Über den Umgang mit Unsicherheit

Dr. Hubert Feyrer
SSP Europe GmbH
<h.feyrer@ssp-europe.eu>

22. Juli 2011

Abstract: Anhand der aktuellen Sicherheits-Situation werden die Begriffe "Sicherheit" und "Unsicherheit" diskutiert, und durch drei Beispielen für Unsicherheit exemplarisch aufgezeigt. Der Umgang mit Unsicherheit wird mit Hilfe von von praktischen Gegenmaßnahmen aufgezeigt. Im Fazit wird geschlossen daß Sicherheit nicht alleine durch eine rein technologische Lösung herbeigeführt werden kann.

Einleitung

Laut dem diesjährigen "Symantec Internet Security Threat" Report ist Deutschland der bevorzugte Logistikstandort für Cyberkriminelle, und von der florierenden Schattenwirtschaft ist Spam noch das kleinste Übel[1], jedoch trotzdem mit entsprechender Reaktion[2,3,4].

Diese und viele ähnliche Nachrichten ließt der Interessierte tagtäglich, in variierender Detail- und Emotionstiefe. Doch was bedeutet dies für den einzelnen Anwender? Er ist bedroht durch viele schreckliche Dinge, aber wie konkret sieht dies für ihn aus? Für ihn, und auch für den bösen Angreifer, der seinen Rechner kompromittiert und in einen Zombie verwandelt der dann als Teil eines Bot-Netzes agiert? Während die "Cloud" mit Firmen wie Sony[5] und Amazon[6,7] in aller Munde ist, weiß man selbst herzlich wenig von dem was eigentlich der eigene Rechner so treibt.

Jeder kennt die Situation, daß man beim Surfen im Web schnell von der digitalen Autobahn auf die Landstraße gerät, und von dort im Rotlichtmillieu landet. Ausreichend Stammtischgeschichten von fiesen Mitbringseln aus eben diesem schrecken zwar vermeintlich ab, aber was geschieht im digitalen Detail?

Nach einer Diskussion der Begriffe "Sicherheit" bzw. "Unsicherheit" wird im Folgenden an drei Beispielen gezeigt wie man Opfer eines Hacking-"Angriffs"

1 Symantec Corp. (2011)
2 Heise Security (2011b)
3 Computerwoche (2011)
4 Spiegel Online (2011)
5 Heise Online (2011)
6 ZDNet (2011)
7 Financial Times Deutschland (2011)

wird (wobei hier eher das Passiv zu gebrauchen ist, da in allen Fällen die Probleme erst durch Aktionen des Benutzers verursacht werden, er sich also quasi selbst ans Messer liefert), wie sich dies für den vermeintlichen Angreifer darstellt, und auch welche Gegenmaßnahmen v.a. im Firmenumfeld wirksam sind.

Definition

Akademisch betrachtet existiert eine Vielzahl von Definitionen für den Begriff "Sicherheit". Werner Poguntke sieht IT-Sicherheit als den Schutz von Informationen und Kommunikationssystemen[1]. Die Norm ISO/IEC 61508 für elektrische, elektronische und programmierbare elektronische (E/E/PE) Systeme spricht von einer "Freiheit von unvertretbaren Risiken"[2], und Manfred Bromba definiert "Sicherheit := 1 - Risiko"[3].

Der im Zusammenhang mit Sicherheit immer auftauchende Begriff des "Risikos" stammt ursprünglich vom griechischen Wort für "Gefahr"[4], und ist somit naturgemäß mit negativen Ereignissen verbunden. Oft wird "Risiko" auch über die Eintritts-Wahrscheinlichkeit solch negativer Ereignisse bestimmt.

Sicherheit ist also verbunden mit negativen Ereignissen. Als Gegenteil ist "Unsicherheit" die Negation von Sicherheit, also die Abwesenheit von Sicherheit bzw. wird Unsicherheit durch das Vorhandensein negativer Ereignisse oder solche auslösender Faktoren bestimmt. Oder eben, daß die Wahrscheinlichkeit, daß etwas Negatives eintrifft, relativ hoch ist. Im Umkehrschluß führt also die Existenz negativer Aspekte zu einem Zustand der Unsicherheit, dem durch Maßnahmen gegen diese Aspekte begegnet werden kann.

Unsicherheit an drei Beispielen

Nach der allgemein und abstrakt gehaltenen Definition von Sicherheit bzw. Unsicherheit, von negativen Aspekten und Gegenmaßnahmen hier im Folgenden drei konkrete Beispiele.

