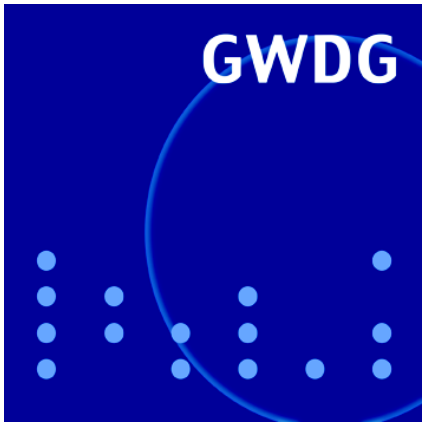


Norman Virus Control
und Sophos Anti-Virus

Intrusion Detection und
Prevention im GÖNET

GWDG Nachrichten

8 / 2006

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

29. Jahrgang, Ausgabe 8 / 2006

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

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

Redaktion und
Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

1. Umstieg von Norman Virus Control auf Sophos Anti-Virus

Da die Universität Göttingen zum 31.10.2006 den Lizenzvertrag für **Norman Virus Control** gekündigt hat (s. GWDG-Nachrichten 2/2006), besteht ab dem 01.11.2006 kein Anspruch mehr auf Updates. Nutzer dieses Virenscanners sollten somit rechtzeitig auf das Produkt **Anti-Virus** der Firma **Sophos** umsteigen. Wie das im Einzelnen vor sich gehen könnte, wird in diesem Artikel exemplarisch für Windows XP dargelegt. Für die anderen Betriebssystemvarianten wie Windows 95, 98, ME und NT finden sich Anleitungen auf dem Sophos-Update-Service der GWDG:

`http://antivir.gwdg.de`

Bevor jedoch die Installation in Angriff genommen wird, sollte zuvor der Norman-Virenscanner deinstalliert werden, da ansonsten unvorhersehbare Wechselwirkungen zu befürchten sind.

1.1 Deinstallation von Norman Virus Control

Eine funktionstüchtige Installation von **Norman Virus Control** dokumentiert sich im Allgemeinen durch das Symbol eines weißen „**N**“ auf grünem Grund in der Taskleiste. Zuerst sollte das Programm auf dem üblichen Wege über **Start > Systemsteuerung > Software** entfernt werden. Sodann startet der Norman-Uninstaller und bietet die Möglichkeit zur Entfernung (Auswahl: **Entfernen**) an. Nach einer kurzen Zeit meldet die Routine die erfolgreiche Deinstallation und empfiehlt einen Neustart des Systems, um auch die derzeit noch laufenden Prozesse des Virenscanners zu beenden.

Nach erfolgtem Neustart wird sich zumindest bei Windows XP mit Service Pack 2 das Sicherheitscenter melden, weil der Rechner ja nun nicht mehr durch eine Antivirensoftware geschützt ist. Dieser riskante Zustand soll schließlich auch durch die Installation von **Sophos Anti-Virus** wieder behoben werden.

Doch zuvor bietet es sich an, auch noch das Verzeichnis „*Norman*“ auf dem Standard-Laufwerk zu entfernen, um den so freigewordenen Platz für andere Daten nutzen zu können. Wenn diese Löschaktion nach dem Neustart vorgenommen wird, wird sie auch nicht durch noch laufende Prozesse behindert. Danach kann mit der Installation von **Sophos Anti-Virus** begonnen werden.

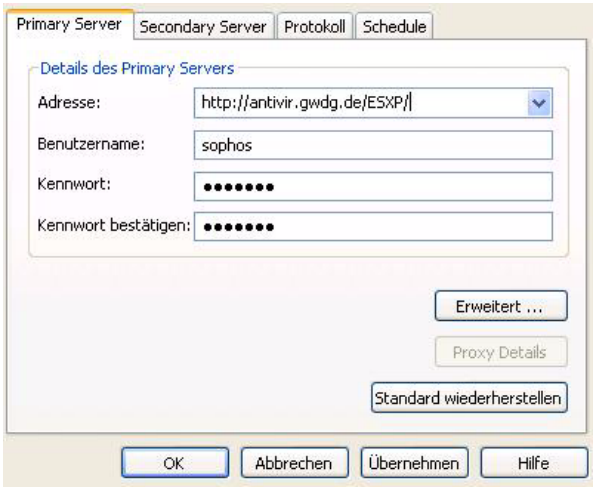
1.2 Installation von Sophos Anti-Virus

Die Installation der akuellen Version 6.0 von **Sophos Anti-Virus** für Windows 2000/XP/2003 erfolgt nun nicht mehr, wie noch bei älteren Versionen, über ein separates Update-Tool, sondern es wird - wie auch bei anderen Antivirensoftware-Produkten üblich - zuerst das Programm installiert und dann der dort integrierte Update-Mechanismus gestartet. Die Software kann von folgendem Ort heruntergeladen werden, an dem sich auch eine ausführliche Installationsanleitung befindet:

`http://antivir.gwdg.de/winxp.html`

Um die Installationsdatei herunterladen zu können, ist natürlich die bekannte Zugangskennung erforderlich, die im Bedarfsfall beim Helpdesk der GWDG (Tel.: 0551 201-1523) in Erfahrung gebracht werden kann. Nach dem Download dieser Datei erfolgt die Installation durch Doppelklick. Dabei werden die Dateien zuerst in ein temporäres Verzeichnis *c:\savxpsa* entpackt und von dort aus dann die eigentliche Installation gestartet. Über die obligatorische Einwilligung zum Lizenzvertrag gelangt man durch fortwährendes Klicken auf die „*Weiter*“-Schaltfläche zu der Dialogbox, in der die Frage nach den Zugangsdaten gestellt wird. Diese Frage kann hier zunächst übergangen und dann nach erfolgter Installation beantwortet werden. Dazu muss lediglich das in der Taskleiste erscheinende neue Sophos-Symbol mit der rechten Maustaste angeklickt und der Menüpunkt „**Updates konfigurieren...**“ ausgewählt werden.

In der nun erscheinenden Dialogbox sind die bekannten Zugangsdaten einzugeben:



Adresse: **http://antivir.gwdg.de/ESXP**

Benutzername: **sophos**

Kennwort: *kann bei der GWDG erfragt werden (ist gegenüber den älteren Sophos-Versionen unverändert geblieben)*

Sobald Installation und Konfiguration von **Sophos Anti-Virus** abgeschlossen ist, sollte umgehend die Aktualisierung angestoßen werden, damit der

Virenscanner auch über die aktuellen Signaturdateien verfügt. Dies geschieht wiederum durch Klick mit der rechten Maustaste auf das Sophos-Symbol in der Taskleiste und Auswahl des Menüpunktes „**Jetzt aktualisieren**“.

Nach Abschluss dieses Update-Vorgangs kann man sich über den Erfolg dieser Aktion vergewissern, indem man den Virenscanner selbst aufruft - wiederum über Klick mit der rechten Maustaste auf das Sophos-Symbol und Aktivierung des Menüpunkts „**Sophos Anti-Virus öffnen**“. Dort sollten sich dann in dem linken oberen Statusbereich das aktuelle Update-Datum, die entsprechende Produktversion und vor allem der aktivierte Hintergrundwächter (On-Access-Überprüfung) dokumentieren. Die Produktversion kann natürlich von Fall zu Fall varieren.

Damit sollte der Schutz des Rechners wieder gewährleistet sein. Weil sich aber gerade auch in letzter Zeit die Viren und Würmer sehr schnell verändern und verbreiten, kann selbst ein stets aktuell gehaltener Virenscanner nicht immer den optimalen Schutz gewährleisten. Das bedeutet aber für uns nur, dass wir uns auf diese Schutzprogramme nicht uneingeschränkt verlassen dürfen, sondern den Gefahren aus dem Internet stets mit einem gesunden Misstrauen begegnen sollten.

Reimann

---

2. Intrusion Detection und Prevention im GÖNET (Teil 2)

Im ersten Teil des zweiteiligen Artikels wurden Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) dargestellt sowie die Produktauswahl bei der Suche nach einer geeigneten Lösung zum Schutz des GÖNET vorgestellt (s. GWDG-Nachrichten 7/2006).

Der zweite Teil beschreibt nun das bei der GWDG produktiv eingesetzte IPS im Detail und verdeutlicht die Vorteile für die am GÖNET angeschlossenen Institute und Benutzer.

Die Wahl eines für das GÖNET geeigneten IPS fiel zugunsten der Firma Tippingpoint (3COM). Nicht nur die hohe erreichbare Bandbreite, sondern auch das einfache und überschaubare Management des Gesamtsystems waren ausschlaggebend für die Auswahl des Produktes.

2.1 Das IPS von Tippingpoint

Tippingpoint hat unterschiedliche Systeme im Produktportfolio, die sich in Bezug auf IPS im Wesentlichen in der Bandbreite und der Anzahl der Ports unterscheiden. Das für die GWDG geeignete Gerät ist das „Tippingpoint 2400 E“ (s. Abb. 1), welches sich seit Anfang Dezember 2005 bei der GWDG im produktiven Einsatz befindet.

Abb. 1:

Die IPS von Tippingpoint arbeiten vollständig transparent. Das Gerät wird in den Kommunikationsweg installiert, sodass die Kommunikationspartner das IPS im Netzwerk nicht wahrnehmen. Die Netzwerkpakete werden vom IPS unverändert an den jeweils anderen Port weitergeleitet, solange in dem Datenstrom keine Attacke enthalten ist. Das IPS 2400 arbeitet bidirektional, sodass die Richtung einer etwaigen Attacke für das System keine Rolle spielt. Angriffe werden damit in beide Richtungen erkannt und entsprechend unterdrückt.

Die Features des IPS 2400 E sind:

- Bandbreite: 2 GBit/s
- vier Gigabit-Doppelports
- Kombination aus Hardware & Software (Management)
- Failover-Betrieb (Hot Standby)
- diverse Eventkategorien (Minor bis Critical)

2.1.1 Aufbau der Tippingpoint-Lösung

Die IPS-Hardware

Das Tippingpoint besteht aus zwei Komponenten: Zunächst werden durch das eigentliche IPS-Gerät der Datenverkehr analysiert und bei Attacken bestimmte Ereignisse ausgelöst. Dieses System besitzt mehrere spezielle Netzwerkprozessoren, um die hohe Bandbreite bei der Analyse der Datenpakete zu gewährleisten. Das IPS 2400 E besitzt vier Gigabit-Doppelports, die vollständig transparent arbeiten.

