Sicherheit von Breitbandanschlüssen bei Privatanwendern

Prof. Dr. Heinzmann, Marcel Liebi, Felix Müller, Thomas Bruhin
Institut für Internettechnologien und –Anwendungen, Hochschule Rapperswil (ITA-HSR)
cnlab Information Technology Research AG, 8640 Rapperswil

Version 1.2

Abstract

Im Auftrag von SFDRS Kassensturz haben die Firma cnlab Information Technology Research AG und die Hochschule für Technik Rapperswil (HSR) die Sicherheit von Breitbandanschlüssen für Privatanwender untersucht. Es konnten signifikante Unterschiede aufgezeigt werden, welche im Privatbereich vor allem auf die Verbreitung der unterschiedlichen Anschlussarten (via Breitband-Modem oder NAT-Router) zurückzuführen sind.

1 Einleitung

1.1 Ausgangslage und Testauftrag

Als Verkaufsargument für Breitband-Internet-Abos gilt vor allem die Geschwindigkeit. Das Thema Sicherheit von Breitbandanschlüssen wurde bei den ADSL-Cablenet-Performance-Messungen Anfang 2003 andiskutiert, aber bisher kaum weiter vertieft. SFDRS Kassensturz hat Ende 2003 Prof. Peter Heinzmann von der Hochschule Rapperswil und der Firma cnlab angefragt, die Sicherheit von ADSL und Cablenet-Providern zu untersuchen. Anhand verschiedener Beispiele sollte aufgezeigt werden, ob selbst ohne Hacken mit einfachen Programmen Daten von privaten Breitband-PCs eingesehen, verändert oder gelöscht werden könnten. Privatanwender sollten sich bewusst werden, welchen Gefahren sie sich beim Surfen im Internet aussetzen. Ferner sollte untersucht werden, ob es Unterschiede gibt in Bezug auf die Sicherheit zwischen den verschiedenen Internet Service Providern.

Getestet wurden die Provider Bluewin, Cablecom, Econophone, Green, Init7, Solnet, Sunrise, Tele2 und Tiscali. Die Messungen wurden im 4. Quartal 2003 und 1. Quartal 2004. durchgeführt.

1.2 Übersicht zur Sicherheit beim Breitbandanschluss

Ein Problem beim Breitbandanschluss besteht darin, dass die Heimrechner im Gegensatz zum Internet-Zugang via Dialup-Modem, auch mit dem Internet verbunden sind, wenn längere Zeit keine Internet-Kommunikation besteht. Diese so genannte „always-on“ Situation hat zur Folge, dass sich via Breitbandnetz angeschlossene Rechner länger potentiellen Angreifern aussetzen als Rechner mit Dialup-Modem-Verbindungen.

Für den Anschluss der Heimrechner an Breitband-Netze werden zwei grundsätzlich verschiedene Technologien eingesetzt:

- Beim Anschluss des Heimrechners ans Internet via Breitband-Modem ist dieser direkt mit dem Internet verbunden und die Kommunikation ist in keiner Art und Weise eingeschränkt. Dies kann einerseits von Vorteil sein, wenn jemand beispielsweise Sprachverbindungen oder spezielle Spiele via Internet betreiben will. Andererseits können jederzeit beliebige Datenpakete – auch unerwünschte - vom Internet aus direkt zum Heimrechner geschickt werden.[1]
- Beim Anschluss des Heimrechners ans Internet via Router (mit Network Address Translation, NAT) sind keine Verbindungen vom Internet aus auf den Heimrechner möglich, welche nicht explizit vom Heimrechner initiiert wurden. D.h. der NAT-Router leitet nur Datenpakete von Antworten auf Anfragen des Heimrechners zu diesem weiter. Dies bietet einen Schutz gegen unerwünschte Verbindungsversuche zum Heimrechner. Es schützt aber nicht vor Viren oder bösartigen Programmen, welche man via Mail oder spezielle Webseiten auf seinen Rechner kopiert hat.

