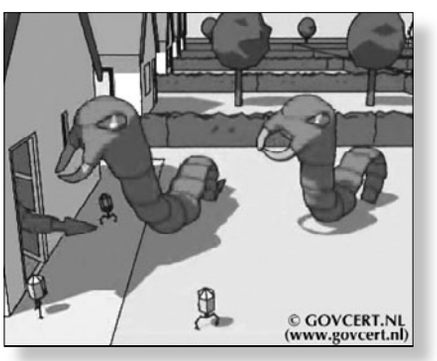
Kammerjäger im Netz: Jetzt geht's den Viren an den Kragen

Vom Scherzkeks zum Security-Problem

Vor wenigen Jahren waren Computerviren[1] noch lustig oder höchstens lästig: Sie spielten zu bestimmten Zeiten eine Melodie, verlangten vom Anwender ein Keks oder löschten im schlimmsten Fall die Festplatte und stellten damit die Wichtigkeit des hoffentlich vorhandenen Backups unter Beweis.

Heute, in der Informationsgesellschaft, sind Computer die Grundlage von Prozessen in allen Lebensbereichen – von Handel über Gesundheitswesen und U-Bahn-Steuerung bis hin zur hoheitlichen Verwaltung. Folgerichtig bleiben Computermanipulationen nicht mehr auf „die Kiste" beschränkt, sondern betreffen das reale Leben. Damit hat sich auch die Virenszene verändert: Computerviren sind keine Spielerei unausgelasteter Technikfreaks mehr, sondern ein Geschäftsmodell. Die aktuellen Viren dienen zwei Zwecken: Möglichst viele Computer und ihren Internetzugang nachhaltig zu bewirtschaften und geldwerte Informationen zu beschaffen. Dieses Business wird so professionell betrieben, dass Viren zum Security-Problem Nummer Eins geworden sind, weit vor Hard- und Softwarefehlern, HackerInnen, unloyalen MitarbeiterInnen etc.



Das größte Rechenzentrum der Welt ...

... ist nicht etwa ein mit High Tech vollgestopftes Gebäude im Silicon Valley, in dem Klimaberechnungen, Crashtest-Simulationen oder dergleichen durchgeführt werden. Die mächtigsten Computercluster sind Zusammenschlüsse von ganz normalen PCs, die sich hinter dem Rücken ihrer BesitzerInnen unter dem Kommando von Viren – bzw. deren UrheberInnen – zu so genannten *Botnets* zusammengerottet haben. Einen Eindruck davon, was das ist und wie es funktioniert, vermittelt auf schauerlich-anschauliche Weise ein englischsprachiger Film des GOVCERT.NL[2], der unter dem URL `www.waarschuwingsdienst.nl/render.html?cid=106` heruntergeladen werden kann und aus dem auch die Illustrationen zu diesem Artikel stammen.

Das Prinzip ist äußerst simpel: Sobald ein Computer befallen wurde, sorgt das moderne Virus für seine Weiterverbreitung, meldet sich bei seinem „Herrn und Meister" und wartet auf weitere Anweisungen, die dann auf Zuruf ausgeführt werden. Den Computer-Besitzer irgendwie zu ärgern, würde zur Entdeckung führen und wird daher tunlichst vermieden.

Wird das Virus aktiv, kann es alles mögliche tun: Spam versenden[3]; Musik und Videos aller Art bis hin zu Kinderpornos downloaden und verbreiten; an einer *Distributed Denial of Service*-Attacke (siehe weiter unten) teilnehmen. Besonders lukrativ ist die Einrichtung einer *Phishing Site*: Hier werden gefälschte Webseiten von Banken, eBay, PayPal etc. angeboten, in der Hoffnung, dass getäuschte AnwenderInnen ihre Passwörter dort eingeben – die dann fleißig missbraucht werden. Der verbrecherischen Phantasie sind kaum Grenzen gesetzt.

