

2 RISIKEN DURCH DAS INTERNET

2.1 Risiken im Internet

Durch den explosionsartigen Anstieg von BenutzerInnen und AnbieterInnen seit 1993 steigen auch die Risiken im Internet. Das Internet wurde zum globalen Marktplatz und zu einer Schlüsseltechnologie des kommenden Jahrzehnts. Damit verbunden sind leider die Zunahme von Missbrauch und kriminellen Handlungen. Ein Internet-Anschluss ohne entsprechende Sicherheitsmaßnahmen kann zu einem Teil- oder Totalausfall der EDV-Infrastruktur führen und so enormen Schaden anrichten.

Auch ohne Internet gibt es bereits Risiken in einem lokalen Netzwerk, wie z. B.:

- fehlende oder fehlerhafte Datensicherung
- Einschleppen von Viren über private Wechseldatenträger
- „..was geschieht, wenn ich das mache ...“: „Man probiert einfach etwas aus und stellt anschließend fest, dass der PC nicht mehr gestartet werden kann!“
- Fehlbedienung des Programms

Zu diesen Unsicherheitsfaktoren kommen noch die speziellen Risiken eines Telekommunikations- oder Internet-Anschlusses:

- Eindringen von nicht autorisierten BenutzerInnen in das Informationsnetz
- Verlust von vertraulichen Informationen
- Störung der Verfügbarkeit (Sabotage, Viren, ...)
- Imageschaden in der Öffentlichkeit
- Einschleusen von Viren durch Datenübertragung

Eine Untersuchung der NCSA (National Computer Security Association) im Jahr 1995 ergab, dass Unternehmen mit einem Internet-Zugang achtmal so häufig Angriffen ausgesetzt sind wie Unternehmen ohne einen solchen Anschluss. 80% der „Angriffe“ über Telekommunikationsmedien erfolgten aus dem Internet.

Der Zugang zu jedem Computer sollte unbedingt durch einen Benutzernamen und ein Kennwort geschützt werden.¹⁴

2.2 Wer sind die AngreiferInnen?

Ein großer Teil der mutwilligen Beschädigungen von PCs und Netzwerken wird von MitarbeiterInnen der Firma aus unterschiedlichen Gründen (Frustration, ungerechte Behandlung, Kündigung, ...) selbst verursacht.

¹⁴ Wenn der Zugang nicht geschützt ist, dann kann jeder, der vor diesem Computer sitzt, Ihre Daten einsehen, Ihre E-Mails abrufen usw. Ich, der Autor, bin sicher, dass Sie das nicht wollen!

Viele Fälle erfolgreicher Netzwerk-Einbruchsversuche beruhen auf Nichtbefolgung von internen Sicherheitsvorschriften. Zum Beispiel wird beim so genannten **social hacking** eine falsche Identität vorgetäuscht, mit dem Ziel eines Zuganges oder einer Kennwortänderung.

Aus den Phone-Freaks der 60er und 70er Jahre haben sich die Hacker (**Cracker**) entwickelt. In eigenen, so genannten Untergrund-E-Mailboxen – kurze Lebenszeit, ständiger Wechsel – tauschen sie ihr Wissen gegenseitig aus. In Hackerzeitschriften (Phrack, 2600) werden regelmäßig Cons (Conventions) abgehalten.

Neben den zu erwartenden Computerkriminellen treten aber auch

- Kriminelle aus dem Drogen- und Mafiaumfeld,
- professionelle Hacker,
- Rechts- und Linksradikale,
- usw.

auf.

Neben dieser kriminellen Szene existieren auch Vereinigungen (z. B. der CCC – Chaos Computer Club), die die Gefahren, Probleme, Risiken und Lücken der derzeitigen Technologie aufzeigen.



Abb.: Phrack, eine Zeitschrift für Hacker

Mögliche Bedrohungsszenarien durch Cracker sind:

- Identitätstäuschung und missbräuchliche Nutzung
- Ausspähen von Daten und Vorgängen
- Verfälschen von Daten und Programmen
- Diebstahl von Daten, Rechen- und Kommunikationszeit
- Unterschieben von Daten
- Image-Verlust

2.3 Schutzmaßnahmen

2.3.1 Authentifizierungssysteme

Netzwerkssysteme können durch Benutzernamen und Kennwörter (Passwörter) vor unberechtigtem Zugriff geschützt werden. Arbeitende Personen in einem Netz sollten immer ein eigenes Benutzerkonto haben, unter dem sie sich anmelden. Wer jedoch einen Benutzernamen und das dazugehörige Kennwort errät, kann sich dem System gegenüber als berechtigter/e BenutzerIn ausgeben!