Beim Cablecom-Angebot werden die Internet-Anschlüsse grundsätzlich mit Breitband-Modem angeboten[2]. Bei den ADSL-Providern kann jeder Kunde selbst entscheiden, ob er das vom ADSL-Provider angebotene Anschlussgerät einsetzen, oder ein eigenes beschaffen will. D.h. bei den ADSL-Providern hat man die Wahl zwischen Breitband-Modem und NAT-Router-Anschlussgeräten. Allerdings haben manche ISP im Rahmen spezieller „Promotionen“ die eine oder andere Lösung bevorzugt verbreitet.

[1] Es ist zu beachten, dass auch gewisse als „Modem“ bezeichnete Anschlussgeräte über eine NAT-Router-Funktion verfügen und daher gleichwertig wie die NAT-Router sind.
[2] Andere, kleinere Cablenet-Anbieter (z.B. Radio Schefer Rorschacher, GGA-Maur) setzen grundsätzlich NAT-Router oder wahlweise NAT-Router oder Modems ein.

Vor allem beim Anschluss mit einem Breitband-Modem ist es extrem wichtig, den Heimrechner stets gut vor unerwünschten Gästen zu schützen. Dazu gehört, dass man keine sogenannte Freigaben hat, auf welche jedermann zugreifen kann und dass man seine Software stets auf dem aktuellsten Stand hat, d.h. die aktuellen Virenschutzprogramme und Sicherheitsupdates (so genannte Patches oder Hotfixes) installiert hat.

Wie stark ein Heimanwender seine Daten oder seine Rechnerumgebung exponiert, hängt von mehreren Faktoren ab:

1. Anschlussart mit oder ohne NAT-Router:
    a. Ist der Rechner via NAT-Router ans Internet angeschlossen, kann nicht direkt auf den Rechner zugegriffen werden. Freigegebene Ressourcen oder allfällig fehlende Software-Updates fallen nicht direkt ins Gewicht.
    b. Wird zusätzlich zum Breitband-Modem NAT-Router oder Firewall eingesetzt, so kann ebenfalls nicht direkt auf den Rechner zugegriffen werden.
2. Schutzmassnahmen auf dem Rechner:
    a. Sind auf dem Rechner keine Ressourcen freigegeben, auf welche via Internet zugegriffen werden kann, so ist zumindest die einfachste Zugangsart auf Daten von Windowsrechnern verunmöglicht.
    b. Sind auf dem Rechner die aktuellen Software-Patches installiert, so kann nicht via allfällige Sicherheitslücken auf den Rechner zugegriffen werden.
    c. Sind aktualisierte Virenschutzprogramme vorhanden, so sollte sich die Verbreitung von Viren, welche direkt oder via E-Mail, Web-Seiten oder andere Übertragungskanäle auf den Rechner gelangt sind, verhindern lassen.
3. Zustand der Rechner in der näheren Umgebung:
    a. Falls viele Rechner in der näheren Umgebung des eigenen Rechners Sicherheitslücken aufweisen oder bereits mit Viren verseucht sind, so steigt die Gefahr einer Übertragung auf den eigenen Rechner.

2 Testbeschreibung

Alle Tests wurden im Auftrag von SFDRS und aus Sicht der Endkunden durchgeführt. Es wurden vier unabhängige Testteile unterschieden:

1. In Rahmen einer ***Sensibilisierungsübung*** wurden ca. 25'000 IP-Adressen durchsucht und es wurde exemplarisch gezeigt, dass auf verschiedensten Windowsrechnern völlig ungeschützte Freigaben zu finden sind, d.h. dass der Zugriff auf Daten dieser Rechner möglich ist. Ferner wurde demonstriert, wie schnell neu ans Netz angeschlossene Windowsrechner von einem Virus/Wurm befallen werden, wenn das Betriebssystem nicht auf den aktuellsten Stand ist.
2. Abschätzung der ***Anzahl Rechner mit Direktzugang*** vom Internet aus: Basierend auf Zugriffsdaten der Performance-Applet-Nutzer wurde abgeschätzt, wie viele Breitband-Kunden mit internen (non-routable) Adressen arbeiten, d.h. wie viele Breitband-Kunden via NAT (oder Firewall) angeschlossen sind.
3. Abschätzung der ***Anzahl Rechner mit Freigaben***: Es sollte abgeschätzt werden, wie viele ungeschützte Rechner bei verschiedenen ISP zu finden sind. Während sieben Tagen wurden rund um die Uhr ausgewählte IP-Adressbereiche von Internet Service Providern in Bezug auf die Erreichbarkeit der Rechner untersucht. In einem zweiten Schritt wurde nach freigegebenen Ressourcen gesucht.
4. ***Häufigkeit von Attacken***: Mit Intrusion Detection Systemen (IDS), welche an die Netze verschiedener ISPs angeschlossen sind, wurden rund um die Uhr mögliche Attacken im Bereich des entsprechenden Netzes erfasst.

Anhand dieser Tests lassen sich zwar keine absoluten Werte, aber dennoch gut fundierte relative Werte ableiten, um die relative Sicherheit im Bereich der Breitbandanschlüsse bei verschiedenen ISP aufzuzeigen.

3 Ergebnisse

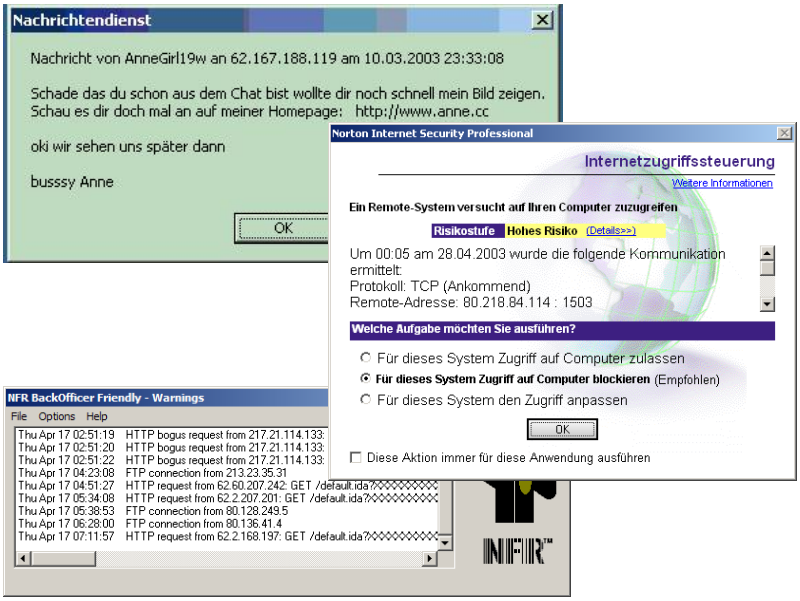
3.1 Sensibilisierungsübungen

Im Sensibilisierungsteil des Tests wurde gezeigt, welchen Gefahren sich unvorsichtige Internet-Nutzer aussetzen.

Am 30. Januar 2004 wurde bei SFDRS demonstriert, wie innerhalb von Stunden unter rund 25'000 IP-Adressen von Schweizer Internet-Service Providern einige Hundert Windowsrechner mit völlig ungeschützten Freigaben identifiziert werden konnten. Verwendet wurden nur frei auf dem Internet verfügbare Werkzeuge[3]. Es wurde auch gezeigt, dass einmal identifizierte Rechner direkt via Windows Explorer angesprochen werden können. Damit wurde klar, wie einfach der Zugang auf ungeschützte Rechner - auch ohne spezielle Fachkenntnisse - möglich ist. Bei diesen ungeschützten Rechnern kann im Prinzip jedermann via Internet auf Dokumente wie beispielsweise Bewerbungsschreiben, Zeugnisse, Abrechnungen, Kundendaten etc. zugreifen[4].

