Sicherheit im Internet und auf dem Heim-PC

Sicherheit ist ein ganzheitliches Konzept und lässt sich leider nicht durch das Einhalten einiger weniger Regeln erreichen. Und auch das beste Sicherheitskonzept ist nur so stark, wie das schwächste Glied der Kette: die beste Firewall nützt nichts, wenn man sich einen Virus über eine heruntergeladene manipulierte Datei einfängt. Dennoch möchte ich in diesem Dokument ein paar einfache Hinweise geben, wie man sich ein wenig sicherer auf dem eigenen PC und im Internet bewegt. Die Einhaltung dieser Regeln ist meist mit ein wenig Arbeit verbunden, doch Sicherheit geht immer einher mit Komfortverlust. Es liegt im eigenen Ermessen abzuwägen, ob der Aufwand der einzelnen Schritte den gewonnenen Sicherheitszuwachs rechtfertigt, aber meiner Meinung nach sind alle vorgestellten Hinweise einfach und schnell umsetzbar.

Wer mehr Informationen zum Thema Sicherheit sucht, kann z.B. meine Bookmarks[1] zu diesem Thema abonnieren oder sich direkt bei mir melden. Für Anregungen bin ich ebenso immer offen. Jetzt aber viel Spaß beim Lesen. – Stefan Macke

Sichere Passwörter

Grundsätzlich gilt, je länger ein Passwort ist, umso sicherer ist es. Zusätzlich muss noch die Anzahl an möglichen Zeichen pro Stelle berücksichtigt werden. Werden bspw. Groß- und Kleinbuchstaben und Zahlen in einem 10-stelligen Passwort verwendet, ist die Anzahl an möglichen Kombinationen für dieses Passwort (26 + 26 + 10) [mögliche Zeichen] ^ 10 [Stellen] = 62^{10} = ca. 839 Billiarden. Selbst wenn ein schneller Computer 10.000 Passwörter in der Sekunde prüfen könnte, bräuchte er 272.868 Jahre, um alle Kombinationen durchzugehen. Wird dagegen ein 8-stelliges Passwort nur aus Kleinbuchstaben verwendet, könnten alle Möglichkeiten bereits in 241 Tagen durchprobiert werden.

Noch schneller können Passwörter geknackt werden, die man in Wörterbüchern[2] finden kann, also z.B. „Passwort“ oder „geheim“. Hier reicht es auch nicht aus, die Schreibweise zu ändern oder Zahlen anzuhängen (z.B. „Passwort1“).

Sichere Passwörter bestehen also mindestens aus Groß- und Kleinbuchstaben und Zahlen. Am besten werden auch noch Sonderzeichen wie „!“, „?“, „$“ o.ä. hinzugenommen. Sie sollten mindestens 8 Stellen lang sein und nicht aus „echten“ Wörtern bestehen. Gute Beispiele sind „D4&Gw3a0“, „mV3m!Su9P“ usw.

Da sich Menschen solche Passwörter jedoch nur schwer merken können, gibt es zwei Möglichkeiten, trotzdem sichere Passwörter zu generieren:

1. Man verwendet Passwortphrasen, also komplette Sätze wie „dashieristmeingeheimesPasswort“ (30 Stellen, 52 Zeichen → 3 * 10^{51} Möglichkeiten), die die mangelnde Anzahl an Zeichen durch ihre große Länge ausgleichen.

[1] http://bookmarks.stefan-macke.de/tags/sicherheit
[2] Die „beliebtesten“ Passwörter 2011: http://splashdata.com/splashid/worst-passwords/index.htm

2. Man merkt sich einen Passwortsatz und nutzt nur die Anfangsbuchstaben für das Passwort, wobei einige Buchstaben durch ähnliche Zahlen (z.B. „O“ → „0“ oder „E“ → „3“) oder Sonderzeichen (z.B. „i“ → „!“) ersetzt werden. Beispiel: „Mein Vater erklärt mir jeden Sonntag unsere neun Planeten“ → „mV3m!SunP“ (72 Zeichen (bei angenommenen 20 Sonderzeichen), 9 Stellen → $51 * 10^{15}$ Möglichkeiten).

Passwörter sollten niemals (!) an andere Personen weitergegeben werden, auch nicht an den IT-Support oder Bekannte, die einem das Heimnetzwerk einrichten.