Passwort-Angriffe mittels unterschiedlicher Strategien:

- Erraten des Kennwortes – Wörterbuchprogramme
- Filtern des Netzwerkverkehrs (Sniffer)
- Passwort-Monitoring
- Social Hacking

Untersuchungen in einem großen Unternehmen ergaben, dass 10% aller BenutzerInnen ihren Vornamen als Kennwort benutzen!

Ein sicheres Kennwort ist kein Wort einer Sprache, sondern eine Kombination von Buchstaben, Ziffern, und Sonderzeichen, die regelmäßig geändert werden sollte.

2.3.2 Firewalls für den Schutz des internen Netzes

Wenn ein Unternehmen sein Datennetz an das Internet anschließt, sollte dies nicht ohne Installation einer so genannten Firewall geschehen. Aufgabe der Firewall ist es, einen ungestörten Betrieb im firmeninternen Netzwerk zu gewährleisten und vor unberechtigten Zugriffen aus dem öffentlichen Netz (= Internet) zu schützen. Daraus folgt, dass auch der Zugang des Unternehmens zum Internet ausschließlich über die Firewall erfolgen darf.

Eine Firewall kann dabei aus mehreren Hard- und/oder Softwarekomponenten bestehen.

Neben der Zugriffskontrolle besteht eine wesentliche Funktion der Firewall darin, auffällige Ereignisse zu erkennen und diese zu melden. Mit Hilfe spezieller Kontroll- und Überwachungsprogramme sollten folgende Informationen möglich sein:

- Anzeige von Verbindungen, geordnet nach Diensten und BenutzerInnen
- Anzeige der Aktivierung von Sicherheitsfunktionen
- Anzeige von wiederholten Versuchen, das Firewall-System zu umgehen.

Kontroll- und Überwachungssysteme sowie die Protokolldateien müssen dabei vor nicht autorisierten Zugriffen geschützt sein. Problematisch ist, dass im Vorhinein schwer abschätzbar ist, welche Daten für eine spätere Analyse benötigt werden.

Firewall-Systeme können Daten, die innerhalb von Applikationen versandt werden (z. B. Viren), nicht filtern und entfernen. Aus alledem folgt, dass neben Firewall-Systemen weitere Sicherungsmaßnahmen durch den Betreiber des Netzes vorgenommen werden müssen, die bis hin zu PGP¹⁵ und verschlüsselter Übertragung von Daten im gesamten Netz reichen.

2.4 Antivirensoftware

Neben ernsthaften Programmierern, die verkäufliche Software herstellen, gibt es leider auch Spaßvögel und Personen mit Geltungsdrang, die Programme in Umlauf setzen, welche effektiv Schaden anrichten können. Sie haben sicherlich bereits von dem Begriff Viren gehört!

2.4.1 Was sind Viren?

Unter Viren versteht man Programme, die sich selbst duplizieren. Neben der Vervielfältigung können Viren aber auch Manipulationen an Daten oder anderen Programmen vornehmen. Eine derartige Manipulation könnte z. B. sein, dass Teile eines Textdokumentes gelöscht oder durch andere Zeichenfolgen ersetzt werden. Derartige Manipulationen verursachen natürlich immaterielle und finanzielle Schäden, die beachtliche Ausmaße annehmen können.

Neben digitalen Viren gibt es jedoch auch Programme, die keine Viren sind, aber trotzdem Schaden verursachen:

- **Malware:** Der zusammengesetzter Begriff aus den beiden Wörtern **malicious** – englisch: böseartig – und **Software**. In diesem Fall handelt es sich um schädliche Software, bei der das Programm einen Schaden am Computer verursacht. Malware wird als Überbegriff für Viren, Würmer, trojanische Pferde, ... verwendet.

¹⁵ PGP – pretty good privacy – ist eine Software zum Verschlüsseln von Daten.