Am 17. Februar 2004 wurde dem Reporterteam von SFDRS demonstriert, wie schnell ein Windowsrechner von einem Virus/Wurm befallen wird, wenn man ihn nicht auf den aktuellsten Betriebssystem-Stand gebracht hat und ungeschützt an ein Breitbandnetz anschliesst.

Auch Ereignisse wie plötzlich erscheinende Windows-Fenster, Alarm-Meldungen allenfalls installierter persönlicher Firewalls oder Alarme von so genannten Honeypot-Programmen beweisen, dass immer wieder versucht wird, ungebeten mit privaten Rechnern Kontakt aufzunehmen, wenn diese ungeschützt ans Internet angeschlossen sind.



Figur 1: Alarm-Meldungen, welche bei direkt ans Internet angeschlossenen Rechnern regelmässig zu beobachten sind

[3] Scan-Programme wie beispielsweise Legion, Ogre, Red-Button oder Languard (ältere Languard Versionen waren frei verfügbar).
[4] Gemäss StGB Art. 143 ist der Zugriff auf Rechner nur dann strafbar, wenn dieser gegen Zugriff „besonders geschützt“ ist. Fälle wie die hier beobachteten, bei denen nicht einmal ein Passwortschutz vorhanden war, lassen sich nicht strafrechtlich verfolgen.

3.2 Anzahl Rechner mit Direktzugang (ohne NAT)

Da vor allem bei den ADSL-Providern die Kunden selbst entscheiden können, ob sie sich per Breitband-Modem oder NAT-Router anschliessen wollen und weil beim Cablecom-Netz viele Leute zusätzlich einen NAT-Router oder Firewall einsetzen, lässt sich ohne weiteres feststellen, wie viele Anschlüsse mit der „unsicheren“ Breitband-Modem-Lösung arbeiten.

Cnlab bietet seit Jahren zusammen mit den Internet Service Providern ein Performance Mess-System an, mit welchem Privatkunden die Leistungsfähigkeit ihres Internet Service Providers überprüfen können. Die Tester laden sich dabei ein Testapplet von einer Web-Seite und starten damit verschiedene Messungen. Im Rahmen dieser Tests werden auch die lokal auf dem Rechner der Tester zugewiesenen Internet Protocol (IP) Adressen erfasst. Handelt es sich dabei um interne, so genannt „non routable“ Adressen, so kann davon ausgegangen werden, dass sich der entsprechende Tester-Rechner hinter einem NAT-Router befindet. Durch die Auswertung dieser Daten, lässt sich aufgeschlüsselt nach Provider abschätzen, wie viele Anschlüsse mit der „unsicheren“ Breitband-Modem-Lösung arbeiten, d.h. jederzeit direkt vom Internet her erreichbar sind.

Anschlüsse mit NAT	**Bluewin**	**Cablecom**	**Green**	**Solnet**	**Sunrise**	**Tele2**	**Tiscali**
192.1x	74%	65%	84%	83%	71%	88%	78%
127.0x	16%	32%	12%	14%	26%	12%	18%
10.0x	10%	3%	4%	3%	3%		4%
172.1.x							
Total Anschlüsse mit NAT Router (private IP Adressen)	86%	46%	90%	86%	60%	74%	78%
Total Anschlüsse mit Modem (öffentliche IP Adressen)	**14%**	**54%**	**10%**	**14%**	**40%**	**26%**	**22%**
Total Messungen	340'101	345'483	18'900	31'166	80'809	12'206	19'408
Total versch. UserID (Benutzer)	83'000	57'000	6'500	7'500	24'000	1'900	5'800
Messungen / IP	4.1	6.1	2.9	4.2	3.4	6.4	3.3

Tabelle 1: Prozentualer Anteil Heimrechner mit NAT für die verschiedenen ISP

In Bezug auf den Anteil der Kundenrechner, welche über NAT-Router (oder Firewall) angeschlossen sind, lassen sich die ISP grob in drei Klassen unterteilen: Jene mit weniger als 15% direkt angeschlossenen Kundenrechnern (Bluewin, Econophone, Green, Solnet), jene mit 20-30% direkt angeschlossenen Kundenrechnern (Init7, Tele2, Tiscali), und jene mit 40% und mehr direkt angeschlossenen Kundenrechnern (Sunrise und Cablecom).

