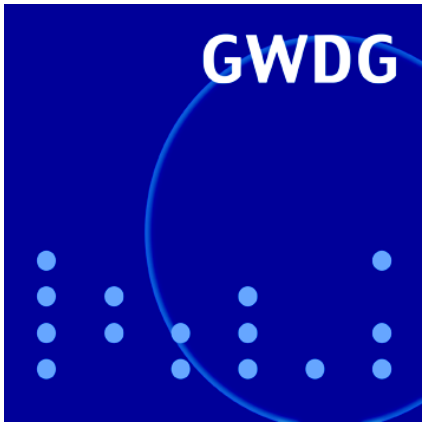

GWDG Nachrichten

5 / 2004

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

27. Jahrgang, Ausgabe 5 / 2004

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg, 37077 Göttingen-Nikolausberg

Redaktion: Dr. Th. Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de
Herstellung: S. Greber Tel.: 0551 201-1518, E-Mail: Sigrun.Greber@gwdg.de

1. Wurmbefall im GÖNET

1.1 Einleitung

Am Mittwoch, den 14.04.2004, - pünktlich zu Semesterbeginn - wurde das GÖNET von einem neuen Wurm mit dem Namen **Agobot** heimgesucht. Zusammen mit den Würmern **Phatbot** und **Sdbot** sorgte er dafür, dass teilweise ganze Abteilungen nicht mehr arbeitsfähig waren. Diese Schädlinge verbreiten sich nicht über die E-Mail, sondern schleichen sich ähnlich wie schon der **W32/Blaster** im vergangenen Jahr (s. GWDG-Nachrichten 9/2003) gewissermaßen hinterrücks in die Windows-Systeme hinein. Dabei nutzen sie verschiedene Einfallswege:

- zu einfache oder fehlende Zugangspasswörter, besonders für den Administrator-Account
- Offene Sicherheitslöcher, für die noch keine Korrekturen eingefahren wurden. Damit sind einerseits die schon vom **W32/Blaster** bekannten **RPC**-Dienste gemeint. Aber auch gerade die jüngsten Sicherheitslöcher in den Diensten **LSASS** (**L**ocal **S**ecurity **A**uthority **S**ubsystem = lokaler Sicherheitsdienst) und **PCT 1.0** (**P**rivate **C**ommunication **T**echnology = eine von Microsoft entwickelte Alternative zu SSL), für die Microsoft bereits im April Korrekturen veröffentlicht hatte, werden offenbar mittlerweile massiv von einigen Varianten ausgenutzt.
- Freigaben von Netzlaufwerken ohne Kennwörter oder mit zu leichten Kennwörtern
- Hintertüren, die von Würmern wie **Bagle** oder **Mydoom** geöffnet wurden

Die Schadfunktionen sind nicht besonders spektakulär, fallen zumeist aber ziemlich lästig aus: so werden fast immer irgendwelche Hintertüren geöffnet, um weitere Daten nachzuladen oder den Rechner fernzusteuern. Bisweilen wird auch eine Verbindung zum **IRC**-Netzwerk (IRC = **I**nter **R**elay **C**hat) zu dem gleichen Zweck aufgebaut. Manche Varianten booten die Rechner unvermittelt und einige initiieren DoS-(**D**enial **o**f **S**ervice)-Attacken gezielt gegen bestimmte Server. Das heimtückische an diesen Schädlingen jedoch ist, dass sie in immer neuen Spielarten auftreten. Der Grund dafür mag in der Tatsache liegen, dass der Viren-Quellcode im Internet aufgetaucht war. Damit ist es für kundige Programmierer relativ einfach möglich, immer wieder neue Varianten zu generieren und neue Funktionalitäten einzubauen, um so z. B. auch neu veröffentlichte Sicherheitslöcher gezielt ausnutzen zu können. Die Hersteller von Antiviren-Programmen zählten bald mehrere hundert Varianten. Dieses Verhalten erleichtert natürlich nicht gerade die Erkennung durch die Virenscanner, weil für jede neue Variante erst die passenden Signaturen erstellt und diese dann über den Aktualisierungsmechanismus auf die Kundenrechner verteilt werden müssen, damit dort der neue Schädling auch entsprechend erkannt wird. Damit verstreicht stets wertvolle Zeit. Die Heuristik der Virenscanner, also das Erkennen der Würmer aufgrund typischer Verhaltensmuster, hilft hier leider nur bedingt, so dass man sich bei der Abwehr gezielt auf die Einfallstore konzentrieren muss, über die sich die Würmer der Rechner bemächtigen. Aufgrund der oben geschilderten Verbreitungswege ergeben sich damit auch die erforderlichen präventiven Maßnahmen:

- Unbedingt komplexere Kennwörter, besonders für den Administrator-Account (Windows NT, 2000, XP und 2003) vergeben (s. hierzu auch die GWDG-Nachrichten 9/2002).
- Netzlaufwerk-Freigaben möglichst vermeiden und dort, wo es unbedingt erforderlich ist, wenigstens ein komplexes Kennwort vergeben.
- Die Windows-Systeme müssen stets auf dem aktuellen Software-Stand gehalten werden. Seitdem es gerade auch Würmer verstehen, die Sicherheitslöcher in den Betriebssystemen gezielt auszunutzen, sollten hier die verfügbaren Korrekturen möglichst immer zeitnah eingefahren werden. Der Software-Update-Service der GWDG ermöglicht hier zumindest für die Windows-Versionen 2000, XP und 2003 eine automatische Aktualisierung und enthebt somit den Anwender von der Pflicht, die zeitraubende Installation der Patches manuell vornehmen zu müssen. Weitere Informationen hierzu finden sich unter

  `http://sus.gwdg.de`
- Einsatz eines stets aktuellen Virenscanners, selbst dann, wenn diese bei den sich derzeit so schnell verändernden Würmern nicht immer den optimalen Schutz bieten können. Das bedeutet aber nur, dass wir uns auf diese Schutzprogramme nicht uneingeschränkt verlassen dürfen und daher unbedingt auch die anderen Maßnahmen im Auge behalten müssen. Als Virenscanner empfiehlt sich nach wie vor das hier schon öfter beschriebene Produkt **Sophos Anti-Virus**, dessen Installation und Aktualisierung komfortabel über den Sophos-Update-Service der GWDG erfolgen kann. Nähere Informationen dazu finden sich unter

  `http://antivir.gwdg.de`

  Das für die Installation erforderliche Kennwort erhält man bei der GWDG.

1.2 Entfernung des Wurmes

Ist der eigene Rechner nun bereits von einem oder mehreren dieser Würmer befallen worden, dann bieten sich verschiedene Maßnahmen zur „Wurmkur“ an. Eine nach dem Befall vorgenommene Installation des Sophos-Virenscanners mag bisweilen nicht zum Erfolg führen, weil oftmals die den Wurm beherbergenden Dateien im laufenden Betrieb nicht entfernt werden können. Hier bietet sich der abgesicherte Modus der Windows-Betriebssysteme an, in den man während des Neustarts unter Betätigung der Taste **F8** gelangt. Danach kann mit Hilfe des **Command Line Scanners** von Sophos der Wurm aufgespürt und entfernt werden. Dieses kommandozeilenorientierte Programm ist Bestandteil jeder Sophos-Installation und findet sich bei Windows NT, 2000 und XP zumeist hier:

```
<Lw>:\Programme\Sophos SWEEP for NT
\SAV32CLI.EXE
```

Zu einer erfolgreichen Überprüfung werden dann nur noch die entsprechenden Signaturen (**ide**-Dateien) benötigt, die man immer aktuell vom Sophos-Server

```
http://www.sophos.de/downloads/ide/
```

beziehen kann. Derzeit kann aber auch alles als komplettes 7 MByte großes Paket von folgendem Ort bezogen werden:

```
http://www.gwdg.de/samba/updates/
                    antivir/sophoscli.exe
```

Solange die Wurm-Epidemie andauert, wird diese Datei nämlich noch täglich aktualisiert, das bedeutet, sie enthält stets die aktuellen Signaturen. Ihr genauer Stand wie auch generell die jeweils aktuellen Verhaltensmaßregeln entnehme man am besten der folgenden Seite:

```
http://www.gwdg.de/service/sicherheit/
                      aktuell/agobot.html
```

Dort findet sich auch eine kurze Anleitung zum Gebrauch des **Command Line Scanners**.

Falls über die Hintertüren, die diese Würmer hinterlassen können, bereits - wie in einigen Fällen geschehen - **Rootkits** wie z. B. *Hacker Defender* Zugang zu dem befallenen Rechner fanden, wird der Virenscanner nichts mehr erkennen, weil die **Rootkits** geschickt die Ausgabe manipulieren und entscheidende Dateien und Prozesse vor der Entdeckung verbergen. Als Ausweg hilft hier nur die Überprüfung von einem fremden Medium aus, z. B. einer bootfähigen CD mit einem eigenständigen Betriebssystem und Virenscanner. Hier böte sich wieder einmal der Einsatz des c’t-Projekts **Knoppicillin** an, einer speziellen Variante des von einer CD lauffähigen Linux-Systems **Knoppix** mit einem sich über das Netz aktualisierendem **FProt**-Virenscanner. Die GWDG hält hier stets die aktuellste Version zum Kopieren bereit und steht auch beim Einsatz mit fachlicher Hilfe gerne zur Seite.

