

# E-Mail, Instant-Messaging & Co. Praktisch! Und sicher?

Vortrag zum eSecurity Day der Wirtschaftskammer Salzburg am 30.11.2004  
**Thiemo Sammern, [info@sammern.at](mailto:info@sammern.at)**

## Ein typischer Tag

Sachbearbeiter Ulrich P. sitzt vor seinem PC und arbeitet die eingehenden E-Mails ab. Bei einigen der eingehenden E-Mails meldet ihm sein Virens scanner, dass die Mails gefährliche Attachments enthalten haben, die vom Virens scanner gelöscht wurden. Eine der Mails, die dennoch durchgekommen ist, weckt sein Interesse. Die Mail enthält ein Foto, das laut Text der Mail schreiend komisch ist und das er sich deshalb unbedingt ansehen soll. Da Ulrich gelernt hat, dass das Betrachten von Fotos unbedenklich ist und es sich ja nicht um eine EXE- oder VBS-Datei handelt öffnet er das Foto. Er findet es nur begrenzt komisch, aber Geschmäcker sind ja bekanntlich verschieden. In einer Arbeitspause surft Ulrich etwas im Netz herum um sich Informationen für den irgendwann geplanten Urlaub nach Australien zu holen. Er findet eine Seite, von der man einen Bildschirmschoner herunterladen kann, der die schönsten Landschaften Australiens zeigt. Das Installationsprogramm arbeitet tadellos (die Software verlangt sogar eine Registrierung, was Ulrich aber mit falschen Daten ausfüllt; schließlich will man ja nicht jedem seine Daten geben!) und nach kurzer Zeit sieht man am Bildschirm eindrucksvolle Fotos von „down-under“. Zum Mittagessen hat er sich via Instant Messaging mit einer Kollegin verabredet und bis diese sich meldet, schreibt er noch einige Berichte und führt eine Bestellung für ein Fachbuch bei einem Buchversand mit der Firmenkreditkarte durch. Da er nicht will, dass der Buchhändler seine Kreditkarte speichert (wer weiß, was der alles damit anstellt?) gibt er sie bei jeder Bestellung neu ein. Als kurze Zeit später eine Mail seiner Bank eingeht, die ihn um Bestätigung seiner Daten mit einem TAN-Code bittet, ruft er den in der Mail enthaltenen Link zur Bankseite auf, um die Daten auszufüllen. Seine TAN-Liste hat er glücklicherweise dabei, da sein Internet-Zugang zuhause gerade gestört ist und er sowieso einige Überweisungen mit Internet-Banking machen wollte. Nach dem Mittagessen arbeitet Ulrich noch 2,5 Stunden (es ist Freitag) und freut sich auf den bevorstehenden Urlaub (3 Wochen kein Büro!). Kurz vor dem Gehen sieht er noch einem Kollegen zu, der das neue Spiel „Waldpute“ heruntergeladen hat. Es sieht sehr unterhaltsam aus und Ulrich fragt seinen Kollegen, ob er das Spiel in seiner Abwesenheit auch auf seinem PC installieren könnte damit sie es in Pausen gegeneinander spielen können.

Als er nach dem Urlaub zurückkommt, ist die Hölle los. Laut seinem Kontostand hat Ulrich im Urlaub um einiges mehr an Geld verbraucht als er gedacht hatte. Und auch in der Firma sind einige seltsame Dinge passiert...

Hat er etwas falsch gemacht?

## Was ist passiert?

Im obigen Beispiel wurden einige Arten beschrieben, wie man sich „Malware“ (Viren, Trojaner, Würmer, Spyware, ...) auf den eigenen PC holen kann. Die Auswirkungen in Form vom leeren Konto bis zum Verlust von Firmendaten sind ebenfalls kurz angeschnitten worden. Sehen wir uns die Bedrohungen im Detail an und auch wie man sich davor schützen kann.