Das Managementsystem SMS

Ein vom IPS abgesetzter Server beinhaltet eine spezielle Managementsoftware, über die das IPS kontrolliert wird. Es heißt „SMS“ (Security Management System) und besteht aus einem Dell-Server und einer für das Management angepassten Software, die eine Bedienung des Systems entweder über eine Webseite oder einen Client erlaubt. Überdies sammelt das SMS alle Ereignisse und speichert diese für weitere Auswertungen in einer internen SQL-Datenbank. Gleichzeitig werden vom SMS automatisch Alarme generiert, wenn bestimmte Ereignisse eintreten. Nicht zuletzt auch das Firmware-Management wird vom SMS übernommen sowie die täglichen Updates an Signaturen für bekannte Attacken.

So sind zwei wesentliche Komponenten auf die zwei Systeme verteilt: Dell-Server sowie IPS-Hardware. Das IPS selbst kann sich damit auf die zeitkritische Analyse der Pakete konzentrieren.

2.1.2 Attacken erkennen, aber wie?

Die Signaturen

Eine der Verfahren zur Erkennung von Angriffen ist der Vergleich der Datenpakete mit bekannten Signaturen. Der größte Teil der Attacken lässt sich über signaturbedingte Filter erkennen, wenngleich nicht alle. Eine große Anzahl an Personen analysieren täglich neue Angriffe und Eindringlingsversuche und generieren daraus Muster, auf deren Basis dann Filter für IPS erzeugt werden. Mit dem Kauf des Tippingpoint-Systems besteht zugleich auch ein Updatevertrag, auf dessen Basis fast täglich neue Signaturen automatisiert auf das System geladen werden, um bei neuen Angriffswellen diesen möglichst schnell begegnen zu können. Tippingpoint nennt diese Signaturupdates sehr treffend „Digital Vaccine“.

Die Gesamtzahl der Signaturen beläuft sich derzeit auf 2700 - 3000. Das IPS unterscheidet auch den Schweregrad der Attacke und aktiviert in dessen Abhängigkeit entsprechende Abwehrmaßnahmen.

Unterschieden werden folgende Einteilungen:

- Minor
- Major
- Critical

Abb. 2 zeigt ein Beispiel (Auszug aus den Signaturen des IPS):

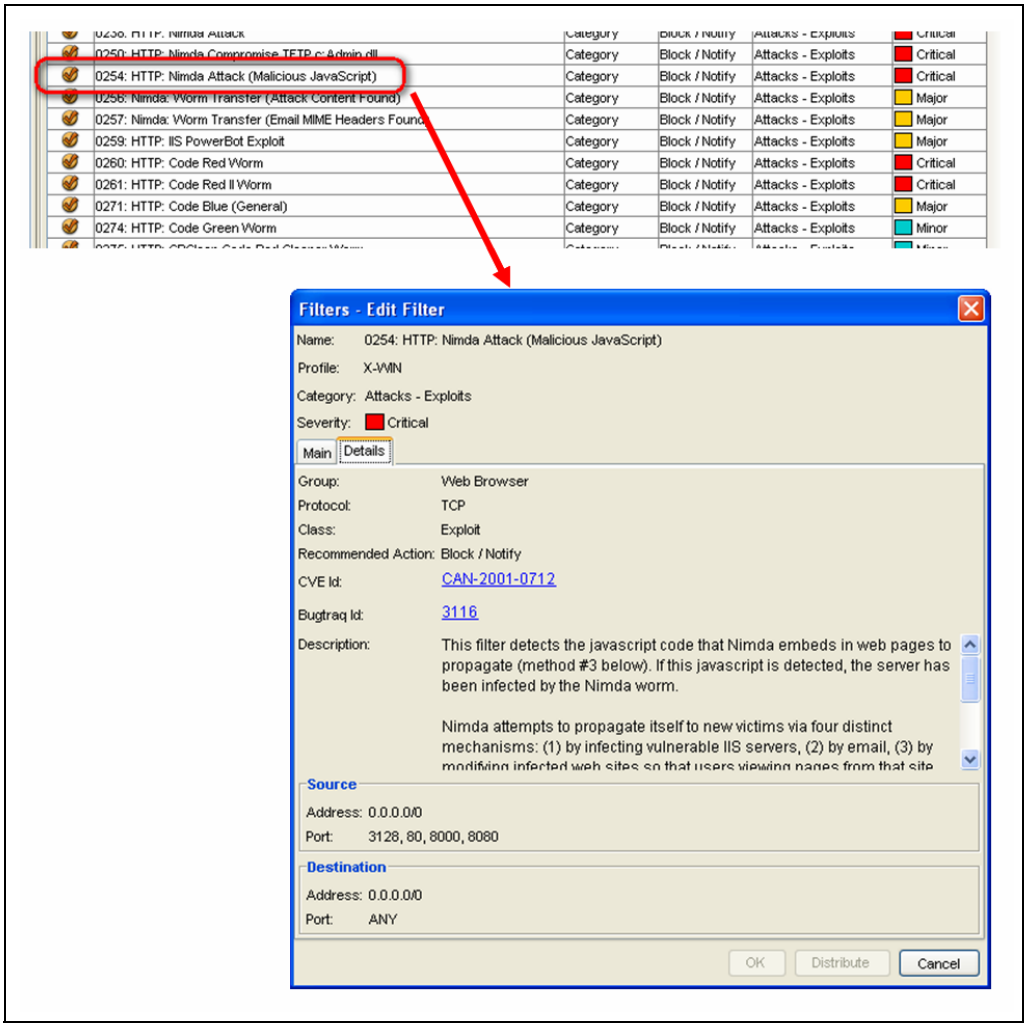


Abb. 2

Jede Signatur besitzt eine interne, eindeutige Tippingpoint-Nummer und basiert auf international eindeutigen Kennnummern für bekannte Attacken. Das IPS (bzw. SMS) gibt bei jeder Attack-Signatur Informationen über die Herkunft, die Schadensbilanz sowie die betroffenen Systeme aus.

Beispiel

Attacke ID=0254 (Tippingpoint-Nummer) unterliegt der internationalen CVE-ID: CAN-2001-0712 bzw. der Bugtraq-ID: 3116. CVE ist eine standardisierte Beschreibung über bekannte Sicherheitslücken (**C**ommon **V**ulnerabilities and **E**xposures; vgl. **`http://www.cve.mitre.org`**).

Bugtraq ist vergleichbar mit CVE und stellt eine weitere große Datenbank für Sicherheitslücken dar (vgl. **`http://www.securityfocus.com`**).

Die detailreichen Informationen aus den verschiedenen Datenbanken helfen dem Netzwerkadministrator, die Attacke und deren Wirkung zu verstehen. Das ist allerdings für den Betrieb des IPS keine Pflicht, da das System vollständig autonom arbeitet und auch ohne Verständnis des Administrators seinen „Dienst“ versieht.

Aktionen bei Attacken

Die Reaktion auf eine als positiv erkannte Attacke kann vom Administrator für jede Signatur selbst definiert werden. Allerdings ist es sinnvoll, die Standardeinstellungen von Tippingpoint so zu belassen (use category settings). Zweckmäßig wird es, wenn gefährdete Systeme trotz bekannter Sicherheitslükken unbedingt in Betrieb und erreichbar bleiben

müssen. Hier würde man z. B. die Aktion von „Block“ auf „Notify“ umstellen.

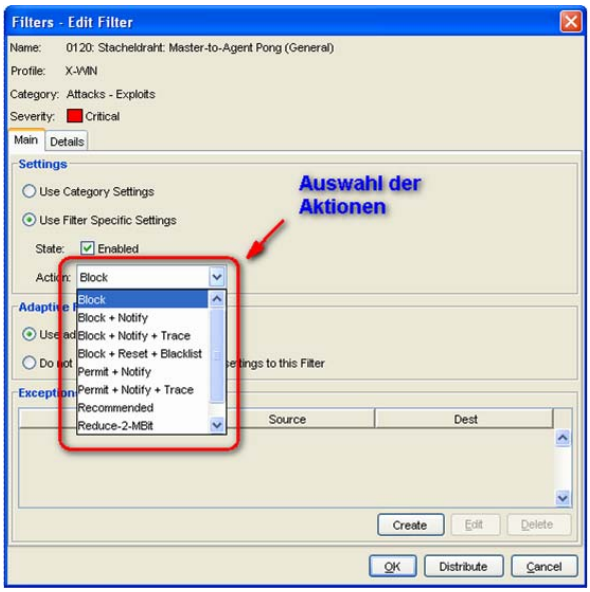


Abb. 3

Überdies kann auch für jeden Filter der Bereich der zu überwachenden IP-Adressen oder -Bereiche als Quelle und/oder Ziel definiert werden. Aber auch hier sollten die Standardeinstellungen genutzt werden.

Arten von Attacken und deren Erkennung im IPS

Viele Attacken benötigen keine Reaktion des vermeintlich betroffenen Systems. Das sind die sog. „SinglePacketAttacks“. Prominentes Beispiel hierfür ist der immer noch sehr verbreitete MS-SQL-Slammer. Hier genügt ein einziges UDP-Paket (Port 1456) auf das Zielsystem. Aufgrund dieser Besonderheit dieser SinglePacketAttacks werden natürlich beliebig viele Zielsysteme schlicht „beschossen“, ohne dass die betroffenen Systeme wirklich verwundbar sind. Diese Art Angriffe gehen wie das „Hornberger Schießen“ aus. Der MS-SQL-Slammer ist auch bei der GWDG die am meisten durch das IPS erkannte und blockierte Attacke und wird aufgrund der Häufigkeit aus unseren Statistiken meist herausgefiltert, da die Anzahl dieser Attacke die anderen Attacken deutlich übersteigt.

