereich der Gesetzgebung, der Bekämpfung, des Datenaustauschs und der Sensibilisierung ist eine internationale Koordination der Anstrengungen auch auf Hersteller-Seite nötig, um Erfolge erreichen zu können.

Die bisher oft zahlreichen Bezeichnungen der einzelnen Hersteller beispielsweise für Viren (aber auch für andere Schädlinge oder Sicherheitslücken) und die unklaren Kriterien zur Bestimmung der Kritikalität erschwerten die ohnehin anspruchsvolle Sicherheitsadministration verteilter, heterogener Systeme. Ob das CVSS allerdings wirklich langfristige Vereinfachungen in der Sicherheitsadministration bringen wird, lässt sich erst beurteilen, wenn die ersten Meldungen und Warnungen abgesetzt werden. Schliesslich ist das CVSS nicht der erste Versuch einer Standardisierung in diesem Bereich.

Microsoft, eBay, PayPal und Visa gründen „Phishing Report Network"

„Wholesecurity", ein US-amerikanisches Sicherheitsunternehmen, hat ein neues Meldesystem für betrügerische Websites begründet: Das so genannte „Phishing Report Network" (www.phishreport.net). Ziel des Netzwerkes, an dem sich unter anderen auch Microsoft, eBay, PayPal und Visa beteiligen, ist die Registrierung möglichst vieler Phishing-Attacken. Die Meldungen sollen in einer zentralen Datenbank gespeichert werden, auf die weitere Firmen zugreifen können, damit sie die betrügerischen Seiten sperren können.

Während sich eBay, PayPal und Visa dank dem Zugriff auf eine zentrale Datenbank eine raschere Beantwortung und Reaktionszeit auf Kundenanfragen versprechen, will Microsoft dank den Daten raschere Anpassungen an seiner Software vornehmen können (wie z.B. E-Mail-Clients).

Im Jahr 2004 wurde mit der Gründung der „Anti Phishing Working Group“ (www.antiphishing.org) bereits ein ähnliches Unternehmen lanciert wie jetzt mit dem „Phishing Report Network“.

Microsoft: Kooperationsprogramm mit Regierungen angekündigt

In einer Rede kündigte Microsoft-Gründer Bill Gates Anfang Februar 2005 ein neues Kooperationsprogramm mit Regierungen an. Das neue „Security Cooperation Program“ weitet das seit 2003 bestehende „Government Security Program“ aus, unter dem Regierungen bereits Einsicht in den Quellcode von Windows XP, Windows 2000, Windows CE und Windows Server 2003 erhalten hatten. Diesem älteren Programm gehören inzwischen 36 Staaten an.

Im Rahmen des neuen Programms will Microsoft Informationen über bekannte Sicherheitslücken und Bedrohungen, über kommende Software-Patches zwecks einer längeren Test- und Vorbereitungsphase für Regierungen sowie Expertenwissen im Falle eines Zwischenfalles anbieten. Zum Angebot gehört auch eine rund um die Uhr bediente Support-Hotline und bei Bedarf die Inanspruchnahme eines Microsoft-Experten-Teams vor Ort.

Kanada, Chile, die USA und Norwegen haben gemäss Microsoft bereits ihre Teilnahme am neuen Programm zugesichert, weitere Regierungen werden mit Sicherheit folgen.

Die neue Initiative muss im Rahmen der andauernden Konkurrenz zwischen Microsoft und Open-Source-Lösungen gesehen werden. Verschiedene Regierungsbehörden – zuletzt zum Beispiel die Stadt Wien – haben in letzter Zeit bekannt gegeben, aus Kosten- und Sicherheitsgründen auf Open-Source-Produkte umzusteigen. Mit dem nun angekündigten Programm hofft Microsoft, mehr Regierungen bei der Stange halten zu können. In den letzten Jahren hat sich Microsoft daher strategisch besonders stark auf Regierungs-Kunden ausgerichtet.

