Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

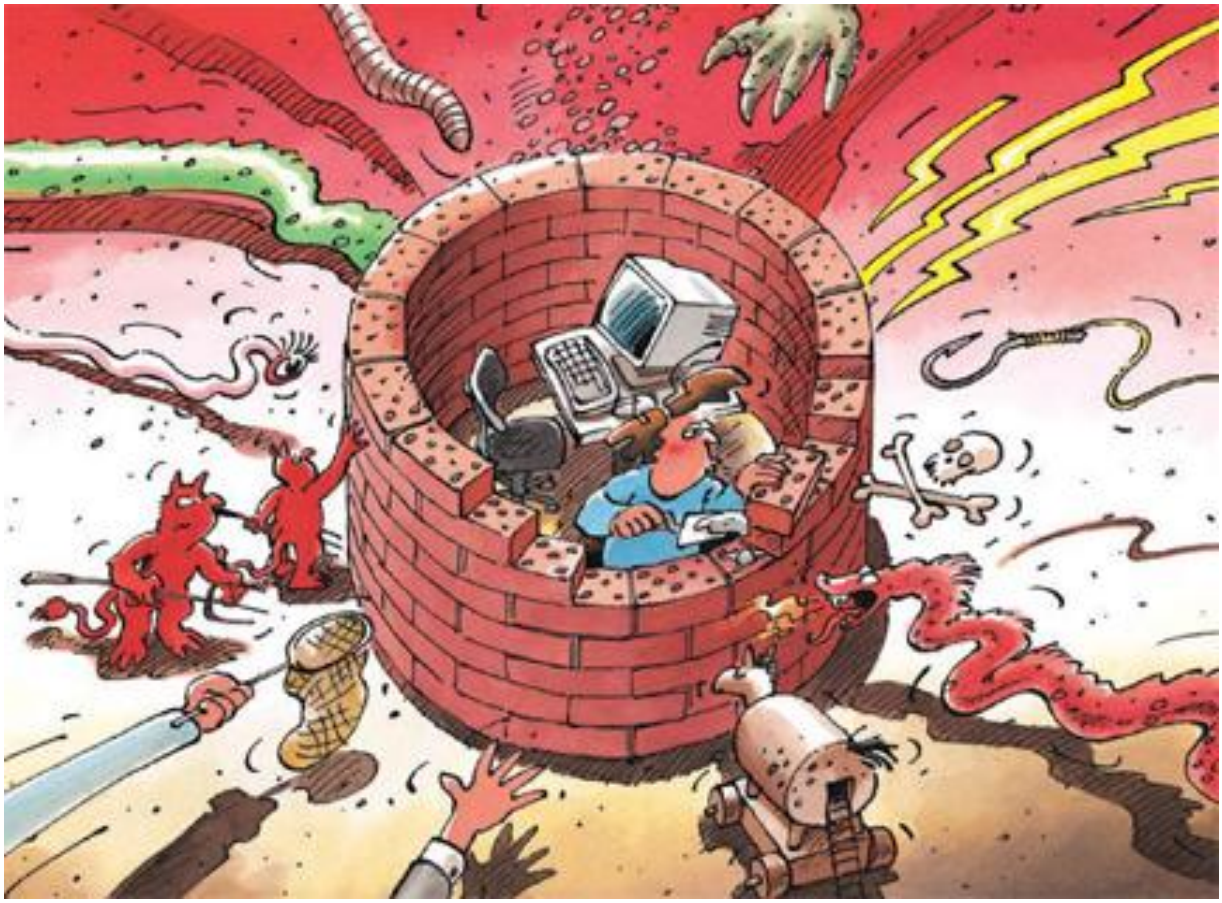
Informatikstrategieorgan Bund ISB
Bundesamt für Polizei fedpol

Melde- und Analysestelle Informationssicherung MELANI

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2006/II (Juli – Dezember)



In Zusammenarbeit mit:

KOBIK SCOCI CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Inhaltsverzeichnis

Schwerpunkte Ausgabe 2006/II

- **Social Engineering**
  Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Personen aus. Sie stellen die am weitesten verbreitete Angriffsart gegen Firmen und Privatanwender dar. Es ist damit zu rechnen, dass Social Engineering mit zunehmender (technischer) Sicherheit von Betriebssystemen und Applikationen weiter an Bedeutung gewinnen und als Folge davon auch professioneller werden.
  ► Aktuelle Lage: Kapitel 2.1
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.1 und 3.2
  ► Beispiele / Vorfälle: Schweiz Kapitel 4.1; international Kapitel 5.2 und 5.3
  ► Prävention: Kapitel 6

- **Spam**
  Spam nahm in der zweiten Hälfte des Jahres 2006 merklich zu. Neue Techniken, insbesondere der Versand der Spamnachricht als Bild statt in Textform, erlauben es, die besser gewordenen Spamfilter zu umgehen. Besonders verbreitet sind auch so genannte „Stock Pump and Dump Spams“, in denen zum Kauf bestimmter Aktien geraten wird.
  ► Aktuelle Lage: Kapitel 2.2
  ► Beispiele / Vorfälle: Kapitel 5.2 und 5.3

- **Daten- und Identitätsdiebstahl**
  Phishing und Daten- oder *Identitätsdiebstahl* mit *Malware* erlebten in der zweiten Jahreshälfte 2006 eine starke Zunahme. Gestohlen werden Daten, mit denen sich Geld machen lässt, wie beispielsweise solche, die zu unrechtmässigen E-Banking-Finanztransaktionen missbraucht werden können. Es ist damit zu rechnen, dass im Verlauf des Jahres 2007 vermehrt auch Finanzinstitutionen, die *Zwei-Faktor-Authentifizierung* einsetzen, ins Visier der Angreifer geraten.
  ► Aktuelle Lage: Kapitel 2.3
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.1 und 3.2
  ► Beispiele / Vorfälle: Schweiz Kapitel 4.1; international Kapitel 5.2 und 5.3

- **Malware / Angriffsvektoren**
  Die Zunahme gezielt eingesetzter *Malware* bei gleichzeitiger Abnahme grossflächiger Malware-Ausbrüche (z.B. in Form von *Würmern)* setzte sich auch im zweiten Halbjahr 2006 fort. Durch die verbesserte Sicherheit von Betriebssystemen werden vermehrt Sicherheitslücken in clientseitigen Applikationen ausgenützt, wie z.B. in Sicherheitssoftware, Plug-Ins, Hardware-Treibern oder MS Office-Produkten. Die Malware wird in ständig neuen Varianten und gezielt verteilt, um der Erkennung durch Antivirensoftware zu entgehen. Die Erkennungsraten werden immer schlechter. An Bedeutung gewonnen haben auch Infektionen beim Besuch präparierter Webseiten.
  ► Aktuelle Lage: Kapitel 2.4
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.1 und 3.2
  ► Beispiele / Vorfälle: Schweiz Kapitel 4.1; international Kapitel 5.2 und 5.3
  ► Prävention: Kapitel 6 (Social Engineering ist der wichtigste Malware-Infektionsweg)

1 Einleitung

Der vierte Halbjahresbericht (Juli – Dezember 2006) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen, gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet die wichtigsten Entwicklungen im Bereich der Prävention und resümiert Aktivitäten staatlicher und privater Akteure. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind in einem farblich hervorgehobenen Abschnitt leichter zu finden.

Kapitel 2 beschreibt die aktuelle Lage, Gefahren und Risiken des vergangenen Halbjahres. Ein Ausblick auf zu erwartende Entwicklungen wird in **Kapitel 3** gegeben.

Kapitel 4 und 5 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der letzten sechs Monate des Jahres 2006 aufgezeigt. Der Leser findet hier illustrative Beispiele und ergänzende Informationen zu den allgemeinen Kapiteln zwei und drei.

Kapitel 6 befasst sich neu jeweils mit einem Schwerpunkt aus der Prävention.

Kapitel 7 legt den Fokus auf staatliche und privatwirtschaftliche Aktivitäten zum Thema Informationssicherung im In- und Ausland.

Kapitel 8 fasst Änderungen in den gesetzlichen Grundlagen zusammen.

2 Aktuelle Lage, Gefahren und Risiken

2.1 Social Engineering

Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Personen aus, um an vertrauliche Daten zu gelangen oder die Opfer zur Ausführung bestimmter Aktionen zu verleiten.

Beispiel eines Social-Engineering-Angriffs auf Privatpersonen ist das so genannte *Phishing*, bei dem das Opfer meist per E-Mail aufgefordert wird, seine E-Banking-Zugangsdaten preiszugeben. Des Weiteren wird mit Hilfe von Social-Engineering-Methoden ein Grossteil der *Malware* in Umlauf gebracht. Meist geschieht dies durch E-Mails mit infizierten Dateianhängen oder durch das Anklicken von in der E-Mail vorhandenen Links.

Im Firmenbereich wird Social Engineering vor allem zur Wirtschaftsspionage eingesetzt. Auch in der zweiten Jahreshälfte wurden bis anhin unbekannte Schwachstellen in MS Office-Produkten genutzt, um gezielt Malware auf Firmenrechner zu schleusen. Im Visier der Angreifer sind meist potenzielle Wissensträger, wobei deren Rolle in der Firma sowie deren persönliche Interessen vorgängig in Erfahrung gebracht werden. Mit diesem Wissen lassen sich die Social-Engineering-Angriffe besonders erfolgreich durchführen, beispielsweise indem die Opfer dazu verleitet werden, infizierte Dateien zu öffnen (*Spear-Phishing*). Doch nicht nur Social-Engineering-Angriffe über das Internet sind für Firmen problematisch. So ist es auch möglich, sich beispielsweise mit einem Drucker unter dem Arm und unter Vortäuschung einer falschen Identität Zugang zu Gebäuden und Büroräumen zu verschaffen, um heikle Daten einzusehen.

Aus Sicht von MELANI wird Social Engineering weiter an Bedeutung gewinnen, weil die aktuellsten Clientbetriebssysteme zunehmend bessere Schutzmechanismen einsetzen. Dank dieser Massnahmen lassen sich selbst unbekannte Schwachstellen nicht mehr so einfach ausnutzen. Entsprechend fallen viele der altbewährten *Angriffsvektoren* weg und Malware gelangt, im besten Fall, nur noch durch Doppelklicken ausführbarer Dateien auf ein System. Dieser Trend dürfte sich in zwei bis drei Jahren noch verstärken.

Beispiele für Social-Engineering-Angriffe sind in Kapitel 5.2 zu finden, während in Kapitel 6 Empfehlungen für die Prävention von Social-Engineering-Angriffen aufgeführt werden.

2.2 Spam

Spam-Mails nahmen in der zweiten Jahreshälfte stark zu. Gemäss mehreren Studien machte Spam Ende 2006 etwa 80% bis 90% des gesamten E-Mail-Verkehrs aus.[1]

Insbesondere die Anteile des so genannten „Image-Spams“ haben zugenommen. „Image-Spam“-Nachrichten enthalten zufällige, in ihrer Kombination sinnlose Wörter als Inhalt sowie

[1] Siehe dazu:
http://www.postini.com/news_events/pr/pr110606.php; http://www.postini.com/news_events/pr/pr120606.php; http://www.barracudanetworks.com/ns/news_and_events/news.php?nid=238; http://www.f-secure.de/f-secure/pressroom/news/fs_news_20070111_1_deu.html (Stand: 5.02.2007).

ein Bild als angehängte Datei (Attachment). Die eigentliche Spam-Nachricht befindet sich im Bild. Die Bilder werden vor dem Versand von *Botnetz*-Rechnern aus marginal verändert (z.B. in ihrer Höhe oder Breite), so dass auch nach bekannten Bildern suchende Spam-Filter sie nicht mehr erkennen können. Der Grossteil der Spam-Nachrichten wird weiterhin über Botnetze versandt. Dies erschwert ihre Filterung zusätzlich, da die Sender-*IP-Adressen* ständig wechseln. So schaffen es Spammer zunehmend, die in den letzten Jahren besser gewordenen Verteidigungsmechanismen gegen Spam zu umgehen.

Eine besonders verbreitete Masche ist diejenige des „Stock Pump and Dump Spams“: Spam-Nachrichten werben für den Kauf von Aktien. Die Spammer kaufen sich vor dem Versand Aktien der betreffenden Firmen, die dann während der Spamwelle teilweise stark an Wert gewinnen, anschliessend jedoch wieder auf den Anfangsstand zurückfallen. Der Spammer hat inzwischen seinen Anteil verkauft und die Preisdifferenz kassiert – während die anderen Aktienkäufer, den Wertzerfall akzeptieren müssen.[2]

Spam hat im Jahr 2006 nicht nur zahlenmässig zugenommen, sondern benötigt aufgrund der mitgeschickten Bilder auch mehr Ressourcen der Internetinfrastruktur. Während dank besserer Filter bis vor kurzem noch mit einem Rückgang gerechnet werden konnte, muss nun befürchtet werden, dass Spam auch künftig ein Problem für die Internetinfrastruktur und die Produktivität der E-Mail-Nutzer bleiben dürfte.