WLAN

Über ein gar nicht oder schlecht gesichertes WLAN können Angreifer den eigenen Internetzugang für ihre (illegalen) Zwecke nutzen. Dank „Störerhaftung“[3] ist der Anschlussinhaber z.B. für über seinen Internetzugang begangene Urheberrechtsverletzungen haftbar. Allerdings nicht mehr dann, wenn er nachweisen kann, geeignete Sicherheitsmaßnahmen getroffen zu haben.[4]

Sichere Konfiguration des eigenen WLANs:

- Verschlüsselung mit WPA2 (WEP hat bekannte Schwachstellen und kann recht einfach geknackt werden)
- Sicheres Passwort („Netzwerkschlüssel“) verwenden (auch WPA2 kann geknackt werden, wenn das Passwort unsicher ist)
- MAC-Zugangskontrolle aktivieren und nur die eigenen bekannten Geräte zulassen
- SSID unsichtbar machen

Firewall

Im Internet gibt es ein sog. Grundrauschen, das laut einigen Providern bis zu 50% des gesamten Datenvolumens im Internet ausmacht.[5] Ein Großteil dieses Rauschens sind automatisierte Angriffe gegen IP-Adressbereiche (z.B. durch „Script Kiddies“ oder Botnetze). Ein Computer sollte daher niemals (!) ohne eine Firewall ins Internet gehen, die den gefährlichen eingehenden Netzwerkverkehr blockiert.

So gut wie alle handelsüblichen Router, die in Heimnetzwerken betrieben werden (z.B. die FritzBox), haben bereits eine Firewall integriert. Allerdings kann man sie auch deaktivieren. Die Konfiguration sollte also definitiv überprüft werden. Hinter solch einem Router ist man dann recht sicher.

Befindet man sich allerdings (z.B. mit dem Laptop) in einem öffentlichen Netzwerk (z.B. in einem Hotel), sieht das ganz anders aus. Dort weiß man nichts über die Konfiguration der Firewall bzw. ob überhaupt eine vorhanden ist. Daher ist es sinnvoll, auch eine lokale Software-Firewall einzusetzen. Die Windows-Firewall reicht hierfür heutzutage aber aus, sodass keine Zusatzsoftware (wie z.B. *ZoneAlarm*) installiert werden muss.

[3] Siehe z.B. http://www.palm-bonn.de/stoerer.htm
[4] Siehe http://www.die-abmahnung.info/urteile/stoererhaftung-e/article/lg-frankfurt-rasch-verliert-filesharingprozess-keine-haftung-des-anschlussinhabers-bei-nachgewies.html
[5] http://cre.fm/cre191

Virenscanner

Durch die Firewall ist man zwar vor Angriffen von außen abgesichert, aber es kann trotzdem auf anderen Wegen zur Infektion mit einem Virus oder einem anderen Schadprogramm (Wurm, Trojaner, Spy-, Scareware usw.) kommen. Damit diese Schadsoftware auf dem Computer kein Unheil anrichten kann, ist ein Virenscanner nötig, der stets auf dem aktuellen Stand gehalten werden muss. Dies macht die Software heutzutage allerdings von allein. Man darf die Updatemeldungen nur nicht einfach wegklicken, sondern muss sie zulassen.

Welchen Virenscanner man einsetzt ist Geschmackssache. Es reicht normalerweise ein kostenloses Programm wie *Avira*[6] oder *Avast*[7]. Wer sichergehen will, findet in einschlägigen Computermagazinen[8] regelmäßig Testberichte aller aktuellen Virenscanner. Ein Hinweis noch: zwei Virenscanner gleichzeitig zu betreiben ist eher kontraproduktiv und verlangsamt das System – einer reicht!

Ob der eigene Virenscanner korrekt funktioniert, kann man z.B. auf http://www.testvirus.de testen. Dort kann man ungefährliche Testviren herunterladen und kontrollieren, ob der Virenscanner Alarm schlägt.

Ist der PC wider Erwarten doch einmal infiziert, helfen Live-CDs mit Virenscannern, wie zahlreiche Hersteller sie anbieten.[9] Von diesen kann man den befallenen Computer direkt booten und die Festplatte scannen und (hoffentlich) säubern.

Betriebssystemupdates

Ein Windows-PC ohne aktuelle Updates ist wie ein offenes Scheunentor für Angreifer, auch trotz Firewall und Virenscanner. Die Updates sollten so konfiguriert werden, dass sie automatisch heruntergeladen und installiert werden. Dies kann bereits bei der Installation des Betriebssystems eingestellt werden und im Nachhinein unter *Systemsteuerung* → *Windows Updates*.