Komplexer wird es, wenn auch Antwortpakete des Zielsystems berücksichtigt werden müssen. Deshalb hält das IPS von Tippingpoint bei einer vermeintlichen Attacke mehrere Netzwerkpakete in einem eigenen Speicher, bis der vollständige „Angriffscode“ im IPS vorliegt. Anschließend wird das IPS die Verbindung i. d. R. blockieren. Stellen sich die gesammelten Pakete als „negativ“ heraus, werden diese natürlich an das Ziel weitergeleitet. Dieser Vorgang geschieht natürlich im Bereich von 10^{-6} sec. bis 10^{-3} sec. Das Verfahren ist deshalb wichtig, da sonst ohne eigene „Queue“ bereits Pakete mit schadhaften Code zum Ziel übertragen werden und bei einer Erkennung durch das IPS die meisten Pakete möglicherweise ihr Ziel bereits erreicht haben.

Keine Virenerkennung und dennoch eine Virenabwehr?

Die signaturbasierte Erkennung von Attacken ist nicht zu verwechseln mit der Erkennung von Viren und Trojanern. Wenngleich auch hier Signaturen verwendet werden, bleibt die Erkennung von Viren die zentrale Aufgabe von Virenscannern. Dennoch hat das Tippingpoint IPS die Möglichkeit, die Verbreitung von Viren und Trojanern an einer wesentlichen Stelle zu unterbinden: nämlich im Netzwerk selbst. Nahezu alle Viren müssen sich über bekannte Wege verbreiten (meist via E-Mail oder direkte Netzwerbindungen). Da das IPS die Verfahren für die Ausbreitung vieler Viren als Signaturen kennt, kann bei bereits aktiven Viren die Ausbreitung im Netzwerk durch das IPS erfolgreich verhindert werden. Die derzeitigen Statistiken bei der GWDG auf dem IPS sind sehr ermutigend. Hier erkennen wir an der versuchten Ausbreitung sehr gut, ob bereits im GÖNET betriebene Rechner von Viren oder Trojanern befallen sind.

Erkennen abnormalen Verhaltens

Ein weiteres Verfahren zur Erkennung von Attacken und Angriffen sind die verhaltensbasierten Mechanismen. Hier wird „normales“ von „abnormalem“ Netzwerkverhalten unterschieden. Das IPS hat Ansätze zur Erkennung ungewöhnlicher Aktivitäten im Netz.

Quarantäne

Das IPS bietet die Möglichkeit, durch eine „Quarantäne“-Funktion bestimmte Ereignisse bei Auftreten bestimmter Verhaltensmuster einzuleiten. Wenn z. B. von einer Quell-IP-Adresse mehrfach innerhalb eines definierten Zeitraumes ein Port-Scan ausgeht, kann die Kommunikation der Quell-IP-Adresse mit dem zu schützenden Netz für einen bestimmten Zeitraum „verboten“ werden. Die Quell-IP-Adresse wird so gesehen in „Quarantäne“ geschickt.

Die Auswahl der Ereignisse ist bei Tippingpoint sehr vielfältig und reicht vom

- Blockieren der IP-Adresse auf Zeit,
- Informieren der Administratoren über den Vorfall via E-Mail oder SMS,
- Abschalten von Ethernet-Ports, über die der Angreifer verbunden ist,
- Generieren von Syslog-Einträgen und
- Abschicken von SNMP-Traps

bis hin zur Kombination aus mehreren Ereignissen.

Abb. 4 zeigt einen Auszug aus dem SMS für den Bereich der Quarantäne (Beispiel: Erkennung von NMAP Scans):

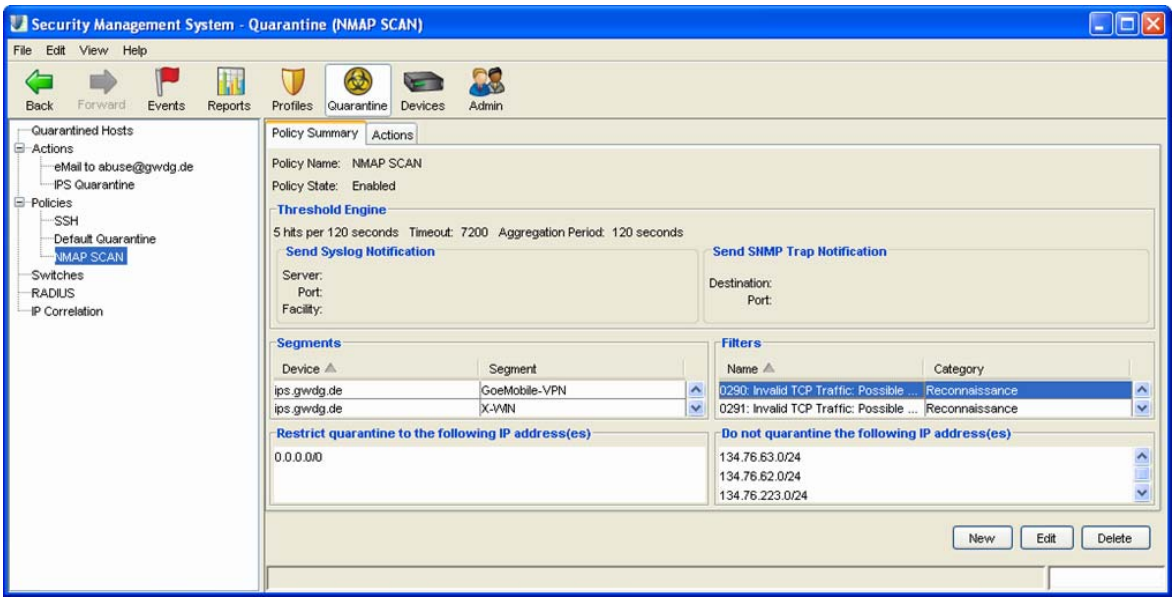


Abb. 4

2.1.3 Kategorien der Attacken

Im Tippingpoint-IPS wird die „bösartige“ Welt in drei unterschiedliche Kategorien unterteilt, die wiederum jeweils eigene Filter und Untergruppen besitzen (s. Abb. 5):

1. Application Protection
2. Infrastructure Protection
3. Performance Protection

Der Bereich „Performance Protection: Misuse and Abuse“ umfasst im Wesentlichen die Tauschbörsen.

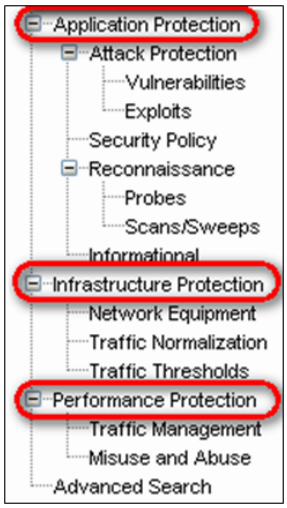


Abb. 5

Unter „Traffic Management“ können Ausnahmen derart definiert werden, dass Quell-IP-Adressen oder -Netze mit Ziel-IP-Adressen/Netze eingerichtet werden (s. Abb. 6), die den gesamten Filtermechanismus des IPS entweder

- umgehen (Trust),
- den Traffic erlauben oder
- oder auf eine definierte Bandbreite begrenzen.

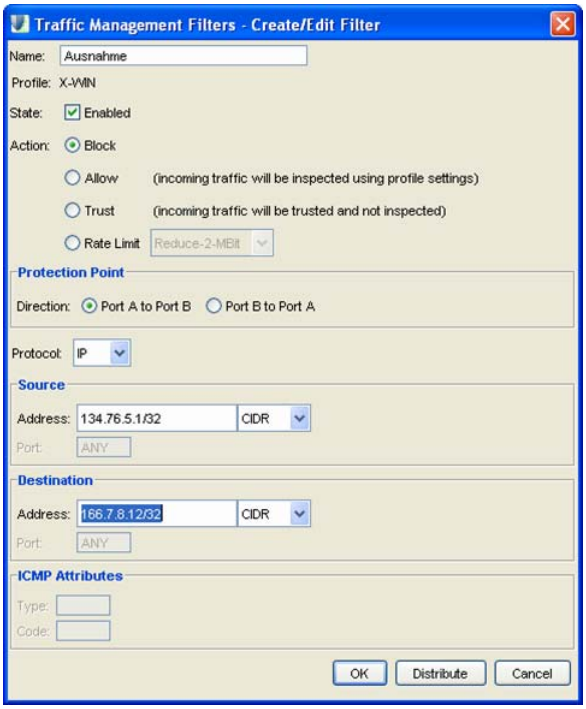


Abb. 6

Diese Einstellungen sind sinnvoll, wenn Netzwerkverkehr trotz verdächtiger Pakete erlaubt werden oder die Bandbreite für bestimmte Systeme begrenzt werden soll.

Im produktiven Betrieb bei der GWDG haben wir Ausnahmen auf dem IPS für unsere FTP-Server eingerichtet, da diese nicht überwacht werden müssen und überdies außerordentlich viel Traffic erzeugen, was lediglich zu einer unnötigen Belastung des IPS führen würde.

Weitere Ausnahmen wurden für spezielle Videokonferenzsysteme innerhalb der Universität Göttingen definiert, welche sehr zeitkritisch sind und dadurch jegliche Verzögerungen im Netzwerk die Bildqualität beeinflussen könnte.

2.2 Die Testphase bei der GWDG

Im September 2005 hatte die GWDG das IPS Tippingpoint 2004 E unter realen Bedingungen in ihrem Netzwerk im Testbetrieb. Das System wurde zunächst am Ausgang des Funk-LANs „GoeMobile“ angebunden sowie am Ausgang der Studierendenwohnheime, da hier die höchste Anzahl von möglichen Attacken zu erwarten war. Später wurde das System direkt in den Kommunikationsweg zum Internet mit einer Gesamtbandbreite von 1 GBit/s angebunden.

Ein Schutz der Anbindung zum Internet stellt nicht zuletzt aufgrund der hohen Bandbreite die größte Herausforderung für ein IPS dar. An diesem Übergang zum DFN-Netz bzw. Internet müssen alle Pakete das IPS passieren. Prinzipiell ist dieses auch der ideale Standort für eine zentrale Eindringlingserkennung.