- **Würmer:** Diese Programme verbreiten sich selbständig. Dabei handelt es sich nicht um Viren, sondern um Störprogramme, die ein Netzwerk, ja sogar das globale Internet lahmlegen können.
- **Trojanische Pferde:** Bei dieser Gruppe von Programmen handelt es sich um Produkte, die offensichtlich für den Anwender einen Nutzen haben. Sie laden sich z. B. aus dem Internet einen neuen Bildschirmschoner herunter. Während der Anwender den neuen tollen Bildschirmschoner und dessen Animation betrachtet, wird im Hintergrund – für den Anwender unsichtbar – eine schädliche Funktion ausgeführt. So könnte z. B. der Bildschirmschoner eine Routine installieren, mit dem Benutzernamen und Kennwörter ausgespäht werden usw.
- **Spyware:** Wie der Name andeutet, spähen derartige Programme den Benutzer aus. Nachdem sie installiert wurden, durchsuchen sie die Festplatte des PCs und schicken Informationen an den Hersteller der Spyware ohne Wissen des Benutzers. In einer anderen Form werden dem Benutzer des befallenen PCs Produkte angeboten.
- **Hoaxe:** Dies ist eine gezielte Falschmeldung per E-Mail. In derartigen E-Mails wird man meist vor einem Virus oder einem anderen Schadensprogramm gewarnt. In weiterer Folge wird man dann noch gebeten, diese E-Mail an Freunde und Bekannte weiterzuleiten, um möglichst viele Anwender vor einem etwaigen Schaden bewahren zu können. Der Schaden, der durch derartige Falschmeldungen entsteht, liegt in der verbrachten Arbeitszeit, der benötigten Kapazität, um E-Mails weiterzuleiten etc.
- Usw. ...

2.4.2 Infektionswege und Schutz gegen Viren

Der wohl **gefährlichste Ort für eine Infektion** – so nennt man den Vorgang, wenn man einen Virus einschleppt – ist mittlerweile **das Internet**. Durch die Installation eines heruntergeladenen Programms aus dem Internet oder eines E-Mails, dem ein Programm beigefügt wurde, werden viele Anwender mit dem Thema Viren konfrontiert. Neben diesen beiden Möglichkeiten können Viren natürlich auch über Datenträger wie USB-Stick oder Disketten übertragen werden. In besonders schweren Fällen genügt bereits ein lesender Zugriff auf ein Speichermedium, um sich mit einem Virus zu infizieren.

Um sich gegen Viren wirksam zu schützen, muss man unbedingt eine Antiviren-Software installieren.

Neben käuflichen Produkten werden auch **Share**¹⁶- und **Freeware-Produkte** angeboten. Nach der Installation laufen die meisten Antivirenprogramme als Dienste, das sind Programme, die im Hintergrund arbeiten und so vor der Infektion mit einem Virus schützen.

¹⁶ Shareware-Produkte unterliegen ebenfalls dem Urheberrecht, dürfen aber weitergegeben werden. Wenn das Produkt genutzt wird, ist eine geringe Shareware-Gebühr an den Programmautor abzuführen.

Trotz allem sollten Sie in regelmäßigen Abständen das Antivirenprogramm manuell starten und Ihre Datenträger und den Hauptspeicher nach Viren untersuchen.