Die Vorteile für den Botnet-Meister liegen auf der Hand:

- Keine Unkosten für Hardware, Internetanbindung, Strom und Wartung der Rechner;
- unvorstellbare Ressourcen (ein Botnet aus 100 000 Rechnern kann als klein gelten);
- keine Probleme mit dem Gesetz: Die Täterausforschung endet spätestens beim PC eines ahnungslosen Benutzers.

Die Macht eines solchen Botnet lässt sich leicht am Beispiel einer *Distributed Denial of Service*-Attacke (DDoS) zeigen: Wenn 100 000 Rechner mit z.B. der Bandbreite eines bei uns üblichen Kabelmodem- oder DSL-Anschlusses gleichzeitig auf ein Ziel „losballern", kommen dort gut und gerne 10 Gbit/s an. Das reicht nicht nur aus, um aus einer Serverfarm – bildlich gesprochen – ein Häufchen Asche zu machen, sondern auch, um das gesamte, wahrlich nicht schwachbrüstig angebundene österreichische Wissenschaftsnetz ACOnet mehrfach zu überlasten. Mit einem solchen Druckmittel in der Hand werden beispielsweise Firmen erpresst, die ihre Umsätze mit Online-Diensten machen.

Auch der volle Zugriff auf die Festplatteninhalte der übernommenen Rechner ist nützlich: Mit den dort gespeicherten eMail-Adressen lassen sich die Spamdatenbanken trefflich erweitern. Kreditkartendaten aus Online-Transaktionen sind ohnehin reines Bargeld. Im Mailklienten oder Webbrowser gespeicherte oder auch auf der Tastatur eingetipp-

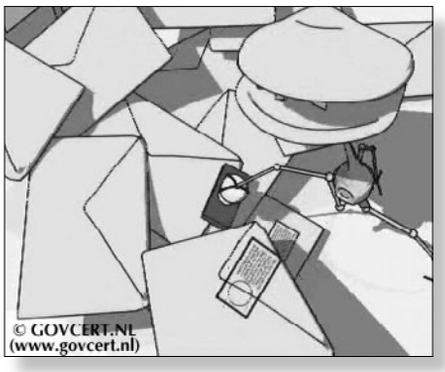
---

1) Die nähere Unterscheidung zwischen Viren, Trojanern, Würmern und anderen Plagegeister-Kategorien ist in diesem Artikel irrelevant. Daher wird hier für alle Arten der landläufige Begriff „Virus" verwendet.

2) GOVCERT.NL ist das *Computer Emergency Response Teams* (CERT) der niederländischen Regierung.

3) Bei Rechnern, die als „Spamschleudern" auffällig werden, ist häufig eine vorangegangene Vireninfektion feststellbar.

te Passwörter sind ebenfalls sehr interessant. Eine beliebte Anwendung dafür ist, zusätzlich zur privaten Homepage des Computer-Besitzers Pornoseiten am Webserver seines Providers unterzubringen. Der Zugriff auf das eMail-Konto des Opfers ermöglicht auch Betrügereien in großem Stil unter fremdem Namen. Gegen all das hilft keine Verschlüsselung und kein noch so sicheres Passwort: Das Virus hat mehr technische Möglichkeiten und kennt (spätestens sobald sie auf der Tastatur eingetippt werden) dieselben Passwörter wie der legitime Anwender.



Um es auf den Punkt zu bringen: Bei Viren geht es um Geld. Mehr noch: um richtig viel Geld. Ein Virus am Rechner ist nicht mehr bloß eine Unannehmlichkeit für den Benutzer, sondern – nicht immer, aber immer öfter – ein kriminelles Werkzeug.

Allzu oft ist doch der Wurm drin

Es gibt wohl niemanden mehr, der noch nie von der Bedrohung eines PCs durch Viren, Würmer und Trojaner gehört hat und nicht weiß, dass ein stets aktueller Virenscanner zumindest auf Windows-Rechnern ein absolutes Muss ist. Für Uni-MitarbeiterInnen steht der Virenscanner von McAfee kostenlos zur Verfügung (siehe `www.univie.ac.at/ZID/gratissoftware/`) – es gibt also wirklich keine Ausrede mehr, wenn kein Wächter den „elektronischen Datenverwurster“ schützt.