Mit dem *Baseline Security Analyzer*[10] von Microsoft kann man sein Windows-System auf einige bekannte Schwachstellen (fehlende Updates, schwache Passwörter usw.) hin untersuchen und ggfs. Gegenmaßnahmen einleiten.

Sonstige Programmupdates

Was wäre der eigene Computer ohne die Programme, mit denen wir überhaupt nur sinnvoll mit ihm arbeiten können? Doch diese Programme können durchaus schwerwiegende Sicherheitslücken haben, die genauso gefährlich sind wie die des Betriebssystems.

Insbesondere ist hier Java zu nennen. Die Laufzeitumgebung für Java-Programme ist auf nahezu jedem Computer und Mobilgerät installiert. Allerdings konnten sich gerade in letzter Zeit viele Schädlinge über Sicherheitslücken in Java verbreiten. Daher ist es absolut notwen-

[6] http://www.avira.com/de/avira-free-antivirus
[7] http://www.avast.de/produkte/freeware/avast-free-antivirus.html
[8] z.B. bei der c't: http://www.heise.de/security/dienste/AntiVirus-2071.html
[9] z.B. http://www.avira.com/de/support-download-avira-antivir-rescue-system
[10] http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c

dig, die Java-Updates zu installieren, sobald sie verfügbar sind, wenn man Java überhaupt auf seinem Gerät benötigt (ansonsten ist es sicherer die Software gar nicht erst zu installieren). Wie das geht, kann man im Internet nachlesen.[11]

Doch auch die zahlreichen anderen Programme, die auf dem Rechner installiert sind, sollten aktuell gehalten werden. Da man bei der Vielzahl an Anwendungen schnell den Überblick verliert, empfehle ich hierfür den *Personal Software Inspector* von Secunia.[12] Dieses Programm untersucht den Computer auf installierte Software und prüft jeweils die Version und ob es ggfs. im Internet eine neuere gibt. Auf Knopfdruck können dann die Updates installiert werden. Einfacher geht es fast nicht mehr.

Surf-VM

Wer ganz sicher sein will, dass sein Computer nicht von Schädlingen befallen wird, der kann sich eine virtuelle Maschine[13] zum Surfen aufsetzen, die bei Befall jederzeit wieder in den Ursprungszustand zurückgesetzt werden kann, ohne dass der Wirts-PC betroffen ist.

Datensicherheit

Der Schutz der eigenen Daten (z.B. eigene Dokumente, Musiksammlung, Bilder) ist gerade auf Mobilgeräten sehr wichtig. Wird z.B. ein Laptop gestohlen, schützt das Windows-Kennwort nicht davor, die Daten direkt von der Festplatte auszulesen. Sollen Daten vor fremdem Zugriff geschützt werden, müssen sie verschlüsselt werden. Dies kann man z.B. mit *TrueCrypt*[14] tun. Mit diesem Programm kann die gesamte Festplatte verschlüsselt werden oder es können einzelne Container angelegt werden, in denen Daten sicher gespeichert werden können.

Eine Datensicherung ist immer zu empfehlen, nicht nur um im Falle eines Diebstahls abgesichert zu sein. Auch Festplatten und DVDs halten nicht ewig (im Durchschnitt 5 bzw. 10 Jahre). Heutzutage sind bereits sehr günstig externe Festplatten[15] mit enormer Speicherkapazität zu bekommen, die für eine Komplettsicherung aller Daten (und sogar inkl. Betriebssystem) ausreichen. Ein Backup-Programm ist in Windows bereits integriert, aber es gibt auch weitere gute kostenlose Werkzeuge im Internet.[16]

Beim Verkauf von alter Speicherhardware ist darauf zu achten, diese sicher zu löschen. Sonst hat der Käufer leichtes Spiel, die Daten wiederherzustellen. Entgegen der verbreiteten Meinung, Datenträger müssten mehrmals überschrieben werden, damit keine Daten wiederher-

[11] z.B. hier: http://scareware.de/2010/07/java-control-applet-manuell-aktualisieren-update-intervalle-aendern/
[12] http://secunia.com/vulnerability_scanning/personal/
[13] z.B. mit https://www.virtualbox.org/
[14] http://www.truecrypt.org/
[15] z.B. 2TB für ca. 130,- EUR bei http://www.amazon.de/gp/product/B0031SZRZG/ref=as_li_ss_tl?ie=UTF8&tag=blovonstemac-21&linkCode=as2&camp=1638&creative=19454&creativeASIN=B0031SZRZG
[16] z.B. *SyncToy* von Microsoft: http://www.microsoft.com/download/en/details.aspx?id=15155

gestellt werden können, reicht das einmalige Überschreiben des gesamten Datenträges aus.[17] Das kann z.B. die Software *Eraser*[18].