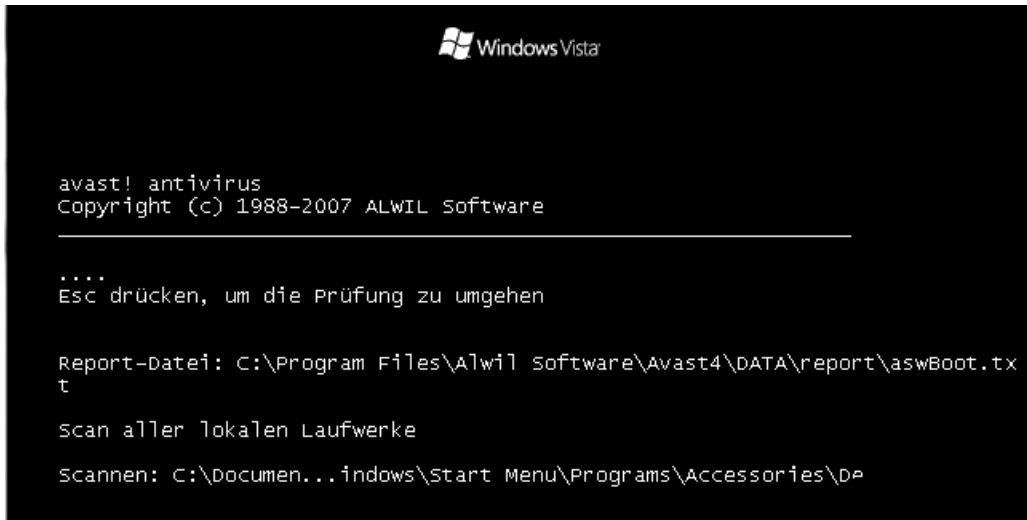


Abb.: Erstprüfung auf Viren nach der Installation von AVAST Antivirus¹⁷

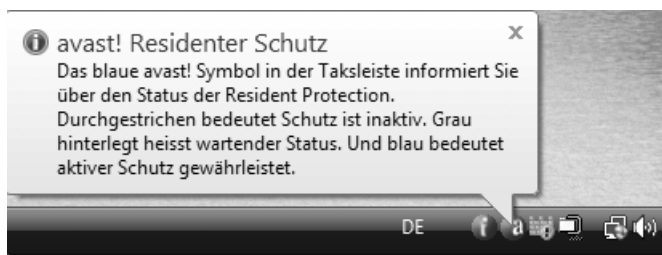


Abb.: Meldung des Antivirenprogramms nach dem Anmelden des Benutzers

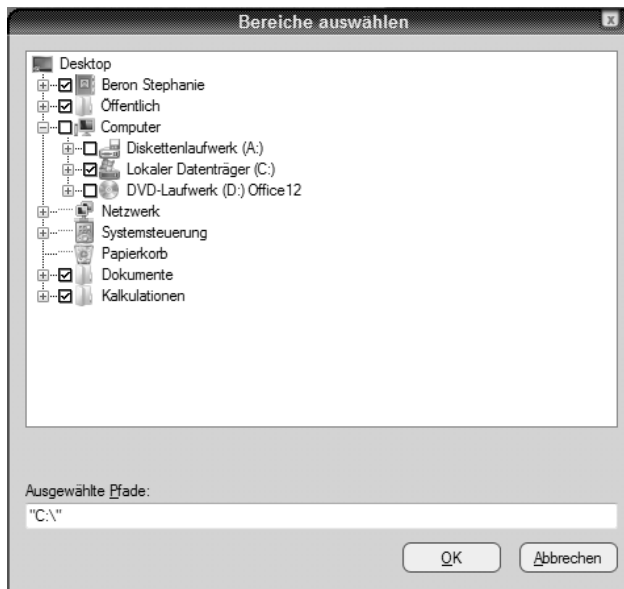


Abb.: Auswahl des Laufwerkes für einen manuellen Virensuchlauf-Scan

¹⁷ AVAST Home Edition ist für Privatanwender ein kostenloses, sehr gutes Antivirenprogramm. Nähere Informationen finden Sie unter <http://www.avast.at/avasthome.htm>.

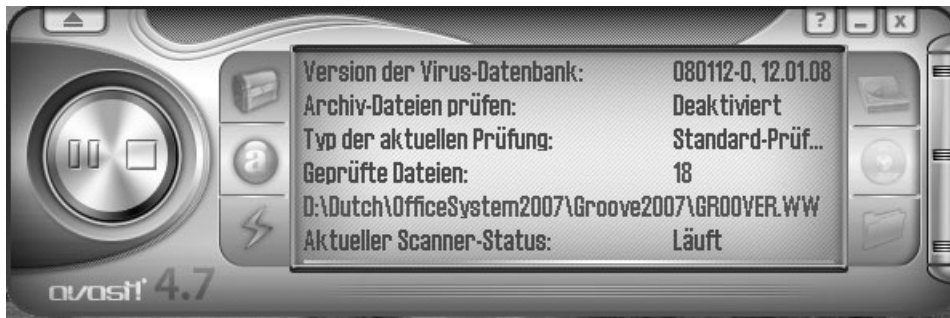


Abb.: Manueller Virensuchlauf mittels Avast

Bei einem derartigen Scan – so nennt man den Vorgang – werden im Falle eines Fundes entsprechende Warnmeldungen ausgegeben.