Die folgende Abb. 7 verdeutlicht den Einsatz im Testbetrieb bei der GWDG Ende 2005:

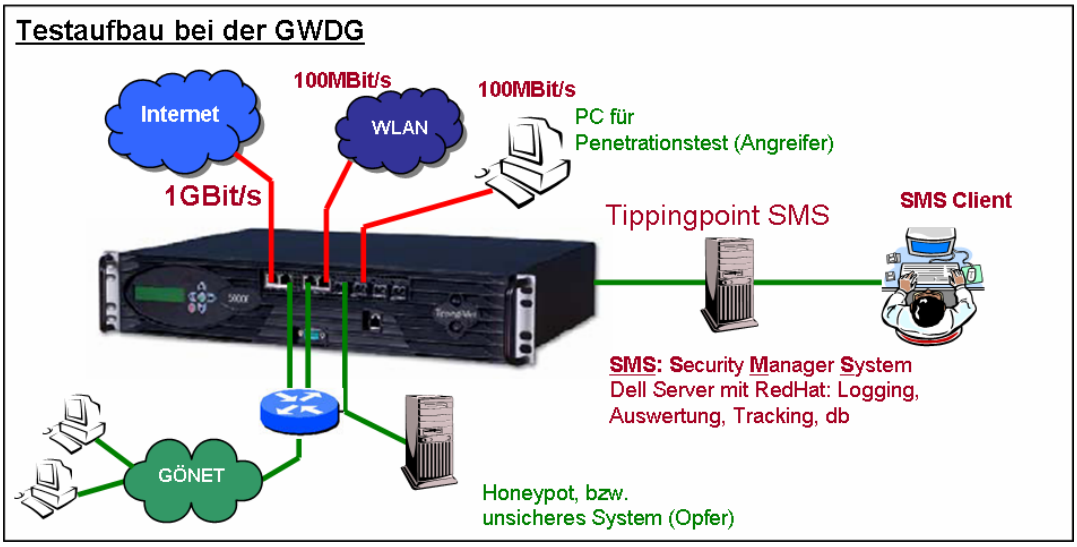


Abb. 7

Am ersten Gigabit-Doppelport wurde das Internet angebunden. Der zweite Doppelport schützt das gesamte Funk-LAN „GoeMobile.“ Am dritten Doppelport wurden für einen Penetrationstest spezielle Systeme angeschlossen. In nahezu unveränderter Konfiguration ist das System derzeit bei der GWDG in Betrieb.

2.2.1 Test im „GWDG-Lab“ (Penetrationstests)

Das IPS wurde im ersten Schritt einer Reihe von Penetrationstests bei der GWDG unterzogen. Hierbei wurden zwei unterschiedlichen Testszenarien aufgebaut:

1.) Bandbreitentest

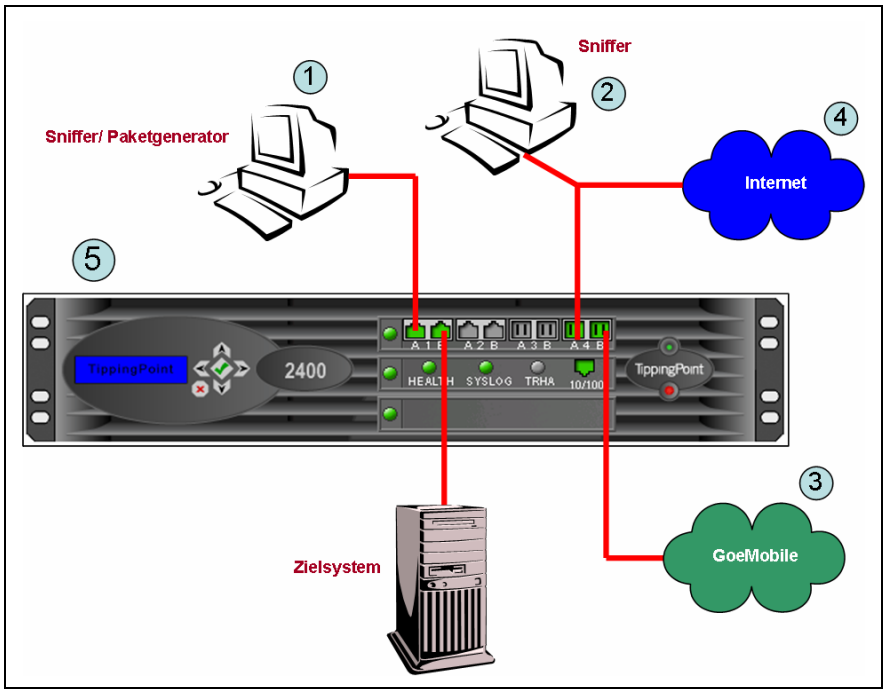


Abb. 8

Mithilfe eines Netzwerksniffers (1), der auch in der Lage ist, eine definierte Netzwerklast zu erzeugen, wurden Pakete bis zu einer Bandbreite von 1 GBit/s generiert. Hierbei wurden UDP- sowie TCP-Pakete beliebiger Auswahl erzeugt. Aber auch UDP-Pakete mit kompromittierendem Inhalt wurden mit Hilfe des Paketgenerators durch das IPS (5) geschickt. Entscheidend für uns war die Reaktion des IPS auf die Netzwerklast in Abhängigkeit der Paketgröße, Anzahl der Pakete pro Sekunde sowie Inhalt und IP-Protokoll. Gleichzeitig wurde auf einem anderen Port-Paar des IPS „normaler“ Netzwerkverkehr durch das IPS geleitet (3) & (4), welcher mit einem weiteren Sniffer (2) am Ausgang des IPS analysiert wurde.

Das Ergebnis war sehr ermutigend. Selbst in der Grenzsituation bei 1 GBit/s an dem Test-Port waren keine Beeinträchtigungen in der Erkennungsleistung auf den anderen Ports des IPS wahrzunehmen. Die Prozessorleistung des IPS stieg erwartungsgemäß an, erreichte aber maximal 65 %. Mit einem weiteren Sniffer am Ausgang des zweiten Port-Paares wurde der „normale“ Traffic beobachtet, während am ersten Port-Paar der Traffic-Generator die künstliche Last erzeugte. Der Netzwerkverkehr wurde auf Paketverluste und Latenzen untersucht. Dabei wurden keine Paketverluste festgestellt. Die Latenzen stiegen nur in sehr geringem Maße an und lagen im Bereich von 1 bis $2 * 10^{-6}$ sec.

2.) Penetrationstest: Attacken und illegaler Traffic

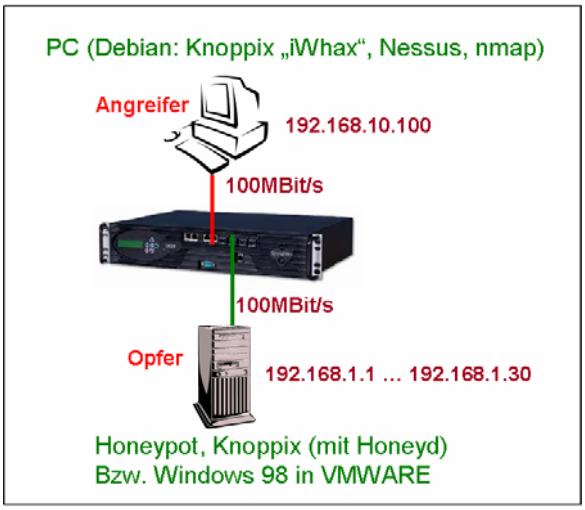


Abb. 9

In einem zweiten Test stand weniger die Bandbreite als vielmehr die Qualität der Erkennung von Attacken durch das IPS im Vordergrund.

Das angreifende System bestand aus einem Linux-System (Debian). Als Portscanner wurde zunächst NMAP verwendet. Weitere Angriffe wurden mit einem von CD bootfähigem Debian-Linux initiiert. Dahinter steht eine speziell für Angriffe produzierte Linux-Version mit dem Namen „iWhax“ bzw. Whoppix. Die CD enthält eine reichhaltige Sammlung von Exploits und weiteren Angriffsprogrammen. Mithilfe dieser CD wurden diverse Attacken auf bekannte

Sicherheitslücken gefahren, um die Erkennungsleistung des IPS überprüfen zu können.

Das Ergebnis war sehr zufrieden stellend. Die folgende Abb. 10 zeigt als Ergebnis die Angriffe (linke Spalte) sowie die Erkennung durch das IPS. Teilweise wurde sogar das Programm, mit dem die Angriffe gestartet wurden, korrekt erkannt (z. B. Nikto WebScan).

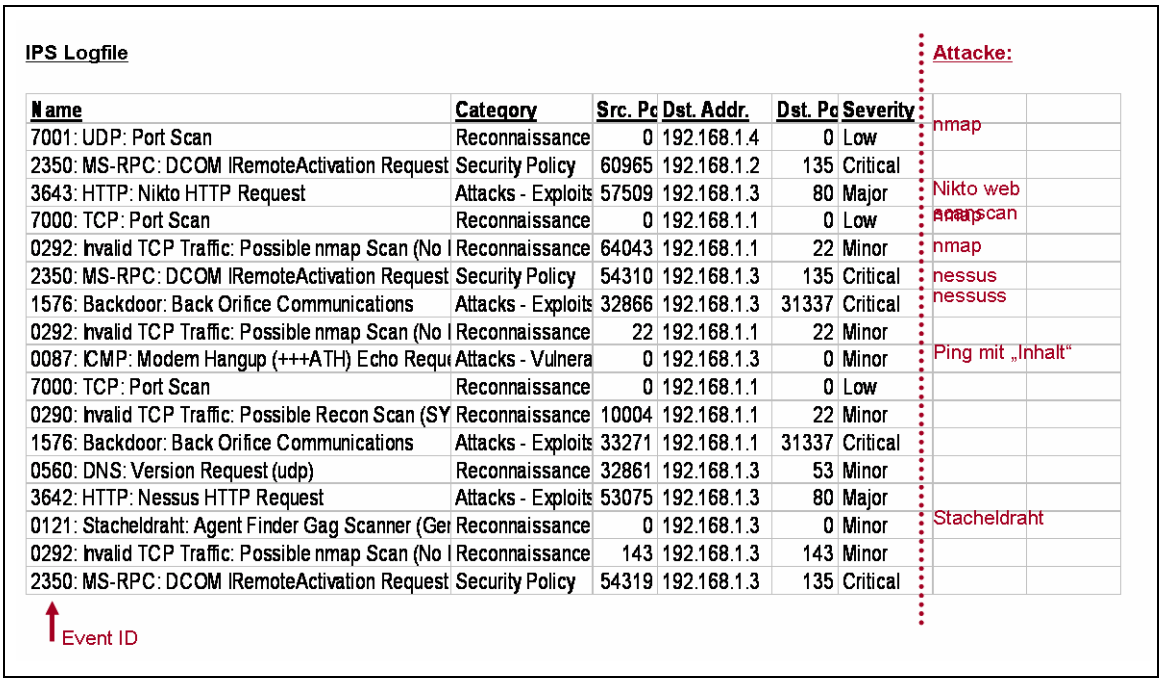


Abb. 10

Honeypot als Opfer-System

Ein Honeypot-System war bei vielen Attacken unser Zielsystem (Opfer). Honeypots simulieren das Verhalten diverser Dienste (Webserver, Mailserver, Telnet-Daemons etc.), ohne jedoch wirklich deren Sicherheitslücken zu besitzen. Überdies werden auch Betriebssysteme simuliert bis hin zu ganzen Netzen von Servern. Ein Honeypot wurde deshalb als Ziel ausgewählt, da es selbst ein Logfile über die Angriffe führt, welches für die Auswertung im Rahmen eines Tests besonders geeignet ist.