Stolperfalle beim Websurfen – Web DriveBy

Eingangs wurde das Bild des digitalen Rotlichtmillieus benutzt. In der Praxis muß die Umgebung nicht in rötliche Töne getaucht sein, damit man sich beim Surfen im Web Probleme zuzieht. Auch Foren, manipulierte oder extra in hinterlistiger Absicht aufgesetzte Webseiten mit vermeintlich gutgemeinten Inhalten können beim Surfen Daten an den Webbrowser liefern, die dieser nicht korrekt verarbeiten kann. Als Folge von Buffer Overflows und ähnlichen Defekten in Anwendungen kann so ohne dem Zutun des Benutzers Schadcode geladen werden, der dann sein Werk verrichtet.

Die Abbildungen zeigen hier exemplarisch eine Browser-Sitzung, die auf eine speziell präparierte Webseite surft (siehe Abbildung 1). Dort angelangt verschluckt sich der Browser, baut eine Verbindung zum wartenden Angreifer auf und lädt Schadcode nach, der sich auf

1 Poguntke (2010) S. 4

2 *ISO 61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems* (1986)

3 Bromba (2011)

4 Wikipedia (2011c) "Risiko"

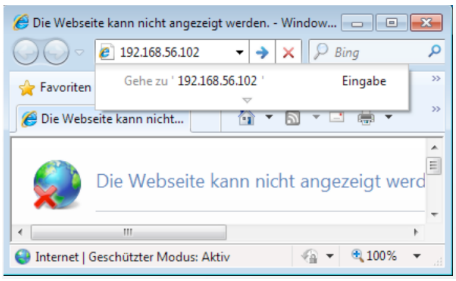

Abbildung 1: Ansurfen einer präparierten Webseite

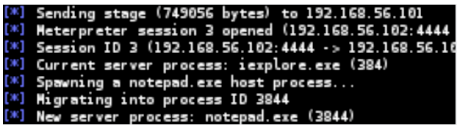

Abbildung 2: Laden von Schadcode

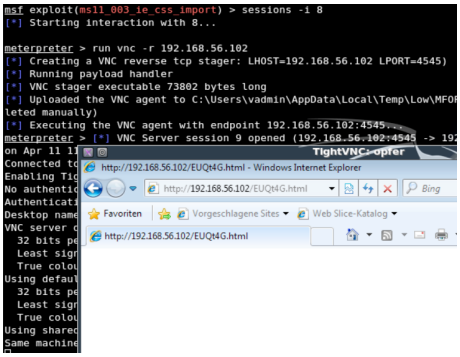

Abbildung 3: Ausspionieren des Opfers

dem Opfer des Rechners als vermeintlich harmloser Texteditor "Notepad.exe" tarnt, wie in Abbildung 2 zu sehen ist. In Wahrheit kann durch diesen Schadcode alles Mögliche geschehen - z.B. wie in der Grafik gezeigt ein Ausspionieren des Opfer-Rechners mittels Remote Terminal Sitzung (VNC, siehe Abbildung 3).

Das Beispiel des Programmierfehlers der durch einen sogenannten "Exploit" ausgenutzt werden kann existiert in der Praxis mannigfaltig. Programme können dabei neben Webbrowsern auch E-Mail Clients[1,2,3] und Server[4,5,6] ebenso wie Spiele[7] und vermeintliche Spiele[8] sein. Darüber hinaus bieten natürlich auch Infrastruktur-Komponenten wie Flash[9], Betriebssysteme oder Frameworks zum Erstellen von Webseiten ebenso Schwachstellen wie spezifische technische Anwendungen. Die Liste läßt sich beliebig fortsetzen, es sei hier lediglich auf die bekannten Ressourcen wie Full Disclosure, Bugtraq und CERT verwiesen.

Unter'm Strich ist also die Unsicherheit groß. Welche Maßnahmen können zur Erreichung eines Zustandes der Sicherheit ergriffen werden? Der versierte IT-Anwender wird im oben genannten Beispiel des Internet Drive-Bys aus seiner Erfahrung sofort wissen daß ein lokaler Virenscanner mit aktuellen Patterns ebenso hilft wie aktuelle Patches nicht

1 SecurityFocus (2000) (pine)
2 Exploit DB (2004) (gaucho)
3 SecurityFocus (2009) (sylpheed)
4 Heise Security (2011a) (IMail)
5 CheckPoint (2011) (exim)
6 Microsoft TechNet (2011) (Microsoft Exchange)
7 Gentoo Linux (2011) (Quake 3)
8 GamesRadar (2011) (Fake Angry Birds)
9 Lilly (2011)

nur für das Betriebssystem, sondern auch den Webbrowser.