## Prinzipielle Vorbemerkungen

Ein auf einem PC installiertes Programm darf im Normalfall alles, was auch der Benutzer darf, der es laufen lässt. Das bedeutet, es kann Dateien erzeugen, verändern und entfernen, es kann auf Daten auf dem Netzwerk zugreifen und normalerweise auch Verbindungen ins Internet aufbauen oder sich für Verbindungen aus dem Internet öffnen. Sehr oft darf es auch Änderungen an der Systemkonfiguration des eigenen PCs vornehmen, in manchen Fällen sogar den Server konfigurieren.

Eine sehr wichtige Erkenntnis:

**Ein Programm tut nicht immer nur das, was es zu tun scheint.**

## Bedrohungen aus dem Internet

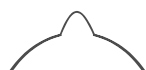
Sehr oft gibt es bei Benutzern die Befürchtung, dass „Hacker“ aus dem Internet in ihren PC eindringen und dann Daten ausspionieren. Sehr häufig ist es jedoch eher so, dass sich die Benutzer die Hacker unabsichtlich in ihr System einschleusen. Um das zu verstehen, muss man etwas Wissen über die Funktionsweise von Datenverbindungen im Internet aufbauen.

## TCP, Ports und IP-Adressen

Das Transaction-Control-Protocol (TCP) kümmert sich um den Verwaltung von Verbindungen zwischen verschiedenen Computern. Eine TCP-Verbindung hat immer eine Quelle (von dort wurde die Verbindung aufgebaut) und ein Ziel. Beide werden in Form von IP-Adressen angegeben. Die IP-Adresse (4 Zahlen zwischen 0 und 255, z.B. 213.229.60.100) werden über das Domain-Name-System (DNS) in Namen umgewandelt, die man sich als Mensch besser merken kann (z.B. [www.orf.at](http://www.orf.at) = 194.232.104.27). Zusätzlich zur IP-Adresse muss bei jeder Verbindung auch ein Quell- und Ziel-Port (Anschluss) angegeben sein. Der Quellport wird dabei normalerweise vom Betriebssystem frei gewählt während der Zielport durch die Art des Dienstes, der benötigt wird, definiert wird. So ist für das Surfen im Internet über http (Hypertext transfer protocol) der Port 80 vorgesehen, das Versenden von E-Mails mit dem Standard-Protokoll SMTP (Simple Mail Transfer Protocol) geht über Port 25 und das Abholen von Mails mit dem POP3-Standard arbeitet mit Port 110. Alle diese Einstellungen sind für den Benutzer normalerweise unsichtbar. Wichtig ist dabei aber, dass sobald eine Verbindung aufgebaut ist, Daten auf dieser Verbindung in beide Richtungen laufen können. Eine Verbindung mit einem „Hacker“ im Internet kann also entweder aufgebaut werden, indem der Hacker einen offenen Port auf dem PC seines Opfers findet, den er ausnutzen kann, oder indem das Opfer von sich aus eine Verbindung zu einem offenen Port des Hackers aufbaut. Meist wird nur auf die erste Möglichkeit Rücksicht genommen, da angenommen wird, dass der eigene PC geschützt und vertrauenswürdig ist.

## Was macht eine Firewall?

Das Schließen von offenen Ports gegenüber dem Internet ist noch recht einfach: viele Unternehmen sind mit kostengünstigen Routern an das Internet angeschlossen. Diese