Unsicheres Betriebssystem als Opfersystem

Dennoch ist ein Honeypot für einen Angriff auf bekannte Sicherheitslücken nur beschränkt sinnvoll, da es nicht exakt das Verhalten der Sicherheitslücke „simuliert“. Teilweise müssen mehrere Pakete sowie Antwortpakete im Netzwerk ausgetauscht werden, damit eine Attacke stattfindet und überhaupt erst erkannt werden kann. Aus diesem Grund wurde als Zielsystem ein Windows-98-Rechner (ohne Security-Patches) installiert. Hier konnten wir diverse Angriffe starten, die nahezu vollständig vom IPS erkannt und verhindert wurden. Das spiegelt auch eher die Realität in lokalen Netzen wieder.

2.2.2 Fazit des Testbetriebs im „GWDG-Lab“

Das Ergebnis der verschiedenen Tests mit dem IPS von Tippingpoint war sehr positiv. Die vom Hersteller offerierte Bandbreite konnten wir im Test nachweisen. Wenngleich wir nicht alle Filter des IPS ausprobieren konnten, hatten wir viele Stichproben erfolgreich durchführen können.

2.2.3 Nicht erkannte Attacke(n)

Einzig die von uns initiierte Attacke via SSH konnte nicht korrekt erkannt werden. Wir hatten versucht, mit diversen Benutzernamen auf ein Zielsystem eine SSH-Sitzung aufzubauen (SSH User Scan). Uns war allerdings schon vor dem Test klar, dass eine Erkennung und Identifizierung von multiplen SSH-Verbindungen als Attacke für das IPS ein „Vabanque-Spiel“ sein muss. Wie unterscheidet man mehrere SSH-Sitzungen auf eine IP-Adresse als Ziel von einer legalen Nutzung eines zentralen SSH-Servers?

Das ist eine Frage, die unser IPS auch nicht wirklich beantworten konnte und folglich die SSH-Sitzungen zum Ziel weiterleitete.

Dennoch hat die nicht korrekt erkannte SSH-Attacke das Gesamtbild kaum trüben können. Das IPS stellte sich mit dem im Test gemessenen Leistungen für den Einsatz im GÖNET als ein sehr geeignetes System heraus. Der produktive Betrieb im GÖNET bestätigte in der Folgezeit unsere Erfahrungen im Test.

2.3 Erfolgreicher Schutz bei Ausbreitungswellen von Viren

Besonders eindrucksvoll waren für uns die erfolgreiche Abwehr der Ausbreitungswellen von Trojanern und Viren in der Praxis.

Hierzu zwei Beispiele.:

Beispiel 1:

Am 28.12.2005 wurde eine Sicherheitslücke „WMF-Lücke“ bekannt:

```
http://www.f-secure.com/weblog/
  archives/archive-122005.html#00000752
```

Am gleichen Tag gegen Abend wurde automatisch ein entsprechender Filter von Tippingpoint im Rahmen der Signatur-Updates auf unser IPS geladen. Am folgenden Tag (29.12.2005) wurde vor der Sicherheitslücke im Internet gewarnt. Die Aufregung im Internet hinsichtlich dieser Lücke konnten wir zunächst gar nicht teilen und fanden auch keine Hinweise auf WMF-Attacken innerhalb des GÖNET. Bis uns dann am 29.12.2005 auffiel, dass bereits seit mehr als 24 Stunden das IPS der GWDG sämtliche WMF-Attacken aus dem Internet erfolgreich herausgefiltert hatte und wir deshalb de facto immun gegen diese Attacke waren. In den weiteren Tagen gab es sehr wenige WMF-Attacken von innen durch „eingeschleppte“ Viren. Dessen Ausbreitung von innen nach außen wurde aber wiederum durch das IPS verhindert. So sind unsere Benutzer hinsichtlich der WMF-Attacken von der Ausbreitungswelle weitgehend verschont geblieben.

Die folgende Abb. 11 zeigt den Anstieg der vom IPS blockierten WMF-Attacken Ende Dezember 2005:

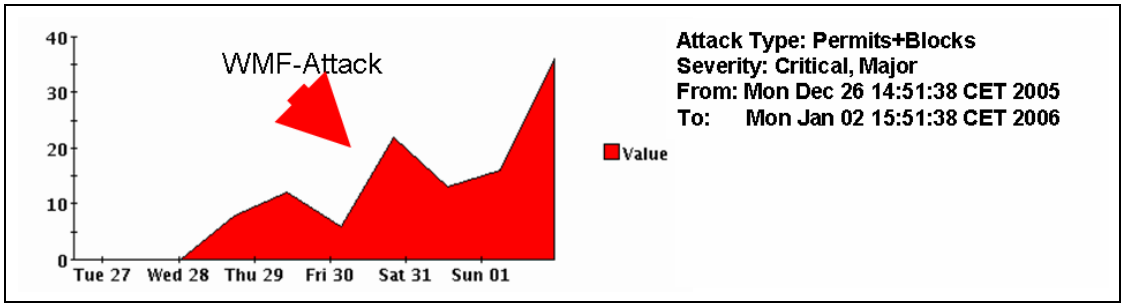


Abb. 11

Beispiel 2:

Am 23.01.2006 wurde vor der „NYXEM.e-Wurm-Ausbreitungswelle“ gewarnt. Am 01.02.2006 hatten wir festgestellt, dass unser IPS bereits einen entsprechenden Filter gegen die Ausbreitung des „NYXEM.e“ geladen hatte. Wir schauten uns die Statistiken an und stellten fest, dass in der Tat alle Mailserver innerhalb des GÖNET das Ziel für die Ausbreitungswelle waren und die Ausbreitung selbst durch das IPS erfolgreich verhindert werden konnte. Da sich „NYXEM.e“ via E-Mail verbreitet, war verständlich, dass ausgerechnet die Mailserver ein primäres Ziel für die Verbreitung darstellten.

Die folgende Tabelle zeigt einen Auszug aus dem Eventlog des IPS bereits wenige Sekunden, nachdem der Filter „aktiv“ wurde:

Filter Name	Filter Number	Source IP	Destination IP	Hits	Severity
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	134.76.10.26	24	Critical
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	193.175.80.133	11	Critical
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	134.76.21.104	10	Critical

Abb. 12 zeigt den Anstieg der vom IPS blockierten NYXEM.e-Attacken unmmittelbar nach dem Laden des Filters:

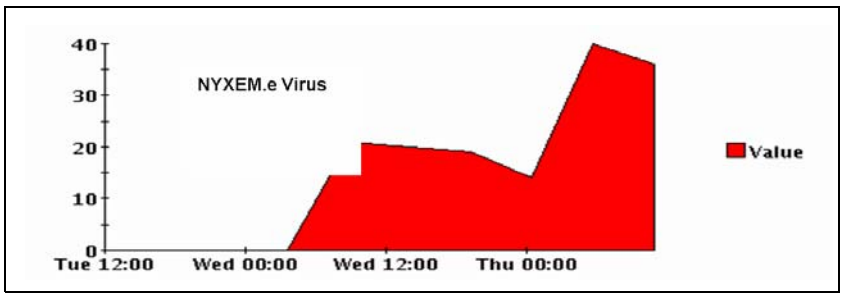


Abb. 12

False Positive Detection

Natürlich ist ein IPS nicht fehlerfrei. Das betrifft auch das Tippingpoint-IPS. Dennoch haben wir im Laborbetrieb sowie auch im produktiven Einsatz lediglich eine einzige nachweisbare False-Positive-Erkennung gehabt. Bei wöchentlich etwa 8 - 9 Millionen Attacken im GÖNET ist das eine sehr akzeptable Leistung.

2.4 Betrieb im GÖNET

2.4.1 Auswertungen und Logfiles

Wenngleich das im GÖNET installierte IPS vollständig autonom agiert, ist ein gelegentlicher Blick auf die „Gefährdungslage“ des GÖNET sehr sinnvoll. Das IPS bietet eine große Anzahl an Möglichkeiten, verschiedene Statistiken zu generieren. Da der zum Tippingpoint-System gehörende SMS eine lokale SQL-Datenbank besitzt, in der alle Ereignisse festgehalten werden, können auch im Nachhinein Statistiken über Angriffe und Gefährdungen erzeugt werden.

Über einen Report-Mechanismus können

- Quell-IP-Adressen,
- Ziel-IP-Adressen,
- Zeiten,
- Attacken und
- der Schweregrad der Attacke

für eine Statistik gefiltert und kombiniert werden.