Während der Heimanwender damit gut bedient ist, warten im Firmenumfeld weitere Herausforderungen: Wo der Heimanwender einen (1) Browser aktuell halten muß ist dies im Firmenumfeld komplexer. Mit Internet Explorer, Mozilla Firefox, Google Chrome und einer langen Liste weiterer Browser hat der IT-Admin hier ein größeres Feld zu beackern. Wenn er dies nicht will oder mangels Zeit nicht kann sollte er sich überlegen, welchen Webbrowser er seinen Benutzern ans Herzen legt – und welche er ihnen vielleicht rundweg verbietet, um die Sicherheit des Unternehmens nicht zu gefährden. Entsprechende Richtlinien sollten hier in Form von Sicherheits-Policies mit der Unternehmensleitung abgestimmt werden.

Ebenso sollte die Software-Benutzung, so sie denn empfehlungsgemäß reglementiert ist, auch entsprechend regelmäßig überwacht werden. Mag der Betrieb eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 hier noch mit Kanonen auf Spatzen geschossen sein (vgl. ISO 27001, A.10.4.1: Maßnahmen gegen Schadsoftware), so ist dennoch zu erwarten, daß in Zukunft selbst bei Steuerprüfungen nachgefragt wird, welche technischen und organisatorischen Maßnahmen im Unternehmen existieren, um eben die Sicherheit der Unternehmenswerte zu gewährleisten.

Beim Virenschutz ergibt sich ein ähnliches Problemfeld: vor allen in wenig IT-Affinen Geschäftsbereichen kann der mittägliche Virenscan die Literatur der Bild-Zeitung empfindlich beeinträchtigen, und was liegt näher als den Scan hier zu deaktivieren? Daß der Anwender hier andere Prioritäten setzt als der Administrator liegt auf der Hand, letzterer sollte sich hier über ein zentral gesteuertes Anti-Viren-Management Gedanken machen, das dem Benutzer am Rechner genau diesen Handlungsspielraum im Sinne der Unternehmenssicherheit verringert.

Generell sollte man sich im Firmenumfeld über das, was der Heimanwender auf einem (1) Rechner an Sicherungsmaßnahmen macht, überlegen, dies zentral vorzuhalten, um Schlupflöcher und Wartungsaufwand zu minimieren. Nennenswert sind hier Firewalls und zentrale Virenscanner an Web- und Mailfiltern. Bei Webfiltern sollte bedacht werden daß aktuell mehr und mehr Webseiten via HTTPS verschlüsselt übertragen werden, und ein entsprechendes SSL-Scanning verfügbar sein sollte[1]. Selbstverständlich sollte die Wirksamkeit der Systeme auch durch regelmäßige Kontrolle der (anonymisierten!) Protokolle sichergestellt werden.

In diesem Beispiel hätten also auch Policies gegen Surfen auf fragwürdigen Seiten, ein zentrale Webfilter mit Sperrung entsprechender Kategorien und eine zentrale Software-Freigabe die Unsicherheit beim Websurfen wesentlich verringern können.

Vorsicht bei E-Mail-Attachments – PDF Exploit

Im nächsten Beispiel versetzen wir uns in die Situation eines Personalbearbeiters, der eine Bewerbung per E-Mail erhalten hat. Aus dem E-Mail-Programm heraus kann der PDF-Anhang mittels eines Programms zur Anzeige von PDF-Dateien angezeigt werden. Auch dieses

1 Wikipedia (2011e) “SSL-Scanning”

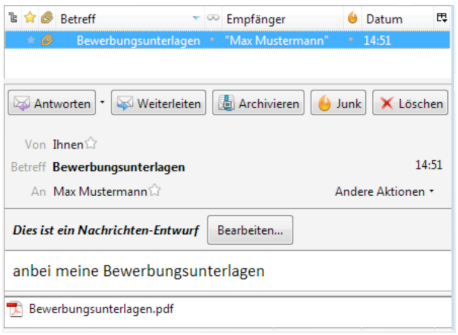

Abbildung 4: E-Mail mit PDF-Attachment

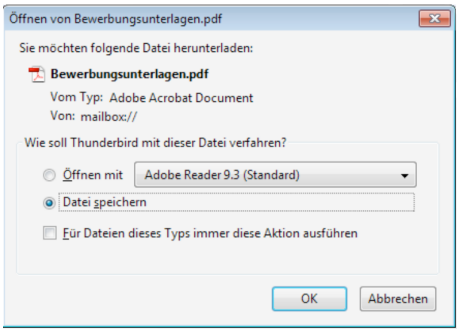

Abbildung 5: PDF-Viewer starten

Programm wiederum kann sich an der PDF-Datei “verschlucken” wenn es entsprechend präparierte (PDF-)Daten erhält.