2.3 Daten- und Identitätsdiebstahl

Phishing und Daten- oder *Identitätsdiebstahl* mit *Malware* erlebten in der zweiten Jahreshälfte 2006 einen neuen Höhepunkt. Die „Anti-Phishing Working Group“ verzeichnete zwischen September und Oktober eine Zunahme an Phishing-Webseiten von mehr als 52%. Diese ist vermutlich auf die grössere Verfügbarkeit von Phishing-Kits zurückzuführen, die es auch technisch weniger versierten Phishern erlauben, Phishingseiten zu erstellen. Gleichzeitig wurde eine Zunahme an Malware verzeichnet, die Tatstatureingaben aufzeichnet oder auf sonstige Weise Datendiebstahl mit finanziellem Motiv durchführt (siehe auch Kapitel 2.4 und 3.1).[3]

Gewisse Arten solcher Malware suchen den gesamten Computer sowie Netzwerkshares nach finanziell verwertbaren Informationen ab, andere zeichnen sämtliche Tastatureingaben auf, sobald eine den Angreifer interessierende Webseite (z.B. Bankenwebseite) angesurft wird. Im Fall einer Bankenwebseite werden die gestohlenen Daten beispielsweise für unrechtmässige Finanztransaktionen benutzt – eine Technik, die das Phishing (d.h. das Versenden von E-Mails, die zur Preisgabe der Login-Daten verleiten sollen) ergänzt.

Eine andere Form von Identitätsdiebstahl geschieht durch Malware, die den Browser manipuliert und so während der E-Banking-Sitzung direkt verfälschen kann, was der Browser darstellt – so merkt das Opfer nicht einmal, dass statt dessen eine andere Zahlung ausgelöst worden ist.

---

[2] Der Gewinn für die Spammer beläuft sich auf jeweils fast 6% gemäss einer Studie aus den USA: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553. Siehe auch: http://www.securityfocus.com/print/news/11435 (Stand: 5.2.2007).

[3] Siehe http://www.antiphishing.org; http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html (Stand: 6.2.2007).

Im Juli ereignete sich zudem in den USA ein erfolgreicher *Man-in-the-Middle*-Angriff gegen ein Finanzinstitut, mit dem die so genannte *Zwei-Faktor-Authentifizierung* umgangen werden konnte (siehe dazu auch Kapitel 3.1 und 5.3).

Opfer von Daten- und Identitätsdiebstahl sind insbesondere Heimanwender, aber auch Unternehmen. Selbst wer glaubt, auf seinem Rechner keine wichtigen Dokumente zu speichern, verfügt dennoch über viele Daten, für die sich Angreifer interessieren. Abgesehen haben es die Angreifer auf jede Art von Daten, die in Geld umzumünzen sind. Das können Passwörter, Daten zur Benutzung von Identitäten von Privatpersonen, Firmengeheimnisse, Kreditkartendaten, Kontoinformationen, Login-Daten für Online-Spiele, Lizenz-Keys für Software, usw. sein.

Angegriffen wird vermehrt mit Malware, die von Antiviren-Software immer weniger zuverlässig erkannt werden kann (siehe Kapitel 2.4). Betroffen sind Firmenrechner, Computer von Heimanwendern, aber auch Webserver, über die E-Commerce-Anwendungen abgewickelt werden und dem Angreifer wertvolle Kreditkartendaten in die Hände geben könnten.[4]

Nach wie vor finden aus dem asiatischen Raum sehr gezielte Wirtschaftsspionageangriffe gegen Unternehmen und Betreiber *kritischer nationaler Infrastrukturen* statt – auch in der Schweiz (siehe auch Kapitel 5.2 sowie den letzten Halbjahresbericht, Kapitel 2.2).

Eine Einschätzung zur weiteren Entwicklung dieser Gefahr wird in Kapitel 3.1 vorgenommen, während Kapitel 4.1, 4.2, 5.2 und 5.3 Beispiele aufgreifen.

2.4 Malware / Angriffsvektoren

Die Zunahme gezielt eingesetzter *Malware*, beispielsweise in Form *Trojanischer Pferde,* und die gleichzeitige Abnahme grossflächiger und einfach wahrzunehmender Malwareausbrüche in Form von *Würmern* setzten sich auch in der zweiten Jahreshälfte fort. Aufgrund verbesserter Schutzmassnahmen bei den Betriebssystemen nutzen Angreifer immer öfter *Sicherheitslücken* in client-seitigen Applikationen aus, um Malware zu installieren. Darunter fallen pikanterweise Sicherheitssoftware (Antivirensoftware, *Firewalls* etc.), Hardware-Treiber (z.B. für *WLAN*-Karten), MS Office-Produkte, aber auch Plug-Ins wie beispielsweise Adobes Flash Player oder Acrobat Reader. Zunehmend ausgenutzt werden auch Sicherheitslücken in Webapplikationen, die anschliessend vom Angreifer übernommen und ausspioniert oder als Verteiler für Malware missbraucht werden.[5]

An Bedeutung gewonnen haben Infektionen durch blosses Surfen im Internet. Durch zufälligen Besuch oder nach dem Anklicken eines Links in einer betrügerischen Mail- oder Instant-Messaging-Nachricht wird der Computer auf einer präparierten Webseite infiziert (so genannte „Drive-by-Infektionen“). Vermehrt fallen auch Webseiten seriöser Anbieter darunter, insbesondere „Social Networking“-Seiten, die von Benutzern generierten Inhalt zur Verfü-

[4] Siehe auch:
http://www.net-security.org/dl/articles/Report-DOJ_Computer_Crime_Prosecutions.pdf;
http://www.computerworld.cz/cw.nsf/id/CDC9ECF819BAAACCC125726A0069222E/$File/McAfee_wp_id_theft_de.pdf; http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html; http://www.fightidentitytheft.com;
http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html (Stand: 06.02.2007).

[5] Siehe http://www.theregister.co.uk/2006/09/18/web_vulnerabilities/; http://cve.mitre.org;
http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html (Stand: 7.2.07).

gung stellen.[6] Die infizierten Rechner werden anschliessend meist zu einem *Botnetz* zusammengeschlossen.

Ziel der Malwareentwickler ist es, die Erkennung der Malware möglichst lange zu verhindern. Die Erkennungsrate signaturbasierter Sicherheitsprogramme nimmt entsprechend ab, wodurch solche Programme je länger je weniger ausreichenden Schutz vor aktuellen Gefahren bieten können.

Gleichzeitig verschieben sich die Angriffsvektoren auf das Internet: Drive-by-Infektionen über Webseiten (wie z.B. „Social Networking"- oder gehackte Internetseiten) nehmen zu. Unüberlegtes Surfen im Internet ist daher eine der grössten Gefahren, die insbesondere von Unternehmen ernst genommen werden sollte.

Beispiele sind in den Kapiteln 5.2 und 5.3 zu finden.

3 Tendenzen / Allgemeine Entwicklungen

3.1 Bedrohungen für den Finanzsektor

Immer mehr Finanzinstitute in den USA und anderen Ländern verstärken ihre E-Banking-Sicherheit und führen *Zwei-Faktor-Authentifizierung* ein. Je mehr die Sicherheit durch technische Massnahmen zunimmt, desto wahrscheinlicher werden neuartige Angriffe gegen E-Banking-Authentifizierungs-Systeme. Bereits ist im Untergrundmarkt ein Toolkit aufgetaucht, mit dem auch technisch weniger erfahrene Angreifer *Man-in-the-Middle*-Angriffe zu *Phishing*-Zwecken implementieren können.

Für das Jahr 2007 ist zu erwarten, dass die bis anhin selten beobachteten Man-in-the-Middle-Angriffe gegen E-Banking-Authentifizierungs-Systeme zunehmen und auch gegen Schweizer Banken eingesetzt werden könnten (siehe für ein Beispiel aus den USA Kapitel 5.3).

Phishing im klassischen Sinn (d.h. Versenden von E-Mails, die zur Angabe von Login-Daten auffordern) wird weiter vorkommen. Der Trend bei den unrechtmässigen Finanztransaktionen im E-Banking, mit denen Bankkonten geplündert werden, geht aber in Richtung clientseitiger Malware (welche die Login-Daten vom Opfer unbemerkt stiehlt) und Angriffe in Echtzeit (wie beispielswiese Man-in-the-Middle-Angriffe).

Die aktuelle Lage wird in Kapitel 2.3 eingeschätzt, Beispiele sind in den Kapiteln 4.1, 4.2, 5.2 und 5.3 zu finden.

[6] Siehe: http://www.aladdin.com/news/2006/eSafe/mySpace.asp (Stand: 7.2.07).

3.2 Cybercrime-Markt ist etabliert: Konsolidierungsphase

Der cyberkriminelle Markt ist etabliert: Mit *Spam*-Versand, Vermietung von *Botnetzen*, der Entwicklung von *Malware*, der Suche nach *Sicherheitslücken*, Expertisenerstellung in Geldwäsche und anderen Tätigkeiten lässt sich Geld verdienen. Insbesondere besteht ein lukrativer Markt für gestohlene Daten (siehe für Beispiele Kapitel 5.3).

Auch die organisierte Kriminalität hat entdeckt, dass sie ihre Geschäfte – insbesondere Betrug, Diebstahl oder Erpressung – im virtuellen Raum mit weniger Risiken abwickeln kann.

Cyberkriminalität ist ein sich lohnendes Geschäft mit relativ kleinen Risiken. Statt einem Opfer eine grosse Summe zu stehlen, entwenden Cyberkriminelle bei vielen Opfern verhältnismässig wenig. Mit technischen Mitteln verschleiern sie ihren wahren Standort und können daher nur schwer gefasst werden.

Während die Angriffe oft über osteuropäische, asiatische oder südamerikanische Länder abgewickelt werden, sind die Urheber keinesfalls nur in diesen Regionen zu suchen. Aber so lange der Informationsaustausch zwischen den Strafverfolgungsbehörden sowie die Gesetzeslage auf internationaler Ebene nicht verbessert und abgestimmt werden, wird es sehr schwierig bleiben, Cyberkriminelle zu identifizieren und festzunehmen.

MELANI geht daher davon aus, dass sich der Markt weiter konsolidieren wird und die Tendenz zu einer weiteren Vergrösserung und Professionalisierung der Cybercrime-Szene bestehen bleibt. Beispiele sind in Kapitel 5.3 zu finden.

4 Aktuelle Lage ICT Infrastruktur national

4.1 Angriffe

Phishing weiterhin verbreitet

Im zweiten Halbjahr 2006 wurde in der Schweiz eine hohe Zahl an Wirtschaftsdelikten über das Internet verzeichnet. *Phishing* zählte dabei zu den beliebtesten kriminellen Machenschaften. Im August erhielten die Kundinnen und Kunden der Migros Bank eine Phishing-E-Mail mit der Aufforderung, den Zugriffscode ihres Kontos anzugeben, um dessen Richtigkeit überprüfen zu lassen. Das Finanzinstitut beschloss daraufhin die Abarbeitung der E-Banking-Transaktionen vorübergehend einzustellen, um allfällige, mit gestohlenen Codes vorgenommene Transaktionen blockieren zu können.

Spuren von Phishing-Attacken im Ausland führten auch in die Schweiz. Im September warnte das Finanzinstitut Australia and New Zealand Banking Group Limited (ANZ) die Schweizer Behörden, dass sich hinter einer Schweizer Domäne eine Phishing-Webseite verstecke. Wenige Tage später ereignete sich ein ähnlicher Fall; diesmal waren die Smile Internet Bank und die Suntrust Bank betroffen. Nach Abklärung des Sachverhalts wurden die Domänenamen blockiert.

Obwohl die jüngsten Phishing-Attacken nach anderen Mustern ablaufen (siehe Kapitel 2.3, 3.1 sowie die Beispiele in Kapitel 5.3), gibt es das klassische Phishing auch weiterhin. Alle in dieser Branche tätigen Unternehmen (Banken, Online-Auktionshäuser, usw.) tun gut daran, vorsichtig zu bleiben und ihre Präventionsbemühungen fortzusetzen.

In PDF-Dateien versteckte Malware

Ein Schweizer Finanzinstitut wurde zur Zielscheibe zweier unterschiedlicher Vorfälle.