Überdies hindern die Virenscanner an den zentralen Mailservern des ZID sowie an vielen Stellen auch noch Firewalls die elektronischen Schädlinge am Zutritt zum Uni-Datennetz. Damit, so sollte man meinen, ist das Virenproblem Geschichte – doch weit gefehlt. Zwar sind die üblichen Maßnahmen ausgesprochen wirksam und wichtig, aber vollständige Sicherheit gibt es auch in diesem Bereich nicht.

- *Virenscanner* haben eine prinzipbedingte Schwachstelle: Trotz aller Bemühungen der Hersteller, jede erdenkliche Intelligenz in die Scanner zu packen, beruhen sie primär auf dem Wiedererkennen bereits bekannter Schädlinge. Neue Viren sind so lange „unsichtbar“, bis die Scanner-Hersteller ein Update zur Verfügung gestellt haben und dieses auch tatsächlich den Virenscanner erreicht hat. In der Praxis muss man oft mit mit einem Zeitraum von mindestens einem Tag zwischen dem Auftauchen eines neuen Schädlings und der Immunisierung des PCs rechnen.

  Die Mail-Virenscanner des ZID schützen zwar – mit der obigen Einschränkung – die zentralen Mailserver der Universität Wien (Unet, Mailbox) vor Virenmails, nicht aber die von Instituten in Eigenregie betriebenen Mailserver, und schon gar nicht verhindern sie den Download einer infizierten Nachricht von außerhalb, etwa von einem Freemail-Account oder von kommerziellen Providern.

- *Firewalls* hingegen bieten einen wirksamen Schutz vor zahlreichen unerwünschten Datenverbindungen und können damit eine Reihe von Angriffen abwehren. Sie verhindern aber nicht die Übertragung von böser Software über prinzipiell zugelassene Kanäle, beispielsweise über eine Webseite.

An dieser Stelle sei auch ein Wort zu so genannten *NAT-Routern* gesagt, die oft irrtümlich als Sicherheitsmaßnahme betrachtet werden: Dadurch, dass alle vermeintlich geschützten Rechner unter derselben IP-Adresse erscheinen, wird im Virenfall der „Feuerwehreinsatz“ zur Schnitzeljagd, da nicht mehr festzustellen ist, welcher Rechner befallen wurde.

Ist die Kiste infiziert, ...

... virt sich's völlig ungeniert: Hat, auf welchem Weg auch immer, ein Virus einmal den Weg in den PC gefunden, ist jede Sicherheit dahin. Es gehört zum Stand der einschlägigen Viren-Technik, im Zuge der Infektion des Rechners allfällige Virenscanner dauerhaft auszuschalten und oft sogar den Zugang zu den Webseiten der Antiviren-Hersteller zu unterbinden.

Firewalls werden häufig nach dem Grundsatz konzipiert, dass der Feind nur außerhalb des eigenen Netzes sein kann, und erlauben ausgehende Verbindungen jeder Art. Damit erlauben sie auch die Kontaktaufnahme eines Virus mit seinem Botnet. Ist ein Rechner aber erst einmal im Botnet angemeldet, ist die Firewall ausgehebelt: All das, woran sie einen Angreifer hindern würde, kann dieser nun vom infizierten Rechner – sozusagen von innen – machen lassen.

Einmal im System, kann sich ein Virus überdies mit Hilfe so genannter *Rootkits* (siehe auch Seite 19) hervorragend vor anderer Software, insbesondere Virenscannern, verstecken. Beispielsweise ist es möglich, dass das Rootkit jedem anderen Programm, das eine Datei liest (etwa einem Virenscanner, der das Vorhandensein eines Virus prüfen soll), deren unangetasteten Originalzustand vorgaukelt, obwohl sie ein Virus enthält.