Die Abbildungen 4 und 5 zeigt den Eingang der E-Mail, das Starten eines PDF-Betrachters sowie erneut den Aufbau der Verbindung vom Opfer zum Angreifer, gefolgt vom Nachladen des Schadcodes auf den Opferrechner. Der Schadcode tarnt sich wiederum als Texteditor, und in den Abbildungen 6 bis 9 ist zu sehen welche weiteren Möglichkeiten neben einer Remote Terminal Sitzung exis-

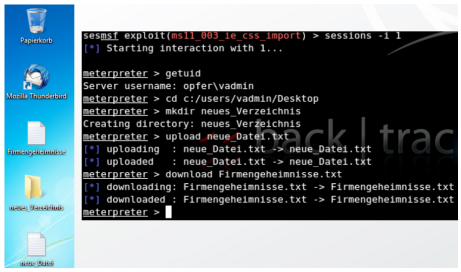

Abbildung 6: Manipulieren des Opfers

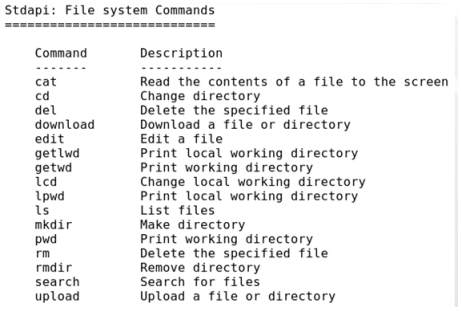

Abbildung 7: Befehle zur Manipulation des Dateisystem

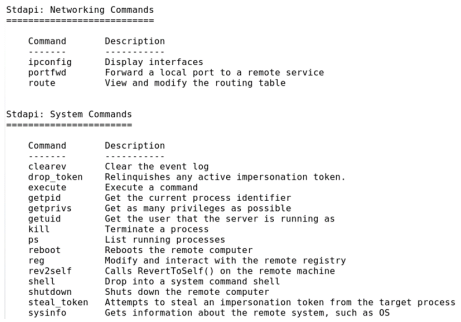

Abbildung 8: Befehle zur Manipulation von Netzwerk und System

```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components

Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
```

Abbildung 9: Befehle für Keylogger, Screenshots und Webcam

tieren:

Das Dateisystem des Opfers kann beliebig ausgespäht werden, Dateien und Daten geladen und ggf. nach Manipulation wieder hochgeladen werden. Neben Manipulation des Dateisystems auf dem Opfer-Rechner kann auch die Netzwerk- und System-Konfiguration sowohl ausgelesen als auch manipuliert werden. Wem dies noch nicht reicht der sei auch auf die Möglichkeiten hingewiesen, daß von einer vorhandenen Webcam ebenso Fotos gemacht werden können wie vom Bildschirm des Rechners, und selbstverständlich kann auch das Mikrofon des Rechners remote angeschaltet werden. Während ein schlauer Angreifer nicht durch einen unbedachten Neustart des Systems auf sich aufmerksam macht[1] steht dem passiven Belauschen von Unterhaltungen im Raum nichts im Weg!

Die Unsicherheit in diesem Fall ist dieselbe, doch wie kann ihr begegnet werden? Patchen einer Überschaubaren Anzahl von Mailreadern und PDF-Betrachtern in Verbindung mit entsprechenden Firmen-Richtlinien wurde bereits ebenso thematisiert wie Virenschutz auf Mail-Gateways und Firewall-Systemen, die die Verbindung zwischen Opfer und Angreifer blockieren können. Letztendlich bleibt die Schwachstelle Mensch, die sich auch hier der Gefahren bewußt sein sollte - Phishing-Nachrichten überschwemmen uns heute in der Spam-Flut, und eben hier muß ein Bewusstsein geschaffen werden, welches Gefahrenpotential hier lauert[2]. Reden Sie mal mit Ihren Kollegen darüber!

Umgang mit mobilen Datenträgern – CD AutoRun

Das letzte Beispiel zeigt als Angriffsvektor die Verteilung von vorbereiteten CDs und USB Sticks, in Zusammenhang mit dem Verhalten eines gängigen Betriebssystemes. Dieses will beim Einlegen des Datenträgers den Benutzer unterstützen, damit dieser leicht an die ihm (vermeintlich) vorliegenden neuen Kundendaten gerät. Da der Benutzer die IT-Landschaft beobachtet weiß er, daß ein Klick auf den ersten Punkt “Kundendaten öffnen” wie auch beschrieben ein eventuell vorhandenes Programm installieren oder ausführen würde. Entsprechend wird er wie in Abbildung 10 gezeigt mit einem Klick rechts-oben das Fenster schließen, und wie in Abbildung 11 im Windows Exlorer auf das Gerät zugreifen. Das benutzerfreundliche Betriebssystem wird jedoch auch hier das hinterlegte Programm per AutoRun starten, und der vorliegende Schadcode wird direkt ausgeführt. Ein Angreifer kann so ohne sich auf Sicherheitslücken zu verlassen jeden beliebigen Programmcode auf dem Rechner des Opfers ausführen, mit Sicherheitsfolgen wie etwa oben aufgezeigt.