1.3 W32.Sasser

Kaum waren die schlimmsten Auswirkungen der oben beschriebenen Würmer beseitigt, folgte zum 1. Mai gleich der nächste Schädling: **W32.Sasser**. Dieser nutzte vorwiegend bei **Windows 2000** und **XP** nun ganz gezielt die **LSASS**-Schwachstelle aus und führte bei all den Systemen, die entweder die letzte Korrektur von Microsoft noch nicht eingefahren oder keine Personal Firewall aktiviert hatten, zu einem massiven Befall. Das Ergebnis war zumeist ein kaum mehr brauchbares System, da der Wurm ständig bestrebt war, einen Neustart herbeizuführen und durch die Tatsache, dass er über 128 gleichzeitig aufgebaute Verbindungen versuchte, sich weiter zu verteilen, eine extrem hohe Netzlast erzeugte. Auch dieser Wurm öffnete auf dem befallenen System Hintertüren, über die Programme nachgeladen werden oder aber sogar andere Würmer wie **Phatbot** in das System eindringen konnten. Da das Einfallstor von **W32.Sasser** nun eindeutig bekannt war, galt es lediglich, die bereits drei Wochen zuvor veröffentlichte Korrektur **MS04-011** einzufahren, um so dem Wurm die Angriffsfläche zu entziehen. Zudem konnte, wie schon damals beim **W32.Blaster**, eine **Personal Firewall** selbst bei nicht gepatchten Systemen einen Angriff vereiteln. Da bei **Windows XP** eine solche Schutzfunktion zwar mitgeliefert, aber leider nicht auch automatisch gestartet wird, sollte diese **Internetverbindungsfirewall** (ICF = **I**nternet **C**onnection **F**irewall) stets aktiviert sein. Dazu geht man folgendermaßen vor:

- Im Menü **Start > Systemsteuerung > Netzwerk- und Internetverbindungen** auf **Netzwerkverbindungen** klicken (falls die Symbole anders aussehen sollten, weil man sich gerade in der klassischen Ansicht befindet, muss man nur über den Eintrag **Zur Kategorieansicht wechseln** links oben in die Kategorienansicht verzweigen).
- Unter der Rubrik **DFÜ** oder **LAN oder Hochgeschwindigkeitsinternet** das entsprechende Symbol auswählen, welches für die gerade aktive Verbindung steht.
- Links im Aufgabenbereich unter Netzwerkaufgaben auf **Einstellungen dieser Verbindung ändern** gehen (oder aber mit der rechten Maustaste auf die Verbindung direkt klicken, um so über das Kontextmenü die **Eigenschaften** anzuwählen).
- In der folgenden Dialogbox muss über die Registerkarte **Erweitert** unter der Rubrik **Internet-**

verbindungsfirewall der Eintrag **Diesen Computer und das Netzwerk schützen** aktiviert werden.

Damit wird der Zugriff auf diesen Computer vom Internet aus entsprechend eingeschränkt und die Angriffe von Würmern wie **Blaster** oder **Sasser** ganz verhindert.

Die Anwender von **Windows-2000**-Systemen besitzen diese Firewall-Funktion leider noch nicht und müssen deshalb Fremdprodukte einsetzen, um die gleiche Schutzfunktion zu erzielen. Empfehlenswert sind hier die für den privaten Einsatz kostenfreie Produkte von **ZoneAlarm** oder **Kerio**. Siehe hierzu auch die folgende Seite:

`http://www.gwdg.de/service/sicherheit/aktuell/perwfw.html`

1.4 Schlussfolgerungen

Das massive Aufkommen von Würmern wie **Agobot/Phatbot** und **Sasser** deuten an, was uns in Zukunft noch alles heimsuchen wird. Neben den klassischen Varianten, die sich wie **Bagle** oder **Netsky** über E-Mail verbreiten, werden wir es in Zukunft immer mehr mit Würmern zu tun bekommen, die ganz gezielt die (Windows-)Betriebssysteme attakkieren und eventuell dort vorhandene Schwachstellen ausnutzen. Dabei können sie über eigens eingerichtete Hintertüren Rechner fernsteuern, neue Programm-Module für zusätzliche Funktionalitäten nachladen, Rootkit-Funktionen einsetzen, um die eigene Existenz zu verbergen, gezielt andere Überwachungsprogramme wie Virenscanner und Personal Firewalls deaktivieren und vieles mehr. Für uns Anwender heißt dies, den Schädlingen auch in Zukunft möglichst eine geringe Angriffsfläche zu bieten, indem wir unbedingt alle Sicherheitskorrekturen einfahren, die eingebaute Firewall aktivieren, komplexe Kennwörter verwenden, nicht benötigte Dienste abschalten und einen stets aktuellen Virenscanner einsetzen. Weitaus wichtiger noch ist aber die zeitnahe Information über drohende Gefahren und ihrer Abwehr. Hierzu bietet die GWDG ihren Nutzern verschiedene Informationsquellen an:

- Wichtige **aktuelle Nachrichten** finden sich stets auf der folgenden Web-Seite:

  `http://www.gwdg.de/aktuell/`

- Neueste Informationen zum Thema **Sicherheit** finden sich hier:

  `http://www.gwdg.de/service/sicherheit/aktuell/index.html`

- Wer immer automatisch per Mail informiert werden möchte, kann sich auf die folgenden beiden Mailing-Listen setzen lassen:

  GWDG-SEC: für die aktuellen Informationen zum Thema Sicherheit

  GOENET: für Informationen zu Vorkommnissen im Göttinger Übertragungsnetz

Die beiden Mailing-Listen sind öffentlich und können von jedem Interessierten abonniert werden. Hierzu muss lediglich eine Mail an **listproc@gwdg.de** ohne Betreff mit dem folgenden Inhalt gesendet werden:

`subscribe gwdg-sec` ***`Vorname Nachname`*** (für die GWDG-SEC-Liste) bzw.

`subscribe goenet` ***`Vorname Nachname`*** (für die GOENET-Liste)

Über diese Informationskanäle werden wir Ihnen immer möglichst aktuelle Informationen, Warnungen und Ratschläge zu sicherheitskritischen Themen zukommen lassen.

Reimann

---

2. Schnelle Erkennung von Viren und Trojanern im Funk-LAN

2.1 Einleitung

Die Viren und Trojaner der letzten Wochen machten auch vor dem GÖNET und Funk-LAN nicht halt (siehe hierzu den entsprechenden Artikel in dieser Ausgabe).

Insbesondere Agobot, Phatbot, W32.Sasser und deren diverse Varianten waren im GÖNET und Funk-LAN „GoeMobile“ mehrfach aufgetreten und führten zu einer außerordentlich hohen Netzwerkbelastung, sodass einige Benutzer Probleme mit der zur Verfügung stehenden Bandbreite bekamen.

Die GWDG hat ein Programm entwickelt, um im Funk-LAN virulentes Verhalten schnell erkennen zu können und die betroffenen Benutzer frühzeitig zu warnen. Seit dem 23.04.2004 ist dieses Programm im Funk-LAN aktiv.

2.1.1 Warum ist das Funk-LAN virenanfällig?

Das Funk-LAN besteht aus einer großen „Broadcastdomain“. Jeder Rechner im Funk-LAN sieht die „Broadcasts“ der anderen Rechner, solange diese sich nicht mit dem VPN-Gateway verbunden haben.

In dieser zeitlichen „Zwischenphase“ können sich Viren leicht über das gesamte Netz ausbreiten.

2.1.2 Wie breitet sich ein Virus aus?

Viren und Trojaner haben eine gemeinsame unangenehme Eigenschaft. Sie wollen sich möglichst schnell über das lokale Netz ausbreiten und andere Rechner befallen. Exakt an diesem Verhalten setzt die GWDG bei der frühzeitigen Erkennung von Viren an. Die Aufgabe ist es, ein virulentes Verhalten im Netzwerk sehr frühzeitig erkennen zu können.

2.2 Typische Charakteristika bei der Ausbreitung von Viren

Ist ein Rechner von einem Virus oder Trojaner befallen, so erkennt dieser, in welchem lokalen Netz (IP-Netz) sich der Rechner befindet. Die Kombination aus der IP-Adresse und Subnetzmaske gibt dem Virus ausreichend Informationen über die direkte Netzwerkumgebung, in der er sich ausbreiten könnte.

Entweder sofort oder nach einer gewissen Zeit versucht der Virus, andere Rechner in seinem lokalen Netzwerk zu kontaktieren und diese zu infizieren. Einige Varianten bauen zusätzlich Verbindungen zu externen IP-Adressen im Internet auf, nachdem der Virus das lokale Netzwerk bereits „durchforstet“ hat.

Beispiel:

Besitzt ein befallener Rechner die

`IP-Adresse = 10.100.4.17`

mit der z. B. im Göttinger Funk-LAN üblichen

`Subnetzmaske = 255.255.0.0`

so weiß der Virus, dass der Rechner an einem Netzwerk angebunden ist, in dem sich bis zu 2^{16} - 2 = 65.534 weitere Rechner befinden könnten.

Alle diese Rechner befinden sich wahrscheinlich in einer Broadcastdomain und sind durch „Broadcasts“ direkt erreichbar.

Manche Viren ignorieren die Subnetzmaske und gehen einfach nach der vorhandenen IP-Adresse, welche durch die ersten 3 Bits das „eigentlich“ dazugehörige Netzwerk verrät. Im Fall der IP-Adresse **`10.100.4.17`** wäre es die dazu passende Subnetzmaske **`255.0.0.0`**. Damit würde sich die Anzahl der „theoretisch“ im lokalen Netzwerk befindlichen Rechner auf immerhin 16.777.216 erhöhen.

Versucht der Virus, diese Reihe von IP-Adressen zu kontaktieren, so wird deutlich, dass dadurch eine nicht unerhebliche Netzwerklast durch Broadcasts die Folge ist. Darüber hinaus würde der „Scan“-Vorgang des Virus zumindest im letztgenannten Fall erhebliche Zeit in Anspruch nehmen.

Logische und unsystematische Reihenfolge der IP-Adressen:

Einige Viren/Trojaner beginnen, in logischer Reihenfolge die IP-Adressen

`10.100.4.1`
`10.100.4.2`
`10.100.4.3`
`….`
`10.100.255.255`

zu kontaktieren, um die Rechner im lokalen Netz zu befallen.

Andere Varianten gehen etwas unsystematischer vor und versuchen zwar, die gleiche Anzahl an IP-Adressen zu erreichen, aber diese in einer scheinbar beliebigen Reihenfolge:

…
`10.100.23.7`
`10.100.129.222`
`10.100.4.78`
…

2.2.1 Vor der Ausbreitung erfolgen die Broadcasts

Prinzipbedingt muss ein Virus, wie auch jedes andere Programm, welches eine Netzwerkverbindung über IP aufbauen möchte, zunächst ein ARP-Request (ARP = **A**ddress **R**esolution **P**rotocol) in das lokale Netzwerk schicken. ARP-Requests sind „Broadcast“-Pakete, welche von allen im Netzwerk befindlichen Rechner empfangen werden.