Microsoft richtet sich strategisch auf den IT-Sicherheitsmarkt aus

In letzter Zeit begann sich Microsoft durch den Ankauf von Sicherheits-Software-Entwicklern immer mehr auf den Sicherheits-Markt auszurichten. Bereits im Juni 2003 erwarb sich Microsoft durch den Kauf der Anti-Virus-Firma „GeCAD“ Know-how in diesem Bereich – im Dezember 2004 folgte der Kauf des Anti-Spyware-Spezialisten „Giant Company Software“ und Anfang Februar 2005 wurde die Akquisitionsrunde mit dem Kauf des Anti-Virus- und Anti-Spam-Spezialisten „Sybari Software“ abgerundet.

Erstes Resultat dieser Aktivitäten sind zwei neue Tools, die Microsoft seit Kurzem anbietet. Einerseits steht neuerdings auf den Microsoft-Servern die Beta-Version einer „Windows AntiSpyware“-Software zum Download zur Verfügung, andererseits wird per AutoUpdate ein Programm zur Entfernung von Viren und Würmern verteilt (das so genannte „Malicious Software Removal Tool“). Das erste Tool basiert auf ehemaligen Anti-Spyware-Produkten der „Giant Software Company“, das zweite auf der Anti-Viren-Software von „GeCAD Software“.

Zudem kündete Bill Gates an der RSA-Konferenz in San Francisco eine neue, auf Sicherheit ausgerichtete Version des Internet-Explorer auf den Juni 2005 sowie ein eigenes Anti-Viren-Programm von Microsoft bis Ende Jahr an. Die Anti-Spyware Software von Microsoft soll nach der definitiven Fertigstellung zudem gratis zum Download verfügbar sein.

Momentan sind die Ressourcen von Microsoft primär auf die Sicherheit fokussiert, wie Bill Gates Anfang Februar am „Government Leader's Forum" in Prag erklärte: „The No. 1 thing for Microsoft in terms of investment and research and development is security." In der Tat: Wie anlässlich der jährlichen „TechFest"-Konferenz der verschiedenen Microsoft Research & Development Teams Anfang März bekannt wurde, arbeitet Microsoft an verschiedenen Ideen, darunter ein vollautomatisiertes System zur Bekämpfung von Würmern. Ziel von Microsoft ist es, nicht mehr auf eine rasche Reaktionszeit der Administratoren zu hoffen, sondern eine automatisierte Lösung zu entwickeln.

Die von vielen Experten als Ursache vieler Sicherheitsprobleme bemängelte, durch die Übermacht von Microsoft-Produkten begründete Monokultur im Bereich der Informations- und Kommunikationssysteme bietet somit gleichzeitig eine realistische Chance auf eine technische Verbesserung des Sicherheitsniveaus im Internet. Mit aktuellen, auf Sicherheit konzentrierten Produkten könnte so nämlich auf einen Schlag ein Grossteil der am Internet angeschlossenen Computersysteme sicherer gemacht werden.

Microsoft verfolgt mit den Akquisitionen der letzten Monate seine alte Strategie des Aufkaufs innovativer Firmen zwecks Ausbaus der eigenen Produktelinie.

Cyber Incident Detection Data Analysis Center (CIDDAC) beginnt Pilotprojekt

Mitte April begann eine neue Non-Profit-Organisation, das Cyber Incident Detection Data Analysis Center (CIDDAC), ein Pilotprojekt zur Sammlung von Netzwerk-Intrusion Daten von einer Gruppe von Firmen aus dem Bereich der Kritischen Infrastrukturen. Ziel ist es, ein automatisiertes Cyber Early-Warning Center zu etablieren.

Beim Projekt handelt es sich um die ersten privaten Anstrengungen, neben der Regierung ein Cybercrime-Detection Netzwerk aufzubauen. Das Operationszentrum wurde am Institute of Strategic Threat Analysis and Response Laboratory der University of Pennsylvania eingerichtet und wird finanziell vom Department of Homeland Security unterstützt. Bis in fünf Monaten erhofft man sich die erste nützliche Datensammlung auf Grund von Meldungen der bis zu 30 angeschlossenen Unternehmen.