Die folgende Abb. 13 zeigt den ReportManager des Tippingpoint-SMS:

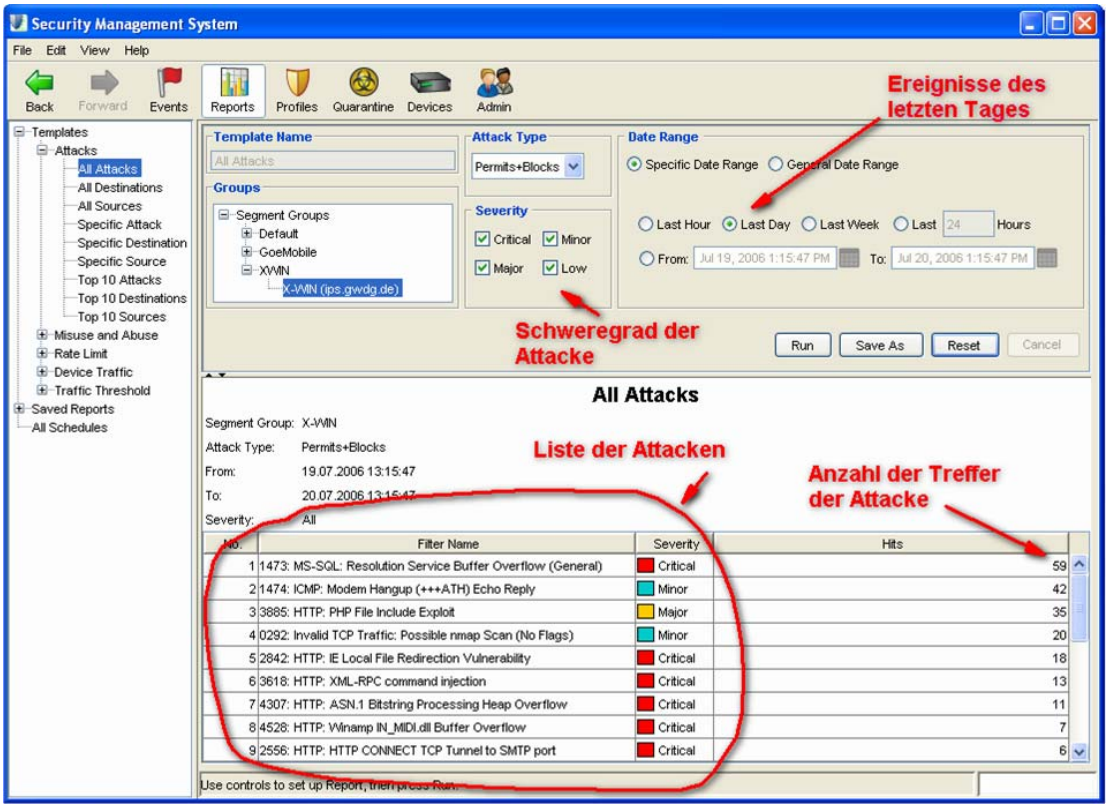


Abb. 13

Überdies sind auch die „TopTen-Angriffe“ über den Report-Mechanismus des SMS verfügbar.

Abb. 14 zeigt als Beispiel die „TopTen“ vom 09.07.2006:

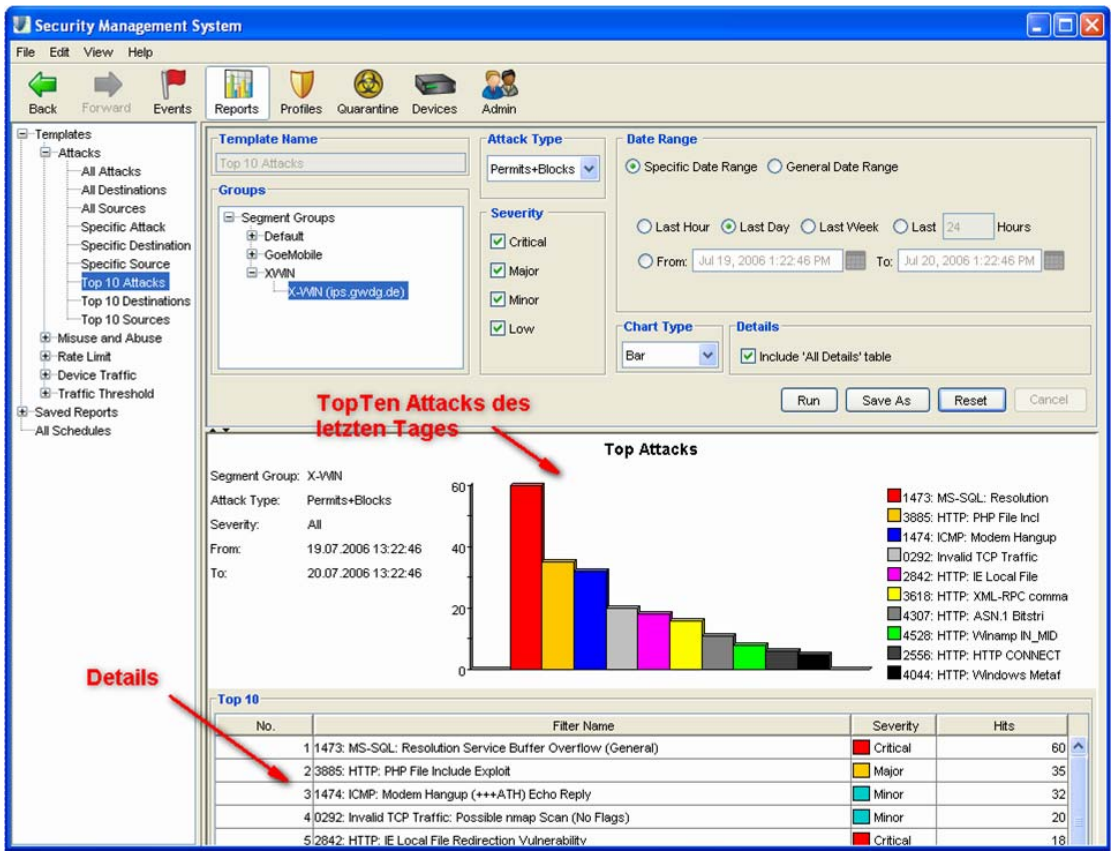


Abb. 14

Das SMS erlaubt auch die zeitgesteuerte Generierung von Statistiken in beliebigen Formaten. Diese können dann entweder per E-Mail verschickt, auf Fileserver kopiert oder via FTP übertragen werden.

Als Formate sind „CSV“, Excel, XML, Bitmap-Bilder oder PDF möglich. Gerade diese Kombinationen lassen kaum noch Wünsche offen.

2.4.2 Bandbreitenbegrenzung

Neben der Erkennung von Angriffen kann das IPS auch die Bandbreite reduzieren. Gerade im Bereich des „Misuse“ setzen wir diesen Mechanismus erfolgreich ein.

Tauschbörsen

Das IPS erkennt nahezu alle am Markt existierenden Tauschbörsen (derzeit etwa 200 Tauschbörsen). Hierbei werden die Tauschbörsen aber nicht einfach an den bekannten UDP- oder TCP-Ports identifiziert, sondern vielmehr auf hohe Protokollebenen (Layer 7) erkannt. Auch Tauschbörsen, die sich über „well known ports“ wie z. B. Port 80 durchtunneln, werden erfolgreich identifiziert. Der Tauschbörsenverkehr wird bei der GWDG durch das IPS bewusst nicht blockiert, sondern für alle Tauschbörsen zusammengenommen auf einen Wert von 20 MBit/s limitiert. Auch für das GoeMobile werden Tauschbörsen in der Summe auf einen Wert von 2 MBit/s begrenzt. Tauschbörsen sind also möglich, stören aber aufgrund der Limitierung nicht den anderen Traffic des GÖNET.

Die folgende Abb. 15 zeigt den gesamten Datenverkehr mehrerer Tage, der zum Internet durch das IPS läuft, sowie (rot) alle im GÖNET existierenden Tauschbörsen in der Summe. Hier erkennt man auch deutlich die Bandbreitenlimitierung durch das IPS. Am Tag wird die Grenze von 20 MBit/s erreicht, in der Nacht gehen die Werte deutlich herunter, sodass die Limitierung nicht greifen muss.

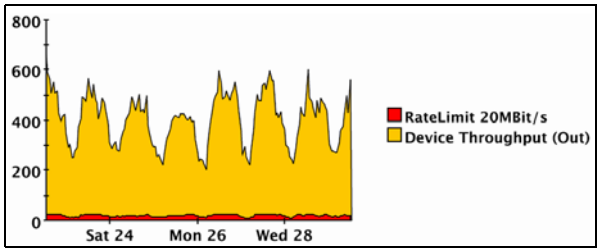


Abb. 15

Ähnlich sieht das Bild auch im GoeMobile aus, allerdings aufgrund der geringeren Bandbreite der Inter-

faces dann mit entsprechend geringerer Grenze (2 MBit/s).

Durch Bandbreitenbegrenzung für bestimmte Dienste kann das IPS sicherstellen, dass andere wichtige Anwendungen nicht durch Fehlnutzung in deren Funktion beeinträchtigt werden.

2.4.3 Überwachung des IPS

Das IPS selbst besitzt eine ganze Reihe von Überwachungsmechanismen, um die korrekte Funktion zu gewährleisten. Werden z. B. mehr als 1 % aller Pakete vom IPS aufgrund von ungeklärten Problemen nicht übertragen, schaltet das IPS selbständig in einen sog. Layer-2-Fallback zurück. Das bedeutet, dass die Erkennung des IPS in diesem extrem seltenen und kritischen Fall ausgesetzt wird und die Anschlüsse des IPS einfach durchgeschaltet werden.

Überschreitet die CPU-Belastung des IPS bei der sehr rechenintesiven Analyse der Pakete eine gewisse Schwelle, so werden zunächst alle Logging-Mechanismen ausgesetzt, um die CPU zu entlasten. Dieses Ereignis ist bei uns in dem neunmonatigen Betrieb bislang dreimal aufgetreten. Das System hatte dann selbstständig das Logging nach wenigen Minuten wieder aktiviert, sobald die Belastung für das System gesunken war. Ursache dafür waren neben dem ohnehin hohen Traffic-Aufkommen des gesamten GÖNET auch die Belastung durch die FTP-Server der GWDG. Immer dann, wenn neue Linux-Distributionen herauskamen, wurde der FTP-Server der GWDG außerordentlich start frequentiert. Wir haben in der Folge die FTP-Server der GWDG im IPS aus der Überwachung herausgenommen.