In diesem Beispiel war der Benutzer be-

1 Dang und Ferrie (2010)

2 SPAMfighter (2011)

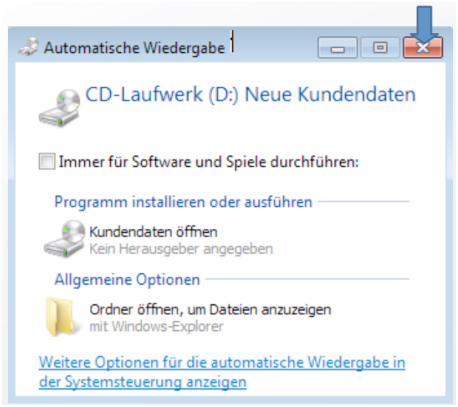

Abbildung 10: Fenster mit Vorschlägen zum Öffnen am besten schließen

Abbildung 11: Öffnen im Explorer startet Autorun-Programm ebenfalls!

reits durch seine Erfahrung vorgeprägt, die Erfolgsquote bei diversen vor mehreren Firmentoren "verlorenen" USB-Sticks liegt laut aktueller Studien bei 60%[1,2].

Abhilfe gegen dieses Einfallstor liefern in forderster Front Anti-Viren-Software und Firewalls mit der Blockung ausgehender Verbindungen ebenso wie die Schulung aller Mitarbeiter. Darüber hinaus sollten auch Richtlinien bedacht werden, die die Benutzung mobiler Datenträger regeln (die beste Firewall hilft nichts, wenn Viren durch private USB-Sticks/Festplatten eingeschleust werden).

Umgang mit Unsicherheit

Die vorangegangenen Abschnitte haben eine Auswahl von Schwachstellen aufgezeigt, über die Anwender und Systeme bedroht sind. Mögliche technische und organisatorische Maßnahmen, die der aus den Angriffen resultierenden Schwachstellen begegnen, wurden kurz diskutiert, und sollen hier gesammelt dargestellt werden.

Technische Maßnahmen

Auf jeden Fall zu betrachten ist das Thema "Endpoint Security" - Anti-Viren Software und Firewalls blockieren Angriffe ebenso wie Patches und aktuelle Betriebssysteme[3,4].

Sind mehrere Rechner zu schützen, so

1 Sawers (2011)
2 Edwards, Kharif und Riley (2011)
3 Iyengar, Sachdev und Raja (2007)
4 Wikipedia (2011a) "Comparison of Operating Systems"

bietet es sich an, auch an den Zugangspunkten zum Netz entsprechende Schutzmaßnahmen zu errichten, und Firewalls[1] sowie Filter für Web[2] und E-Mail[3] mit Virenschutz zu installieren. Für den gesicherten Zugang zum Firmennetz von außen sollten speziell abgesicherte Remote Access und Virtual Private Network (VPN) Systeme wie z.B. IPsec VPN Clients eingesetzt werden[4].

Die Liste der auf dem Markt verfübaren Lösungen ist hier lang, und soll an dieser Stelle nicht näher ausgeführt werden.

Organisatorische Maßnahmen

In den bisherigen Ausführungen wurde ebenfalls erwähnt, daß Sicherheit kein rein technisches Problem ist. Ob der Vielzahl von Webbrowsern, Betriebssystemen, Anwendungsprogrammen und nicht zuletzt Benutzerverhalten bietet sich hier die Einschränkung durch Regulierung an. In der Praxis existieren bereits eine Reihe solcher Regulierungen in Form von "Best Practices", Empfehlungen und Vorschriften bis hin zu Gesetzen.

Wo das Handelsgesetzbuch noch vage von den Pflichten der Geschäftsführung als denen eines "ordentlichen Kaufmannes" spricht [5], so geht etwa das Bundesdatenschutzgesetz hier schon weiter. Es bestimmt, daß sich über die reine Technik hinaus auch Gedanken gemacht wird, wie der physikalische Zugang zu Datenverarbeitungseinrichtungen geschieht, und wie Transport bzw. Weitergabe von Daten organisiert und abgesichert werden[6].