Der erste ereignete sich Anfang September und betraf eine *Phishing*-E-Mail, die im Namen eines Schweizer Finanzinstitutes verschickt worden war. Ihre Empfängerinnen und Empfänger wurden aufgefordert, die Logindaten für ihr Bankkonto einzugeben. Allerdings war dieser Angriff nicht dazu geeignet, die Sicherheitsvorkehrungen der Bank zu umgehen und zielte auch nicht direkt auf deren Kunden.

Der zweite Vorfall stand im Zusammenhang einer angeblich vom Informationsportal N-24 stammenden E-Mail, in der behauptet wurde, dem Schweizer Finanzinstitut seien bei einem Raubüberfall 6 Milliarden Euro gestohlen worden. Um den ganzen Artikel zu lesen, müsse man aus dem Anhang der E-Mail ein PDF-Dokument herunterladen – nur handelte es sich dabei in Wirklichkeit um Malware, nämlich um ein *Trojanisches Pferd* der Malware-Familie Goldun.

4.2 Kriminalität

Fiktive Banken wollen vom Ruf des Finanzplatzes Schweiz profitieren

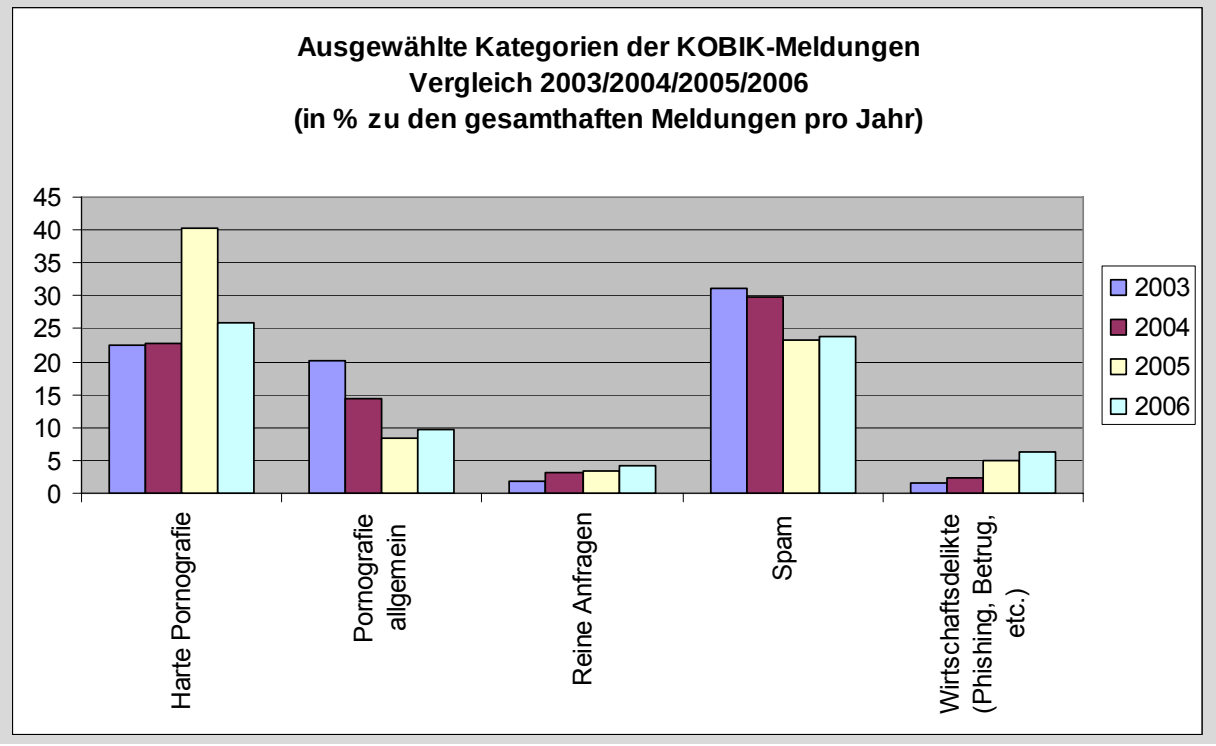
Man stösst im Internet immer wieder auf fiktive Banken, die vorgeben, Filialen in der Schweiz zu haben oder sich mit dem Adjektiv „swiss“ schmücken. Bereits 2003 tauchten Webseiten wie “www.swissbankservices.com”, “www.swissprivatebank.com” oder “www.swissroyalbank.com” auf. Offenbar wird versucht, das Ansehen der schweizerischen Finanzinstitute zu nutzen, um Opfer anzulocken. Der Bericht der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK (www.kobik.ch) “Wirtschaftskriminalität im Internet auf dem Vormarsch” befasst sich eingehend mit dieser Betrugsvariante, welche auch 2006 vorgekommen ist.

Meldungen aus verschiedenen Quellen zufolge versteckte sich beispielsweise hinter der Webseite “www.swiss-invest.biz” ein fiktives Finanzinstitut, dessen Absicht es war, “Finanzagenten” anzuwerben. Besser bekannt sind diese unter der Bezeichnung “money mules”. Das sind Personen, die sich gegen Kommission und durch das zur Verfügung stellen eigener Bankkonten an der Überweisung von Geldern unrechtmässiger Herkunft beteiligen (→ Geldwäscherei, siehe nächster Abschnitt). Eine weitere fiktive Bank bediente sich der URL www.rhssonline.com. Auf ihrer Webseite stellte sie sich als Bank mit Sitz in der Schweiz vor und ihr Angebot umfasste die klassischen Finanzprodukte des E-Bankings. Ausserdem wurde die Möglichkeit geboten, online ein Bankkonto zu eröffnen.

Es hat noch offene Stellen für Finanzagenten!

Mittels E-Mails, die im Dezember an verschiedene Schweizer Bürgerinnen und Bürger gelangten, wurden Finanzagenten gesucht. Die Mail stammte von einem fiktiven Finanzdienstleister mit Namen Porex GmbH mit Sitz in Sursee. Ein Finanzagent müsse sich nur eine bestimmte Summe auf sein Konto überweisen lassen, könne für den geleisteten Dienst einen Anteil als Provision behalten und müsse dann die Differenz auf ein drittes Konto weiterleiten. Die versprochene Provision sollte bis zu 10 Prozent der erhaltenen Summe betragen. Wer akzeptierte, machte sich allerdings der Beihilfe zur Geldwäscherei schuldig. Die zu überweisenden Summen stammten von Konten, die mit Hilfe betrügerischer *Phishing*-Methoden geplündert worden waren. Im zweiten Halbjahr 2006 registrierte MELANI zahlreiche ähnliche Fälle. Nebst Porex hatte es auch eine unter dem Namen Vicent Reality tätige Firma auf Schweizer Bürgerinnen und Bürger abgesehen. Dieses Unternehmen, das sich als im Immobilienbereich tätiges Finanzinstitut ausgab, behauptete in einer E-Mail, verschiedene Schweizer Kundinnen und Kunden hätten sich für den Erwerb von Immobilien an der Côte d'Azur, in Griechenland und in Spanien interessiert. Es fehle nur noch ein Finanzagent als Vermittler, damit der Vertragsabschluss vollzogen werden könne.

Die Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK verzeichnet seit 2003 eine Zunahme von Meldungen, welche die Wirtschaftskriminalität im Internet betreffen. Dieser Trend hat sich auch 2006 fortgesetzt (siehe Grafik).



Verurteilung eines Hackers wegen unbefugter Datenbeschaffung

Zum ersten Mal seit der Einführung des Artikels 143 StGB im Jahre 1995 fällte ein Schweizer Gericht ein Urteil wegen unbefugter Datenbeschaffung. Im Kanton Bern wurde im Dezember ein Informatikexperte der unbefugten Beschaffung und Zerstörung von Daten, die seinen Konkurrenten und Kunden gehörten, für schuldig befunden.

Der betreffende Mitarbeitende der Firma Datasport hatte zwischen November 2003 und Juni 2004 ein Dutzend *Trojanische Pferde* verschickt, mit denen er das Verhalten der Konkurrenz

ausspionieren und deren Geschäftsgang stören wollte. Auf diese Weise soll er an 27'000 sensible Datensätze herangekommen sein und Offertanfragen im Maileingang der ausspionierten Firmen gelöscht haben. Die Berner Kantonspolizei schaltete sich ein, nachdem eine der Firmen Meldung erstattet hatte, weil sie den Verdacht hegte, ausspioniert zu werden. Der verurteilte Informatiker benutzte eine Software, die er von einer US-Firma erworben hatte, welche in der Entwicklung von Anwendungen zur Fernüberwachung von Computern spezialisiert ist.

4.3 Diverses

Initiative der Schweizer Provider zwecks Spambekämpfung

Die vier grössten Internet Service Provider (ISP) der Schweiz haben eine Initiative mit dem Ziel der gemeinsamen *Spam*bekämpfung gestartet. Bluewin, Cablecom, Sunrise und Green schalteten im November eine Webseite live (www.stopspam.ch), auf der man Informationen zur *Spam*-Thematik findet. Die Webseite enthält Ratschläge zur Spambekämpfung und beschreibt einschlägige technische Massnahmen, wie zum Beispiel die Aktivierung der SMTP-Authentifizierung beim E-Mail-Versand.

5 Aktuelle Lage ICT Infrastruktur International

5.1 Pannen

Internetverkehr in Südostasien wegen Erdbebenschäden beeinträchtigt

Ein Erdbeben vor Taiwan beschädigte am 26. Dezember 2006 unter anderem auch Unterseekabel, über die Telefon-, Daten- und Internetverbindungen abgewickelt werden. In der Folge mussten weit über 100 Millionen Betroffene erhebliche Beeinträchtigungen im Internetverkehr hinnehmen.

Während mehrerer Tage waren insbesondere Internetverbindungen zu ausländischen Webseiten für Benutzer in China, Taiwan, Singapur und Südkorea massiv eingeschränkt. Durch den Unterbruch waren offenbar auch wichtige Finanzdienste und Unternehmen betroffen. Beispielsweise konnte die Reuters Group PLC Kunden in Südkorea und Hongkong nicht mehr mit den aktuellsten Finanzdaten versorgen. Die Reparaturarbeiten erstreckten sich

über mehrere Wochen und die Verbindungen konnten erst allmählich und schrittweise wieder hergestellt werden.[7]

Der Vorfall illustriert, wie abhängig vom Internet inzwischen ganze Wirtschaftsräume geworden sind. Werden kritische Verbindungen oder Knotenpunkte der globalen Kommunikationsnetzwerke in Mitleidenschaft gezogen, kann dies erhebliche und nur schwer vorhersehbare Auswirkungen auf die Wirtschaft in den betroffenen Regionen haben.

5.2 Attacken

Beispiele für Angriffsvektoren: Instant Messaging, E-Mails, Sicherheitslücken in Browser-Plug-Ins, „Social Networking"-Webseiten, Software-Downloads

Einzelne Angriffsvektoren werden von Angreifern zunehmend kombiniert. Über *Instant Messaging*-Dienste (IM) sind beispielsweise im zweiten Halbjahr 2006 Angriffe vorgekommen, die entweder *Malware* gleich im Attachment („Pipeline" im September) oder aber Links zu präparierten Webseiten enthielten („Heartworm", ebenfalls im September). Die IM-Nachrichten schienen von einem befreundeten Kontakt zu kommen und forderten zum Anklicken des Attachments oder eines Links auf (siehe zu *Social Engineering* Kapitel 2.1 und 6). Wer den Anweisungen in den Nachrichten folgte, machte seinen Rechner unbemerkt zum Mitglied in einem *Botnetz*.[8]

Ebenfalls weit verbreitet ist Software, die sich als etwas anderes ausgibt (*Trojanisches Pferd*). Beispielsweise gab eine Malware vor, ein *Plug-In* für den Firefox-Browser zu sein. In einem anderen Beispiel musste auf einer Pornoseite ein bestimmter Mediaplayer heruntergeladen werden, angeblich um die Filme zu sehen. Statt des Mediaplayers installierte das Opfer Malware, die zum Ausspionieren oder für *Phishing* eingesetzt werden kann („Zcodec", Ende August). In beiden Beispielen wurden die Opfer unter Anwendung von Social-Engineering-Techniken per Spam-Mail angelockt.

Im Juli und Dezember tauchte auf „MySpace", der bekanntesten Social Networking"-Webseite, Malware auf. Die Infektion im Juli war über eine Bannerwerbung erfolgt, die eine Internet-Explorer-*Sicherheitslücke* ausnutzte. Der Angriff vom Dezember bediente sich hingegen einer Sicherheitslücke in Apples Quick-Time-Player.[9]
Webseiten mit Benutzer-generiertem Inhalt laden beinahe dazu ein, von Kriminellen ausgenutzt zu werden. Bei den herkömmlichen Webseiten stellt man fest, dass während früher fast ausschliesslich solche mit zweifelhaften Angeboten betroffen waren, heute zunehmend auch Webseiten mit seriösen Angeboten präpariert werden. Im September war der US-

[7] Siehe: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006860; http://www.heise.de/newsticker/meldung/83007 (Stand: 15.2.07).
[8] Siehe: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003623&source=rss_news50 (Stand: 8.2.07).
[9] Siehe: http://www.heise.de/newsticker/meldung/75707, http://www.securityfocus.com/news/11427; http://www.theregister.co.uk/2006/08/10/fsocial_sites_breed_malware/; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005607&intsrc=hm_list (Stand: 8.2.07).