Sie werden sich jetzt sicherlich fragen, wie man Viren erkennen kann. Damit ein Virus sich nicht mehrfach in ein bereits befallenes Programm schreibt, benutzt er in der Regel eine Kennung – genannt **Signatur** –, um den Befall eines Computersystems möglichst effektiv zu machen. Antivirenprogramme benutzen unter anderem diese Signatur, um Viren zu erkennen.

Wird ein Virus anhand seiner Signatur erkannt, stellen die Antivirenprogramme auch die Möglichkeit zur Verfügung, ein befallenes Programm zu desinfizieren. In diesem Fall wird der virale Code aus dem Anwendungsprogramm entfernt. Die Folge ist dann, dass die Datei wieder virenfrei ist. Manchmal kann der virale Code jedoch nicht entfernt werden. In diesem Fall können die befallenen Dateien in einen speziellen Ordner verschoben werden. Welche Aktion das Programm durchführen soll, muss dabei durch den Benutzer konfiguriert werden.

2.4.3 Update der Virendatenbank

Da leider täglich neue Viren in Umlauf gebracht werden, müssen Sie Ihre Antiviren-Software unbedingt auf dem neuesten Stand halten. Antivirenprogramme speichern die Signaturen unterschiedlicher Viren in einer Virendatenbank. Um diese Datenbank zu aktualisieren und auch neuere Programmversionen zu erhalten, verwenden die meisten Antivirenprogramme ein Zusatzprogramm. **Bei einer aktiven Internetverbindung wird die Virendatenbank automatisch und täglich aktualisiert.** Der Vorteil für den Anwender liegt auf der Hand. Ohne sich darum kümmern zu müssen, wird die Antivirensoftware auf dem neuesten Stand gehalten, wodurch der Anwender den größtmöglichen Schutz gegen Viren erhält.

2.5 Weitere Onlinegefahren

Zu den bereits genannten Risiken sind in letzter Zeit weitere hinzugekommen. Das Internet als allgegenwärtige Kommunikationsplattform, die von niemandem kontrolliert wird, bietet natürlich Platz für Tätigkeiten, die bis hin zu Mobbing und Rufschädigung reichen.

- **Internet-Belästigung (Harassment), Cyber-Bullying:** Durch das Internet als Kommunikationsmedium wird einer Person Schaden zugefügt. Durch Blogs wird jemand beschimpft, ein heimlich gedrehtes Video wird auf YouTube gestellt oder eine Person wird durch Internetaktivitäten wie dem wiederholten Versenden von bedrohlichen und beleidigenden Botschaften über E-Mail permanent belästigt.
- **Cyber Grooming:** Darunter versteht man die sexuelle Belästigung von Kindern und Jugendlichen.
- **Opfer von Betrügereien (Predators):** Das Internet wird dazu genutzt, um leichtgläubigen Nutzern finanziellen Schaden zuzufügen. Über gefälschte Websites werden User dazu gebracht, die Daten von Kreditkarten oder die Codes für Online-Banking zu übermitteln. Beliebte ist auch die Methode, für die Unterstützung bei Geld-Transaktionen hohe Provisionen in Aussicht zu stellen, allerdings muss vorher ein Betrag auf ein Konto überwiesen werden. Selbstverständlich sehen die Geschädigten weder eine Provision noch den überwiesenen Geldbetrag je wieder. Im englischen Sprachraum wird der Begriff Predator (Raubtier) für die Aktivitäten rund um die Verbreitung von verbotenen pornografischen Material verwendet.

Diese Gefahren entstehen teilweise durch soziale Netzwerke – Web 2.0 –, in welchen Personen teilweise sehr offen Dinge über sich preisgeben.

Zitat aus Wikipedia¹⁸ bezüglich Cyber-Bullying:

„In letzter Zeit gewann der Begriff vor allem im Zusammenhang mit Schülern, die Videos oder Bilder von Lehrern bearbeitet und anschließend ins Internet gestellt haben, an Bedeutung. Weit verbreitet ist diese Form des Mobbing auch unter Schülern, die per Handy, Chat, sozialen Netzwerken wie SchülerVZ oder Videoportalen wie You Tube oder extra erstellten Internetseiten virtuell belästigt werden.“

2.5.1 Phishing

Beim Phishing versucht der Kriminelle, durch Gutgläubigkeit des Anwenders geheime Informationen zu erhalten. In erster Linie zielen diese Versuche darauf ab, Zugangsdaten von Internet-Bankkunden auszuspähen.