Die im Gesetz recht allgemein gehaltenen "Technischen und Organisatorischen Maßnahmen" können Stand heute mit freiem Spielraum umgesetzt werden. Nationale Vorgaben wie der "IT-Grundschutz" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit seinen sehr umfangreichen Grundschutz-Katalogen[7], vergleichbaren Empfehlungen der "800 Series"[8] des NIST Computer Security Resource Center in den USA und internationale Standards wie die "IT Infrastructure Library" (ITIL)[9] unterstützen hier mit Empfehlungen und "Best Practices". Standardisierte Managementsysteme für IT-Service Management[10] und Informationssicherheit[11] können zudem hinzugezogen werden, um die Umsetzung der Empfehlungen zu kontrollieren, und damit die Standards für Qualität und Sicherheit in Unternehmen zu setzen[12].

Es ist abzusehen daß hier in Zukunft auch von Seiten der Gesetzgeber weitere Vorschriften kommen. Das Bundesdatenschutzgesetz ist hier ein federführendes Beispiel was den Schutz personenbezogener Daten betrifft, auch im internationalen Vergleich. Weitere Beispiele existieren mit Vorschriften wie Basel II mit seinem vorgeschriebenen Risikomanage-

1 Strobel (2003)

2 Ferrari und Thuraisingham (2005) S. 112ff

3 Schneier (1995)

4 Wikipedia (2011f) "Virtual Private Network"

5 Bundesministerium der Justiz (2011) §86 HGB

6 Bundesministerium der Justiz (2009) Anlage zu §9 Satz 1 BDSG

7 Bundesamt für Sicherheit in der Informationstechnik (2011)

8 National Institute of Standards and Technology (2011)

9 APM Group Ltd. (2011) (ITIL)

10 ISO/IEC (2005a) (ISO 20000)

11 ISO/IEC (2005b) (ISO 27000)

12 Bayrisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie (2011)

ment, und auch US-Gesetzen wie der Sarbanes Oxley Act (SOX)[1] und der Health Insurance Portability and Accountability Act (HIPPA)[2].

Um der wachsenden Anzahl gesetzlicher Auflagen der einzelnen Bereiche Herr zu werden etablieren sich hier weitere Standards, um diese Bereiche zu prüfen und zu überwachen. Stellvertretend seien hier die "Control Objectives for Information and related Technology" (COBIT) für den gesamte Bereich der IT-Governance genannt[3].

Weitere Maßnahmen

Neben den bisher besprochenen technischen und organisatorischen Dimensionen ist "Sicherheit" noch wesentlich weiter faßbar. Im Wesentlichen sind damit auch Begriffe wie "Angst", "Risiko" und "Schutz" verbunden. Diese können auch aus psychologischer Sicht betrachtet werden, stellvertretend sei hier auf Stefan Schumacher 2011 und weitere Veröffentlichungen von Stefan Schumacher der Universität Magdeburg verwiesen.

Im politischen Raum spielt nicht nur die Gesetzgebung im nationalen Raum wie oben diskutiert eine Rolle, auch international definiert hier die Sicherheitspolitik Verhalten und Aktionen. Dies ist neben der nationalen Ebene auch bei Gemeinschaften wie der Europäischen Union zu beobachten, wie Jan Meine in seinem Essay "Die Europäische Sicherheitsstrategie 2003 – Europas Versuch einer Positionierung als eigenständiger sicherheitspolitischer Akteur" beschreibt[4].

1 Wikipedia (2011d) "SOX"

2 Wikipedia (2011b) "HIPPA"

3 Audit und Association (2011) (COBIT)

4 Jan W. Meine (2011)

Fazit

Der vorliegende Text zeigt, daß Sicherheit ein weites Feld ist, und weit über den Bereich der rein technischen Maßnahmen hinausgeht. Organisation bildet eine wichtige Rolle, und wird zunehmend wichtiger um Auflagen von Gesetzgebern und Branchen nachzukommen.

Im Bundesdatenschutzgesetz ist heute bereits ein Datenschutzbeauftragter zum Schutz von personenbezogenen Daten vorschreibt. Es ist zu erwarten, daß der Gesetzgeber hier in Zukunft eine ähnliche Institution bestimmen wird, deren Aufgabe der Umgang mit Unsicherheit aller Art sein wird.

Über den Autor

Dr. Hubert Feyrer ist als IT-Manager bei der SSP Europe GmbH tätig. Er leitet Teams in den Bereichen IT-Security und Datacenters, begleitet die Entwicklungen in den Bereichen Hard- und Software, und betreut als IT-Security-Manager die Bereiche Compliance und ISMS/ISO 27001 mit.