Internetauftritt von Samsung kompromittiert und zum Verteilen von Malware missbraucht worden; im Dezember wurde der Webserver von Asus zum selben Zweck missbraucht. Immer häufiger werden Sicherheitslücken in Web-Applikationen entdeckt, so dass der Missbrauch von Webseiten in nächster Zeit zunehmen dürfte.[10]

Allgemein konzentrieren sich Angreifer vermehrt auf Applikationen oder Hardware-Treiber und weniger auf die Betriebssysteme, welche tendenziell sicherer werden. Im letzten Halbjahr wurden beispielsweise Sicherheitslücken in Adobes Acrobat Reader und Flash-Player, in Apples Quick-Time-Player oder in Treibern für *WLAN*-Karten genutzt (für die Sicherheitslücken in Microsoft-Produkten siehe den separaten Beitrag weiter unten).[11]

Problematisch ist, dass Antivirensoftware immer weniger zuverlässig wird. Der Grund dafür liegt in den zahlreichen Varianten, die Malware-Entwickler in immer kürzeren Abständen produzieren. Sobald eine Variante entdeckt und in Antiviren-Signaturen aufgenommen wird, setzen die Angreifer bereits die nächste ein. Von „Warezov“ oder „Stratio“, einer primär für den Spam-Versand eingesetzten Malware, tauchten im November beispielsweise über 1000 Varianten auf.[12]

Angriffsmethoden werden stärker kombiniert: E-Mails oder IM-Nachrichten mit Links auf präparierte Webseiten tauchten vermehrt auf.

Aufgrund der weit verbreiteten Sicherheitslücken in Webapplikationen und der zunehmenden Popularität von Webseiten mit Benutzer-generiertem Inhalt (der entsprechend leicht manipuliert werden kann), taucht Malware häufiger auf legitimen, offiziellen Homepages auf. In Kombination mit der Zunahme von Sicherheitslücken in Applikationen und Plug-Ins wird es wahrscheinlicher, beim normalen Surfen mit Malware infiziert zu werden.

Eine Einschätzung dieser Bedrohungen wird in Kapitel 2.4 vorgenommen. Kapitel 2.1 thematisiert die eingesetzten Social-Engineering-Techniken, während Kapitel 6 erläutert, wie man sich vor solchen Gefahren schützen kann.

Erneute Exploits von Sicherheitslücken in Microsoft-Produkten – Einsatz zur gezielten Wirtschaftsspionage, auch in der Schweiz

Einige der Sicherheitslücken wurden erst aufgrund von *0-Day-Exploits* entdeckt, wie beispielsweise in Microsoft PowerPoint im Juli,[13] im Internet Explorer im September,[14] oder gleich mehrfach in Word im Dezember.[15] Nach Bekanntgabe und Behebung von Sicherheitslücken durch Microsoft jeweils am zweiten Dienstag jeden Monats („Patch-Tuesday“) tauch-

[10] Siehe http://www.theregister.co.uk/2006/09/18/web_vulnerabilities (Stand: 7.2.07).
[11] Siehe z.B. http://www.theregister.co.uk/2006/08/04/hackers_bypass_os/ (Stand: 7.2.07).
[12] Siehe http://www.sophos.com/virusinfo/whitepapers/sophos-security-threats-2007_wsrus (Stand: 7.2.07).
[13] Siehe http://isc.sans.org/diary.html?storyid=1484 (Stand: 12.2.07).
[14] Siehe http://www.heise.de/newsticker/meldung/78372; http://isc.sans.org/diary.html?storyid=1727 (Stand: 12.2.07).
[15] Siehe http://www.heise.de/newsticker/meldung/82521; http://blogs.technet.com/msrc/archive/2006/12/15/update-on-current-vulnerability-reports.aspx; http://isc.sans.org/diary.html?storyid=1940 (Stand: 12.2.07).

ten häufig innert weniger Stunden *Exploits* auf, welche die bekannt gewordenen Sicherheitslücken ausnutzten.[16]

Angriffe, welche die Office-Sicherheitslücken ausnutzen, erfolgen meist sehr gezielt und betreffen gemäss Microsoft nur wenige ausgewählte Opfer.[17] Insbesondere für die mit „Titan Rain" bezeichneten, seit längerem anhaltenden, gezielten Wirtschafts- und Industrie-Spionageangriffe aus Nordostasien (siehe auch den letzten Halbjahresbericht) werden diese Sicherheitslücken häufig eingesetzt. Solche Angriffe ereigneten sich in der zweiten Jahreshälfte 2006 beispielsweise in den USA gegen das State Department, das Commerce Department oder das Naval War College.[18] Auch in der Schweiz haben sich erneut solche Angriffe gegen die Rüstungsindustrie ereignet.

Für das Jahr 2007 ist weiterhin mit Sicherheitslücken und 0-Day-Exploits gegen Microsoft Office Produkte und den Internet Explorer zu rechnen. Entsprechend dürften die gezielten Spionage-Attacken speziell gegen Betreiber *kritischer Infrastrukturen*, Regierungen und Regierungszulieferer (speziell aus der Rüstungsindustrie), aber auch allgemein gegen Firmen, eher zunehmen. Die Schweiz dürfte davon ähnlich betroffen sein wie andere westliche Industriestaaten.

Im Falle der Angriffe aus Nordostasien dürften die Opfer vermehrt auch über präparierte, für das Fachgebiet des Mitarbeitenden wichtige Webseiten unter Ausnutzung von Office-Sicherheitslücken infiziert werden.

Kapitel 2.1 befasst sich mit Social Engineering, während Kapitel 6 mögliche Präventionsmassnahmen gegen solche Angriffe thematisiert.

USA: Anzahl verlorener Datensätze mit persönlichen Inhalten durchbricht 100-Millionen-Marke

Wie das US-amerikanische „Privacy Rights Clearing House" Mitte Dezember 2006 bekannt gab, waren seit Anfang 2005 persönliche Daten von über 100 Millionen US-Bürgern verloren gegangen.[19] Ursache dafür waren Angriffe, Laptop-Diebstähle oder Verluste von Backupmedien. Besonders betroffen in den USA sind das Gesundheitswesen sowie Regierungsstellen.[20] Gemäss einer Studie wird jedoch lediglich ein kleiner Teil der Betroffenen später tatsächlich Opfer eines Identitätsdiebstahls.[21]

---

[16] Siehe: http://blog.washingtonpost.com/securityfix/2006/10/patch_tuesday_exploit_thursday.html. Eine gute Übersicht über das Problem und Statistiken zu entdeckten Sicherheitslücken bietet eine Serie von Artikeln der Washington Post: http://blog.washingtonpost.com/securityfix/2007/01/microsoft_achilles_heel_offic_1.html; http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html; http://blog.washingtonpost.com/securityfix/2007/01/cricital_microsoft_mozilla_pat.html (Stand: 12.2.07).

[17] Siehe für eine Stellungnahme von Microsoft: http://blogs.technet.com/msrc/archive/2006/12/08/what-very-limited-targeted-attacks-means.aspx (Stand: 12.2.07).

[18] Siehe http://www.cnn.com//2006/US/07/11/state.hackers.ap/index.html; http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html; http://washingtontimes.com/national/20061130-103049-5042r.htm (Stand: 12.2.07).

[19] Siehe http://www.privacyrights.org/ar/ChronDataBreaches.htm (Stand: 12.2.07).

[20] Siehe http://www.gao.gov/new.items/d06676.pdf; http://oversight.house.gov/Documents/20061013145352-82231.pdf (Stand: 12.2.07).

[21] Siehe http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003343 (Stand: 12.2.07).

Im August wurde beispielsweise bekannt, dass einer US-amerikanischen Bank sowie dem US Department of Transportation persönliche Kundendaten abhanden kamen, weil Laptops gestohlen worden waren. Wenige Tage später musste AT&T bekannt geben, dass durch die Kompromittierung eines ihrer Webshops die Kreditkartendaten von etwa 19'000 Kunden gestohlen worden seien.[22] Im Dezember gab die University of California/Los Angeles (UCLA) bekannt, durch einen Hackerangriff seien persönliche Daten von über 800'000 Angestellten, Studenten und Dozenten preisgegeben worden.[23] Boeing schliesslich verlor ebenfalls im Dezember durch einen Laptopdiebstahl persönliche Daten von 382'000 Angestellten.[24]

Die Vorfälle aus den USA illustrieren nach Einschätzung von MELANI einen Trend, der vermehrt auch in der Schweiz an Bedeutung gewinnen dürfte. Cyberkriminelle interessieren sich für alle Arten persönlicher Daten, die sich (im Untergrund) zu Geld machen lassen.

Auch wenn gezielte Angriffe auf Webshops oder Datendanken häufiger vorkommen, gehen noch immer die meisten Personendaten durch Verluste oder Diebstähle mobiler Geräte verloren. Unternehmen, die sensible Daten handhaben, wird daher empfohlen, Daten auf mobilen Geräten (insbesondere Laptops, PDAs, aber auch auf Backupbändern) zu verschlüsseln. Betreibern von Webshops wird empfohlen, ihre Web-Applikationen aktuell zu halten und Kreditkartendaten besonders zu schützen. Das britische „Centre for the Protection of National Infrastructure CPNI“ (vormals NISCC) stellt nützliche Hinweise dafür bereit.[25]

USA: Systeme einer Kläranlage durch Laptop eines Angestellten infiziert

Anfang Oktober 2006 erhielten Hacker über einen infizierten Laptop Zugriff auf die Computersysteme eines Wasserwerkes in Harrisburg, Pennsylvania (USA). Der Laptop eines Angestellten wurde über das Internet mit *Malware* infiziert, mit welcher die Kontrolle über den Laptop erlangt werden konnte. Offenbar installierten die Angreifer anschliessend *Spyware* auf dem Computer, um sensible Daten auszuspionieren. Auch wenn gemäss dem FBI das Wasserwerk nicht gezielt angegriffen, sondern der Laptop eher zufällig infiziert worden sei, wäre eine Störung der Steuerungsanlage des Wasserwerkes durchaus denkbar gewesen. Möglich wäre beispielsweise eine Manipulation des Chlorgehaltes im Trinkwasser gewesen.[26]

Die zur Überwachung und Steuerung von Industrieanlagen konzipierten *„Supervisory Control and Data Acquisition“ (SCADA)* Systeme setzen zunehmend auf Standard-Internet-Technologien und Protokolle und werden mit dem Internet verbunden. Damit sind SCADA-Systeme vergleichbaren Bedrohungen ausgesetzt, wie wir sie vom Internet her kennen. Anstrengungen, die durch SCADA-Systeme gesteuerten Industrieanlagen angemessen zu schützen, müssen voran getrieben werden.

Das britische „Centre for the Protection of National Infrastructure (CPNI)“ hat eine Reihe von Best-Practice-Empfehlungen für den Einsatz von SCADA-Systemen publiziert.[27]

---

[22] Siehe http://www.computerworld.com/action/article.de?command=viewArticleBasic&articleId=9002828 sowie http://www.heise.de/newsticker/meldung/77455 (Stand: 12.2.07).

[23] Siehe http://www.heise.de/newsticker/meldung/82437 (Stand: 12.2.07).

[24] Siehe http://www.computerworld.com/action/article.de?command=viewArticleBasic&articleId=9006098 (Stand: 12.2.07).

[25] Siehe http://www.niscc.gov.uk/ProtectingYourAssets/ElectronicSecurity/applications.aspx (Stand: 15.2.07).

[26] Siehe http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004659 (Stand: 12.2.07).

[27] Siehe http://www.cpni.gov.uk/Products/guidelines.aspx (Stand: 12.2.07).

5.3 Kriminalität

Phishing / Identitätsdiebstahl: Kosteneinschätzung sowie wichtige Vorfälle (Zwei-Faktor-Authentifizierung umgangen / RockPhish)

Phishing und *Identitätsdiebstahl* haben in der zweiten Jahreshälfte 2006 zugenommen, auch wenn die Verluste verglichen mit traditionellem Betrug noch immer kleiner sind.[28] Allgemein ist es schwierig, Kosten zu benennen. Ohne zwischen Online-Identitätsdiebstahl und traditionellem zu unterscheiden, schätzen die USA und Grossbritannien die Kosten für die letzten Jahre auf mehrere Milliarden Dollar.[29] Für die Schweiz liegen keine vergleichbaren Schätzungen vor.