Monitoring

Ein bei der GWDG eingesetztes Monitoringsystem (CACTI) überwacht, neben vielen anderen Netzkomponenten, auch die Aktivitäten des IPS.

Es ist für jeden Benutzer unter

`http://monitor.gwdg.de`

erreichbar (Bereich: Intrusion Prevention System).

Abb. 16 stellt die CPU-Belastung des GWDG-IPS über eine Woche dar:

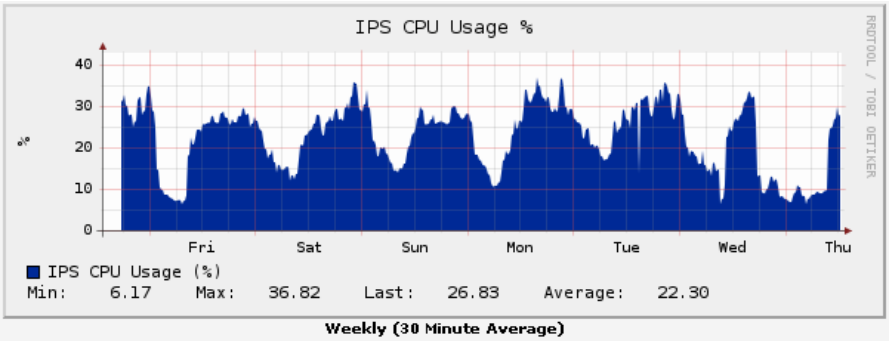


Abb. 16

Dort wird u. a. auch die CPU-Belastung via SNMP aufgezeichnet. Aber auch die Netzwerklast an den Interfaces sowie die „TopTen-Attacken“ werden im CACTI dargestellt.

2.4.4 Angriffe und Statistiken im GÖNET

Die Angriffe vom Internet in das GÖNET sind vielfältig. Die folgenden Bilder illustrieren den typischen Alltag eines IPS bei der Abwehr von Attacken im GÖNET.

Abb. 17 zeigt die „TopTen-Angriffe“ eines Tages sortiert nach Quell-IP-Adressen:

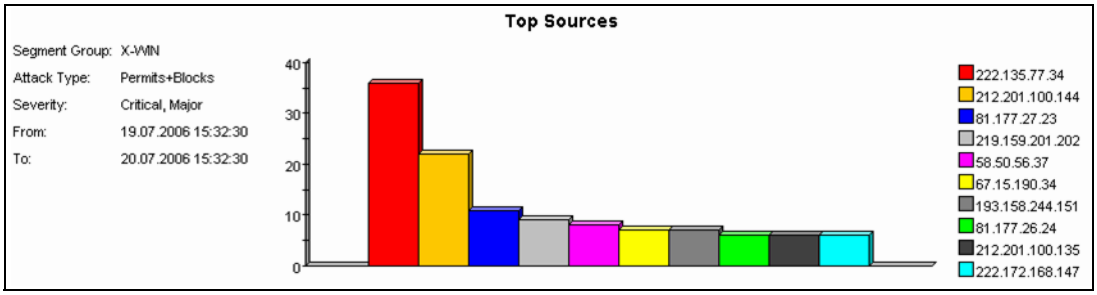


Abb. 17

Abb. 18 stellt die „TopTen-Attacken“ des gleichen Tages sortiert nach Art der Attacke sowie Häufigkeit dar:

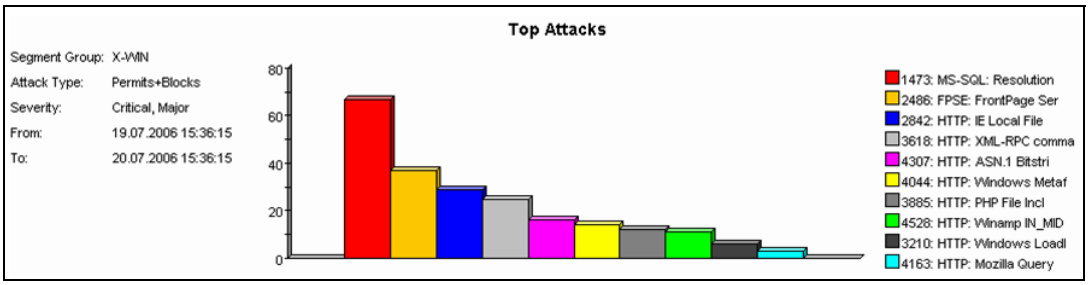


Abb. 18

Abb. 19 verdeutlicht die Anzahl der Angriffe in einer (typischen) Woche:

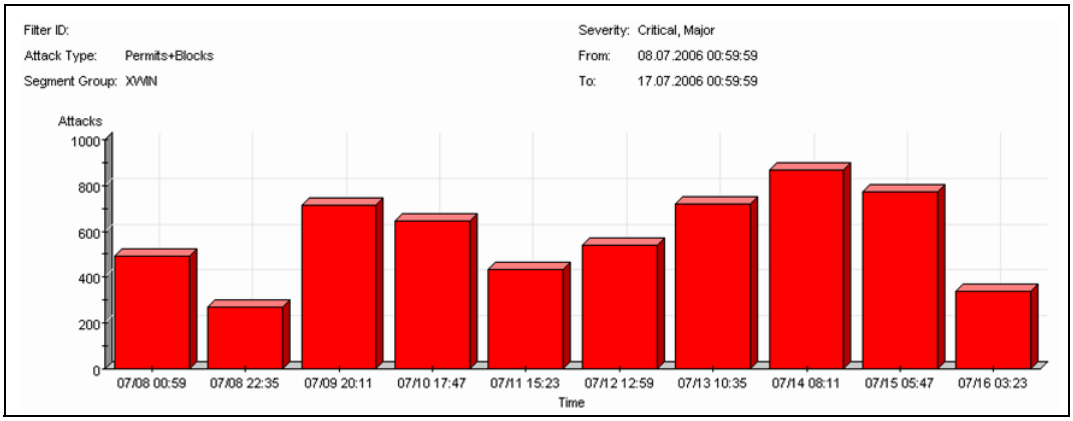


Abb. 19

Täglich werden etwa 1000 - 2000 Angriffe in das GÖNET blockiert. In der Statistik wird dabei nicht der MS-SQL-Slammer berücksichtigt, da er in der Summe alle anderen Attacken überdecken würde.

Die folgende Tabelle zeigt die Attacken eines Tages sortiert nach der Art der Attacke:

No.	Filter Name	Severity	Hits
1	3885: HTTP: PHP File Include Exploit	Major	2.326
2	4307: HTTP: ASN.1 Bitstring Processing Heap Overflow	Critical	421
3	1473: MS-SQL: Resolution Service Buffer Overflow (General)	Critical	340
4	2842: HTTP: IE Local File Redirection Vulnerability	Critical	299
5	2486: FPSE: FrontPage Server Extensions Chunked Transfer Overflow	Critical	290
6	2289: MS-RPC: DCOM ISystemActivator Overflow	Critical	207
7	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port	Critical	193
8	4193: SMB: ASN.1 Bitstring Processing Heap Overflow	Critical	180
9	1279: HTTP: Shell Command Execution (winnt/system32/cmd.exe)	Critical	158
10	4044: HTTP: Windows Metafile (WMF) Vulnerable Function	Critical	137
11	0238: HTTP: Nimda Attack	Critical	115
12	3979: HTTP: Illegal ActiveX Object Instantiation	Critical	104
13	4163: HTTP: Mozilla QueryInterface() Heap Buffer Overflow	Critical	65
14	3642: HTTP: Nessus HTTP Request	Major	61
15	0495: HTTP: Shell Command Execution (cmd.exe)	Major	60
16	3273: HTTP: AWStats Multiple Vulnerabilities	Critical	48
17	3618: HTTP: XML-RPC command injection	Critical	40

2.5 Derzeitiger Betrieb

Das IPS ist derzeit fast unverändert so in Betrieb, wie es im Rahmen der ersten Tests installiert wurde. Mittlerweile gab es natürlich eine Reihe von Firmware-Updates des Herstellers, die einige Features hinzugefügt haben.

Das IPS besitzt vier transparente Gigabit-Doppelports, von denen ein Portpaar für die Absicherung des gesamten GÖNET dient. Hier ist direkt das DFN/Internet-Netz mit einer Bandbreite von 1 GBit/s über das IPS mit dem GÖNET verbunden.

Das zweite Portpaar sichert die Kommunikation direkt hinter unserem zentralen VPN-Gateway ab. Das VPN-Gateway wird hauptsächlich vom GoeMobile benutzt und bedarf einer getrennten Absicherung.

Abb. 20 illustriert den Einsatz des IPS im Netz der GWDG (Stand: 7/2006):

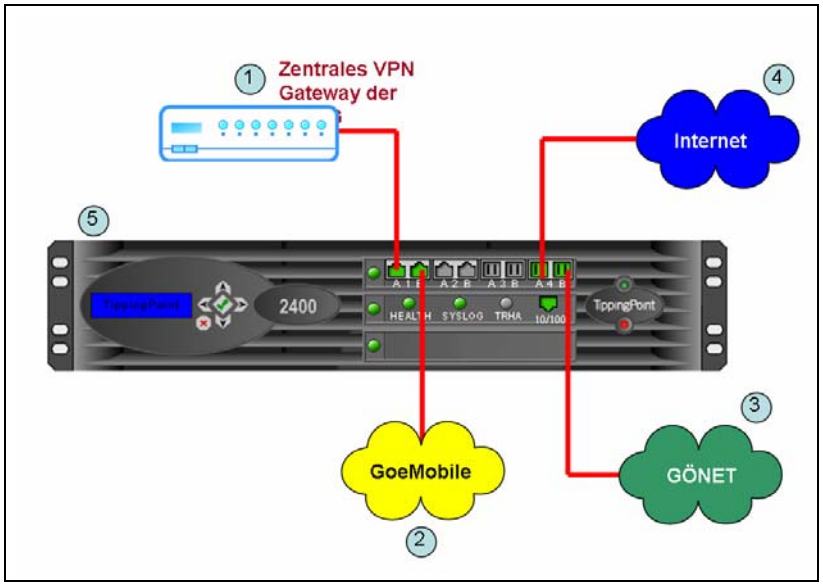


Abb. 20

Die anderen beiden freien Portpaare werden in den kommenden Monaten in Betrieb genommen und bestimmte Servernetze absichern, sodass auch Attacken, die nicht aus dem Internet kommen, die Server nicht gefährden können.