Dateidownloads

Trotz aktuellem Virenscanner können sich Schadprogramme über manipulierte Dateidownloads ins System einschleusen. Die Schadsoftware hängt sich dabei an eine valide Datei, z.B. das Installationsprogramm eines Browsers, an und wird beim Ausführen unbemerkt im Hintergrund installiert. Dieses Einschleusen kann man nur verhindern, wenn man heruntergeladene Dateien auf unerwünschte Veränderungen hin überprüft. Dies geht allerdings nur, wenn man weiß, wie die unveränderte Datei aussehen müsste.

Daher ist man hierbei auf die Informationen des Herstellers angewiesen. Viele seriöse Softwarehersteller, gerade im Bereich sicherheitsrelevanter Software (also z.B. die in diesem Dokument erwähnte Verschlüsselungssoftware), stellen auf ihren Websites parallel zum Download einen sog. Hash-Wert für die Dateien zur Verfügung. Eine Hash-Funktion ist eine mathematische Einwegfunktion, die Daten beliebiger Länge auf eine Zeichenkette fixer Länge (z.B. 64 Zeichen) abbildet. Sie hat die Eigenschaft, dass die Hashwerte zweier Eingangsdaten sich deutlich voneinander unterscheiden, auch wenn nur ein einziges Zeichen der Eingangsdaten unterschiedlich ist. Mittels Hashwerten kann man also recht einfach prüfen, ob die heruntergeladene Datei manipuliert wurde. Ein kostenloses Tool, dass Hashes von beliebigen Dateien anzeigt, ist *FileAlyzer*.[19]

Webbrowser

Obwohl Microsoft den *Internet Explorer* in letzter Zeit deutlich überarbeitet und sicherer gemacht hat, empfehle ich immer noch *Firefox*[20] zum Surfen, da es für ihn einige interessante AddOns bzgl. der Sicherheit im Internet gibt (s.u.). Noch sicherer ist allerdings Googles *Chrome*[21], da er in einer sog. Sandbox läuft, aus der heraus Schadsoftware den Computer nicht so leicht infizieren kann. Das BSI bietet eine gute Übersicht über Sicherheitseinstellungen verschiedener Browser.[22]

Alle modernen Browser haben eine Warnfunktion eingebaut, die bei bösartigen Websites (z.B. Phishing oder attackierende Seiten) Alarm schlägt. Wenn solch eine Warnung angezeigt wird, sollte man sie im Zweifelsfall lieber ernst nehmen und den Aufruf abbrechen.

Beim Browser ist es noch wichtiger, die Updates einzuspielen, als beim Betriebssystem, da er den direkten Kontakt zu möglicherweise schadhaften Websites herstellt. Daher sollten die automatischen Updates immer sofort installiert werden, auch wenn dadurch ggfs. installierte AddOns vorübergehend nicht mehr funktionieren.

---

[17] http://www.heise.de/security/meldung/Sicheres-Loeschen-Einmal-ueberschreiben-genuegt-198816.html
[18] http://www.computerwoche.de/hardware/storage/2486506/
[19] http://www.safer-networking.org/de/filealyzer/index.html
[20] http://www.mozilla.org/firefox/
[21] http://www.google.de/chrome/
[22] https://www.bsi-fuer-buer-ger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/SicherheitsCheck/sicherheitscheck_node.html

Da immer noch viele Angriffe gegen den Browser mit JavaScript arbeiten, kann ich für den Firefox das AddOn *NoScript*[23] empfehlen. Es unterbindet zunächst die Ausführung jeglicher JavaScript-Aktivitäten im Browser, kann jedoch für einzelne Seiten oder sogar Teile einer Seite freigeschaltet werden, sodass nur die bekannten und gewollten Scripts ausgeführt werden.