Im Juli wurde ein erfolgreicher *Man-in-the-Middle*-Angriff gegen das durch *Zwei-Faktor-Authentifizierung* geschützte E-Banking-Portal der Citibank in den USA durchgeführt und die Angriffsart damit auch zum ersten Mal der breiten Öffentlichkeit bekannt. Bei der Zwei-Faktor-Authentifizierung muss sich der Kunde nicht nur mit Benutzernamen und Passwort anmelden, sondern benötigt zusätzliche Angaben, wie beispielsweise eine Streichlistennummer oder, wie im Fall der Citibank, einen von einem Hardware-Token regelmässig neu generierten Code. Beim Citibank-Angriff wurde das Opfer per E-Mail auf eine Phishing-Seite gelockt. Diese baute im Hintergrund eine Verbindung zum E-Banking-Server der Citibank auf. Während der Bankkunde glaubte, mit der Bank zu kommunizieren, fing der Phishing-Server (als „Mann in der Mitte“) seine Eingaben ab und leitete diese im Namen des Kunden über die zuvor bereitgestellte Verbindung an den Banken-Server weiter. Nach dem erfolgreichen Login des Angreifers erhielt der Kunde eine Störungsmeldung und der Angreifer konnte im Namen des Opfers Transaktionen auslösen.[30]

Die Zunahme an Phishing-Seiten in der zweiten Jahreshälfte wurde von verschiedenen Seiten “RockPhish” zugeschrieben. Wer oder was „RockPhish“ genau ist, bleibt umstritten – in Berichten wird „RockPhish“ entweder als automatisiertes Tool zur Erstellung von Phishing-Seiten oder aber als Hackergruppe bezeichnet, die hinter etwa der Hälfte der grösseren Phishing-Attacken vermutet wird.[31] „RockPhish“ ist in der Lage, den Standort des Phishing-Servers zu verschleiern, indem es den Verkehr zuerst über einen *Bot* leitet. Der wahre Standort des Phishing-Servers wird so effizient verborgen – kann ein Bot abgeschaltet werden, steuern die Angreifer künftige Opfer einfach über einen neuen Bot auf die noch existierende Phishing-Seite. Aus Sicht der Phishing-Mails scheint es, als wäre für jedes Opfer eine eigene Phishing-URL eingerichtet worden.[32]

---

[28] Siehe z.B. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004429 (Stand: 13.2.07).

[29] Siehe http://www.ftc.gov/os/2003/synovatereport.pdf; http://www.identity-theft.org.uk (Stand: 13.2.07).

[30] Siehe http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html (Stand: 13.2.07).

[31] Siehe z.B. http://en.wikipedia.org/wiki/Rock_Phish (Stand: 13.2.07).

[32] Siehe zu „RockPhish“ (Stand: 13.2.07):
http://blog.washingtonpost.com/securityfix/2006/12/phishing_scams_soared_in_octob.html;
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005958; sowie
http://www.heise.de/tp/r4/artikel/23/23964/1.html.

Eine Einschätzung von MELANI zu Identitätsdiebstahl und Phishing ist in den Kapiteln 2.3 (aktuelle Lage) sowie 3.1 (Tendenzen), weitere Beispiele in den Kapiteln 4.1 und 4.2 zu finden.

Cybercrime und organisierte Kriminalität: Untergrund-Markt mit Handel und Arbeitsteiligkeit ist etabliert – immer mehr und jüngere Teilnehmer

Cyberkriminalität hat sich im Verlauf des Jahres 2006 definitiv zu einer verbreiteten Tätigkeit von Kriminellen entwickelt. Die organisierte Kriminalität hat ebenfalls längst entdeckt, dass sie ihre erprobten Geschäfte – insbesondere Betrug, Diebstahl oder Erpressung – im virtuellen Raum mit weniger Risiken abwickeln kann. Zu diesem Zweck werden vermehrt erfahrene Hacker und auch Teenager rekrutiert, für welche die Cyberkriminalität offenbar eine grosse Anziehungskraft besitzt. IT-Spezialisten werden direkt ab Studium teilweise mit dubiosen Methoden rekrutiert. Viele Cyberkriminelle können von ihrer Tätigkeit leben und gehen ihrem „Beruf" zu Bürozeiten nach wie „gewöhnliche Arbeitnehmer".[33]

Für Handel, Informationsaustausch, Rekrutierung und Zusammenarbeit hat sich ein Untergrundmarkt gebildet. Die Szene ist arbeitsteilig organisiert: Es gibt Spezialisten, die nach *Sicherheitslücken* suchen, diese verkaufen oder *Exploit*-Code dafür entwickeln. Andere wiederum kümmern sich um die Entwicklung von *Malware* und arbeiten gemeinsam und mit professionellen Mitteln an ständig neuen Varianten. *Botherder* konzentrieren sich auf Aufbau und Unterhalt von *Botnetzen*, die sie anschliessend vermieten – sei es für *Distributed Denial of Service (DDoS)*-Angriffe, den Versand von *Spam*, die Verteilung von Malware*, Adware* und *Spyware* oder für die Spionage auf den dem Botnetz zugehörigen Rechnern. Spammer spezialisieren sich auf den Versand von Spam und die Entwicklung von E-Mails, die an Spamfiltern vorbeikommen. Für die Geldwäsche (den Transfer der Gelder von inkriminierten Konten) sowie die Bestellung und Weiterleitung von Artikeln unter Einsatz gestohlener Kreditkartennummern oder E-Bay-Accounts sind Spezialisten in der Szene zu finden oder werden ahnungslose Personen angeheuert. Gehandelt werden auch Informationen zu Sicherheitslücken, Exploits (ein Exploit für Windows Vista wurde im Dezember angeblich für US$50'000 angeboten), Malware für Datendiebstahl (auf Datendiebstahl spezialisiertes *Trojanische Pferd* z.B. für US$1'000 – 5'000), Malware für den Aufbau von Botnetzen (US$5'000 – 20'000), gestohlene Daten (Kreditkarte mit PIN für ca. US$500, US-Fahrausweise für US$150, Kreditkarte mit Security-Code und Ablaufdatum für Online-Einkauf zwischen US$7 und 25), Mietzeit für Botnetze, Expertise für Spamming und vieles mehr.[34]

Eine Einschätzung des cyberkriminellen Untergrunds ist in Kapitel 3.2 zu finden.

---

[33] Siehe: http://www.mcafee.com/us/local_content/white-papers/threat_center/wp_virtual_criminology_report_2007.zip; http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html; http://www.washingtonpost.com/wp-dyn/content/article/2006/12/26/AR2006122600922.html (Stand: 7.2.07).

[34] Siehe http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf; http://www.theregister.co.uk/2006/12/12/cybercrook_xmas_wish_list/; http://www.heise.de/newsticker/meldung/82679 (Stand für alle: 07.02.07).

5.4 Terrorismus

Al-Qaida-Foren mit Terrorverherrlichungen nun auch in Deutsch / vermehrt deutsche Bombenbauanleitungen im Internet

Die „Global Islamic Media Front“ (GIMF) war vor zwei Jahren quasi zur offiziellen Medienagentur Al-Qaidas erklärt worden – inzwischen ist jedoch unklar, ob überhaupt ein direkter Kontakt zwischen der GIMF und Al-Qaida besteht. Im August wurde bekannt, dass die GIMF bereits seit Mai 2006 eine Webseite auf Deutsch betreibt. Über sie werden die neusten Videos, Verlautbarungen und Neuigkeiten der Al-Qaida im Irak nur mit wenigen Tagen Verzögerung auch in Deutsch zur Verfügung gestellt. Die Übersetzungen sind von guter Qualität, so dass davon ausgegangen werden muss, dass es sich nicht um automatisierte Übersetzungen handelt.[35]

Die deutsche, auf die Entwicklung von Sicherheits- und Filterungs-Software spezialisierte Firma „Pan Amp“ teilte ausserdem im Dezember mit, auf dem Internet über 200'000 Bombenbauanleitungen auf Deutsch entdeckt zu haben. Von der einfachen Briefbombe bis zu Bomben, mit denen Züge gesprengt werden könnten, sei alles zu finden.[36]

Bereits in den letzten beiden Halbjahresberichten wurde herausgestrichen, dass die Bedrohung durch den Cyberterrorismus – also den Angriff auf das Internet oder auf kritische *nationale Infrastrukturen* mit informationstechnologischen Mitteln – überschätzt wird. Terroristen nutzen das das Internet jedoch für Propaganda, Ideologisierung, Finanzmittelbeschaffung und Kommunikation.

Auch wenn die Unabhängigkeit der Firma „Pan Amp“ aufgrund ihres Geschäftsfeldes (Internetfilterungen und -überwachungen) in Frage gestellt werden muss, ist ihre Aussage doch ein Hinweis auf die Ernsthaftigkeit des Problems: Auch für deutschsprachige Sympathisanten sind die nötigen Ressourcen im Internet immer leichter zu finden. Zusammen mit der Tatsache, dass insbesondere in Europa ein Potenzial zur Extremisierung und Ideologisierung besteht, muss davon ausgegangen werden, dass diese Entwicklung zu einer Erweiterung des potenziellen Empfängerkreises solcher Botschaften führt.

USA: Finanzwirtschaft vor Al-Qaida-Angriff auf Bankingsysteme gewarnt

Ende November warnte das Computer Emergency Readiness Team (US-CERT) des amerikanischen Department of Homeland Security (DHS) die amerikanische Finanzwirtschaft vor einem drohenden Angriff der Al-Qaida gegen amerikanische Aktienhandelsportale und Bankenwebseiten. Wie das DHS erklärte, erfolgte die Warnung jedoch aus reiner Vorsicht und ohne konkrete Hinweise auf eine drohende Gefahr.[37] Ein Angriff fand nicht statt.

Grund für die Warnung war die Entdeckung eines am 27. November auf einem passwortgeschützten dschihadistischen Forum geposteten Aufrufs unter dem Titel „The Electronic Battle of Guantanamo“. Die US-Finanzwirtschaft sollte mit *Denial-of-Service (DoS)*-Attacken aus Rache für die im Gefängnis auf Guantanamo-Bay, Kuba, einsitzenden Muslime angegriffen

---

[35] Siehe http://www.spiegel.de/politik/deutschland/0,1518,434203,00.html (Stand: 13.2.07).

[36] Siehe http://www.heise.de/newsticker/meldung/82108 (Stand: 13.2.07).

[37] Siehe http://money.cnn.com/2006/11/30/news/economy/al_qaeda/; http://www.spiegel.de/netzwelt/web/0,1518,451862,00.html (Stand für beide: 14.2.07).

werden. Die Angriffe sollten am 1. Dezember beginnen und bis Ende Jahr anhalten. Gleichzeitig rief der Autor der Meldung seine Brüder dazu auf, vorsichtig mit persönlichen Daten umzugehen und wenn möglich immer Anonymisierungssoftware einzusetzen.[38] Am 5. Dezember wurde in einem einschlägigen Forum bekannt gegeben, der Angriff sei abgebrochen worden, weil die Finanzwirtschaft frühzeitig gewarnt worden sei. Die heftigen Reaktionen in den Medien hätten jedoch gezeigt, wie folgenreich Angriffe auf Webseiten seien, die für den Westen wirtschaftlich wichtig sind.[39]

Es ist sehr unwahrscheinlich, dass terroristische Kreise bereits über das notwendige Know-how für einen Angriff auf eine kritische Infrastruktur über das Internet verfügen. Auch in diesem Fall wäre grosses Insiderwissen für einen effektiven Angriff nötig gewesen. Es ist jedoch nicht auszuschliessen, dass Terroristen sich künftig in diesem Bereich Know-how beschaffen könnten. Diese Know-how-Beschaffung konzentriert sich momentan jedoch eher auf die sichere Nutzung des Internets als auf Angriffe gegen dasselbe.

„Technical Mujahid" und „Mujahideen Secrets": Periodisches Magazin zu technischen Fragen sowie Software für Computer- und Internetsicherheit in islamistischen Foren

Am 28. November 2006 wurde erstmals innerhalb passwortgeschützter dschihadistischer Foren ein auf Informationstechnologie und Sicherheit fokussiertes Magazin namens „Technical Mujahid" verteilt. Es wird publiziert von einer Gruppe namens „Al-Fajr Information Center", die bereits mehrfach Gewaltvideos veröffentlicht hatte. Das Magazin soll künftig periodisch erscheinen. Ursache für die Publikation war laut den Editoren ein Ruf des Al-Qaida-Führers im Irak nach technischem Support. Betont wurden im Magazin auch die Notwendigkeit und der grosse Nutzen des Internets für den Dschihad.