Router lassen (sofern entsprechend konfiguriert) nur Verbindungen nach außen aber keine Verbindungen nach innen zu. Für bestimmte Anwendungen (z.B. den Fernwartungszugang für den EDV-Techniker oder den Mailaustausch mit dem internen Mail-Server) werden wohldefinierte Ausnahmeregeln konfiguriert. Zusätzlich werden manchmal auch auf den jeweiligen Arbeitsplätzen Personal Firewalls installiert, bei denen für jedes Programm gesondert eingestellt werden kann, ob dieses Programm eine Verbindung ins Internet aufbauen darf und wenn ja, wohin. Klarerweise bedarf die korrekte Konfiguration derartiger Programme eine ausgedehnte Analyse durch den Administrator. Der „normale“ Benutzer sollte nicht die Möglichkeit haben, die Firewall-Konfiguration zu ändern, denn das führt oft dazu, dass die Meldungen der Programme (z.B. „Programm waldpute.exe will eine Verbindung zu 198.38.292.220 auf Port 7382 aufbauen. Blocken J/N?“ oder „Programm myicq.exe will den Port 3839 für eingehende Verbindungen öffnen. Zulassen J/N?“) von den Benutzern „weggeklickt“ werden, weil sie nicht verstanden werden. In so einem Fall kann man sich den Aufwand für die Firewall gleich sparen, denn sie ist mit einem Mausklick unschädlich gemacht. Manche PCs (speziell Server) erfordern es, dass manche Ports für die eingehende Kommunikation geöffnet bleiben. Sonst könnte man z.B. keine Daten über das Netzwerk hin- und herschicken, denn beim Aufbau der Netzwerk-Verbindung muss es ja bei der Gegenstelle einen Port geben, den man „anrufen“ kann. Einfach alles zu schließen ist also nicht unbedingt eine Lösung.

## **Sicherheitslücken, Buffer Overflows & Co**

Sehen wir uns den „typischen Tag“ unseres Internet-Users nochmals etwas genauer an.

### **Virens Scanner filtert schädliche Mails**

Jedes PC-System, das auch nur irgendwie mit anderen Systemen in Verbindung steht (und das sind so gut wie alle) benötigt einen Virens Scanner. Weiters ist es auch schon allgemein bekannt, dass der Virens Scanner nur dann arbeiten kann, wenn er mit aktuellen Virendefinitionsdateien aktuell gehalten wird. Nachdem die Virenepidemien immer schneller ablaufen, sollte das Aktualisierungsintervall im Bereich von Stunden bis wenigen Tagen liegen. Zum Schutz von Unternehmen gibt es eigene Produkte, die über einen Server zentral verwaltet werden können, sodass ein Administrator immer auch sieht, ob alle Arbeitsplätze über einen aktuellen Virenschutz verfügen. Die Benutzer müssen sich also nicht darum kümmern.

---

#### **Tipp:**

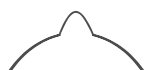
- Virens Scanner immer aktuell halten (Stunden bis wenige Tage Intervall)
- Aktualisierung zentral steuern (Unternehmensversionen)
- Regelmässig prüfen, ob die Aktualisierungen funktionieren

---

#### **Gefahr:**

Die Benutzer werden durch den Virens Scanner „übermütig“, da sie sich in Sicherheit wiegen: „wenn ein E-Mail vom Virens Scanner nicht als gefährlich erkannt wird, muss es ungefährlich sein“. Das ist falsch. Erstens wäre es möglich, dass man eine Mail mit einem ganz neuen Virus erhält, die der Virens Scanner noch nicht kennt und zweitens gibt es auch Attachments, die vom Virens Scanner nicht unbedingt als gefährlich erkannt werden, weil es sich scheinbar um ganz normale Programme handelt.

Ähnliches Verhalten kennt man auch bei Autofahrern, die den Vorteil der aktiven Sicherheit durch ABS, ESP, DSC, Allrad, etc. durch höheres Risiko kompensieren.



### **Eine Mail mit einem Foto ist ungefährlich?**

Was vielleicht gestern noch als ungefährlich gegolten hat, muss heute nicht mehr so sein. So wurde vor wenigen Wochen eine Sicherheitslücke in mehreren Windows-Programmen<sup>1</sup> bekannt, die durch das Betrachten einer manipulierten JPEG-Datei einen Buffer Overflow erzeugte, der zum Einschleusen von fremder Software genutzt werden konnte. Diese fremde Software „darf“ dann alles, was der aktuelle Benutzer darf.