HTTPS

Die zwischen Browser und Webserver übertragenen Daten werden bei normalen Websites unverschlüsselt über das Internet verschickt, sodass z.B. ein Angreifer im Internetcafé oder auf dem Webserver alle geheimen Informationen wie Passwörter, PIN/TAN usw. ohne großen Aufwand auslesen und missbrauchen kann. Hiergegen hilft nur die verschlüsselte Übertragung der Daten mittels HTTPS.

HTTPS basiert auf einer sog. asynchronen Verschlüsselung. Im Gegensatz zur synchronen Verschlüsselung, bei der Sender und Empfänger das gleiche Passwort zum Ver- und Entschlüsseln der Daten benutzen, gibt es bei der asynchronen Verschlüsselung ein sog. Schlüsselpaar aus einem geheimen (privaten) und einem öffentlich zugänglichen Schlüssel. Daten, die mit dem privaten Schlüssel verschlüsselt werden, können nur mit dem passenden öffentlichen Schlüssel wieder entschlüsselt werden und umgekehrt.

Würde bei HTTPS ein synchrones Verschlüsselungsverfahren verwendet, hieße das, dass jeder Besucher einer Website einen individuellen geheimen Schlüssel mit dem Webserver aushandeln müsste. Dieser Schlüssel müsste dann irgendwie zwischen Browser und Webserver übermittelt werden, ohne dass er von Angreifern mitgelesen werden kann, also z.B. per E-Mail oder Telefon. Man kann sich vorstellen, dass ein solches Verfahren bei einer gut besuchten Website praktisch nicht durchführbar ist.

Beim asynchronen Verfahren hingegen kann der öffentliche Schlüssel ohne weiteres der gesamten Welt zur Verfügung gestellt werden, z.B. per Download. Lediglich der private Schlüssel darf auf keinen Fall kompromittiert werden. Bei HTTPS besitzt der Webserver einen privaten Schlüssel. Den passenden öffentlichen Schlüssel kann sich der Browser dann einfach herunterladen und ihn nutzen, um Daten zu verschlüsseln, die nur der Webserver mit seinem privaten Schlüssel wieder entschlüsseln kann.

Asynchrone Verschlüsselungsverfahren haben zwei Anwendungsfälle:

1) A verschlüsselt Daten mit dem öffentlichen Schlüssel von B. Nur B kann die Daten nun mit seinem privaten Schlüssel wieder entschlüsseln. → Vertraulichkeit der Daten
2) B verschlüsselt Daten mit seinem privaten Schlüssel. Wenn A die Daten nun mit dem öffentlichen Schlüssel von B wieder entschlüsseln kann, weiß A mit Sicherheit, dass die Daten nur von B stammen können. → Authentizität der Daten

Beide Anwendungsfälle werden bei HTTPS genutzt. Der erste Fall ist offensichtlich: Der Browser verschlüsselt geheime Daten wie Passwörter und PINs mit dem öffentlichen Schlüs-

[23] https://addons.mozilla.org/de/firefox/addon/noscript/

sel des Webservers und schickt ihm die verschlüsselten Daten. Nun kann nur der Webserver mit seinem privaten Schlüssel die Daten wieder entschlüsseln und sie wurden damit sicher übertragen.

Doch woher weiß der Browser, dass der ihm angebotene öffentliche Schlüssel auch wirklich dem Webserver gehört und nicht einem Angreifer, der den Server vielleicht gehackt hat? Hier kommt der zweite Anwendungsfall und eine dritte Partei ins Spiel: die sog. Zertifizierungsstellen (engl. CA = Certificate Authority). Diese Unternehmen beglaubigen öffentliche Schlüssel von Webservern, indem sie diese mit ihrem eigenen privaten Schlüssel „unterschreiben“, also verschlüsseln. Dieses Konstrukt aus öffentlichem Webserver-Schlüssel, der mit dem privaten CA-Schlüssel verschlüsselt wurde, nennt man Zertifikat. Alle Browser haben die gültigen öffentlichen Schlüssel aller wichtigen CAs schon integriert und können daher aus dem Zertifikat den Webserver-Schlüssel entschlüsseln. Wenn dies funktioniert, weiß der Browser, dass es sich beim entschlüsselten öffentlichen Schlüssel um den echten (weil von der CA beglaubigten) öffentlichen Schlüssel des Webservers handelt.