Das 64-seitige Magazin enthielt Artikel zu Computer- und Internetsicherheit, GPS-Satelliten-Systemen und zur Codierung und Editierung von Videos. Unter anderem erschienen Beiträge mit Titeln wie „The Technique of Concealing Files from View" oder „How to Protect your Files, Even if Your Device was Penetrated", welche die Befürchtungen der Terroristen vor informationstechnologischer Überwachung zum Ausdruck bringen. Auch Links zu benötigten Tools für anonymes Surfen im Internet und das sichere Speichern von Dateien sowie ein Artikel über Pretty Good Privacy (PGP), einer Software zur Verschlüsselung von E-Mails, waren im Magazin enthalten.[40]

Am 1. Januar 2007 gab ausserdem die „Global Islamic Media Front" (GIMF) bekannt, es werde nächstens ein Softwarepaket namens „Mujahideen Secrets" erhältlich sein. Gemäss der Ankündigung sei dieses das erste „islamische Computerprogramm" für einen sicheren Informationsaustausch über das Internet und versorge die Benutzer mit Verschlüsselungsalgorithmen, symmetrischen (256bit) und asymmetrischen Schlüsseln (2048bit) sowie Tools zur Datenkomprimierung.[41]

---

[38] Siehe http://siteinstitute.org/bin/articles.cgi?ID=publications231106&Category=publications&Subcategory=0 (Stand: 14.2.07).

[39] Siehe http://www.memri.org/bin/opener_latest.cgi?ID=IA32907 (Stand: 28.02.07).

[40] Siehe http://www.siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0; http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP137506 (Stand: 14.2.07).

[41] Siehe http://memri.org/bin/articles.cgi?Page=subjects&Area=iwmp&ID=SP140707 (Stand: 14.2.07).

Beide Beispiele illustrieren ein offenbar zunehmendes Interesse dschihadistischer Extremisten an informationstechnologischen Themen. Von besonderer Bedeutung ist für sie momentan die Frage, wie man sicher im Internet kommuniziert, Dateien versteckt oder verschlüsselt und sich so besser vor Überwachung und Strafverfolgung schützen kann.

Setzen sich in dschihadistischen Kreisen vermehrt solche Kenntnisse durch, ist damit zu rechnen, dass viele der sicherheitspolitischen Massnahmen zur Überwachung des Internets, wie sie momentan in der EU und besonders in Deutschland zur Debatte stehen, ihren eigentlichen Zweck der präventiven Terrorismusbekämpfung verfehlen könnten.

6 Prävention

Schwerpunkt: Social Engineering

Allgemein

Social Engineering ist sehr vielfältig. Da dank verbesserter Sicherheitsvorkehrungen heute meist eine Benutzeraktion notwendig ist, um ein Programm zu starten, versuchen Angreifer immer häufiger, den Menschen als schwächstes Glied auszunutzen. Ob es darum geht, jemanden zur Preisgabe seiner Login-Daten, zur Installation eines Programms oder sogar zu einer Vorauszahlung an einen Unbekannten zu überreden – die angewandten Methoden werden ständig angepasst und verbessert. Social Engineers versuchen, beim Opfer ein Überraschungsmoment auszunutzen, an seine Hilfsbereitschaft zu appellieren, mit dessen Angst zu spielen oder zu drohen. Dem Einfallsreichtum der Angreifer sind kaum Grenzen gesetzt. Ein Versuch, der im letzten halben Jahr für Schlagzeilen gesorgt hat, zeigt dies recht deutlich: In einer Firma wurde geprüft, ob die Mitarbeitenden Social Engineering-Angriffe erkennen.[42] Das Besondere am hier beschriebenen Versuch ist, dass die Mitarbeitenden vorgängig über dessen Durchführung informiert worden waren. Trotzdem gelang es, einen Teil der Angestellten zu täuschen, indem USB-Memory-Sticks auf dem Gelände vor der Firma verteilt wurden. Viele Mitarbeitende steckten diese anschliessend in die Firmencomputer. Dabei installierte sich ein Spionageprogramm und sicherte somit den Angreifern theoretisch einen Zugang zu den Firmen-Daten. Dieses Beispiel zeigt, dass es mit einer einmaligen Sensibilisierung der Mitarbeitenden nicht getan ist, sondern dass es regelmässige und angepasste Sensibilisierung braucht, die auch neueste Trends und Methoden berücksichtigt.

Technische Lösungen bieten keinen umfassenden Schutz

Technische Lösungen schützen vor Social-Engineering-Angriffen nur bedingt. „Anyone who thinks that security products alone offer true security is settling for the illusion of security“, meint beispielsweise Kevin Mitnick, einer der prominentesten ehemaligen Hacker, zu dieser

[42] Siehe http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1 (Stand: 19.2.07).

Frage.[43] Antiviren-Programme oder Spam-Filter bieten zwar Basisschutz gegen einen Grossteil der *Malware*, die mittels Social Engineering verbreitet wird. Gerade jedoch bei gezielten Spionageangriffen ist eine automatische Erkennung fast unmöglich. Die zu diesem Zweck eingesetzten Spionageprogramme werden in so zahlreichen Varianten entwickelt und bewusst nur in kleiner Zahl verbreitet, so dass Antiviren-Programme diese nicht immer erkennen. Blindes Vertrauen in Schutzprogramme ist daher kontraproduktiv. Das Gefühl, die Technik könne alles lösen, kann den Mitarbeitenden ein falsches Gefühl von Sicherheit vermitteln, und damit deren Vorsicht schmälern.

Allgemeine Erkennungsmerkmale

Der Angreifer versucht meist das Überraschungsmoment auszunutzen. Oft gibt er sich als eine bekannte Person aus, in grösseren Firmen als (persönlich unbekannter) Arbeitskollege oder als Mitarbeitende bzw. Servicetechniker eines vertrauenserweckenden Zulieferers oder bekannten Unternehmens. Beim Angriff mit Malware enthält die zugespielte Nachricht meist zuvor recherchierte Fakten aus dem Arbeitsgebiet des Empfängers und benutzt den einschlägigen Fachjargon. Beinhaltet die Nachricht zudem eine Aufforderung zu einer Aktion und ist diese Aufforderung gekoppelt mit einer Täuschung, Erpressung, Einschüchterung, Bedrohung, einem Appell an die Hilfsbereitschaft oder dem Ausnutzen der Arglosigkeit, ist prinzipiell Vorsicht geboten. Angriffe werden nicht nur über E-Mail durchgeführt – auch per Telefon oder SMS wurden Angriffe beobachtet.

Um ein Opfer zu bestimmten Taten zu verleiten, muss eine Vertrauenskulisse aufgebaut werden. Die vom Angreifer dazu benötigten persönlichen Informationen über eine Firma oder eine bestimmte Person sind beispielsweise nicht nur in den Papierkörben der Firmen zu finden. Jeder hat schon erlebt, dass morgens im Zug vertrauliche Informationen mitgelauscht werden können. Aber auch im Internet sind Angaben über Angestellte oder Firmen zu finden. Manchmal findet sich dort ein ganzer Lebenslauf oder eine private Homepage mit persönlichen Daten eines Mitarbeitenden. Ebenfalls sehr nützlich für Angreifer sind Geschäftsberichte, (interne) Telefonbücher, Organigramme, Medienberichte, Börsenberichte und viele andere öffentlich leicht erhältliche Informationen zur anzugreifenden Firma.

Absenderadressen lassen sich einfach fälschen, persönliche Informationen der Opfer, wie oben beschrieben, leicht zusammentragen. Eine sichere Erkennung solcher Angriffe ist auch bei guten Kenntnissen schwierig, weshalb den Mitarbeitenden eingeschärft werden sollte, im Zweifelsfall beim (angeblichen) Absender anzufragen.

Spezialfall Phishing

Eine spezielle Art von Social Engineering ist das so genannte *Phishing*. Neben der Ausnutzung des Überraschungsmoments wird dem Opfer mit der meistens angedrohten Kontosperrung auch Angst gemacht. Im letzten Jahr kamen vermehrt Programme auf den Markt, die Opfer vor Phishing-Seiten warnen sollen. Der letzte Halbjahresbericht ging detailliert darauf ein. Mit dem Release des Internet Explorer 7 kommt nun ein neues Programm hinzu. Der neue Internet Explorer soll mit seinem Phishing-Filter eine grosse Anzahl betrügerischer Seiten erkennen. Doch auch hier birgt blindes Vertrauen in einen solchen Filter Gefahren. Anti-Phishing-Programme helfen zwar recht gut, Phishingseiten zu erkennen, können aber nicht alle Seiten von Anfang an identifizieren. Am Schluss bleibt die Verantwortung beim Anwender. Deshalb gilt es, einfache und einprägsame Verhaltensweisen zu definieren. So bietet die

[43] Mitnick, Kevin & Simon, William L., “The Art of Deception: Controlling the Human Element of Security”, Hungry Mind Inc., 2002.

Eingabe der E-Banking-Seite in die Adresszeile des Browsers von Hand bereits einen guten und einfachen Schutz. Wichtig ist auch zu wissen, dass ein Finanzinstitut seine Kunden niemals in einer E-Mail zur Bekanntgabe von Login, Passwort und TAN auffordern würde.

Richtlinien und User-Awareness

Für Angreifer ist es sehr wichtig, vor dem Angriff möglichst viele Daten über Firma und Mitarbeitende zu sammeln. Durch eine gezielte Schulung der Angestellte, aber auch durch eine restriktive Handhabung ihrer persönlichen Daten auf dem Internet, kann die Verfügbarkeit solcher Informationen für einen Angreifer eingeschränkt werden. Jeder Mitarbeitende sollte wissen, welche Information wie verwendet werden dürfen. Ein entsprechendes Klassifizierungssystem muss einfach und klar sein. Neben dem sicheren Umgang mit den Informatikmitteln muss beispielsweise auch der Helpdesk genaue Richtlinien befolgen, welchen Personen welche Zugangsdaten unter welchen Umständen gegeben werden dürfen. Diese Richtlinien müssen auch unter Zeitdruck oder bei besonderen Vorkommnissen eingehalten werden. Ebenfalls sinnvoll ist die Einführung der einfachen Regel, im Zweifelsfall beim (angeblichen) Absender nachzufragen.

Problem: Abwehr gezielter Spionage

Gerade bei gezielten Spionagefällen werden häufig E-Mails oder CDs verschickt, welche beispielsweise (echt aussehende) Rechnungen, Offerten, Berichte oder Newsmeldungen enthalten. Öffnet man diese Dokumente, werden bisweilen auch unbekannte Sicherheitslücken ausgenutzt. Ist der Computer mit dem Internet verbunden, ist ein ungewollter Datentransfer die Folge. Diese Art von Social-Engineering-Angriffen ist schwer zu erkennen, da der Mitarbeitende in seiner täglichen Arbeit ähnliche Dokumente entgegennehmen muss. In solchen Fällen können auch Verhaltensregeln versagen. Massnahmen wie die Trennung der Verbindung zum Internet oder das Testen aller eingehenden Dokumente in einer virtuellen Maschine könnten helfen, diese Bedrohung weiter einzuschränken. Kommerzielle Lösungen sind bereits auf dem Markt. Ausserdem sollten Mitarbeitende in regelmässigen Schulungen nicht nur über die Angriffe informiert werden, sondern auch erfahren, wen sie im Zweifelsfall informieren müssen – auch über Systemabstürze, langsamere Arbeitsstationen oder anderes abnormales Verhalten des PCs.

Neue Kommunikationsmittel, neue Gefahren

Neue Programme und Kommunikationsmittel haben oft auch neue Angriffsvektoren zur Folge. *Instant Messaging (IM)* oder *Voice over IP (VoIP)* haben in den letzten Monaten als Angriffsvektoren an Bedeutung gewonnen. Diese Technologien werden allzu oft sorglos in Firmen eingesetzt, obwohl sich gerade diese Kommunikationsmittel gut für Social Engineering einsetzen lassen. Firmen müssen sich sehr genau die Frage stellen, welche Dienste sie den Mitarbeitenden zur Verfügung stellen. Bei dieser Entscheidung müssen die Bedürfnisse nach einer Produktivitätssteigerung gegen die Überlegungen zur Sicherheit abgewogen werden.

- Leicht verständliche und einprägsame Verhaltensregeln tragen wesentlich zum Schutz vertraulicher (Firmen-)Daten bei.
- Jeder Benutzer/Mitarbeitende kann mit seinem Verhalten zur Sicherheit beitragen.
- Regelmässige, den aktuellsten Trends angepasste Schulungen und Tests helfen, die Angestellten zu sensibilisieren und mögliche Gefahren zu erkennen.
- Technische Massnahmen gehören zum Grundschutz, können aber nicht sämtliche Angriffsvektoren abdecken.