### **Was ist ein Buffer Overflow?**

Die meisten der aktuellen Sicherheitslücken entstehen durch sogenannte „Buffer Overflows“. Diese entstehen dadurch, dass einem Programm, das auf bestimmte Werte wartet, ganz andere übermittelt werden, auf die das Programm nicht vorbereitet ist. Viele Programmierer scheuen den Aufwand die Eingabewerte für ihre Programme auf Gültigkeit oder maximale Länge zu überprüfen. Die Programme arbeiten dann zwar vielleicht absolut korrekt, solange sich die Eingabewerte im erwarteten Rahmen befinden. Wenn Werte außerhalb dieses Bereichs kommen stürzen die Programme jedoch entweder ab (Denial-of-Service Attacke) oder werden durch gefinkelte Angriffe dazu gebracht, andere Software im Sinne des Angreifers auszuführen.

### **Installieren von fremder Software**

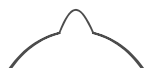
Das Installieren von fremder Software auf dem eigenen Arbeitsplatzrechner ist eine weit verbreitete Unart. Es soll hier nicht um die Frage der Lizenzierung gehen sondern allein um die Tatsache, dass klar sein muss, dass jede Software potentiell großen Schaden anrichten kann. Daher sollte man nur Software installieren, die man wirklich braucht, die aus vertrauenswürdiger Quelle stammt und bei der keine Seiteneffekte auf das System zu erwarten sind.

Einige Beispiele, was geschehen kann:

- Das Installationsprogramm für den Bildschirmschoner könnte Spyware installieren, das das Surfverhalten aufzeichnet (dafür ist der Bildschirmschoner kostenlos!) und manchmal Werbeeinblendungen macht. Das kann dann z.B. dazu führen, dass beim Öffnen des Internet Browsers der Bildschirm mit leichtbekleideten Damen gefüllt wird oder dass man Suchergebnisse statt in Google von einer ganz anderen, unbekanntenen Suchseite zurückbekommt. Außerdem wird der PC immer langsamer, aber das wird von vielen Benutzern ja als normal angenommen.
- Das kleine lustige Spiel aus dem Internet könnte einen Keylogger installieren, der jeden Tastendruck protokolliert und darauf wartet, dass man Passwörter oder Kreditkartennummern eingibt. Diese wertvollen Informationen werden dann ins Internet hinausgeschickt wo sie sicher bei jemand landen, der mit ihnen etwas anzufangen weiß.
- Das AddOn für den installierten Instant Messenger erinnert nicht nur an den Geburtstag der Kollegen sondern stellt außerdem eine Verbindung zu einem IRC-Server auf, durch die es auf Befehle seines „Herren und Meisters“ wartet, z.B. das Versenden von 100.000 Spam-Mails über die Firmenstandleitung.
- Der „Geheimtipp“ zum Schutz gegen Viren beginnt im Hintergrund mit einer BruteForce-Attacke gegen die Passwort-Datenbank des Servers, um das Administrator-Kennwort zu erhalten, damit es dann wirklich viel Schaden anrichten kann.

---

<sup>1</sup> <http://www.microsoft.com/germany/ms/security/jpegsec.mspx>



## Was kann man tun?

### Sicherheitsupdates installieren

Für die meisten der bekannten Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen werden von den Herstellern recht schnell Updates programmiert, die diese Lücken schließen. Diese Updates sind dann in vielen Fällen schon verfügbar, bevor die Sicherheitslücke von Hackern im großen Stil ausgenutzt werden kann.

Viele Unternehmen warten mit der Installation dieser Updates zu lange oder ignorieren sie ganz, weil sie sich nicht mit den Hintergründen beschäftigen, die Kosten für die Installation scheuen oder schädliche Auswirkungen auf die Systeme befürchten. Sehen wir uns die Gründe im Detail an:

#### **Argument „Nach dem Update geht dann sicher die Hälfte meiner Programme nicht mehr!“**

Obwohl die Updates von den Herstellern natürlich vor der Veröffentlichung getestet werden, ist es faktisch unmöglich, jede mögliche Kombination aus Hardware und Software zu testen. Manchmal tritt durch die Installation eines Updates ein Fehler, der sich vielleicht schon lange im System versteckt hat, erst zu Tage. Gefährdet sind hier vor allem Server, da sie nur sehr selten neu gestartet werden (Durchgehende Laufzeiten von mehr als 100 Tagen sind bei den heutigen Betriebssystemen die Regel und nicht mehr die Ausnahme).