Die Zieladresse eines ARP-Request-Broadcast ist

bei Layer 3 (IP-Ebene): **`255.255.255.255`**

bei Layer 2 (MAC): **`FF.FF.FF.FF.FF.FF`**

2.2.2 ARP-Requests

ARP-Requests dienen dazu, eine MAC-Adresse im Netzwerk für eine bekannte IP-Adresse zu „erfragen“. Wenn der anfragende Rechner die MAC-Adresse für eine IP-Adresse bekommen hat, speichert er diese lokal ab, um anschließend die Kommunikation auf Layer 2, also zwischen den beiden MAC-Adressen, aufbauen zu können. In der Regel wird die dann erhaltene MAC-Adresse für eine gewisse Zeit lokal im Rechner in einer speziellen Tabelle gehalten (ARP-Table), damit für die gleiche IP-Adresse kein erneuter ARP-Request mehr erforderlich ist. In dieser Tabelle stehen alle dem Rechner bekannten „MAC-IP“-Zuordnungen.

Dass es so etwas gibt, kann jeder Benutzer selbst unter Windows/Linux durch die Eingabe des Befehls **`arp -a`** herausbekommen. Dabei wird die lokale „ARP-Tabelle“ ausgegeben. Diese MAC-IP-Adresspaare deuten auf eine Kommunikation zwischen dem eigenen und den in der Tabelle aufgeführten IP-Adressen hin.

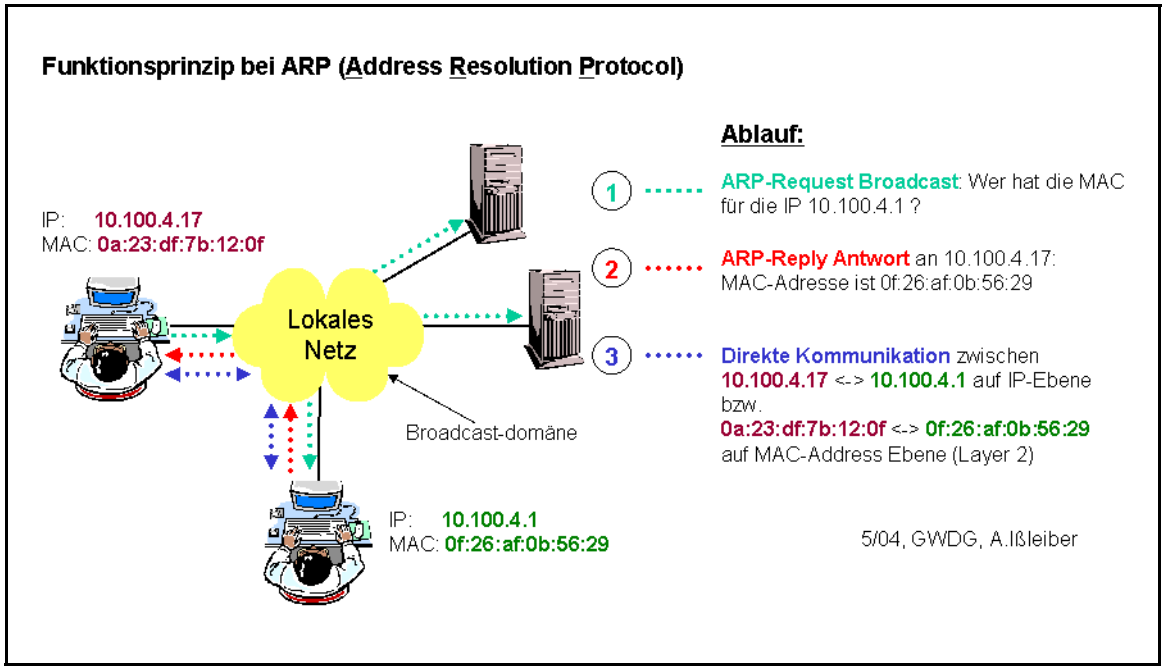

Abb. 1: Funktionsprinzip bei ARP

2.3 Wie funktioniert die Virenerkennung im Göttinger Funk-LAN „GoeMobile“?

2.3.1 Vier Verfahrensschritte

Zur Erkennung virulenten Verhaltens ist ein Rechner am Funk-LAN angeschlossen, auf dem neben anderen Diensten mehrere Programme zur Netzwerküberwachung gestartet sind. Das Betriebssystem ist Linux. Eines der Programme ist ARP-WATCH.

Schritt 1: ARPWATCH

Das kontinuierlich laufende Programm ARPWATCH schreibt die Kombination aus MAC-Adresse und IP-Adresse in eine lokale Textdatei. Dabei genügt lediglich ein einziges Ethernet-Paket/IP-Paket, welches ARPWATCH im Netzwerk „gesehen“ hat. Auch der genaue Zeitpunkt des Auftretens des Paketes wird erfasst.

Die Datei sieht wie folgt aus:

Mac-Adresse	IP-Adresse	Uhrzeit (Anzahl Sek. seit 1.1.1970)
…		
00:34:4b:f0:1f:23	10.100.4.214	1082447389
0d:5d:6d:25:23:2c	10.100.5.76	1083780490
00:22:df:78:5f:32	10.100.5.23	1083200653
00:c6:f1:25:98:7a	10.100.5.65	1082644826
…		

Schritt 2: TCPDUMP

Ein zweites Programm (TCPDUMP) startet alle fünf Minuten und erfasst alle ARP-Requests im Funk-LAN.

Dabei werden die ARP-Pakete des gesamten Funk-LANs für eine Zeit von 120 Sekunden gespeichert. Das Ergebnis wird nach IP-Adressen sortiert. Anschließend werden die IP-Adressen herausgefiltert, die innerhalb von 120 Sekunden mehr als 200 ARP-Requests verschickt haben. Dies lässt auf

virulentes Verhalten schließen, da hierbei eine IP-Adresse versucht, innerhalb ihres lokalen Netzes mehr als 200 weitere Rechner zu erreichen. Das wäre für eine „normale“ Rechnerkommunikation ein eher ungewöhnliches Verhalten.

Beispielhafte Ausgabe der mit TCPDUMP erfassten ARP-Requests:

Uhrzeit		Zieladresse		Quelladresse
…				
12:08:52.765935	arp who-has	10.100.64.204	tell	10.100.4.124
12:08:52.857136	arp who-has	10.100.75.151	tell	10.100.4.124
12:08:52.864701	arp who-has	10.100.21.8	tell	10.100.4.124
12:08:52.866496	arp who-has	10.100.128.38	tell	10.100.4.124
12:08:52.923046	arp who-has	10.100.4.22	tell	10.100.4.22
12:08:52.963029	arp who-has	10.100.181.181	tell	10.100.4.124
12:08:52.976712	arp who-has	10.100.32.211	tell	10.100.4.124
12:08:52.989600	arp who-has	10.100.234.67	tell	10.100.4.124
12:08:52.994498	arp who-has	10.100.85.226	tell	10.100.4.124
12:08:53.008105	arp who-has	10.100.138.113	tell	10.100.4.124
12:08:53.067755	arp who-has	10.100.192.0	tell	10.100.4.124
12:08:53.160800	arp who-has	10.100.187.105	tell	10.100.4.124
12:08:53.162120	arp who-has	10.100.37.135	tell	10.100.4.124
12:08:53.163122	arp who-has	10.100.144.165	tell	10.100.4.124
…				

In der obigen Tabelle sieht man deutlich, dass ein Rechner **10.100.4.124** schnell hintereinander versucht, weitere Rechner in seinem lokalen Netz zu erreichen. In diesem Beispiel war der Sasser-Wurm auf dem Rechner aktiv.

Schritt 3: Sammeln der Verbindungsdaten

Ein spezielles, für das Funk-LAN geschriebenes Programm (Script) sammelt nun die Verbindungsdaten, die zu der als „verdächtig“ identifizierten MAC-Adresse gehören; das sind:

- IP-Adresse,
- eingetragener Benutzer der MAC-Adresse in der Funk-LAN Datenbank,
- externe IP-Adresse, wenn der Benutzer das VPN-Gateway benutzt,
- Volumina, Byte incoming und Byte outgoing des VPN-Gateways,
- Uhrzeit des ersten Auftretens der MAC-Adresse im Funk-LAN (Tabelle von ARPWATCH) und
- E-Mail-Adresse des Benutzers.

Selbstverständlich werden dabei die Vorschriften des Datenschutzgesetzes eingehalten. Insbesondere werden die gesammelten Verbindungsdaten bereits wieder nach zwei Tagen gelöscht.

Schritt 4: Automatische Benachrichtigung per E-Mail

Im letzten Schritt wird dem Benutzer automatisch eine E-Mail mit dem Hinweis einer wahrscheinlichen Infektion seines Rechners zugeschickt. Gleichzeitig bekommt der Benutzer in der E-Mail Vorschläge zu deren Beseitigung sowie Links zu weiteren Informationen und Hinweise zur Absicherung seines PCs.