---

4) Aus lizenzrechtlichen Gründen kann diese CD derzeit leider nicht für Studierende zur Verfügung gestellt werden.

5) siehe auch Notiz *ACOnet-CERT in Betrieb* (*Comment 03/2*, Seite 23 bzw. unter `www.univie.ac.at/comment/03-2/032_23.html`) und Artikel *Freiwillige Feuerwehr im Datennetz: Das ACOnet-CERT* (*Comment 04/1*, Seite 28 bzw. unter `www.univie.ac.at/comment/04-1/041_28a.html`)

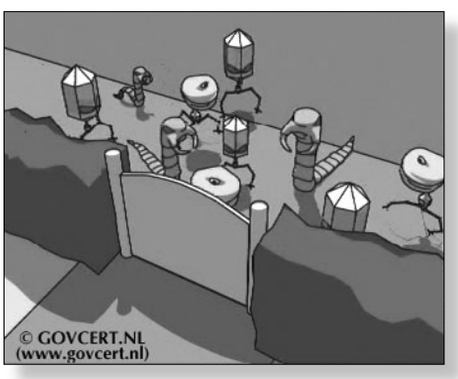
Um ganz sicherzugehen, dass der Virenscanner richtig arbeitet und danach das System wirklich sauber ist, muss man also den Rechner bereits mit einem garantiert sauberen System starten. Hier ist guter Rat gar nicht teuer: Am Helpdesk des Zentralen Informatikdienstes (siehe `www.univie.ac.at/ZID/helpdesk/`) kann von Uni-MitarbeiterInnen[4] eine bootfähige CD mit einem aktuellen Virenscanner gegen einen geringen Kostenersatz erworben werden. Damit diese CD die neuesten Virensignaturen enthält, wird sie stets frisch gebacken – wir bitten daher um Vorbestellung.

Neue Besen für das Netz

Angesichts dieser Bedrohung wurde im Security-Bereich ein Schwerpunkt auf die konsequente Suche nach Viren und deren Entfernung gesetzt. Um eine breitestmögliche Wirkung zu erzielen, finden diese Anstrengungen im Rahmen des von der Uni Wien betriebenen ACOnet-CERT (das *Computer Emergency Response Team* des österreichischen Wissenschaftsnetzes ACOnet; siehe `https://cert.aco.net/`)[5] statt. Wie bei der Feuerwehr bestehen die Sicherheitsaktivitäten eines CERT aus zwei Teilen:

- den Einsätzen mit Blaulicht und Sirene, wenn ein Unglück bereits eingetreten ist (der so genannten *Incident Response*), und
- allen vorbereitenden Maßnahmen wie Vorbeugung, Schulung, PR, Forschung, Einsatzplanung und Einrichtung entsprechender Systeme, um Probleme frühzeitig erkennen zu können.

Um vom ACOnet-CERT überhaupt wahrgenommen und verfolgt zu werden, musste ein von einem Virus befallener Rechner bisher entweder durch ungewöhnliches Verhalten an einer Firewall des ZID auf sich aufmerksam machen oder per eMail an `abuse@univie.ac.at` bzw. `cert@aco.net` gemeldet werden. Automatisierte Community-Services wie MyNetWatchman (Näheres dazu siehe `www.mynetwatchman.com`) haben in dieser Hinsicht sehr wertvolle Dienste geleistet.



Im Rahmen des Antiviren-Schwerpunkts konnten neue Informationsquellen erschlossen und dadurch zahllose Viren entdeckt werden, die bislang gar nicht oder bestenfalls wesentlich später aufgefallen wären. Die erste Maßnahme war, weitere Community-Services auszuwerten und die dort erhältlichen Informationen in einer Datenbank zu speichern. Darüber hinaus wurden die Virenscanner an den zentralen Mailservern des ZID in das System miteinbezogen. Sogar die Nameserver (im Netzwerk verantwortlich für das Übersetzen von Domainnamen wie `www.univie.ac.at` in numerische IP-Adressen) schlagen jetzt bei bestimmten verräterischen Zugriffsmustern Alarm: Das Mytob-Virus etwa versucht, sich an Mailserver mit den eher ungewöhnlichen Namen MXS.*DOMAIN*, GATE.*DOMAIN*, RELAY.*DOMAIN* etc. zu versenden, und kann anhand dieser Kriterien entlarvt werden.