„Normale“ Sicherheitsupdates wie sie z.B. zwei-wöchentlich beim Microsoft Patch-Day erscheinen, sind meist eher ungefährlich einzuspielen. Etwas anders sieht es bei den „großen“ Updates wie z.B. dem Microsoft Service Pack 2 für Windows XP aus. Hier sollte der PC vor der Installation wirklich genau geprüft werden, um auf allfällige Probleme schnell reagieren zu können.

#### **Argument: „Ich zahle doch nicht alle 2 Wochen für ein paar Stunden einen Techniker, der überall Updates einspielt“**

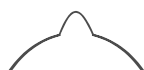
Neuere Software-Programme und Betriebssysteme verfügen über die Funktion zum automatischen Herunterladen und Installieren von Updates. Dabei werden üblicherweise nur die sicherheitsrelevanten Updates berücksichtigt. Es gibt auch die Möglichkeit, die anstehenden Updates zuerst zentral auf einen internen Server herunterzuladen, dort explizit zur Installation freizugeben und automatisiert an die einzelnen Arbeitsplätze verteilen zu lassen<sup>2</sup>. Die Benutzer merken von dieser ganzen Prozedur wenig bis gar nichts. Gute EDV-Betreuungsunternehmen bieten „all-inclusive“ Dienstleistungen pro Arbeitsplatz an, bei denen auch das Einspielen von allfälligen Updates etc. inkludiert sind. Damit sind auch die Kosten gut kalkulierbar.

#### **Gilt das alles nur für Microsoft Windows-Systeme?**

Durch die hohe Verbreitung der Microsoft Betriebssysteme und –Anwendungen sind diese ein beliebtes Ziel für Angriffe. Im Prinzip gelten die genannten Aussagen jedoch auch für andere Betriebssysteme inklusive Linux. Mit steigender Verbreitung werden auch diese Systeme für Angriffe immer interessanter. Die Updates für Windows-Betriebssysteme konzentrieren sich vor allem auf die aktuellen Betriebssysteme Windows 2000 und Windows XP bzw. Windows Server 2003. Für Windows98 (das aufgrund seiner Konzeption für den Unternehmenseinsatz nicht wirklich geeignet ist) gibt es noch

---

<sup>2</sup> <http://www.microsoft.com/germany/ms/security/guidance/prodtech/SUS.msp>



kritische Updates bis 30.6.2006, für Windows NT 4.0 ist der Support bereits eingestellt<sup>3</sup>. Der Umstand, dass es z.B. für Windows95 keine Sicherheitsupdates gibt bedeutet leider nicht, dass dieses System sicher ist (wie es von manchen Win95-Benutzern ernsthaft zu hören ist) sondern dass dieses System schon von seiner Konzeption her in vielen Bereichen so offen ist, dass es gar keinen Sinn mehr hat dafür Updates zu erstellen.

### **Bringt der Umstieg auf alternative Browser, E-Mail-Clients<sup>4</sup>, etc. einen Sicherheitsvorteil**

Ja, aber es können auf diese Weise nicht alle Sicherheitslücken geschlossen werden. Manche befinden sich wirklich auf Betriebssystem-Ebene oder sind durch Anwendungen wie den Internet Explorer sehr mit dem Betriebssystem verbunden. So wurde z.B. die zuvor erwähnte Komponente zur Anzeige von JPEG-Fotos nicht nur von Outlook für die Darstellung von Bildern verwendet sondern auch vom normalen Explorer für die Vorsicht von JPEG-Dateien in Ordnern.