Abb. 2 verdeutlicht das beschriebene Verfahren zur frühen Virenerkennung im Funk-LAN:

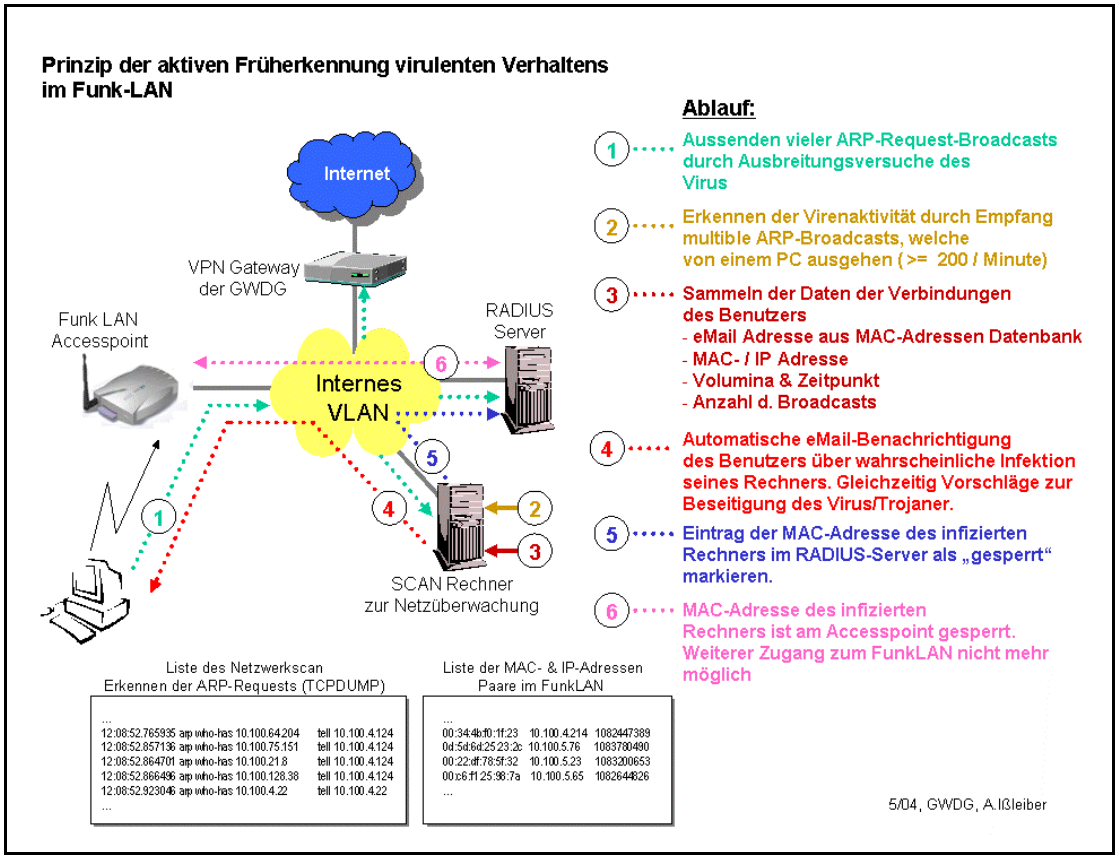

Abb. 2: Prinzip der aktiven Früherkennung virulenten Verhaltens im Funk-LAN

2.3.2 Positive Resonanz bei den Benutzern im Funk-LAN

Durch das seit dem 23.04.2004 eingeführte Verfahren wurden bereits eine Vielzahl von Benutzern per E-Mail über eine vermutliche Infektion des Rechners informiert. Die Resonanz der Benutzer war überaus positiv. Die meisten konnten uns nach Erhalt der E-Mail den Virusbefall bestätigen und waren durch die in der E-Mail mitgelieferten Beseitigungsverfahren sehr schnell selbst in der Lage, den Virus/Trojaner wieder zu entfernen.

2.3.3 Frühe Erkennung

Die beiden Viren/Trojaner Agobot sowie Sasser konnten wir durch das System bereits einen Tag vor Erscheinen der ersten Virensignatur der bekannten Antivirenprogramme erkennen. Der Name des Virus/Trojaner war natürlich zu diesem Zeitpunkt noch nicht bekannt, jedoch sein Verhalten im Funk-LAN eindeutig. Virenscanprogramme sind häufig auf Signaturen angewiesen, um diese erkennen zu können.

Entscheidend ist auch die Tatsache, dass ein Entdecken virulenten Verhaltens, bei noch unbekannten Viren, eine effektive Erkennungsvariante darstellt. Das bringt gerade bei der immer schneller werdenden Verbreitung von Viren einen kleinen, aber entscheidenen Zeitvorteil.

2.3.4 Ein eigener Virenscanner ist trotzdem erforderlich

Das im Funk-LAN eingesetzte Verfahren entlastet den Benutzer jedoch keineswegs von der nötigen Installation eines immer aktuellen Antivirenprogrammes. Meist ist eine Kombination aus

- Antivirenprogramm,
- Personal Firewall und
- aktuellen Patches des Betriebssystems

für einen sicheren Rechner erforderlich und auch ausreichend.

2.3.5 Ein stets aktuelles Betriebssystem gehört zum Virenschutz

Die GWDG stellt hierfür seit einiger Zeit einen **S**oftware **U**pdate **S**ervice (SUS) zur Verfügung, dessen Dienst die Infektion vieler Varianten der neuesten Viren und Trojaner schon verhindern würde. Benutzer des GÖNET sollten den SUS in jedem Fall verwenden.

Unter

http://sus.gwdg.de/

steht dieser Dienst allen Benutzern zur Verfügung.

2.3.6 Trefferquote, Fehl-Erkennung (false positive) und Nicht-Erkennung

Natürlich kann das beschriebene System keinen 100-prozentigen Schutz garantieren. Aber die Erfahrungen zeigen, dass wir Viren und Trojaner durch diese Methode sehr schnell in den Griff bekommen können. Dabei sind wir natürlich auf die Mithilfe der Benutzer angewiesen, die letztlich den Virus entfernen müssen.

Die Früherkennungsrate im Funk-LAN war recht hoch. Ab dem ersten Tag des Ausbruchs von Agobot/Phatbot waren ca. 95 Rechner als virulent erfasst worden. Bereits zwei Tage später waren es nur noch 2 Rechner.

Als falsch positiv wurden von nunmehr insgesamt 156 Rechnern lediglich 2 identifiziert. In dem einen Fall erfolgte von dem Rechner ein „Portscan“ im lokalen Netz. Portscans zu erkennen ist überdies durchaus sinnvoll, da dieses einen ersten Hinweis in Richtung „Hacking“ geben kann. In einem anderen Fall war ein spezieller Printserver-Dienst auf einem Rechner die Ursache überaus vieler ARP-Broadcasts, was zur Fehl-Erkennung führte.

Speziell im Funk-LAN wurden einige Benutzer angeschrieben, deren Rechner nicht befallen waren. Ursache dafür ist die Eintragung der MAC-Adresse einer Funkkarte von mehreren Benutzern, von denen aber meist nur einer tatsächlich den Virus hat. Es wurden immer alle Benutzer einer Funk-LAN-Karte per E-Mail informiert, also auch die „Vorbesitzer“ z. B. einer Leihkarte.

2.4 Ausblick

2.4.1 Erkennung im Festnetz

Wir denken darüber nach, diesen Mechanismus zur Früherkennung auch auf das „kabelgebundene“ Netz auszuweiten. Dort ist die Erkennung etwas schwieriger, da wir es mit kleineren Broadcastdomains zu tun haben. Ein „Zählung“ der ARP-Requests müsste jeweils in jedem Subnetz getrennt erfolgen. Hier ließe sich die Erkennung auf einige sicherheitsrelevante Subnetze des GÖNET reduzieren. Eine weitere Methode der Erkennung im Festnetz ist der Einsatz eines Honeypot-Systems.

Honeypot-Systeme

Die Installation eines Honeypot-Systems im GÖNET ermöglicht, auch über Broadcast-Grenzen hinweg ein virulentes Verhalten zu erkennen.

Siehe dazu:

http://wwwuser.gwdg.de/~aisslei/vortraege/Security%20Workshop%20GWDG%20Honeypotsysteme%202003/

Syslogfiles

Parallel dazu können Syslogfiles der zentralen Router im GÖNET als Erkennungsgrundlage genutzt werden.

2.4.2 Erkennung weiterer Formen „abnormalen“ Verhaltens in Netzen

Wir überlegen, das von der GWDG entwickelte Programm dahingehend zu erweitern, dass auch weitere Formen „abnormalen“ Verhaltens im Funk-LAN und in kabelgebundenen Netzen automatisch erkannt werden können. Im Funk-LAN sind wir schon ein gutes Stück weiter. Dort erkennt das oben beschriebene Verfahren auch Netzwerkadressen, die in diesem Netz nicht existieren sollten. Überdies ist dadurch auch

- „IP-Spoofing“; siehe hierzu:

  http://www.bsi.de/fachthem/sinet/vulner/g5048.htm

- „MAC-Adressen-Spoofing“; siehe hierzu:

  http://www.bsi.de/literat/studien/ids/doc0012.htm

- und der Einsatz von Systemen, die ProxyArp durchführen,

erkennbar.

2.5 Fazit

Das Verfahren zur frühzeitigen Erkennen virulenten Verhaltens hatte in den letzten Wochen viele Benutzer über eine nicht entdeckte Virusinfektion informieren können. Das wurde von der Benutzerschaft sehr positiv aufgenommen. Darüber hinaus erfordert das Programm sehr wenig administrativen Aufwand. Es arbeitet vollkommen automatisch, was nicht zuletzt auch die Funk-LAN-Hotline der GWDG und der Universität entsprechend entlastet.

Die bisherigen, noch recht frischen Erfahrungen sowie die Statistiken zeigen, dass die Erkennung gerader in frühen Vergangenheit ein echter Gewinn für das Funk-LAN ist und sich als zusätzlicher, sehr sinnvoller Netzwerkdienst herausstellt.

Ißleiber

3. Betriebsausflug der GWDG am 26.05.2004

Am Mittwoch, den 26.05.2004, findet der diesjährige Betriebsausflug der GWDG statt. Das Rechenzentrum bleibt an diesem Tag zwar zu den üblichen Zeiten geöffnet, es wird aber nur eine Minimalbesetzung an Personal anwesend sein. Wir bitten alle Benutzer und Besucher der GWDG, sich hierauf einzustellen.

Otto

---

4. Öffnungszeiten des Rechenzentrums um Pfingsten 2004

Das Rechenzentrum der GWDG ist an den beiden Pfingstfeiertagen, 30. und 31.05.2004, geschlossen.

Am 29.05., Pfingstsamstag, ist das Rechenzentrum von 10.00 bis 18.00 Uhr geöffnet, jedoch ist während dieser Zeit nur unbedienter Betrieb möglich. Die Aufsicht wird durch Wachpersonal geführt.

Am 01.06., Dienstag nach Pfingsten, ist das Rechenzentrum ab 7.10 Uhr wieder wie üblich geöffnet.