Die so gewonnenen Informationen werden in einer Datenbank gesammelt, im Fall von dynamisch vergebenen Adressen einem Account zugeordnet und täglich zu Berichten zusammengefasst.

Der große Kehraus

Die Interpretation der automatisch generierten und der per eMail empfangenen Berichte stellt eine besondere Herausforderung dar. Werden schwache Indizien zu ernst genommen, besteht die Gefahr, die BenutzerInnen durch irrtümliche Warnungen zu verunsichern und Glaubwürdigkeit einzubüßen. Fatal wäre es aber auch, echte Probleme aus Angst vor Fehldiagnosen zu übergehen.

Wenn ausreichend Grund zu der Annahme besteht, dass ein Problem vorliegt, verständigt das ACOnet-CERT die zuständige Kontaktadresse und ersucht um Prüfung bzw. Behebung (ein Beispiel einer solchen Benachrichtigung finden Sie im Kasten auf Seite 34). Gleichzeitig wird um eine kurze Rückmeldung gebeten – erstens, um den Fall abschließen zu können, und zweitens als Feedback für die weitere Interpretation eintreffender Berichte.

Dieses einfache Modell hat leider zwei Schönheitsfehler. Der eine, seltenere, ist, dass diese Benachrichtigungen mitunter nach dem Motto *„Ich habe ja eh eine Firewall“* oder *„Es geht ja um nix“* ignoriert werden. In solchen Fällen bemüht sich das ACOnet-CERT – nach Abwägung von Gefahrenpotential und dem Wunsch, Härtefälle zu vermeiden – entweder weiter um Kontaktaufnahme oder sieht sich gezwungen, den Rechner oder Zugang zu sperren, nicht zuletzt im Interesse des Benutzers selbst. Der Vollständigkeit halber sei gesagt, dass es in ganz seltenen Ausnahmefällen auch Sperren ohne Vorwarnung geben kann: Wenn wirklich Feuer am Dach ist, oder wenn es sich um IP-Adressen im Datennetz der Universität Wien handelt, die nicht vom ZID vergeben wurden und die keinen DNS-Eintrag aufweisen.

Sollte ein Rechner oder ein bestimmter Dienst im Universitätsdatennetz (beispielsweise das Einwählen mit Modem) gesperrt worden sein, wenden Sie sich bitte an den Helpdesk des Zentralen Informatikdienstes. Dort kann diese Sperre in den meisten Fällen sofort wieder aufgehoben werden. Eines sei noch besonders betont: Derartige Maßnahmen sind keine Strafen, sondern stellen lediglich das Ziehen der „digitalen Notbremse“ dar – besonders auch zu Ihrem eigenen Schutz.

Beispiel für eine Viren-Benachrichtigung des ACOnet-CERT:

```
Date: Sun, 29 Jan 2006 17:56:15 +0100 (CET)
From: "Alexander Talos via RT" <cert@aco.net>
To: alexander.talos@univie.ac.at
Subject: [ACOnet-CERT #13620] Virus (Mydoom): 131.130.2.235 / kling.cc.univie.ac.at

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1


Sehr geehrte Damen und Herren,

Wir haben Berichte (s.u.) erhalten, dass vom Rechner
131.130.2.235 / kling.cc.univie.ac.at
Viren verschickt werden. Vermutlich hat sich ein Virus/Trojaner auf diesem Rechner eingenistet. Ich
bitte um Pruefung/Bereinigung und um eine kurze Rueckmeldung (vorzugsweise auch darueber, ob/welche
Schaedlinge gefunden wurden), damit ich das Ticket schliessen kann. Sollten Sie Hilfe beim
Virenscannen benoetigen, wenden Sie sich bitte an unseren Helpdesk
(http://www.univie.ac.at/ZID/helpdesk/).

Mit freundlichen Gruessen,
Alexander Talos

eMail-Virus (W32/Mydoom.o) k0U8wt9G095747
  Timestamp: 2006-01-28 08:59:04 UTC
  Source:    aconet-cert-mx4.univie.ac.at-2006-01-29
- --
Alexander Talos, ACOnet-CERT
https://cert.aco.net/
Phone: +43 1 4277 14024
Fax: +43 1 4277 9140
Universitätsstrasse 7, A-1010 Vienna

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (FreeBSD
iD8DBQFD3POvvDA926Qg/Y4RAnzlAJ9DQsYk5VqpsiCA7lqN4iFfQLjB6gCgiTGo
bXZdGy1lE0tNyzAVDBccq50=
=vDaK
-----END PGP SIGNATURE-----
```