- Neue Kommunikationsmittel eröffnen neue Möglichkeiten, beinhalten aber meist auch neue Gefahren.
- Im Moment werden vermehrt auf E-Mail basierende Angriffe beobachtet. Eine Sensibilisierung, die einen sorgsamen Umgang mit E-Mails beinhaltet, ist daher besonders wichtig.

7 Aktivitäten / Informationen

7.1 Staatlich

Deutschland: Verdachtsunabhängige Vorratsdatenspeicherung, Antiterrordatei und Verfassungsschutzgesetz

Wie bereits im letzten Halbjahresbericht erwähnt, werden im Zusammenhang mit dem Kampf gegen den Terrorismus in der EU und in Deutschland Massnahmen für eine bessere Überwachung des Internets getroffen. Im Zentrum der Debatte stehen die Speicherung bestimmter Daten sowie deren Austausch zwischen verschiedenen Sicherheitsbehörden. Anlässlich seiner EU-Ratspräsidentschaft für das erste Halbjahr 2007 möchte Deutschland eine erhöhte Internet-Überwachung sowie eine verstärkte Verknüpfung von Fahndungsdatenbanken auch auf europäischer Ebene fördern.

Im November 2006 stellte die deutsche Bundesjustizministerin einen Gesetzesentwurf zur Neuregelung der Telekommunikationsüberwachung vor. Auf Widerstand stösst vor allem die geplante Umsetzung der EU-Richtlinie zur verdachtsunabhängigen Vorratsdatenspeicherung (siehe zur EU-Richtlinie den Halbjahresbericht 2005/II).[44] Die Richtlinie schreibt den EU-Staaten vor, Verbindungs- und Standortdaten, welche beim Telefonieren, SMSen und E-Mailen anfallen, für eine Dauer von 6 bis 24 Monaten zu speichern.[45] Der deutsche Gesetzesentwurf legt die Speicherungsfrist auf 6 Monate fest. Das Gesetz soll bis Mitte 2007 im Bundestag verabschiedet werden. Von Bürgerrechtlern, Datenschützern sowie Oppositionspolitikern wird der Gesetzesentwurf als verfassungswidrig verurteilt und der „Arbeitskreis Vorratsdatenspeicherung“[46] ruft alle besorgten Bürgerinnen und Bürger online zu einer „Sammelklage“ auf.

Anfang Dezember 2006 entschied der deutsche Bundestag über die Einrichtung einer Antiterrordatenbank, welche als gemeinsame Datenbank der Polizeibehörden und der Nachrichtendienste von Bund und Ländern dienen soll. Das Gesetz, welches die rechtliche Grundlage dazu bietet, ist Ende 2006 in Kraft getreten.[47] Mit der Antiterrordatenbank soll der Informati-

[44] Siehe http://www.bmj.bund.de/enid/968152a666b778952bc9da769d9fb82a,6f1ad6706d635f6964092d0933313733093a095f7472636964092d0933303334/Pressemitteilungen_und_Reden/Pressemitteilungen_58.html (Stand: 19.2.07).

[45] Siehe MELANI-Halbjahresbericht 2006/I, Kapitel 8: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=de (Stand: 19.2.07).

[46] Siehe http://www.vorratsdatenspeicherung.de (Stand: 19.2.07).

[47] Siehe http://bundesrecht.juris.de/bundesrecht/atdg/gesamt.pdf (Stand: 19.2.07).

onsaustausch und dadurch eine engere Zusammenarbeit zwischen den verschiedenen Sicherheitsbehörden ermöglicht werden. Die Antiterrordatenbank ist heftig umstritten. Bundesinnenminister Wolfgang Schäuble bewertet sie als „unverzichtbares Instrument im Kampf gegen den Terror“ und unterstreicht die Notwendigkeit eines freiheitlichen Rechtsstaats in der Lage zu sein, seinen Bürgern Sicherheit zu gewährleisten.[48] Die Gegner kritisieren vor allem die Gefährdung der gesetzlich gebotenen Trennung von Polizei- und Nachrichtendiensten und dass die Datei explizit nicht nur der Bekämpfung des internationale Terrorismus, sondern auch „anderen Zwecken“ dienen kann.[49]

Als erstes deutsches Bundesland hat Nordrhein-Westfalen Ende Dezember 2006 ein geändertes Verfassungsschutzgesetz verabschiedet, welches eine rechtssicherere Grundlage bieten soll, um im Falle des Verdachtes auf extremistische Straftaten verdeckt private Computer zu durchsuchen.[50] Diese so genannten Online-Durchsuchungen stellen den Zugriff auf Computer dem Abhören von Telefonaten durch die Staatsschutzorgane gleich. Dabei soll *Malware* auf die Rechner der Verdächtigen eingeschleust werden, um die dort gespeicherten Dateien zu durchsuchen. Die Befürworter des neuen Gesetzes halten die Kontrolle des Internets für nötig, um Informationen über Anschlagspläne, Selbstmordattentate oder den geplanten Bau von Bomben zu erhalten.[51]

Bundesweit plant das Bundesinnenministerium im Rahmen des „Programms zur Stärkung der inneren Sicherheit“ ebenfalls erweiterte Mittel und Befugnisse für Internetfahndungen des Bundeskriminalamts. Online-Durchsuchungen sollen darin ebenfalls eine wichtige Rolle spielen. Zudem wird beim Bundeskriminalamt eine Internet-Monitoring- und Analysestelle (IMAS) aufgebaut, welche den Kampf gegen den Terrorismus durch Überwachung und Analyse einschlägiger Internetseiten stärken soll.[52] Die Rechtmässigkeit der neuen Gesetzgebung ist jedoch heftig umstritten. Unklar ist vor allem, ob das Ausspähen von Daten, welche auf einem Computer gespeichert sind, mit deutschem Gesetz vereinbar ist. Bereits im November 2006 hat der Bundesgerichtshof Online-Durchsuchungen von Computersystemen für illegal erklärt, weil dafür die erforderliche Rechtsgrundlage fehle.[53]

Was die Situation in der Schweiz bezüglich der Speicherung von Vorratsdaten betrifft, so müssen die Provider gewisse Internetverbindungsdaten während sechs Monaten speichern. Eine Debatte über eine allfällige Verschärfung ist im Gange, wobei der Bundesrat einer Erhöhung positiv gegenübersteht.

Online-Durchsuchungen ohne konkreten Tatverdacht sind in der Schweiz bislang verboten. Das Eindringen in Computer ist jedoch im neuen Entwurf zum Bundesgesetz zur Wahrung der inneren Sicherheit (BWIS) enthalten. Diese Massnahme dürfte nur in Ausnahmefällen und unter strengen Voraussetzungen eingesetzt werden. Zudem müsste die betroffene Per-

---

[48] Siehe (Stand: 19.2.07) http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/09/Antiterrordatei.html.

[49] Siehe http://bundesrecht.juris.de/bundesrecht/atdg/gesamt.pdf, Paragraph 6 (Stand: 19.2.07).

[50] Siehe http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/XMMGVB0638.pdf?von=620&bis=621; http://www.landtag.nrw.de/portal/WWW/P/Presse/Oeffentlichkeitsarbeit/Informationen/2006/12/2012_Plenum_aktuell.jsp (Stand: 19.2.07).

[51] Siehe http://www.heise.de/newsticker/meldung/82814; http://www.nzz.ch/2006/12/21/al/articleERN8M.html (Stand: 19.2.07).

[52] Siehe http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2006/11/Programm__zur__Staerkung__der__Inneren__Sicherheit.html; http://www.sueddeutsche.de/computer/artikel/965/93872/; http://www.heise.de/newsticker/meldung/82154 (Stand: 19.2.07).

[53] Siehe http://www.heise.de/newsticker/meldung/82341 (Stand: 19.2.07).

son über ihre Überwachung nach Beendigung der Operation unterrichtet werden. Die Beratung des Gesetzesentwurfs in den eidgenössischen Räten steht noch an.

Eine Einschätzung von MELANI über die Nutzung des Internets durch terroristische Kreise sowie Überlegungen zu deren Vorbereitungen gegen die Internetüberwachung sind in Kapitel 5.4 zu finden.

EU: Stärkung von Europol / Ausweitung der Internet-Überwachung

Die Europäische Kommission sieht vor, die Befugnisse des Europäischen Polizeiamtes (Europol) auszudehnen. Unter anderem soll eine bessere Bekämpfung der Cyberkriminalität sowie eine zentralisierte und effizientere Verarbeitung der bei Europol gespeicherten Daten ermöglicht werden.

Der Auftrag von Europol soll auf den gesamten Bereich der internationalen Schwerkriminalität ausgedehnt werden. Somit soll diese Behörde ihren Tätigkeitsbereich auch im Bereich der Cyberkriminalität und Internetüberwachung erweitern. Ferner schlägt die Kommission vor, die Verarbeitung der bei Europol gespeicherten Daten zu verbessern. Eine Möglichkeit bestehe darin, dass Europol für bestimmte Fälle eine Datenbank mit Internetseiten, von welchen eine Gefährdung ausgehen könnte, errichte.[54]

Bereits mit der Erstellung des „Check the Web"- Programms im Frühling 2006 einigten sich verschiedene EU-Staaten auf die Schaffung einer länderübergreifenden Internet-Überwachung unter Beteiligung Europols.[55] Bei Europol soll ein Informationsportal eingerichtet werden, über das Mitgliedstaaten Informationen austauschen können. In diesem Zusammenhang ist auch die Einführung eines gemeinsamen Visa-Informationssystems geplant. Deutschland will während seiner EU-Ratspräsidentschaft den Informationsaustausch und die Internet-Überwachung auf EU-Ebene vorantreiben.

MELANI beurteilt einen effizienten internationalen Informationsaustausch bei gleichzeitig gewährtem Datenschutz für hilfreich und notwendig für eine Gewährleistung der inneren Sicherheit. Eine Zusammenarbeit auf europäischer Ebene für die Beobachtung und Analyse einschlägiger Seiten auf dem Internet ist ebenfalls zu begrüssen.

Deutschland und Grossbritannien: Reformen der Computerstrafrechte

Ende 2006 haben Deutschland und Grossbritannien Gesetzesentwürfe erlassen, welche unter anderem darauf abzielen, den Straftatbestand „hacking" weiter auszudehnen. Verboten werden sollen neu auch Herstellung und Verbreitung von „Hacker-Tools" sowie *Denial-of-Service-Attacken (DoS)*. Beide nationalen Gesetze sollen an den EU-Rahmenbeschluss über

[54] Siehe http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1861&format=HTML&aged=0&language=DE&guiLanguage=en; http://www.heise.de/newsticker/meldung/82820 (Stand: 19.2.07).

[55] Siehe MELANI-Halbjahresbericht 2006/I, Kapitel 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=de (Stand: 19.2.07).

Angriffe auf Informationssysteme sowie an die Cybercrime-Konvention des Europarates angepasst werden.[56]

In Grossbritannien wurde gleichzeitig ein neues Gesetz erlassen, welches *Phishing* unter dem Tatbestand Betrug einschliesst und somit neu bereits den alleinigen Phishing-Versuch strafbar macht.[57]

Beide Gesetzesentwürfe stossen auf scharfe Kritik. Hauptsächlich wird eine „Überkriminalisierung" von Software befürchtet, welche auch zur Analyse von Sicherheitslücken gebraucht werde und somit für die IT-Sicherheitsbranche unverzichtbar sei. Befürchtet wird zudem eine Rechtsunsicherheit bei der Entwicklung und Verbreitung von Software. Auch MELANI beurteilt es als problematisch, Herstellung und Verbreitung von Software zu illegalisieren, die auch dazu benötigt wird, die Verwundbarkeit und Sicherheit von Informationssystemen überhaupt erst beurteilen zu können.

USA ratifizieren Cybercrime-Konvention des Europarates und treten per 1. Januar 2007 bei

Ende September 2006 ratifizierte der US-Senat nach einer Verzögerung die Cybercrime-Konvention des Europarates. Damit sind die USA der 16. Staat, welcher die Konvention ratifiziert hat.[58]

Die Konvention ist das erste internationale Übereinkommen im Bereich der Cybercrime-Bekämpfung. Die Vertragsstaaten werden verpflichtet, ihr Straf- und Strafprozessrecht sowie die Bestimmungen über die internationale Zusammenarbeit in Strafsachen der fortgeschrittenen Informationstechnologie anzupassen.