Zu den Zeiten, in denen das Rechenzentrum im unbedienten Betrieb arbeitet oder geschlossen bleibt, werden die Rechenanlagen ohne Operateure betrieben. Wir bitten die Benutzer deshalb, sich darauf einzustellen. Die Betriebsbereitschaft der Rechenanlagen und Netze wird durch freiwillige Mitarbeiter gewährleistet.

Grieger

---

5. Informationsveranstaltung „Sicherheit im GÖNET“ am 29.06.2004

Im Dezember 2003 hatte die GWDG alle System- und Netzbetreuer im GÖNET eingeladen, um über die Sicherheit im GÖNET zu informieren und zu diskutieren. Die Teilnehmer äußerten den Wunsch, solche Veranstaltungen regelmäßig zu wiederholen.

Diesem Wunsch will die GWDG gern entsprechen und lädt daher zu einem erneuten Treffen ein.

Termin: Dienstag, 29.06.2004, um 14.00 Uhr

Dauer: ca. 2 Stunden

Ort: Hörsaal des MPI für biophysikalische Chemie, Göttingen, Am Faßberg

Diese Veranstaltung richtet sich an die Rechner- und Netzwerkbetreuer der am GÖNET angeschlossenen Institute. Auch diesmal wird die GWDG zunächst über die aktuelle Lage und zukünftige Planungen berichten. Anregungen aus dem Nutzerkreis für die Gestaltung des Treffen sind auch im Vorfeld erwünscht (z. B. per E-Mail an Holger.Beck@gwdg.de).

Weitere Informationen zur Veranstaltung werden zeitnah über die GÖNET-Mailing-Liste und im WWW unter

`http://www.gwdg.de/forschung/veranstaltungen/workshops`

zur Verfügung gestellt.

Wir hoffen wiederum auf eine lebhafte Diskussion und eine ebenso rege Beteiligung wie im Dezember.

Beck

6. Aufbau einer Public-Key-Infrastruktur in Göttingen

6.1 Einleitung

Das Internet bietet mit seiner dezentralen Struktur eine ideale Basis für Anonymität. Häufig ist es schwierig, die wahre Identität eines am Internet angeschlossenen Rechners oder eines von ihm angebotenen Dienstes exakt zu ermitteln. Seine Authentizität wird nicht zuletzt durch die zunehmenden Angriffe auf Rechner und Dienste im weltweiten Netz gefährdet. Während die Anonymität im Internet von vielen Teilnehmern akzeptiert bzw. sogar geschätzt wird, sind die Grenzen für diese Akzeptanz fest abgesteckt. Nur wenige Nutzer dürften verständlicherweise Interesse an einem Home-Banking-Angebot mit einem anonymen Kreditinstitut bekunden. Dabei spielt die Authentifizierung des Kreditinstituts eine zentrale Rolle. Ohne diese eindeutige Identifizierung des Kommunikationspartners entsteht keine Vertrauensbasis z. B. für die anschließende Verschlüsselung oder Integritätsprüfung der Übertragung.

Die Authentifizierung der Kommunikationspartner kann über ein Zertifikat erfolgen, das die Identität des Zertifikatinhabers anhand der Beglaubigung durch einen vertrauenswürdigen Dritten eindeutig nachweist. Für die Verwaltung solcher Zertifikate und die Festlegung vertrauenswürdiger Dritter werden Public-Key-Infrastrukturen (kurz: PKIen) verwendet. Aus diesem Grund bilden bei vielen Internet-Diensten im Hintergrund PKIen die notwendige Basis für einen vertrauenswürdigen Datenaustausch.

Aus dem World Wide Web bekannt ist die Verwendung des Protokolls HTTPS [BaRiSc03] wie z. B. beim unter **`https://mailer.gwdg.de`** erreichbaren Webmailer der GWDG. Hierbei werden die Protokolle Secure Sockets Layer [SSL] bzw. Transport Layer Security [TLS] verwendet, die die Gewährleistung der Authentizität der Kommunikationspartner anhand von Zertifikaten nach dem X.509-Standard [X509] realisieren. Neben der Verwendung im World Wide Web kommen Zertifikate für nahezu alle Facetten der Authentifizierung in Frage. Beispielsweise für die Signierung von versendeten E-Mails als digitale Unterschrift oder die Verschlüsselung von privaten Dateien.

Auch in Göttingen werden bereits vereinzelt eigene PKIen betrieben. Da diese jedoch untereinander in keinem Vertrauensverhältnis stehen und insbesondere viele weitere Anforderungen in Göttingen existieren, die eine Public-Key-Infrastruktur (PKI) voraussetzen, plant die GWDG seit einigen Monaten den Betrieb der eigenen **Zertifizierungsstelle GWDG-CA** (Certification Authority, kurz: CA) und einer damit verbundenen PKI. Dabei sollen PKI-Leistungen sowohl für den Standort Göttingen im Allgmeinen sowie die Georg-August-Universität im Besonderen, als auch für die Max-Planck-Gesellschaft angeboten werden.

6.2 Definition von PKIen

Eine PKI ermöglicht die Verteilung und Verwaltung von öffentlichen Schlüsseln aus asymmetrischen Schlüsselpaaren. Ein asymmetrisches Schlüsselpaar beinhaltet zwei gewissermaßen komplementäre Schlüssel, die zum Verschlüsseln bzw. zum Entschlüsseln verwendet werden können. Im Vergleich zu einem symmetrischen Schlüssel, wie z. B. aus der klassischen Chiffrierung bekannt, bei der derselbe Schlüssel für die Ver- und Entschlüsselung der Daten verwendet wird, können Daten, die mit einem der beiden asymmetrischen Schlüssel verschlüsselt wurden, nur dem jeweiligen anderen Schlüssel des Paares entschlüsselt werden (siehe z. B. auch [BaRiSc03]).

Im Umfeld der asymmetrischen Verschlüsselung spricht man im Bezug auf die Schlüssel eines Paares auch von einem privaten und einem zugehörigen öffentlichen Schlüssel. Öffentlich bedeutet hierbei, dass dieser Schlüssel freizügig verteilt werden kann, um damit z. B. Daten für den Besitzer des Schlüsselpaares zu verschlüsseln. In diesem Fall können die übermittelten Daten ausschließlich vom Besitzer des privaten Schlüssels entschlüsselt werden, was implizit eine Authentifizierung des Empfängers ermöglicht. Private Schlüssel müssen vor dem Zugriff durch Dritte in geeigneter Weise geschützt werden.

Verwendet der Besitzer des Schlüsselpaares im Gegenzug seinen privaten Schlüssel zum Verschlüsseln der Daten, so kann jeder Empfänger anhand des öffentlichen Schlüssels nachprüfen, ob die Nachricht tatsächlich vom Besitzer des Schlüsselpaares stammt. Diese Verwendung des geheimen (privaten) Schlüssels wird auch als digitale Signatur oder kurz Signatur bezeichnet. Häufig wird hierbei nicht die gesamte Nachricht mit dem geheimen Schlüssel verschlüsselt bzw. signiert, sondern ein eindeutiger Komprimat (nicht invertierbarer Hash-Wert) des Textes. Der geheime Schlüssel kann nicht anhand des öffentlichen Schlüssels ermittelt werden.

Wird der geheime Schlüssel zum Signieren untergeordneter öffentlicher Schlüssel verwendet, so spricht man im Bezug auf den damit signierten öffentlichen Schlüssel auch von einem Zertifikat. Der Vorgang der Signatur wird zusammen mit der

Prüfung der zugewiesenen Identität auch als Zertifizierung bezeichnet. Die Signatur eines Zertifikats kann über den öffentlichen Schlüssel der Signaturinstanz auf Ihre Echtheit überprüft werden. Da zu diesem öffentlichen Schlüssel zugehörige Zertifikate nur mit dem geheimen Schlüssel erstellt werden können, der aus dem öffentlichen Schlüssel nicht ermittelt werden kann, können Zertifikate bei richtiger Anwendung derzeit als fälschungssicher angesehen werden.

Zertifikate können somit eindeutig auf eine Identität zurückgeführt werden, so dass eine sichere Authentifizierung möglich ist.

Zertifikate unterstützen verschiedene Verwendungsarten. Einem Zertifikat können mehrere Verwendungsarten zugewiesen werden, womit eine einheitliche Authentifizierung einer Identität über ein Zertifikat für verschiedene Dienste möglich wird. Die Verwaltung einer Vielzahl solcher Zertifikate für unterschiedliche Verwendungszwecke bildet schließlich eine PKI. Der Einsatz von PKIen hat in den letzten Jahren deutlich zugenommen. Dies hängt zum einen mit dem gesteigerten Bedürfnis an IT-Sicherheit zusammen. Zum anderen resultiert der Zuwachs aus der weitgehenden Vereinfachung der notwendigen Software sowie der preisgünstigen Verfügbarkeit von Drittanbietern (z. B. Thawte oder Trust Center), die eine Signierung mit einer weltweit akzeptierten Signatur anbieten.

Eine ausführliche Beschreibung der technischen und theoretischen Grundlagen von PKIen kann u. a. in [Raina_03] nachgelesen werden.

6.3 Anwendungen für PKIen in Göttingen

Die PKI-Leistungen der GWDG beziehen sich auf unterschiedliche Anforderungen, die in der Vergangenheit von der GWDG selbst oder angebundenen Einrichtungen gestellt wurden. Einige dieser Anforderungen führten bereits zu konkret geplanten bzw. teilweise bereits realisierten Anwendungen am Standort Göttingen. Im Folgenden werden einige dieser Anwendungen exemplarisch aufgelistet:

6.3.1 PKI-Leistungen für Einrichtungen am Standort Göttingen und externe Dritte

Häufigstes Anwendungsgebiet für Zertifikate ist die server-seitige Authentifizierung z. B. von Webservern über SSL. Webserver am Standort Göttingen könnten Zertifikate aus der PKI der GWDG verwenden. Auch die Verschlüsselung / Signierung von E-Mails oder die Benutzerauthentifizierung könnte über solche Zertifikate erfolgen. Es könnte z. B. auch eine Authentifizierung der Benutzer am Webserver mittels Zertifikat erfolgen. Dadurch würde die teilweise eingesetzte „Authentifizierung“ über IP-Adressen gegen eine fälschungssichere und flexible Lösung ersetzt.