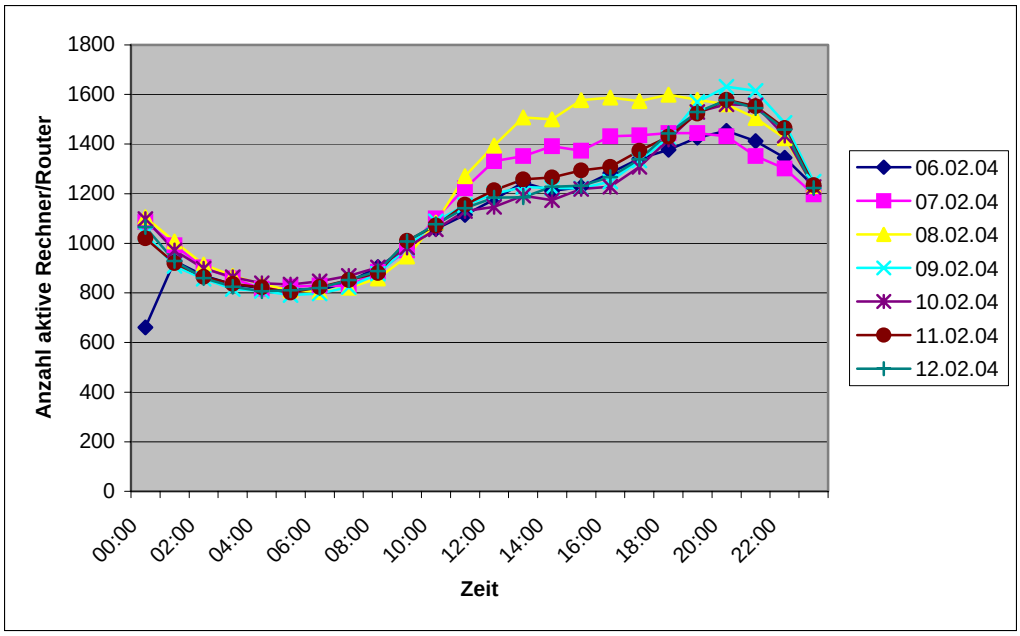
Der Prozentsatz der direkt ans Internet angeschlossen und damit eher exponierten Kundenrechnern dürfte direkt mit der Art der im Rahmen von Promotion-Packages angebotenen Anschlussgeräte zusammen hängen: ADSL-Provider, welche in grossem Stil USB-Modems angeboten haben, weisen einen grösseren Anteil direkt erreichbare Rechner auf als ADSL-Provider, welche ihren Kunden vor allem NAT-Router empfehlen. Ferner ist der Anteil NAT-Router höher, wenn die ADSL-Provider vor allem Firmenkunden bedienen.

3.3 Anzahl Rechner mit Freigaben

Um abschätzen zu können, wie viele völlig ungeschützte, direkt vom Internet her erreichbare Windowsrechner bei den verschiedenen Internet-Service-Providern zu beobachten sind, wurden stichprobenweise Adressbereiche der zu testenden ISP nach Rechnern mit Freigaben durchsucht[5]. Diese Messungen wurden während einer Woche rund um die Uhr durchgeführt.

In einem ersten Schritt wurde die Anzahl der aktiven Anschlüsse bestimmt. In einem zweiten Schritt wurde untersucht, bei wie vielen der aktiven Anschlüsse direkt auf Rechner mit freigegebenen Ressourcen zugegriffen werden könnte.

Bei allen ISPs zeigten sich die erwarteten tageszeitlichen Schwankungen in der Anzahl aktiver Anschlüsse (eingeschaltete Rechner oder Router). Bei den Hauptnutzungszeiten der Privatnutzer (am Abend) waren mehr aktive Rechner und Router zu beobachten als nach Mitternacht bis in die frühen Morgenstunden.