Beispiel (PK = public key = öffentlicher Schlüssel, SK = secret key = privater Schlüssel):

1) Webserver übermittelt sein Zertifikat an den Browser: $SK_{CA}(PK_{WS})$
2) Browser schaut in seiner integrierten Liste an CA-PKs nach, ob er den passenden Schlüssel PK_{CA} zum Zertifikat hat. Wenn ja, entschlüsselt er das Zertifikat: $PK_{CA}[SK_{CA}(PK_{WS})] = PK_{WS}$
3) Da der Browser der CA vertraut, weiß er nun, dass PK_{WS} der gültige öffentliche Schlüssel des Webservers ist und kann ihn zur Verschlüsselung benutzen: PK_{WS}(Passwort)
4) Der Webserver entschlüsselt nun mit seinem privaten Schlüssel die übertragenen Daten: $SK_{WS}[PK_{WS}$(Passwort)] = Passwort

Da das asynchrone Verschlüsselungsverfahren rechenintensiver ist als ein synchrones, wird bei HTTPS durch den Browser ein sog. Sitzungsschlüssel generiert, der dann asynchron verschlüsselt an den Webserver gesendet wird. Mit diesem synchronen Sitzungsschlüssel wird nun der weitere Datenverkehr verschlüsselt. Eine genauere Beschreibung des HTTPS-Verfahrens gibt es im Internet.[24]

Ob man mit einer Website verschlüsselt kommuniziert, erkennt man in der Adresszeile des Browsers: steht dort *https* anstatt *http*, ist die Verbindung verschlüsselt. Zusätzlich markieren alle modernen Browser die Adresszeile deutlich sichtbar blau oder grün, je nach verwendetem Zertifikat. Das Firefox-AddOn *HTTPS Everywhere*[25] erkennt automatisch, ob eine Website eine verschlüsselte Verbindung anbietet, und leitet den Benutzer dorthin um, ohne dass er daran denken muss.

[24] http://www.softed.de/fachthema/https.aspx
[25] https://www.eff.org/https-everywhere

Zertifikatsfehler sollten auf keinen Fall ignoriert und einfach weggeklickt werden, da sie auf einen Angriff hinweisen können (aber nicht müssen). Mehr Informationen zu diesem Thema gibt es z.B. bei Microsoft.[26]

E-Mail

Für die verschlüsselte Übertragung der Anmeldedaten und Mailinhalte an den eigenen Mailserver kann man analog zu HTTPS *SMTPS* konfigurieren. Das muss der Mailprovider allerdings auch anbieten. Ob dies der Fall ist, kann man auf der Website des Providers (z.B. GMX, Web.de) nachlesen. Dort sollte es auch Anleitungen zur Konfiguration der Verschlüsselung in den verschiedenen Mailclients (z.B. Thunderbird, Outlook) geben.

SMTPS verschlüsselt allerdings nur die Verbindung zum eigenen Mailserver. Der Weg zum Mailserver des Empfängers über das Internet ist wieder unverschlüsselt. Will man die Mailinhalte also vertraulich halten, muss die Mail auf andere Weise verschlüsselt werden. Dafür gibt es die Software *PGP*[27] (*Pretty Good Privacy*). Damit kann man beliebige Inhalte (also auch Dateien usw.) auf asynchrone Weise verschlüsseln. Man braucht lediglich den öffentlichen Schlüssel des Empfängers, um ihm eine verschlüsselte Nachricht zu schicken. Detaillierte Anleitungen zu diesem Thema findet man im Internet.[28] Eine gute Integration der Verschlüsselung mit PGP bietet *Enigmail*[29] für Thunderbird.

Ein wichtiger Hinweis noch bzgl. Phishing-Mails: Selbst wenn diese E-Mails inzwischen teils sehr echt wirken: kein seriöses Unternehmen (egal ob Bank, Amazon oder eBay usw.) verschickt Mails mit der Aufforderung zur Anmeldung am eigenen Konto. Und selbst wenn dies einmal der Fall sein sollte, sollte man die angegebenen Links in der Mail niemals (!) direkt anklicken, sondern immer manuell – am besten über gespeicherte Bookmarks – die Website des Unternehmens besuchen, da Links in E-Mails leicht gefälscht werden können.

[26] http://windows.microsoft.com/de-DE/windows-vista/About-certificate-errors
[27] Eine Implementierung für Windows ist z.B. http://www.gpg4win.de/
[28] z.B. http://www.gpg4win.de/doc/de/gpg4win-compendium.html
[29] https://addons.mozilla.org/de/thunderbird/addon/enigmail/