Für den weltweiten Einsatz ist hierbei ein Zertifikat mit hoher allgemeiner Akzeptanz notwendig. Es sollte daher eine übergeordnete Zertifizierungsstelle integriert werden, deren Signatur weltweit hohe Akzeptanz besitzt und die implizit allen Teilnehmern der PKI als Vertrauensbasis zur Verfügung steht.

Durch die Verfügbarkeit einer PKI innerhalb der GWDG können Leistungen im Zusammenhang mit Zertifikaten auch an untergeordnete Teilnehmer delegiert werden. So könnte z. B. ein Institut seine eigene PKI betreiben, um Zertifikate für einen bestimmten Anwendungszweck auszustellen, der ausschließlich in diesem Institut oder mit hohem administrativem Aufwand betrieben wird.

6.3.2 Zugangssicherung von Servern mit hoher Sicherheitsanforderung

Durch die Speicherung von Zertifikaten auf einem sog. Token (Smart Card, USB-Stick, …) wird eine höhere Sicherheit bei der Authentifizierung an Endgeräten möglich. Der geheime Schlüssel des asymmetrischen Schlüsselpaares ist in diesem Fall auf dem Token gespeichert und kann nicht ausgelesen werden. Er verlässt das Token gewissermaßen nicht. Das Token bietet nach Außen lediglich eine Verarbeitung von Eingangsdaten mit dem geheimen Schlüssel an. So kann ein Benutzer i. d. R. nach der Eingabe einer PIN sich durch das Token authentifizieren (2-Faktor-Authentifizierung).

Die GWDG plant den Einsatz von Tokens z. B. an Servern, die eine hohe Sicherheit z. B. aufgrund Ihrer hohen Position in der Hierarchie verteilter Server-Strukturen erfordern. Der Administrator könnte sich dann nur unter Verwendung des Tokens an dem Server anmelden. Dies erhöht im Idealfall auch die Sicherheit vor Hackerangriffen.

6.3.3 Verschlüsselung von Dateien, E-Mails und Daten

Die Verwendung von Zertifikaten ermöglicht eine Verschlüsselung von Dateien auf Fileservern der GWDG und der MPG. Dadurch können für Benutzer Bereiche angelegt werden, in denen sie Daten vor dem Zugriff durch Dritte sicher schützen können. Dies bedeutet im Idealfall auch, dass der Administrator selbst nicht auf diese Daten zugreifen kann. Verliert ein Benutzer seinen geheimen Schlüssel, könnte eine Sicherheitskopie dieses Schlüssels nach dem „Vier-Augen-Prinzip“ z. B. unter Einbeziehung des zuständigen Datenschutzbeauftragten

rekonstruiert und damit eine Ausnahmeregelung für den Zugriff auf dessen Daten ermöglicht werden.

Neben Dateien können auf dieselbe Weise auch andere Daten wie beispielsweise E-Mails verschlüsselt werden. Hierbei kann eine Mail zusätzlich digital signiert werden, um ihre Integrität zu gewährleisten.

6.3.4 Signierung von Daten bei der Langzeitarchivierung

Bei der Speicherung der Daten sollen diese vor Veränderungen sowie dem Zugriff durch unberechtigte Dritte geschützt werden. Hierfür bietet sich eine Signierung der Daten an, bei der ein unveränderlicher Komprimat (Hash-Wert) der Daten mit einem geheimen Schlüssel des Archivars signiert wird. Die Echtheit der Daten kann somit bei der Entnahme über dessen öffentlichen Schlüssel gewährleistet werden.

Über eine Verschlüsselung der Daten mit dem öffentlichen Schlüssel bzw. dem Zertifikat des Archivars der Daten lässt sich zudem ein Zugriffsschutz erreichen. Auf diese Weise könnte auch gesichert werden, dass Nutzungsrechte (z. B. in Form eines Digital Rights Management) erhalten bleiben.

Für die Signierung ist eine separate PKI notwendig, da die gespeicherten Daten eine hohe Lagerzeit besitzen. Teilweise müssen nach gesetzlicher Vorgabe Lebenszeiten von bis zu 30 Jahren für ein Zertifikat vorgesehen werden. Diese Zeiträume werden von externen Trustcentern gar nicht oder nur zu hohen Preisen angeboten.

6.4 Geplante PKI-Struktur

Die derzeit für die GWDG geplante PKI-Struktur stellt eine dreistufige Hierarchie, wie in Abb. 1 gezeigt, dar. Auf der obersten Ebene der Hierarchie (Ebene 1) befindet sich dabei die höchste Zertifizierungsstelle der GWDG, die über keinerlei Netzanbindung verfügt. Zertifizierungsanfragen an diese Zertifizierungsstelle werden über einen separat im Tresor gelagerten Datenträger durchgeführt. Neben Backups wird in diesem Tresor auch der für jede Signatur notwendige geheime Schlüssel gelagert. Der Zugriff auf diesen geheimen Schlüssel ist zusätzlich durch nicht-trivale Passwörter geschützt und kann nur nach dem Vier-Augen-Prinzip im Beisein mehrerer Administratoren bzw. der Geschäftsleitung erfolgen. Die völlige Abtrennung vom Netz (physikalische Trennung) ist notwendig, um einen Zugriff auf den geheimen Schlüssel von Außen auch während dessen Verwendung generell zu unterbinden. Diese Vorgabe wird zudem von den meisten externen Zertifizierungsstellen vorgeschrieben bzw. empfohlen.

Diese und viele weitere Vorgaben bilden die sog. Policy als Richtlinie für den Betrieb der Zertifizierungsstelle. (Hierüber wird in einer der nächsten Ausgaben der GWDG-Nachrichten ausführlicher berichtet.) Die GWDG übernimmt bzw. garantiert dabei zum einen die Einhaltung der Policy der ausgewählten übergeordneten Zertifizierungsstelle. Zum anderen wurde für die GWDG, basierend auf dieser Policy, eine eigene Richtlinie definiert. Diese kann in Kürze unter **`http://ca.gwdg.de`** abgerufen werden. Die Policy umfasst zusätzlich beispiels-

weise Regelungen für den Datenschutz, Sperrung von Zertifikaten usw.

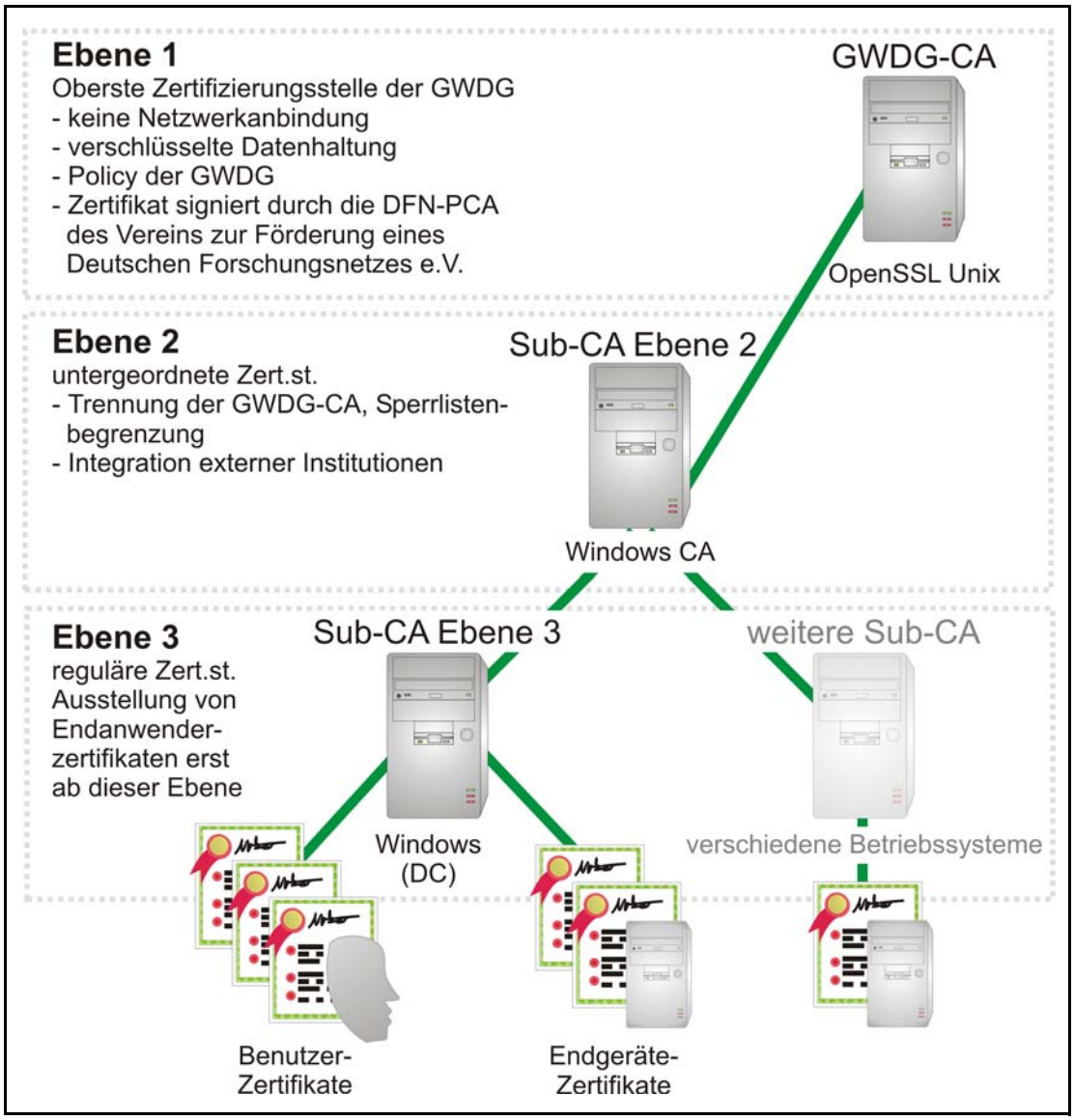

Abb. 1: Public-Key-Infrastruktur der GWDG

Die zweite Hierarchieebene (Ebene 2) ist für Zertifizierungsstellen weiterer Organisationen gedacht. Vorteil dieser Aufspaltung der Zuständigkeiten ist nicht nur die Verteilung des administrativen und organisatorischen Aufwands, sondern auch die Absicherung der obersten Zertifizierungsstelle sowie die anderer Organisationen im Falle eines kompromittierten geheimen Schlüssels. In diesem Fall könnte für die kompromittierte Stelle auf Ebene 2 ein neuer geheimer Schlüssel mit zugehörigem Zertifikat vergeben werden, ohne das verbreitete Zertifikat der obersten Zertifizierungsstelle verändern zu müssen.