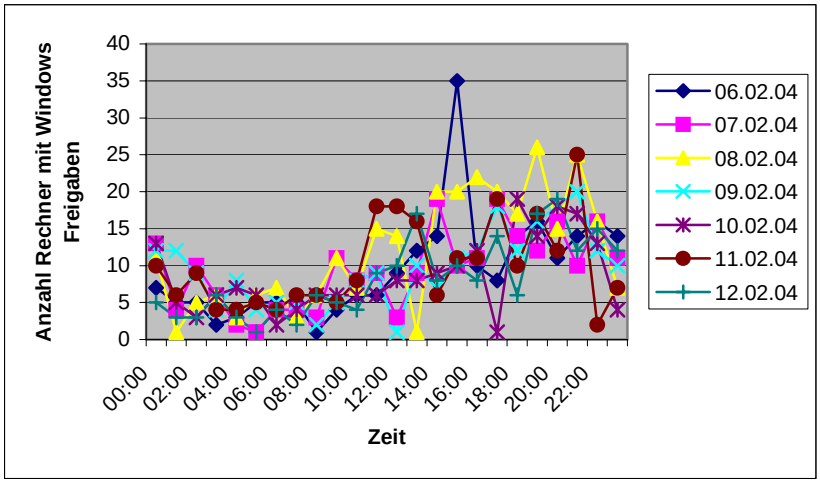
Figur 2: Verlauf der Anzahl der aktiven Anschlüsse in Abhängigkeit von der Tageszeit (aufgezeichnet für verschiedene Wochentage)

Bei wie vielen der aktiven Rechner ein direkter Zugang auf Ressourcen möglich ist, hängt einerseits davon ab, ob der Rechner via Breitband-Modem angeschlossen ist oder nicht und andererseits ist entscheidend, ob die Besitzer der Rechner überhaupt Ressourcen freigegeben haben.

Während der Messwoche wurden nur bei etwa 1 bis 2% der aktiven Anschlüsse völlig offene Rechner beobachtet. Dies mag einerseits als eine sehr kleine Zahl erscheinen. Andererseits bedeutet dies, dass bei den bald rund 1 Million Breitbandanschlüssen in der Schweiz rund 10'000 bis 20'000 Breitbandkunden ihre Daten völlig offen im Internet preisgeben. Auch hier

5 Die Messungen basieren auf einem Ping-Sweep mit dem Programm nmap zur Detektion der aktiven Rechner und Router sowie einem Linux-Programm zur Identifikation von Windowsfreigaben (SMB-client).

sind gewisse tageszeitliche Schwankungen zu beobachten, was wiederum damit zusammenhängt, dass viele Heimrechner nur in den Hauptnutzungszeiten angeschlossen sind[6].



Figur 3: Anzahl beobachtete Rechner mit Freigaben in Abhängigkeit von der Tageszeit (aufgezeichnet für verschiedene Wochentage)

Würde sich das Kundenverhalten unter den verschiedenen Providern nicht wesentlich unterscheiden, so müsste die Anzahl der Rechner mit Freigaben der Aufteilung von direkt erreichbaren Rechnern entsprechen. Der Vergleich mit Tabelle 1 zeigt, dass dies weitgehend zutrifft:

Windows Freigaben (öffentliche Ressourcen)	**Bluewin**	**Cablecom**	**Green**	**Solnet**	**Sunrise**	**Tele2**	**Tiscali**
Durchschnittliche Anzahl aktive Anschlüsse	968	1'149	1'325	1'030	2'187	2'118	947
Durchschnittliche Anzahl Rechner mit offenen Ressourcen	2.6	9.6	2	3.3	9.8	6.8	5
Anteil Rechner mit offenen Ressourcen (bezogen auf Anzahl aktive Anschlüsse)	**0.29%**	**0.79%**	**0.15%**	**0.32%**	**0.42%**	**0.31%**	**0.52%**
Total Anschlüsse mit Modem (öffentliche IP Adressen)	14%	54%	10%	14%	40%	26%	22%

Tabelle 2: Anteil Rechner mit offenen Ressourcen

Man beachte, dass die absolute Anzahl der Rechner mit freigegebenen Ressourcen vom gewählten ISP-Adressbereich abhängt und daher nicht zum Vergleich der ISP beigezogen werden kann.