2.6 Ausblick

In Zukunft werden wir die ausführlichen Loggingmechanismen des SMS nutzen, um die Benutzer im GÖNET frühzeitig auf eine mögliche Infektion des eigenen Rechners hinweisen zu können. Wir sammeln jetzt bereits die Angriffsalarmierungen des IPS in einer eigenen SQL-Datenbank. Uns interessieren hier vor allem die Attacken von innen nach außen, da in diesem Fall ein Rechner im eigenen Netz bereits befallen ist. Da die IP-Adresse des Rechners sowie die Art, Zeitpunkt und die Häufigkeit der Attacke festgehalten werden, können wir ein befallenes System einem Institut zuordnen. Unser späteres Ziel ist es, den dort tätigen Systemadministrator dann automatisch via E-Mail über die kompromittierten Rechner zu informieren.

2.7 Fazit

Das IPS in der GWDG stellt einen idealen und dringend erforderlichen Baustein zur Sicherung des lokalen Netzwerkes dar. Es ersetzt natürlich keine Firewall, kann aber gerade in Kombination mit einer Firewall einen sehr hohen Schutz bieten. Eine Firewall allein ist nicht in der Lage, diesen vielen Arten teilweise sehr subtiler Angriffsmuster adäquat begegnen zu können. Momentan können wir in dieser Kombination einen ausgereiften Gesamtschutz für unsere Institute und deren Benutzer zur Verfügung stellen.

Die Statistiken und vor allem die schnelle automatisierte Reaktion auf Ausbreitungswellen von Viren zeigen, dass mit dem IPS eine wesentliche Lücke zwischen Virenschutz und Firewall geschlossen werden konnte. Damit einher geht auch ein Gewinn an Arbeitszeit, die ansonsten aufgrund erfolgreicher Attacken mit der daraus folgenden „Wiederbelebung“ der infizierten Rechner verloren gehen würde.

Ißleiber

3. Kurse des Rechenzentrums

3.1 Allgemeine Informationen zum Kursangebot der GWDG

3.1.1 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.

3.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf

ein Formular zur Verfügung. 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.2 Kurse von September bis Dezember 2006 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	• 13.09.2006 • 15.11.2006	Dr. Heuer, Nolte, Wagenführ Dr. Heuer, Nolte, Wagenführ
Einführung in die Nutzung des Leistungsangebots der GWDG	• 06.09.2006 • 06.12.2006	Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 31.10.2006	Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 01.11.2006 - 03.11.2006	Eyßell
Führung durch das Rechnermuseum	• 01.09.2006 • 29.09.2006 • 10.11.2006 • 15.12.2006	Eyßell Eyßell Eyßell Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 27.11.2006 - 28.11.2006	Dr. Bohrer
Grundkurs UNIX/Linux mit Übungen	• 17.10.2006 - 19.10.2006	Hattenbach
UNIX für Fortgeschrittene	• 06.11.2006 - 08.11.2006	Dr. Sippel
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	• 11.12.2006 - 12.12.2006	Dr. Heuer, Dr. Sippel
UNIX/Linux-Server - Grundlagen der Administration	• 13.12.2006 - 14.12.2006	Dr. Heuer, Dr. Sippel
UNIX/Linux - Systemsicherheit für Administratoren	• 15.12.2006	Dr. Heuer, Dr. Sippel
Windows 2000/XP/2003 in kleinen Netzwerken	• 13.11.2006 - 14.11.2006	Quentin
Die Windows-Active-Directory-Domäne	• 15.11.2006 - 17.11.2006	Quentin
Cluster- und Raid-Konfigurationen unter Windows 2003	• 31.10.2006	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Sicherheit im Internet für Anwender	• 01.12.2006	Reimann
Web Publishing II	• 31.08.2006 - 01.09.2006	Reimann

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Grundlagen der Bildbearbeitung mit Photoshop	• 06.09.2006 - 07.09.2006	Töpfer
Photoshop für Fortgeschrittene	• 09.10.2006 - 10.10.2006	Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Einführung in das Computeralgebra-System Mathematica	• 11.10.2006 - 12.10.2006	Dr. Schwardmann
MindMapping mit MindManager	• 05.10.2006	Reimann
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	• 20.10.2006	Reimann
Neuer Kurs !!! PDF-Formulare mit Acrobat Professional und Adobe Designer erstellen	• 05.09.2006	Dr. Baier
PowerPoint	• 09.11.2006 - 10.11.2006	Reimann
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	• 25.09.2006 - 28.09.2006	Dr. Bohrer, Dr. Liesegang
DNA-Sequenzierung mit dem Staden Package	• 29.09.2006	Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 14.11.2006	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Programmierung von Parallelrechnern	• 28.11.2006 - 30.11.2006	Prof. Haan, Dr. Boehme, Dr. Schwardmann
Neuer Kurs !!! Entwicklung von Anwendungen mit Visual Studio 2005 Express Editions - eine Einführung	• 12.09.2006	Hindermann

3.3 Kurse von September bis Dezember 2006 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Web Publishing II	Reimann	31.08.2006 - 01.09.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	24.08.2006	8
Führung durch das Rechner-museum	Eyßell	01.09.2006 10.00 - 12.30 Uhr	25.08.2006	0
Neuer Kurs !!! PDF-Formulare mit Acrobat Profes-sional und Adobe Designer erstellen	Dr. Baier	05.09.2006 09.15 - 12.00 Uhr und 13.00 - 16.00 Uhr	29.08.2006	4
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	06.09.2006 - 07.09.2006 09.30 - 16.00 Uhr	30.08.2006	8
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.09.2006 17.00 - 20.00 Uhr (SUB)	30.08.2006	0
Neuer Kurs !!! Entwicklung von Anwendungen mit Visual Studio 2005 Express Editions - eine Einführung	Hindermann	12.09.2006 09.00 - 12.30 Uhr und 13.30 - 17.30 Uhr	05.09.2006	4
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	13.09.2006 16.15 - 17.45 Uhr	06.09.2006	1
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	Dr. Bohrer, Dr. Liesegang	25.09.2006 - 28.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	18.09.2006	16
DNA-Sequenzierung mit dem Staden Package	Dr. Liesegang	29.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	22.09.2006	4
Führung durch das Rechner-museum	Eyßell	29.09.2006 10.00 - 12.30 Uhr	22.09.2006	0
MindMapping mit MindManager	Reimann	05.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	28.09.2006	4
Photoshop für Fortgeschrittene	Töpfer	09.10.2006 - 10.10.2006 09.30 - 16.00 Uhr	02.10.2006	8
Einführung in das Computeralgebra-System Mathematica	Dr. Schwardmann	11.10.2006 - 12.10.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	04.10.2006	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	17.10.2006 - 19.10.2006 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	10.10.2006	12
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	Reimann	20.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	13.10.2006	4

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Cluster- und Raid-Konfigurationen unter Windows 2003	Quentin	31.10.2006 09.15 - 12.30 Uhr und 13.30 - 16.15 Uhr	24.10.2006	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	31.10.2006 09.15 - 12.30 Uhr	24.10.2006	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	01.11.2006 - 03.11.2006 09.15 - 12.30 Uhr	25.10.2006	6
UNIX für Fortgeschrittene	Dr. Sippel	06.11.2006 - 08.11.2006 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	30.10.2006	12
PowerPoint	Reimann	09.11.2006 - 10.11.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	02.11.2006	8
Führung durch das Rechner-museum	Eyßell	10.11.2006 10.00 - 12.30 Uhr	03.11.2006	0
Windows 2000/XP/2003 in kleinen Netzwerken	Quentin	13.11.2006 - 14.11.2006 09.30 - 15.30 Uhr	06.11.2006	8
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	14.11.2006 09.00 - 12.00 Uhr	07.11.2006	2
Die Windows-Active-Directory-Domäne	Quentin	15.11.2006 - 17.11.2006 09.30 - 15.30 Uhr (am 17.11. bis 13.30 Uhr)	08.11.2006	10
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	15.11.2006 16.15 - 17.45 Uhr	08.11.2006	1
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	27.11.2006 - 28.11.2006 13.00 - 16.00 Uhr	20.11.2006	4
Programmierung von Parallelrech-nern	Prof. Dr. Haan, Dr. Boehme, Dr. Schwardmann	28.11.2006 - 30.11.2006 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr	21.11.2006	12
Sicherheit im Internet für Anwender	Reimann	01.12.2006	24.11.2006	2
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.12.2006 17.00 - 20.00 Uhr	29.11.2006	0
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	Dr. Heuer, Dr. Sippel	11.12.2006 - 12.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.12.2006	8
UNIX/Linux-Server - Grundlagen der Administration	Dr. Heuer, Dr. Sippel	13.12.2006 - 14.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	06.12.2006	8
UNIX/Linux - Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	15.12.2006 09.30 - 12.30 Uhr und 13.30 - 15.00 Uhr	08.12.2006	4
Führung durch das Rechner-museum	Eyßell	15.12.2006 10.00 - 12.30 Uhr	08.12.2006	0

4. Betriebsstatistik Juli 2006

4.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	8	269,80
IBM Regatta	124	67.908,48
Linux Parallel	252	147.305,30
Linux Opteron	96	63.721,80

4.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	1	2,00	0	
IBM SP/Regatta	0		0	
Linux Parallel	2	110,33	0	
Linux Opteron	0		0	
PC-Netz	0		0	
Nameserver	0		0	
Mailer	1	2,00	0	

5. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Andreas Ißleiber	• Intrusion Detection und Prevention im GÖNET (Teil 2)	aisslei@gwdg.de 0551 201-1815
Michael Reimann	• Umstieg von Norman Virus Control auf Sophos Anti-Virus	Michael.Reimann@gwdg.de 0551 201-1826