Zertifizierungsstellen ab der Ebene 2 können über einen Netzanschluss verfügen. Eine Absicherung der Systeme erfolgt dabei nach der von der GWDG verwendeten IT-Sicherheitsleitlinie sowie zugehörigen Richtlinien. Dadurch können von diesen Stellen signierte Zertifikate auch direkt in einem Verzeichnis beispielsweise über LDAP eingetragen werden.

Auf der Ebene 3 (vgl. Abb. 1) können schließlich Zertifizierungsstellen eingerichtet werden, die Zertifikate für Endbenutzer bzw. Endgeräte signieren. Die Signierung solcher Zertifikate ist generell erst ab dieser Ebene möglich. Die oberste Zertifizierungsstelle der GWDG darf gemäß der Policy keine Zertifikate für Endbenutzer bzw. -geräte ausstellen.

Die oberste Zertifizierungsstelle der GWDG auf der Ebene 1 ist in die PKI des Vereins zur Förderung eines deutschen Forschungsnetzes e. V. (kurz: DFN-Verein) eingegliedert. Ihr Zertifikat wurde daher von der DFN-PCA als Zertifizierungsstelle

des DFN-Vereins signiert [DFNPCA]. Die Signierung durch den DFN-Verein verschafft der skizzierten PKI dabei noch keine weltweit anerkannte Signatur. Da eine weltweit akzeptierte Zertifizierung mit hohen Kosten verbunden ist, wird für den gegenwärtigen Zeitpunkt eine Zwischenlösung realisiert. Dabei wird das Zertifikat der Ebene 1 bzw. des DFN-Vereins an die zugehörigen Rechner (z. B. über OpenLDAP, automatisch über das Active Directory bzw. die Windows-Domäne) verteilt. Um eine weltweite Vertrauensstellung zur PKI der GWDG zu realisieren, wird das Stammzertifikat außerdem auf einer Web-Seite, die über ein SSL-Zertifikat mit weltweiter Akzeptanz (der Fa. Trust Center) verfügt, abgelegt. Dadurch können Benutzer weltweit gesichert über das allgemein akzeptierte SSL-Zertifikat das Stammzertifikat der PKI der GWDG auf ihrem Rechner hinzufügen bzw. dessen Echtheit überprüfen.

6.5 Implementierung und Zeitplan

Die in Abb. 1 skizzierte Struktur wurde in den letzten Monaten innerhalb der GWDG realisiert. Dies umfasst neben den im vorherigen Abschnitt beschriebenen umfangreichen organisatorischen Vorgaben auch die technische Implementierung der PKI. Wie die Abb. 1 bereits zeigt, wurden hierbei unterschiedliche Betriebssysteme verwendet und keine feste Vorgabe für die verwendete Software in untergeordneten Zertifizierungsstellen getroffen. Einzig das Format der Zertifikate und die Zertifizierungshierarchie sind durch den X.509-Standard festgelegt.

Die Auswahl mehrerer PKI-Produkte für die vorgestellte Struktur begründet sich aus den Nachteilen der Einzellösungen. Während sich die in Windows integrierte CA-Komponente wesentlich schwieriger vom Netzwerk trennen lässt und wesentliche PKI-Funktionen wie den Schutz des privaten Schlüssels der CA über Passwörter nur mit Drittanbieter-Lösungen bietet, zeigt sich die OpenSSL-basierte OpenCA weniger einsatzbereit für unternehmenstypische Anforderungen wie teilautomatisierte Verlängerung von Zertifikaten oder die Wiederherstellung bzw. Archivierung von Schlüsseln. Im Zusammenspiel der beiden PKI-Systeme lösen sich die aufgezählten Nachteile nahezu vollständig auf. Alternative Software-Lösungen, die keine der genannten Nachteile aufweisen, sind hingegen nur gegen hohe jährliche bzw. benutzerabhängige Lizenzkosten erhältlich.

Die Zertifizierungsstellen der Ebenen 1 und 2 befinden sich derzeit im Testbetrieb innerhalb der GWDG. Ab Juni 2004 sollen erste Zertifizierungsstellen auf der Ebene 3 offiziell eingebunden werden. Eine testweise Integration in das Active-Directory-Umfeld der GWDG ist hierbei bereits erfolgt.

Literaturverweise und weitere Informationen

[AdaLlo03]:
Understanding PKI, Addison-Wesley Professional, 2002

[BaRiSc03]:
Badach, Rieger, Schmauch, Web-Technologien, Hanser, 2003

[DFNPCA]:
DFN Policy-based Certification Authority (PCA), World Wide Web Policy **`http://www.dfn-pca.de`**

[Raina03]:
PKI Security Solutions for the Enterprise, Wiley, 2003

[Schmeh01]:
Kryptografie und Public-Key-Infrastrukturen im Internet, Dpunkt, 2001

[SSL]:
`http://wp.netscape.com/eng/ssl3`

[TLS]:
`http://www.ietf.org/html.charters/tls-charter.html`

[X509]:
ITU-T Recommendation X.509 (1997 E): Information Technologie – Open Systems Interconnection – The Directory: Authentication Framework

Informationen zur OpenCA:
`http://www.openca.org`

Windows CA:
`http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx`

Informationen zur Zertifizierungstelle der GWDG (Policy, Zertifikate, Sperrlisten usw.) in Kürze unter:
`http://ca.gwdg.de`

Rieger

7. 10 Jahre WWW-Server der GWDG

Im Mai 1994 war das World Wide Web gerade mal ein Jahr alt geworden. Die Wenigsten kannten es damals bereits. Es gab auch durchaus Ernst zu nehmende Konkurrenten. Man denke beispielsweise an Hyper-G, später Hyperwave genannt, mit den hübschen Browser-Namen Harmony oder Amadeus. Nun ja, diese Software war in Österreich entwickelt worden. Der Gopher, den einige noch als Vorläufer des WWW kennen, befand sich bereits auf dem absteigenden Ast, weil er als textorientiertes Informationssystem die aufkommende bunte Vielfalt nicht so recht darstellen konnte.

Die GWDG hatte sich im Mai 1994 entschlossen, als weiteres Informationssystem einen WWW-Server zu betreiben. In wenigen Wochen wurden die Inhalte aus dem Boden gestampft. Sie deckten schon in der ersten Ausgabe sowohl die Universität Göttingen als auch die Max-Planck-Gesellschaft ab. Einfach war das jedoch nicht: Tabellen unter HTML waren noch nicht erfunden, an Frontpage oder an andere HTML-Composer war noch nicht zu denken. Inhalte wurden mit simplen Texteditoren erstellt, jeder HTML-Tag musste mit den Fingern auf der Tastatur eingetippt werden.

Seit der Zeit hat sich glücklicherweise viel verändert. Das WWW ist riesengroß und unüberschaubar geworden. Schon die Fülle der Inhalte auf einem einzelnen Server sprengt die Fassungskraft einer einzelnen Person.

Nachgefragt werden deshalb jetzt neue Systeme, die die Inhalte und Verknüpfungen darauf verwalten: die Content-Management-Systeme (s. hierzu auch die GWDG-Nachrichten 8/2002). Hätte damals Hyper-G das Rennen um die Gunst des beliebtesten Informationssystems gewonnen und nicht das WWW, so wäre heute die Einführung eines CMS überflüssig, da Hyper-G das enthalten hätte.

Grieger

---

8. Hintergründe für die Störung des Benutzerbetriebs am 20.04.2004

Am Dienstag, den 20. April 2004, kam es gegen 16.00 Uhr zu einer Störung im Storage Area Network (SAN), so dass der Mailer und der zentrale Fileserver nicht mehr auf alle Benutzerdaten (Mailboxen, Homedirectories und Samba) zugreifen konnten. Der Ausfall ließ sich wegen der vorhandenen Redundanz im SAN gegen 16.30 Uhr durch Neustart des Mailers und des zentralen Fileservers relativ schnell beheben.

Ausgelöst wurde diese Störung vermutlich durch einen defekten Netzadapter in einem Backupserver, der ebenfalls das SAN nutzt. Er zeigte seit Dienstagmittag Funktionsstörungen. Ein neuer Adapter wurde bis Donnerstag beschafft, so dass der Backup-Service ab Donnerstag 20.00 Uhr ebenfalls wieder aufgenommen werden konnte.