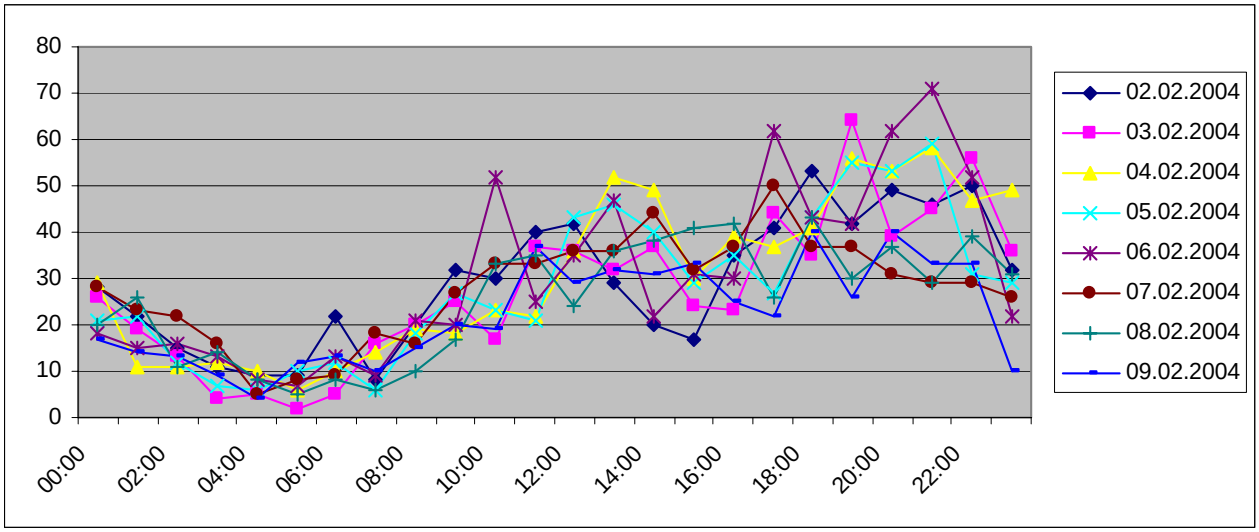
[6] Manche NAT-Router sind so konfiguriert, dass sie automatisch vom Netz getrennt werden, wenn längere Zeit keine Daten mehr übertragen werden.

3.4 Häufigkeit von Attacken

Seit mehreren Monaten erfasst cnlab AG in Zusammenarbeit mir der Hochschule Rapperswil mit so genannten Intrusion Detection Systemen (IDS) die Anzahl der als „Einbruchsversuche“ klassierten Verkehrsmuster bei verschiedenen ISP. Der grösste Anteil der erfassten „Einbruchsversuche“ stammt nicht direkt von Hackern sondern von mit Viren/Würmern befallenen Rechnern, welche versuchen, ihre Programme weiter zu verbreiten. Da aktuelle Viren/Wurm-Programme wie beispielsweise eBlaster versuchen, Rechner mit ähnlichen IP-Adressen anzuwählen, verbreiten sich die „Schädlinge“ in Netzen mit vielen direkt erreichbaren und nicht geschützten Rechnern schneller. Heimnutzer, welche ihre Rechner nicht mit aktuellen Virenschutzprogrammen schützen und das Betriebssystem regelmässig aktualisieren, tragen zusätzlich zur Verbreitung der Viren/Würmer bei.

Das Messsystem umfasst mehrere IDS-Systeme (Typ Snort), welche bei Anschlüssen der wichtigsten Provider über Breitband-Modems oder speziell konfigurierte Router (im Bridging Mode) angeschlossen sind.