Für die Datensammlung soll eine Reihe von automatisierten Netzwerksensoren eingesetzt werden (Real-Time Cyber Attack Detection Sensors, RCADSs), die Einbrüche und Einbruchsversuche feststellen können. Diese befinden sich allerdings ausserhalb der Firewall des jeweiligen Unternehmens, da noch immer grosse Bedenken zur Datensicherheit bestehen und daher die Firmen der Konkurrenz keine Sensoren im eigenen Netzwerk überlassen möchten.

Anhand der Sensoren soll eine Warnung in Echtzeit möglich sein. Falls nötig, plant das Center, seine Daten auch den Strafverfolgungsbehörden zur Verfügung zu stellen – der Fokus liegt jedoch auf den Bedürfnissen der Privatwirtschaft. Vorläufig arbeitet das CIDDAC noch nicht mit ähnlichen Zentren, wie dem CERT Coordination Center oder dem SANS Internet Storm Center (ISC), zusammen.

Microsoft: „Windows OneCare" angekündigt

Microsoft kündigte Mitte Mai einen neuen Abo-Dienst namens „Windows OneCare" an, der künftig sicherstellen soll, dass Windows sicher und schnell bleibt. Nach dem Einstieg in das Security-Geschäft (siehe oben) will Microsoft mit diesem Abo in Kürze aktuelle Virenscanner und Anti-Spyware-Software sowie eine Firewall mit Verbindungskontrolle für ein- und ausgehende Verbindungen anbieten. „OneCare" soll auch ein Backup-Programm umfassen sowie die Systemdateien überprüfen und ordnen können.

Damit bietet Microsoft nichts Neues an, das nicht durch Alternativprodukte – beispielsweise Antiviren-Software von Drittherstellern – bereits abgedeckt wäre, vereint jedoch alle Sicherheitsfunktionen unter einer einheitlichen Oberfläche. Die öffentliche Beta-Phase von „Windows OneCare“ wurde auf Ende Jahr angekündigt. Ab wann der Dienst definitiv zur Verfügung stehen soll und zu welchem Preis man ihn nutzen kann, ist bisher unklar.

Bluewin tritt Messaging Anti-Abuse Working Group (MAAWG) bei

Wie am 6. Juni bekannt wurde, tritt Bluewin der internationalen Messaging Anti-Abuse Working Group (MAAWG) bei. Diese setzt sich vor allem gegen unerwünschte Massenmails und gegen Viren ein und umfasst nun bereits über 500 Millionen Abonnenten. Bluewin ist dem Direktorium als Sponsor beigetreten.

Als unabhängige, gemeinnützige Koalition von Kommunikations- und Technologieunternehmen weltweit hat sich die MAAWG zum Ziel gesetzt, den Missbrauch von Messaging-Technologien durch Zusammenarbeit der Betreiber, Nutzung der verfügbaren Technologie und die Bereitstellung eines branchenweiten Kommunikationsmittels in den Griff zu bekommen.

Trend Micro kauft IP-Filtering-Firma

Der Antiviren-Software-Hersteller Trend Micro baut sein Produktportfolio durch die Akquisition von Kelkea Inc., einem Spezialisten für IP-Filtering, weiter aus. Wie Trend Micro verkündete, wird der Zukauf die Produktlinie um Netzwerkschutz gegen Gefahren wie Phishing, Pharming, Botnetz-Angriffe (DDoS) und Spam erweitern.

Kelkea ist besonders auf die Identifizierung der Quelle von Gefahren, wie z.B. von Spam-Mail, spezialisiert. Ausserdem stellt Kelkea auch so genannte „Reputation Services“ zur Verfügung, mit denen IP-Adressen beobachtet und eingestuft werden, um Spammer, Phishing-Betrüge und andere Angriffe identifizieren zu können. Geplant ist eine vollständige Übernahme der Kelkea-Produkte unter eigenem Namen.

Der Markt für IT-Sicherheits-Produkte ist in stetigem Wachstum begriffen. MELANI geht davon aus, dass in den nächsten Jahren grössere Veränderungen in diesem Bereich zu erwarten sind.