Hattenbach

---

9. Kurse des Rechenzentrums

9.1 Allgemeine Informationen zum Kursangebot der GWDG

9.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

9.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 21119 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen

werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

9.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

9.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

9.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

`http://www.gwdg.de/gwdg/standort/lageplan`

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

9.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

`http://www.gwdg.de/service/kurse`

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

9.2 Kurse von Juni bis Dezember 2004 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Datenschutz - Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG	• 18.06.2004	Dr. Grieger
Einführung in die Nutzung des Leistungsangebots der GWDG	• 09.06.2004 • 15.09.2004 • 08.12.2004	Dr. Grieger Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 13.09.2004	Eyßell

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Führung durch das Rechnermuseum	• 04.06.2004 • 02.07.2004 • 20.08.2004 • 17.09.2004 • 08.10.2004 • 12.11.2004 • 10.12.2004	Eyßell Eyßell Eyßell Eyßell Eyßell Eyßell Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 14.09.2004	Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
UNIX/Linux-Windows-Systemintegration mit SAMBA	• 24.06.2004 - 25.06.2004	Dr. Heuer
Grundkurs UNIX/Linux mit Übungen	• 31.08.2004 - 02.09.2004 • 07.12.2004 - 09.12.2004	Hattenbach Hattenbach
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 07.06.2004 - 08.06.2004 • 05.07.2004 - 06.07.2004 • 29.11.2004 - 30.11.2004	Dr. Bohrer Dr. Bohrer Dr. Bohrer
Installation und Administration von UNIX-Systemen	• 14.12.2004 - 17.12.2004	Dr. Heuer, Dr. Sippel
UNIX für Fortgeschrittene	• 22.11.2004 - 24.11.2004	Dr. Sippel
Die Windows-Active-Directory-Domäne	• 06.10.2004 - 08.10.2004	Quentin
Windows XP für Systembetreuer	• 04.10.2004 - 05.10.2004	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Das Internet als Werkzeug für die Biowissenschaften	• 15.10.2004	Dr. Liesegang
Sicherheit im Internet für Anwender	• 02.12.2004	Reimann
Web Publishing I	• 28.10.2004 - 29.10.2004	Reimann
XML	• 29.09.2004 - 01.10.2004	Reimann, Koch

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Arbeiten mit CAD, Grundlagen	• 06.09.2004 - 10.09.2004	Witt
CorelDRAW - Grundlagen	• 19.10.2004 - 20.10.2004	Wagenführ
Grundlagen der Bildbearbeitung mit Photoshop	• 28.06.2004 - 29.06.2004	Töpfer
Photoshop für Fortgeschrittene	• 10.06.2004 - 11.06.2004 • 23.08.2004 - 24.08.2004	Töpfer Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Datenbanksystem MS Access, Einführung mit Übungen	• 22.11.2004 - 26.11.2004	Dr. Kneser
Anwendungen in Lotus Notes	• 26.10.2004 - 27.10.2004	Greber, Dr. Grieger
Ideenorganisation mit OneNote und MindManager	• 03.06.2004 - 04.06.2004	Reimann
PDF-Dateien: Erzeugung und Bearbeitung	• 07.07.2004 - 08.07.2004	Dr. Baier, Koch
PowerPoint	• 21.12.2004 - 22.12.2004	Reimann
Projektplanung mit MS Project	• 19.08.2004 - 20.08.2004	Reimann
SAS - Grundlagen	• 15.06.2004 - 17.06.2004 • 09.11.2004 - 11.11.2004	Wagenführ Wagenführ
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	• 11.10.2004 - 14.10.2004	Dr. Bohrer, Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 12.11.2004	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Einführung in die Programmiersprache Fortran 90/95	• 27.09.2004 - 28.09.2004	Dr. Schwardmann
Programmierung von Parallelrechnern	• 02.11.2004 - 04.11.2004	Prof. Haan, Dr. Schwardmann

9.3 Kurse von Juni bis Dezember 2004 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Ideenorganisation mit OneNote und MindManager	Reimann	03.06.2004 - 04.06.2004 9.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	27.05.2004	8
Führung durch das Rechner-museum	Eyßell	04.06.2004 10.00 - 12.00 Uhr	28.05.2004	0
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	07.06.2004 - 08.06.2004 13.30 - 16.30 Uhr	31.05.2004	4
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	09.06.2004 17.15 - 20.00 Uhr	02.06.2004	0
Photoshop für Fortgeschrittene	Töpfer	10.06.2004 - 11.06.2004 09.30 - 16.00 Uhr	03.06.2004	8
SAS - Grundlagen	Wagenführ	15.06.2004 - 17.06.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	08.06.2004	12
Datenschutz - Verarbeitung perso-nenbezogener Daten auf den Rechenanlagen der GWDG	Dr. Grieger	18.06.2004 09.15 - 12.00 Uhr	11.06.2004	2
UNIX/Linux-Windows-System-integration mit SAMBA	Dr. Heuer	24.06.2004 - 25.06.2004 09.30 - 12.00 Uhr und 13.30 - 16.30 Uhr	17.06.2004	8
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	28.06.2004 - 29.06.2004 09.30 - 16.00 Uhr	21.06.2004	8
Führung durch das Rechner-museum	Eyßell	02.07.2004 10.00 - 12.00 Uhr	25.06.2004	0
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	05.07.2004 - 06.07.2004 13.30 - 16.30 Uhr	28.06.2004	4
PDF-Dateien: Erzeugung und Bear-beitung	Dr. Baier, Koch	07.07.2004 - 08.07.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	30.06.2004	8
Projektplanung mit MS Project	Reimann	19.08.2004 - 20.08.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	12.08.2004	8
Führung durch das Rechner-museum	Eyßell	20.08.2004 10.00 - 12.00 Uhr	13.08.2004	0
Photoshop für Fortgeschrittene	Töpfer	23.08.2004 - 24.08.2004 09.30 - 16.00 Uhr	16.08.2004	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	31.08.2004 - 02.09.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	24.08.2004	12

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Arbeiten mit CAD, Grundlagen	Witt	06.09.2004 - 10.09.2004 09.00 - 16.00 Uhr, (am 06.09. ab 10.00 Uhr; am 10.09. bis 13.00 Uhr)	30.08.2004	20
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	13.09.2004 09.15 - 12.30 Uhr	06.09.2004	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	14.09.2004 09.15 - 12.30 Uhr und 13.30 - 16.00 Uhr	07.09.2004	4
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	15.09.2004 17.15 - 20.00 Uhr	08.09.2004	0
Führung durch das Rechner-museum	Eyßell	17.09.2004 10.00 - 12.00 Uhr	10.09.2004	0
Einführung in die Programmier-sprache Fortran 90/95	Dr. Schwardmann	27.09.2004 - 28.09.2004 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	20.09.2004	8
XML	Reimann, Koch	29.09.2004 - 01.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	22.09.2004	12
Windows XP für Systembetreuer	Quentin	04.10.2004 - 05.10.2004 09.15 - 15.30 Uhr	27.09.2004	8
Die Windows-Active-Directory-Domäne	Quentin	06.10.2004 - 08.10.2004 09.15 - 15.30 Uhr	29.09.2004	12
Führung durch das Rechner-museum	Eyßell	08.10.2004 10.00 - 12.00 Uhr	01.10.2004	0
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	Dr. Bohrer, Dr. Liesegang	11.10.2004 - 14.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.10.2004	16
Das Internet als Werkzeug für die Biowissenschaften	Dr. Liesegang	15.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	08.10.2004	4
CorelDRAW - Grundlagen	Wagenführ	19.10.2004 - 20.10.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	12.10.2004	8
Anwendungen in Lotus Notes	Greber, Dr. Grieger	26.10.2004 - 27.10.2004 09.15 - 16.30 Uhr	19.10.2004	8
Web Publishing I	Reimann	28.10.2004 - 29.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	21.10.2004	8
Programmierung von Parallel-rechnern	Prof. Dr. Haan, Dr. Schwardmann	02.11.2004 - 04.11.2004 09.15 - 12.15 Uhr und 14.00 - 17.00 Uhr	26.10.2004	12

Kurs	Vortragende	Termin	Anmelde-schluss	AE
SAS - Grundlagen	Wagenführ	09.11.2004 - 11.11.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	02.11.2004	12
Führung durch das Rechner-museum	Eyßell	12.11.2004 10.00 - 12.00 Uhr	05.11.2004	0
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	12.11.2004 09.15 - 12.00 Uhr	05.11.2004	2
Datenbanksystem MS Access, Einführung mit Übungen	Dr. Kneser	22.11.2004 - 26.11.2004 09.00 - 12.00 Uhr	15.11.2004	10
UNIX für Fortgeschrittene	Dr. Sippel	22.11.2004 - 24.11.2004 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	15.11.2004	12
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	29.11.2004 - 30.11.2004 13.30 - 16.30 Uhr	22.11.2004	4
Sicherheit im Internet für Anwender	Reimann	02.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	25.11.2004	4
Grundkurs UNIX/Linux mit Übungen	Hattenbach	07.12.2004 - 09.12.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	30.11.2004	12
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	08.12.2004 17.15 - 20.00 Uhr	01.12.2004	0
Führung durch das Rechner-museum	Eyßell	10.12.2004 10.00 - 12.00 Uhr	03.12.2004	0
Installation und Administration von UNIX-Systemen	Dr. Heuer, Dr. Sippel	14.12.2004 - 17.12.2004 09.30 - 12.00 Uhr und 13.30 - 16.30 Uhr	07.12.2004	16
PowerPoint	Reimann	21.12.2004 - 22.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	14.12.2004	8

10. Betriebsstatistik April 2004

10.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	12	2.426,92
IBM RS/6000 SP	224	99.883,50
IBM Regatta	96	50.429,92
Linux Parallel	198	115.714,24

10.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	1	1,00	0	
IBM SP/Regatta	0		0	
Linux Parallel	0		0	
PC-Netz	0		0	
Nameserver	0		0	
Mailer	2	1,20	1	1,00

11. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Dr. Holger Beck	• Informationsveranstaltung „Sicherheit im GÖNET“ am 29.06.2004	Holger.Beck@gwdg.de 0551 201-1554
Dr. Wilfried Grieger	• Öffnungszeiten des Rechenzentrums um Pfingsten 2004	wgriege@gwdg.de 0551 201-1512
Dr. Wilfried Grieger	• 10 Jahre WWW-Server der GWDG	wgriege@gwdg.de 0551 201-1512
Jürgen Hattenbach	• Hintergründe für die Störung des Benutzer-betriebs am 20.04.2004	jhatten@gwdg.de 0551 201-1517
Andreas Ißleiber	• Schnelle Erkennung von Viren und Troja-nern im Funk-LAN	aisslei@gwdg.de 0551 201-1815
Dr. Thomas Otto	• Betriebsausflug der GWDG am 26.05.2004	totto@gwdg.de 0551 201-1828
Michael Reimann	• Wurmbefall im GÖNET	mreiman1@gwdg.de 0551 201-1826
Sebastian Rieger	• Aufbau einer Public-Key-Infrastruktur in Göttingen	srieger1@gwdg.de 0551 201-1878