Literaturverzeichnis

APM Group Ltd. (2011). ITIL Website. Zugriff am 29. Mai 2011, unter http://www.itil-officialsite.com/

Audit, I. S. & Association, C. (2011). COBIT – Control Objectives for Information and related Technology. Zugriff am 4. Juni 2011, unter http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Bayrisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie. (2011). Aktuelle normierte Managementsysteme. Zugriff am 4. Juni 2011, unter http://www.stmwivt.bayern.de/fileadmin/Web-Dateien/Dokumente/wirtschaft/Managementsysteme_aktuell_normiert.pdf

Bromba, M. U. A. (2011). Stochastische Sicherheitstheorie. Zugriff am 29. Mai 2011, unter http://www.bromba.com/knowhow/Was_ist_Sicherheit.htm#Sicherheit

Bundesamt für Sicherheit in der Informationstechnik. (2011). IT-Grundschutz. Zugriff am 4. Juni 2011, unter http://www.bsi.de/gshb/

Bundesministerium der Justiz. (2009). Bundesdatenschutzgesetzt (BDSG). Zugriff am 29. Mai 2011, unter http://www.gesetze-im-internet.de/bdsg_1990/

Bundesministerium der Justiz. (2011). Handelsgesetzbuch (HGB). Zugriff am 23. Juni 2011, unter http://www.gesetze-im-internet.de/hgb/

CheckPoint. (2011). Heap Buffer Overflow Vulnerability in Exim Mail Transfer Agent. Zugriff am 29. Mai 2011, unter http://www.checkpoint.com/defense/advisories/public/announcement/2011/100111-exim-mta-cve-2010-4344.html

Computerwoche. (2011). Die Schattenwirtschaft im Web floriert. Zugriff am 29. Mai 2011, unter http://www.computerwoche.de/security/1879814/

Dang, B. & Ferrie, P. (2010). Adventures in analyzing Stuxnet. In *Proceedings of the 27th Chaos Communication Congress*. Berlin, Germany. Zugriff am 29. Mai 2011, unter http://events.ccc.de/congress/2010/Fahrplan/events/4245.de.html

Edwards, C., Kharif, O. & Riley, M. (2011). Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy. Zugriff am 3. Juli 2011, unter http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html

Exploit DB. (2004). Gaucho 1.4 Mail Client Buffer Overflow Vulnerability. Zugriff am 29. Mai 2011, unter http://www.exploit-db.com/exploits/421/

Ferrari, E. & Thuraisingham, B. (2005). *Web and Information Security*. Anderson, CA, USA: IRM Press.

Financial Times Deutschland. (2011). Amazons Wolke versagt tagelang. Zugriff am 29. Mai 2011, unter http://www.ftd.de/it-medien/medien-internet/:instabile-cloud-server-amazons-wolke-versagt-tagelang/60044292.html

GamesRadar. (2011). Fake Angry Birds level exposes Android security hole. Zugriff am 29. Mai 2011, unter http://www.gamesradar.com/android/angry-birds/news/fake-angry-birds-level-exposes-android-security-hole/a-20101171910531650 26/g-20101015104552293014

Gentoo Linux. (2011). Quake 3 engine based games: Buffer Overflow. Zugriff am 29. Mai 2011, unter http://www.gentoo.org/securit

y/en/glsa/glsa-200605-12.xml

Heise Online. (2011). Sony-Kundendaten im Internet aufgetaucht. Zugriff am 29. Mai 2011, unter http://www.heise.de/newsticker/meldung/Sony-Kundendaten-im-Internet-aufgetaucht-1239500.html

Heise Security. (2011a). Buffer Overflow in Mailserver IMail. Zugriff am 29. Mai 2011, unter http://www.heise.de/security/meldung/Buffer-Overflow-in-Mailserver-IMail-115908.html

Heise Security. (2011b). Symantec: Deutschland bevorzugter Logistikstandort für Cyberkriminelle. Zugriff am 29. Mai 2011, unter http://heise.de/-1221704

ISO 61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. (1986). International Organization for Standardization. Geneva, Switzerland.

ISO/IEC. (2005a). *ISO/IEC 20000:2005 IT Service Management System*. Geneva, Schweiz: International Organization for Standardization.