Anmerkungen:

1. Benachrichtigungen des ACOnet CERT tragen den Absender `cert@aco.net` und sind digital mit folgendem Schlüssel signiert: `1024D/A420FD8E 2005-12-10 [expires: 2007-01-31]`
   Key fingerprint = `8B79 1528 FAD5 20F2 761C B9DD BC30 3DDB A420 FD8E`
   Die GPG-Keys der Team-Mitglieder finden Sie unter `https://cert.aco.net/`
2. Mit dem Siegel `[ACOnet-CERT #13620]` kann der bearbeitete Fall in der Datenbank leicht aufgefunden werden. Bitte führen Sie diese Nummer bei allfälliger Korrespondenz an.
3. In der Regel besteht der Betreff aus drei oder vier Teilen: Kurze Benennung des Problems, IP-Adresse und DNS-Name des betroffenen Rechners, und gegebenenfalls zusätzliche Informationen wie Username bei Dialin-Accounts oder Netzname.
4. genaue Beschreibung des Problems und mögliche Gegenmaßnahmen
5. sofern vorhanden: Logfiles oder sonstige Informationen, die technisch Versierten zusätzliche Aufschlüsse über den Vorfall geben können

Mit dem zweiten Schönheitsfehler ist wesentlich schwieriger umzugehen: Welche ist die zuständige Kontaktadresse? Für den Bereich des ACOnet ist die Sache relativ klar: Der Security-Kontakt des jeweiligen ACOnet-Teilnehmers (das sind u.a. alle Universitäten und Bildungseinrichtungen Österreichs) wird verständigt und ist im eigenen Bereich dafür verantwortlich, alles Weitere zu veranlassen. Beim Kehren vor der eigenen Haustüre – nämlich im Datennetz der Uni Wien – erweist sich die bisherige Praxis des ZID, IP-Adressen so unbürokratisch wie möglich zu vergeben, als Herausforderung:

Allzu oft wurde von den Instituten nicht rückgemeldet, wessen PC an welche Steckdose angeschlossen und welche IP-Adresse aus dem Institutsnetz welchem Rechner zugewiesen wurde. Mitunter kennt der ZID nicht einmal den EDV-Betreuer für ein Institut – sei es, weil es nie einen gab oder weil der ehemals genannte schon lange nicht mehr im Amt ist. Im Zweifelsfall muss der Institutsvorstand, der ja ex lege das Institut nach außen vertritt, mit dem Virenproblem behelligt werden.

Hinsichtlich der Endgeräte-Dokumentation im Universitätsdatennetz hat sich in den letzten Jahren einiges getan. Insbesondere bemühen wir uns, die IP-Datenbank (siehe auch Seite 38) zu vervollständigen.

Hierbei bitten wir um Mithilfe:

Nehmen Sie sich die Zeit, sofern Ihr PC noch nicht erfasst ist, das Webformular unter `www.univie.ac.at/ZID/ipdb/` auszufüllen. So wie es für die Feuerwehr wichtig ist, dass ihre Zufahrt freigehalten wird, hilft es allen Beteiligten, wenn wir Sie im Ernstfall rechtzeitig verständigen können.