### **Nicht mit Administratorrechten arbeiten**

Wenn ein PC neu installiert wird, machen es sich die Techniker oft etwas leicht und geben jedem Benutzer Administratorrechte auf dem PC. Damit kann jeder Benutzer auf diesem PC Software installieren und die Systemkonfiguration verändern. Das ist meistens gut gemeint, denn man will nicht, dass sich der Benutzer mit Meldungen über Zugriffsverbote auf einzelne Ordner auf der Festplatte herumärgern muss.

Diese Einstellung ist allerdings recht gefährlich, denn wenn der Benutzer alles tun kann, kann er auch alles kaputt machen. So kommt es dann zu den Geschichten von Benutzern, die z.B. den Windows-Ordner „zusammengeräumt“ haben, weil sie Platz auf der Festplatte brauchten und daher alle Dateien gelöscht haben, von denen sie glaubten sie nicht zu brauchen...

Wenn eine Schadsoftware von so einem Benutzer mit Administratorrechten auf dem PC installiert wird, hat diese leichtes Spiel den ganzen PC zu übernehmen und kann sich auch oft viel schneller auf andere Systeme verbreiten. Wenn dann auch noch der Server nicht entsprechend geschützt ist (Kein Administratorpasswort, Domänenbenutzer=Domänenadministrator, etc.) ist der GAU perfekt.

Oft wird als Gegenargument gebracht, dass es eine ganze Anzahl von Software gibt, die nur mit Administratorrechten läuft wobei als Beispiel oft CD-Brennprogramme genannt werden. Das rührt daher, dass viele Software-Entwickler selbst (fast notgedrungen) als Administrator arbeiten und daher die Software oft auch nur als Administrator getestet wird. Dazu ist zu sagen, dass die Situation hier bei weitem nicht mehr so schlecht ist, wie vor 3-4 Jahren noch. Sollte ein Programm auf den ersten Versuch hin wirklich nicht ohne Administratorrechte laufen so kann man mit Tools wie filemon und regmon<sup>5</sup> feststellen, wo es happert und die entsprechenden Berechtigungen manuell erteilen. Für das beliebte CD-Brennprogramm „Nero“ gibt es bereits seit langer Zeit das Zusatzprogramm „Nero BurnRights“ mit dem die entsprechenden Einstellungen vorgenommen werden. Und als allerletzten Ausweg kann man das „runas“-Kommando mit der „/savecred“-Option<sup>6</sup> verwenden um ein störrisches Programm explizit in einem anderen Benutzerkontext (dann mit Administratorrechten) zu starten.

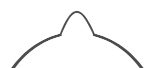
---

<sup>3</sup> <http://support.microsoft.com/gp/lifewin>

<sup>4</sup> <http://www.mozilla.org/products/firefox/> und <http://www.mozilla.org/products/thunderbird/>

<sup>5</sup> <http://www.sysinternals.com>

<sup>6</sup> <http://www.wintotal.de/Tipps/Eintrag.php?RBID=2&TID=523&URBID=13>



## Vorsicht! Vorsicht! Vorsicht!

Die tollste Hardware und Software nützt nichts, wenn sie von den Benutzern unterlaufen werden. So sind die Methoden des „social hacking“ erschreckend erfolgreich und können mit Leichtigkeit äußerst aufwendige technische Vorkehrungen sinnlos machen. Es handelt sich dabei meist um e-mails in denen man aufgefordert wird, geheim zu haltende Daten unter einem Vorwand herauszugeben. Allen diesen Mails ist gemeinsam, dass sie anscheinend aus vertrauenswürdiger Quelle wie z.B. dem eigenen Internet Provider oder von der eigenen Bank stammen. Die Absenderadressen sind jedoch natürlich gefälscht, was keine besonderen EDV-Kenntnisse erfordert. Meist verweisen die Mails auf täuschend echt nachgemachte Webseiten der scheinbaren Absender und verlangen dort die Angabe von Passwörtern, PINs und TANs, was natürlich zu großen Schäden führen kann. Da viele Menschen ihre Kontoauszüge nur wenige Male pro Monat überprüfen können die Betrüger mit den erlangten Informationen in kurzer Zeit einen hohen finanziellen Schaden anrichten und ihre Spuren verschleiern noch bevor Ermittlungen eingeleitet werden können.