ISO/IEC. (2005b). *ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards*. Geneva, Schweiz: International Organization for Standardization. Zugriff am 5. Juni 2011, unter http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip

Iyengar, K., Sachdev, V. & Raja, M. (2007). A Security Comparison of Open-Source and Closed-Source Operating Systems. In *Proceedings of Decision Science Institute Southwest Region 2007*. Zugriff am 26. Mai 2011, unter http://www.swdsi.org/swdsi07/2007_proceedings/papers/236.pdf

Jan W. Meine. (2011). Die Europäische Sicherheitsstrategie 2003 – Europas Versuch einer Positionierung als eigenständiger sicherheitspolitischer Akteur. *Magdeburger Journal zur Sicherheitsforschung, Band 1*. Zugriff am 4. Juni 2011, unter http://www.wissens-werk.de/index.php/mjs/article/view/74

Lilly, P. (2011). Adobe Patches Critical Security Hole in Acrobat, Reader, and Flash. Zugriff am 29. Mai 2011, unter http://www.maximumpc.com/article/news/adobe_patches_critical_security_hole_acrobat_reader_and_flash

Microsoft TechNet. (2011). Vulnerability in SMTP Could Allow Remote Code Execution. Zugriff am 29. Mai 2011, unter http://www.microsoft.com/technet/security/bulletin/ms04-035.mspx

National Institute of Standards and Technology. (2011). Computer Security Resource Center – Special Publications: 800 Series. Zugriff am 4. Juni 2011, unter http://csrc.nist.gov/publications/PubsSPs.html

Poguntke, W. (2010). *Basiswissen IT-Sicherheit: Das Wichtigste für den Schutz von Systemen und Daten*. Witten: W3L Verlag.

Sawers, P. (2011). US Govt. plant USB sticks in security study, 60% of subjects take the bait. Zugriff am 3. Juli 2011, unter http://thenextwe

b.com/industry/2011/06/28/us-govt-plant-usb-sticks-in-security-study-60-of-subjects-take-the-bait/

Schneier, B. (1995). *E-Mail Security*. Hoboken, NJ, USA: Wiley.

SecurityFocus. (2000). Pine 'From:' Field Buffer Overflow Vulnerability. Zugriff am 29. Mai 2011, unter http://www.securityfocus.com/bid/1709

SecurityFocus. (2009). Sylpheed Mail Client Buffer Overflow Vulnerability. Zugriff am 29. Mai 2011, unter http://www.securityfocus.com/bid/12730

SPAMfighter. (2011). RSA Reveals and Explains Data-Hack against It. Zugriff am 23. Juni 2011, unter http://www.spamfighter.com/RSA-Reveals-and-Explains-Data-Hack-against-It-16030-News.htm

Spiegel Online. (2011). Spammer lieben Deutschland. Zugriff am 29. Mai 2011, unter http://www.spiegel.de/netzwelt/web/0,1518,755055,00.html

Stefan Schumacher. (2011). Die psychologischen Grundlagen des Social Engineerings. *Magdeburger Journal zur Sicherheitsforschung*. Zugriff am 4. Juni 2011, unter http://www.wissens-werk.de/index.php/mjs/article/view/74

Strobel, S. (2003). *Firewalls und IT-Sicherheit: Grundlagen und Praxis sicherer Netze: IP-Filter, Content Security, PKI, Intrusion Detection, Applikationssicherheit*. Heidelberg: dpunkt-Verlag.

Symantec Corp. (2011). Internet Security Threat Report, Volume 16. Zugriff am 29. Mai 2011, unter http://www.symantec.com/business/threatreport/index.jsp

Wikipedia. (2011a). Comparison of Operating Systems. Zugriff am 29. Mai 2011, unter http://en.wikipedia.org/wiki/Comparison_of_operating_systems

Wikipedia. (2011b). Health Insurance Portability and Accountability Act. Zugriff am 4. Juni 2011, unter http://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&oldid=431938728

Wikipedia. (2011c). Risiko. Zugriff am 29. Mai 2011, unter http://de.wikipedia.org/w/index.php?title=Risiko&oldid=89164950

Wikipedia. (2011d). Sarbanes–Oxley Act. Zugriff am 4. Juni 2011, unter http://en.wikipedia.org/w/index.php?title=Sarbanes%E2%80%93Oxley_Act&oldid=431004462

Wikipedia. (2011e). SSL-Scanning. Zugriff am 29. Mai 2011, unter http://de.wikipedia.org/w/index.php?title=SSL-Scanner&oldid=76434060

Wikipedia. (2011f). Virtual Private Network (VPN). Zugriff am 4. Juni 2011, unter http://en.wikipedia.org/wiki/Virtual_private_network

ZDNet. (2011). Amazon's Web Services outage: End of cloud innocence? Zugriff am 29. Mai 2011, unter http://www.zdnet.com/blog/btl/amazons-web-services-outage-end-of-cloud-innocence/47731