Zusammenfassung

Die bisherigen Empfehlungen[6] zum Thema Virenschutz sind zwar nicht mehr ausreichend, aber keineswegs veraltet oder verzichtbar. Eine grundsätzliche Lösung des Problems gibt es nicht. Daher gilt es, den Schaden, wenn er eintritt, möglichst früh zu erkennen und möglichst gering zu halten.

Sie können einiges tun, und zwar vorbeugend:

- Stellen Sie sicher, dass Ihr PC durch einen Virenscanner mit aktueller Signatur-Datenbank[7] sowie durch eine Firewall geschützt ist, und sorgen Sie für regelmäßige Updates Ihres Betriebssystems und Ihrer Software.[8]
- Erwägen Sie die Verwendung eines weniger gängigen Betriebssystems (Apple, Linux, ...).
- Seien Sie skeptisch, bevor Sie Software installieren oder Attachments anklicken.
- Organisieren Sie die zuverlässige Sicherung Ihrer Daten oder verwenden Sie die Fileservices des ZID (siehe `www.univie.ac.at/ZID/fileservices/`) statt Ihrer lokalen Festplatte.
- Bereiten Sie sich auf den Ernstfall vor: Registrieren Sie Ihren PC und die dazugehörigen Kontaktdaten in der IP-Datenbank des ZID (`www.univie.ac.at/ZID/ipdb/`) und halten Sie die Telefonnummer des EDV-Betreuers Ihres Instituts (sofern vorhanden), des Helpdesk etc. griffbereit.

Für den Fall, dass doch etwas passiert:

- Achten Sie auf eMail von `cert@aco.net` (siehe Beispiel auf Seite 34).
- Schalten Sie Ihren Computer ab oder setzen ihn in den Schlafmodus, wenn Sie gerade nicht daran arbeiten:
  - ➠ Es ist besser, wenn Ihr Rechner nur 40 statt 168 Stunden pro Woche Spam und Viren verschickt.
  - ➠ Ihr PC kann nur dann durch ungebührliches Verhalten auffallen, wenn Sie in der Nähe sind – d.h. Sie sind im Ernstfall für uns erreichbar und können sofort Maßnahmen setzen.
  - ➠ Das erhöht die Chancen, dass Sie die Immunisierung vor dem Virus erreicht: Mit etwas Glück erscheinen, während Ihr Computer schläft, die Updates, die das Virus abwehren, das sonst über Nacht eingedrungen wäre.
- Falls nötig, wenden Sie sich an den Helpdesk des ZID (`www.univie.ac.at/ZID/helpdesk/`). Hier wird Ihnen auch telefonisch beim Entfernen von Viren geholfen.
- Ändern Sie nach einem überstandenen Virenbefall Ihre Passwörter: Es könnte sein, dass sie durch das Virus „ausgeplaudert“ wurden.

Der Computer – ein Teufelszeug? Mit Sicherheit nicht, aber ein mächtiges Werkzeug, das alles tut, was ein Programm ihm gebietet. In falschen Händen bedeutet das: Der PC kann innerhalb von kürzester Zeit ungeheuer viel Schaden anrichten. Und deswegen sind Vorbeugung, rasche Diagnose und Schadensbegrenzung hier so wichtig.

Alexander Talos ■

---

6) siehe Artikel *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* (*Comment 04/1*, Seite 16 bzw. unter `www.univie.ac.at/comment/04-1/041_16.html`)

7) siehe Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* (*Comment 04/1*, Seite 21 bzw. unter `www.univie.ac.at/comment/04-1/041_21.html`)

8) siehe Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* (*Comment 04/1*, Seite 18 bzw. unter `www.univie.ac.at/comment/04-1/041_18.html`)

Bildnachweis: Die Bilder sind dem Botnet-Film des GOVCERT.NL (`www.waarschuwingsdienst.nl/render.html?cid=106`) entnommen. Wir danken GOVCERT.NL für die Druck-Erlaubnis.