Mit Hilfe einer E-Mail-Adresse und einer gefälschten Website wird versucht, dem Benutzer Daten zu entlocken.

¹⁸ <http://de.wikipedia.org/wiki/Cyberbullying>

Wenn Sie nach dem Aufruf einer Website der Meinung sind, dass es sich hierbei um eine Phishing Site handelt, können Sie dies folgendermaßen überprüfen:

- ▲ Drücken Sie die Taste [F 10], um das Menü des IE anzuzeigen:
- ▲ Wählen Sie den Menüpunkt **EXTRAS ▶ PHISHINGFILTER ▶ DIESE WEBSITE ÜBERPRÜFEN** aus.

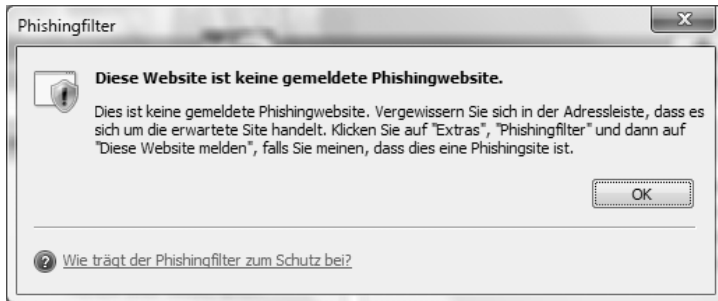


Abb.: Überprüfung einer Website auf Phishing

Beachten Sie jedoch: Dies ist zwar eine Möglichkeit der Überprüfung – aber keine Garantie!

2.5.2 Aufforderung zur Geldwäsche

In diesem Fall wird mit Hilfe eines E-Mails versucht, den Empfänger zu einer kriminellen Handlung – der Geldwäsche – zu drängen.

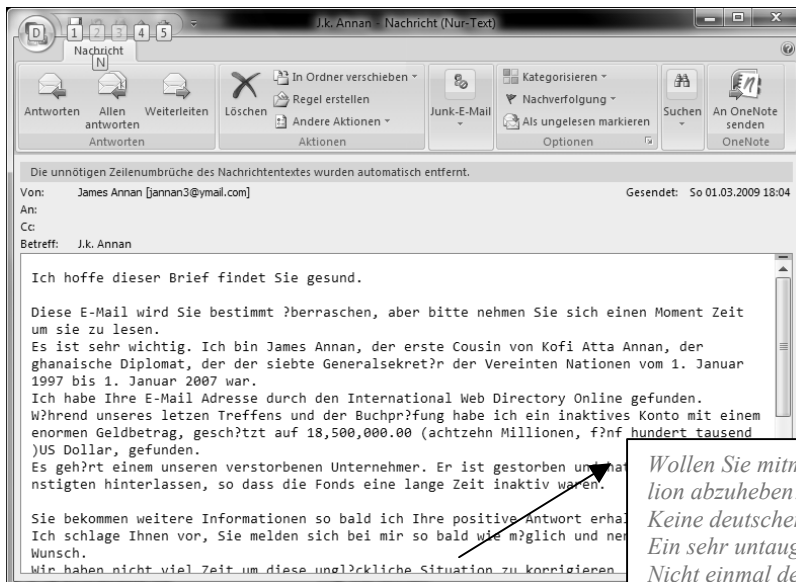


Abb.: Ein dubioses E-Mail

Geldwäsche ist eine strafbare Handlung!

Wenn Sie auf dieses E-Mail antworten, so werden Sie im für Sie günstigsten Fall in Zukunft mit unerwünschten E-Mails bombardiert. Solche Mails werden als Spam-Mails oder Junk-Mails bezeichnet. Sie sind ein Ärgernis, da sie die Aufmerksamkeit von wich-

tigen Mails ablenken. Meist handelt es sich dabei um Werbemails. Mit Ihrem Internet-provider können Sie vereinbaren, dass solche Mails ausgefiltert werden.

Solche unerwünschten E-Mails, die Sie leider immer wieder in Ihrem Postfach finden werden, sollten Sie einfach löschen!