Figur 4 zeigt den zeitlichen Verlauf der beobachteten IDS-Alarme für eine Messperiode von einer Woche. Auch hier ist die tageszeitliche Abhängigkeit entsprechend den Hauptnutzungszeiten der Heimnutzer zu beobachten.



Figur 4: Anzahl Snort Alerts in Abhängigkeit der Tageszeit

Beim Vergleich der verschiedenen Provider sind signifikante Unterschiede zu beobachten.

IDS-Alerts (Häufigkeit von Attacken)	Bluewin	Cablecom	Green	Solnet	Sunrise	Tele2	Tiscali
maximale Anzahl Alerts pro Stunde	17.5	31.5	11.0	9.4	28.8	13.3	12.7
durchschnittliche Anzahl Alerts pro Stunde gemittelt über eine Messwoche	**8.5**	**29.9**	**8.4**	**8.1**	**20.3**	**10.6**	**7.3**
Total Anschlüsse mit Modem (öffentliche IP Adressen)	14%	54%	10%	14%	40%	26%	22%
typischer Abstand zwischen eBlaster-Attacken in Minuten	**7.1**	**2.0**	**7.1**	**7.4**	**3.0**	**5.7**	**8.2**

Tabelle 3: Häufigkeit von Attacken bzw. IDS-Alerts

Schliesst man einen ungeschützten Rechner direkt ans Netz an, so dauert es typisch nur Minuten, bis der Rechner attackiert wird.

4 Fazit

Die Sicherheit der Breitbandanschlüsse im Privatbereich wird in erster Linie durch die Art des Anschlussgeräts, Breitband-Modem oder NAT-Router bestimmt. Je nach Internet Service Provider sind nur 10% (Green) bis über 54% (Cablecom) der Kundenrechner direkt per Breitband-Modem ans Internet angeschlossen und daher sehr exponiert. Es wird geschätzt, daß jeder 100ste bis 1000ste der direkt erreichbaren Rechner Windows-Freigaben hat, womit jeder vom Internet her auf diese zugreifen kann. Es ist unbedingt erforderlich, daß auch die Heimanwender ihre Rechner regelmäßig auf den neusten Stand bringen (Patches installieren), aktualisierte Virenschutzprogramme einsetzen und sich allenfalls mit Personal Firewalls zusätzlich schützen. Ein völlig ungeschützter Rechner wird innerhalb von wenigen Minuten nach dem Anschluß ans Internet von einem Virus/Wurm befallen sein.

Weil viele Heimanwender mit solchen Schutzmaßnahmen überfordert sind, wären Hilfestellungen der Internet Service Provider, welche über die reine Beschreibung von Maßnahmen hinaus gehen (z.B. Managed Security Dienste) sicher sinnvoll.

Erste Massnahmen zur Verbesserung des Sicherheitsbewusstseins und zur Unterstützung der Kunden sind bei den Internet Service Providern bereits zu erkennen.

Referenzen / weitere Informationen:

1. Die meisten Internet Service Provider bieten speziell auf ihre Kunden zugeschnittene Sicherheitsinformationen an.

2. Beim Sicherheitsportal von Microsoft findet man im Bereich „Sicherheit für Privatanwender“ Beschreibungen und Checklisten zur Sicherheitsproblematik.
   http://www.microsoft.com/switzerland/de/security/privat/

3. Spezialisten können bei der von Vincent Dorsch und Tobias Schoch im Wintersemester 2003/04 an der HSR realisierten Anwendung „Browser Vulnerability“, Beispiele von Verletzlichkeiten studieren und diverse Verweise zu Quellen finden.
   http://securitycheck.cnlab.ch

4. Verschiedene Organisationen bieten so genannte Browser-Checks an, mit welchen allfällige Sicherheitslücken aufgedeckt werden können. Hier sind zwei Beispiele von Schweizer Firmen:
   Studerus-Telecom / Celeris: http://www.security-check.ch/
   Compass Security: http://www.sicherheitstest.ch