Man spricht bei dieser Methode des Betrugs auch von „phishing“ (=password fishing). Genauso wie heute hoffentlich niemand mehr seine Kreditkartennummer auf einer unverschlüsselten Seite eingibt sollte es eigentlich auch selbstverständlich sein, vertrauliche Informationen vor dem Versenden per E-Mail zu verschlüsseln oder zumindest digital zu signieren bzw. misstrauisch zu werden, wenn man selbst an sich vertrauliche Daten unverschlüsselt und nicht digital signiert erhält.

---

### Tipp:

- Ihr Internet-Provider wird sie NIE per Mail um ihren Benutzernamen und ihr Kennwort fragen
- Microsoft oder ein anderer großer Software-Hersteller wird von Ihnen NIE verlangen, dass Sie Lizenznummern per unverschlüsselter e-mail übermitteln
- Ihre Bank wird Sie nicht um Zusendung Ihres Internet-Banking PINs oder TANs bitten
- Geben Sie bei Internet-Banking o.ä. die Adressen direkt in das Browser-Fenster ein und nicht durch Klicken auf einen Link in der e-mail

Sollte z.B. eine Mail über Bank-PINs und TANs ihr Misstrauen wecken kontaktieren Sie den scheinbaren Absender (also die Bank) und fragen Sie nach, ob die Mail authentisch ist (eine Nachfrage, die man sich bei digital signierten und geprüften Mails sparen könnte). Falls das nicht der Fall sein sollte, kann die Bank gleich Schritte zur Warnung ihrer Kunden setzen.

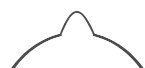
Ein kleines Beispiel, wie ein manipulierter Link zu einer Bankseite aussehen kann:

Echter Link: <http://www.meinebank.at/apps/737299938/kunden/login.php>

Manipuliert: <http://www.meinebank.at:apps@3248397892/kunden/login.php>

Der zweite Link sieht zwar recht ähnlich aus, führt aber zu einem völlig anderen Server.

Andere Angriffe des „social hacking“ gehen eher in den Bereich des „Denial-of-Service“, d.h. dass es nicht um einen direkten finanziellen Gewinn geht sondern das Opfer dadurch geschädigt werden soll, dass es das eigene Computer-System so sehr schädigt, dass nicht mehr gearbeitet werden kann. So kursierten z.B. Mails mit einer wichtigen Nachricht, die vor einem neuen Virus warnte, der von allen bekannten Anti-Virus-Tools nicht erkannt würde und großen Schaden anrichten würde, wenn man ihn nicht rechtzeitig aus dem System entfernen würde. Viele besorgte Computer-Benutzer wandten sogleich die mitgelieferte Anleitung an und löschten die betreffende Datei von ihrem PC. Bevor sie den Rechner dann neu starteten schickten sie die Mail noch an alle Bekannten weiter. Leider handelte es sich bei der gelöschten Datei um eine Systemdatei,



die für manche Funktionen des PCs benötigt wird sodass der PC durch die „Rettungsaktion“ erst recht beschädigt wurde.

Daher: Gesundes Misstrauen ist angesagt !

## **Zusammenfassung**

„Sicherheit ist kein Produkt sondern ein Prozess!“<sup>7</sup> Ein umfassendes Sicherheitskonzept muss die Teile Hardware, Software, Update-Prozesse, Benutzerrechte und „Wetware“ (=Menschen) zu einem ausgewogenen Ganzen machen. Jedes Defizit bei einem der Teile kann zu einem Totalversagen des ganzen Systems führen.

---

<sup>7</sup> <http://www.schneier.com/crypto-gram-9912.html>