Internet-Kriminalität ist ein grenzüberschreitendes Problem. Eine der Hauptschwierigkeiten in ihrer Bekämpfung liegt deshalb in den unterschiedlichen nationalen Gesetzgebungen. Für eine erfolgreiche Bekämpfung sind gesetzliche Anpassungen sowie eine erhöhte internationale Zusammenarbeit entscheidend (siehe dazu auch Kapitel 3.2 sowie 5.3). Die Cybercrime-Konvention des Europarates ist ein viel versprechendes Instrument. Die Schweiz hat die Konvention im Jahr 2001 zwar unterzeichnet, jedoch noch nicht ratifiziert.[59]

---

[56] Siehe http://www.bmj.bund.de/enid/2f99c147790664d0475a936f509414f9,792f747072657373656617274696b656c5f6964092d0932353638093a096d795f79656172092d0932303036093a096d795f6d6f6e7468092d093039093a095f7472636964092d0932353638/Presse/Pressemitteilungen_58.html; http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en.pdf (Stand: 19.2.07).

[57] Siehe http://www.opsi.gov.uk/ACTS/acts2006/ukpga_20060035_en.pdf (Stand: 19.2.07).

[58] Siehe http://www.state.gov/r/pa/prs/ps/2006/73353.htm; http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=2/14/2007&CL=GER (Stand: 19.2.07).

[59] Siehe (Stand: 19.2.07) http://www.ejpd.admin.ch/ejpd/de/home/themen/kriminalitaet/cybercrime/ref_cybercrime__europarat.html.

USA: DHS setzt Cybersecurity-Verantwortlichen ein

Im September 2006 setzte das Department of Homeland Security (DHS) nach längerem Zögern einen Cybersecurity-Verantwortlichen ein, der erstmals im Rang eines stellvertretenden Departementsleiters agiert. Damit soll das Land besser in der Lage sein, seine *kritischen Informationsinfrastrukturen* gegen allfällige Cyberattacken zu schützen. Dieser Posten wurde somit erst 14 Monate nach seiner Schaffung durch den Kongress im Juli 2005 besetzt.[60]

Im Februar 2006 führte das DHS eine Übung namens „Cyber Storm Exercise" durch, in welcher eine Cyberattacke gegen die kritischen Informationsinfrastrukturen der USA simuliert wurde.[61] Dabei wurde erneut erkannt, dass es in den USA an einer klaren Strategie sowie an der Koordination von Massnahmen bei Notfällen fehle. Der neue Cybersecurity-Verantwortliche soll nun in enger Zusammenarbeit mit der Privatwirtschaft eine neue Strategie implementieren und einen Notfallschutzplan erstellen.[62]

7.2 Privat

Schweiz: PostFinance führt SmartCards für die E-Banking-Authentifizierung ein

PostFinance wird die Streichlisten für die Authentifizierung an ihrem E-Banking-System Yellownet durch Authentifizierung per SmartCard ersetzen. Ab März 2007 wird Postfinance den dafür benötigten Kartenleser gratis an seine Kunden abgeben. Durch diese technische Massnahme soll die Gefahr durch *Phishing*-Attacken verringert werden.

Diese technische Vorkehrung stellt sicher, dass ein Kunde nicht dazu verleitet werden kann, seine gesamten Login-Daten einem Phisher preiszugeben.

---

[60] Siehe http://www.dhs.gov/xnews/releases/pr_1158759756150.shtm sowie die Ausführungen im MELANI-Halbjahresbericht 2005/II, Kapitel 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=de (Stand: 19.2.07).

[61] Siehe http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm (Stand: 19.2.07).

[62] Siehe http://www.washingtonpost.com/wp-dyn/content/article/2006/09/18/AR2006091800928.html (Stand: 19.2.07).

8 Gesetzliche Grundlagen

Deutschland: Unverschlüsseltes WLAN kann juristische Folgen haben

Von einem an ein nicht gesichertes Funknetzwerk angeschlossenen Computer waren in Hamburg Ende 2005 Audiodateien abrufbar gewesen. Die Betreiber des Funknetzwerkes (*WLAN*) wurden ermittelt und vom Rechteinhaber abgemahnt. Die Abmahnung wurde aber mit der Begründung abgelehnt, ein unbekannter Dritter habe über das ungesicherte WLAN die Musikdateien angeboten. Der Musikkonzern beantragte daraufhin erfolgreich eine einstweilige Verfügung beim Landgericht. Das Gericht griff beim Entscheid auf die Grundsätze der Störerhaftung zurück. Auch Dienstanbieter, die durch die blosse Zugangsgewährung zu fremden Inhalten einen mittelbaren Tatbeitrag zur Rechtsverletzung leisten, sind als Störer zu qualifizieren. Wer seine Internetverbindung drahtlos betreibt, muss für die Sicherung seines Routers sorgen, andernfalls verstösst er gegen die zumutbaren Prüfungspflichten. Nach Ansicht der Richter hätte es dem Beklagten als Betreiber des Zugangs oblegen, sich zu informieren, wie er solchen Verletzungen vorbeugen kann.

Der Entscheid des Landgerichts Hamburg könnte in Deutschland eine neue Dimension in Haftungsfragen eröffnen. Allerdings ist das Urteil vom Bundesgerichtshof noch nicht bestätigt worden. Auch in der Schweiz könnte ein Musikkonzern auf das Urheberrecht zurückgreifen und seine Rechte geltend machen. Dass urheberrechtlich geschützte Produkte öffentlich zugänglich gemacht und unerlaubt verbreitet werden, verstösst auch in der Schweiz gegen das Urheberrecht.

Gemäss Einschätzung der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) ist es in der Schweiz zum jetzigen Zeitpunkt kaum denkbar, dass ein Betreiber eines WLAN in so einem Fall strafrechtlich zur Verantwortung gezogen würde. Auch eine Haftung gemäss Art. 41 des Obligationenrechts ist in der Schweiz zum heutigen Zeitpunkt kaum denkbar. Dies bedeutet nicht, dass die Problematik offener Funknetze rechtlich keine Schwierigkeiten bereiten würde. Bereits sind KOBIK erste Fälle bekannt, bei denen ein offenes WLAN für Straftaten benutzt wurde. Es handelt sich hierbei um Erpressungen, sexuelle Nötigung und den Download von Kinderpornographie.

Deutschland: Urteile gegen Finanzagenten

Im letzten Halbjahr wurde im deutschsprachigen Raum vermehrt nach Finanzagenten gesucht, um *Phishing*-Gelder ins Ausland zu transferieren (siehe auch Kapitel 4.2). In diesem Zusammenhang liegen in Deutschland nun verschiedene Gerichtsurteile vor.

Das Oberlandgericht Hamburg entschied, dass Bankkunden, welche Unbekannten ihr Konto für Überweisungen aus Phishing-Attacken zur Verfügung stellen und dieses transferierte Geld zwecks Weiterleitung abheben, die Beträge dem betroffenen Finanzinstitut zurückerstatten müssen. Der Kunde könne auch nicht einwenden, die Bank hätte die Barabhebungen verhindern müssen. Auslöser waren Barabhebungen im Wert von rund 33’000 Euro. Nachdem die Bank eine Mitteilung eines Geschädigten erhalten hatte, erfolgte eine Überprüfung des Kontos der Klägerin, die in der Stornierung der Gutschriften endete. Ferner kündigte das Kreditinstitut das Konto und forderte die Rückzahlung der rund 33’000 Euro. Die Kundin reagierte daraufhin mit einer Klage und verlangte ihrerseits eine Gutschrift in voller Höhe.

Das Abfischen von Kontodaten kann aber auch mit Freiheitsstrafe enden, wenn Kontoinhaber als Mittelsmänner der Betrüger fungieren. Dies wird von den Gerichten als strafbare

Geldwäsche angesehen. Ein 46 Jahre alter Mann aus Meersburg ist für den Versuch, von Dritten unberechtigt veranlasste Überweisungen über sein Konto ins Ausland zu transferieren, vom Amtsgericht Überlingen per Strafbefehl zu einer Geldstrafe von 30 Tagessätzen verurteilt worden. Unbekannte hatten sich per Phishing unberechtigt Zugang zu Bankdaten der Geschädigten verschafft und damit Geldbeträge auf das Konto des Verurteilten überwiesen. Dieser sollte das Geld abzüglich einer Provision von 8,5 Prozent bar abheben und über Western Union ins Ausland transferieren.

Auch in der Schweiz dürften mehrere Personen bewusst oder unbewusst auf die Jobangebote der Phishing-Betrüger reingefallen sein und als Finanzagenten gearbeitet haben. Ob es auch in der Schweiz zu einer Verurteilung kommt, wird sich zeigen. Präzedenzurteile gibt es in der Schweiz noch keine.

9 Glossar

Dieses Glossar enthält sämtliche *kursiv* hervorgehobenen Begriffe. Ein ausführlicheres Glossar mit mehr Begriffen ist zu finden unter:
http://www.melani.admin.ch/glossar/index.html?lang=de.

0-Day-Exploit	*Exploit*, der am selben Tag erscheint, an dem die Sicherheitslücke öffentlich bekannt wird.
Adware	Adware, eine Wortkombination aus Advertisement und Software, wird vielfach für Werbezwecke verwendet, indem die Surfgewohnheiten des Benutzers aufgenommen und dazu benutzt werden, entsprechende Produkte (z.B. durch Links) zu offerieren.
Angriffsvektor	Benutzter Weg oder angewandte Technik eines Angreifers für das Eindringen in ein Computersystem.
Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte *Malicious Bots* können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Botherder	Betreiber eines *Botnetzes*.
Botnetz	Eine Ansammlung von Computern, die mit *Bots* infiziert sind. Diese lassen sich durch einen Angreifer (den *Botherder*) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.
DDoS-Attacke	Distributed-Denial-of-Service Attacke Eine *DoS* Attacke, bei der das Opfer von vielen verscheiden Sys-

	temen aus gleichzeitig angegriffen wird.
DoS-Attacke	Denial-of-Service Attacke Hat zum Ziel, einen bestimmten Dienst für dessen Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Exploit-Code	(kurz: Exploit) Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf Ihrem Rechner – installiert.
Identitätsdiebstahl	Diebstahl und missbräuchliche Nutzung personenbezogener Daten (Passwörter, Daten zur Benutzung von Identitäten von Privatpersonen, Firmengeheimnisse, Steuererklärungen, Kreditkartendaten, Kontoinformationen etc.) durch Dritte.
Instant Messaging (IM)	Dienst, der es ermöglicht, in Echtzeit mit anderen Teilnehmern zu kommunizieren (chatten) und oft auch Dateien auszutauschen. Millionen Benutzer auf der ganzen Welt sind bei den zahlreich existierenden IM-Diensten (AOL, MSN, ICQ, Yahoo etc.) registriert.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Kritische Infrastrukturen / kritische Informationsinfrastrukturen	Infrastruktur oder Teil der Wirtschaft, deren Ausfall oder Beschädigung massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt einer Nation hat. In der Schweiz sind folgende Infrastrukturen als kritisch definiert worden: Energie- und Wasserversorgung, Notfall- und Rettungswesen, Telekommunikation, Transport und Verkehr, Banken und Versicherungen, Regierung und öffentliche Verwaltungen. Im Informationszeitalter hängt ihr Funktionieren zunehmend von Informations- und Kommunikationssystemen ab. Solche Systeme nennt man kritische Informationsinfrastrukturen.
Malware	Setzt sich aus den englischen Begriffen "Malicious" und "Software" zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, trojanische Pferde).
Man-in-the-Middle-Angriff (MitM)	Angriff, bei dem sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-

	Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Plug-In	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plug-Ins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
SCADA Systeme	Supervisory Control And Data Acquisition Systeme Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Social Engineering	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.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spear Phishing	Gezielte *Phishing*-Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
Spyware	Spyware soll ohne Wissen des Benutzers Informationen über dessen Surfgewohnheiten oder Systemeinstellungen sammeln und diese an eine vordefinierte Adresse übermitteln.
Trojanisches Pferd	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.
Virus	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
Voice over IP (VoIP)	Telefonie über das Internet Protokoll (IP). Häufig verwendete Protokolle: H.323 und *SIP*.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Wurm	Im Gegensatz zu *Viren* benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie *Sicherheitslücken* oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten.
Zwei-Faktor-	Login-Verfahren, das neben Usernamen und Passwörtern einen weiteren (zweiten) Faktor vom User verlangt. Zum Einsatz kom-

Authentifizierung	men mehrere Varianten: Streichlisten, durch ein Hardware-Token generierter Code, mit kryptographischen Verfahren errechneter Code, biometrische Daten. Aus den drei Grundbestandteilen „etwas, das man weiss“ (z.B. Passwort), „etwas, das man hat“ (z.B. Security Token) oder „etwas, das man ist“ (biometrische Daten) werden bei der Zwei-Faktor-Authentifzierung zwei verlangt.