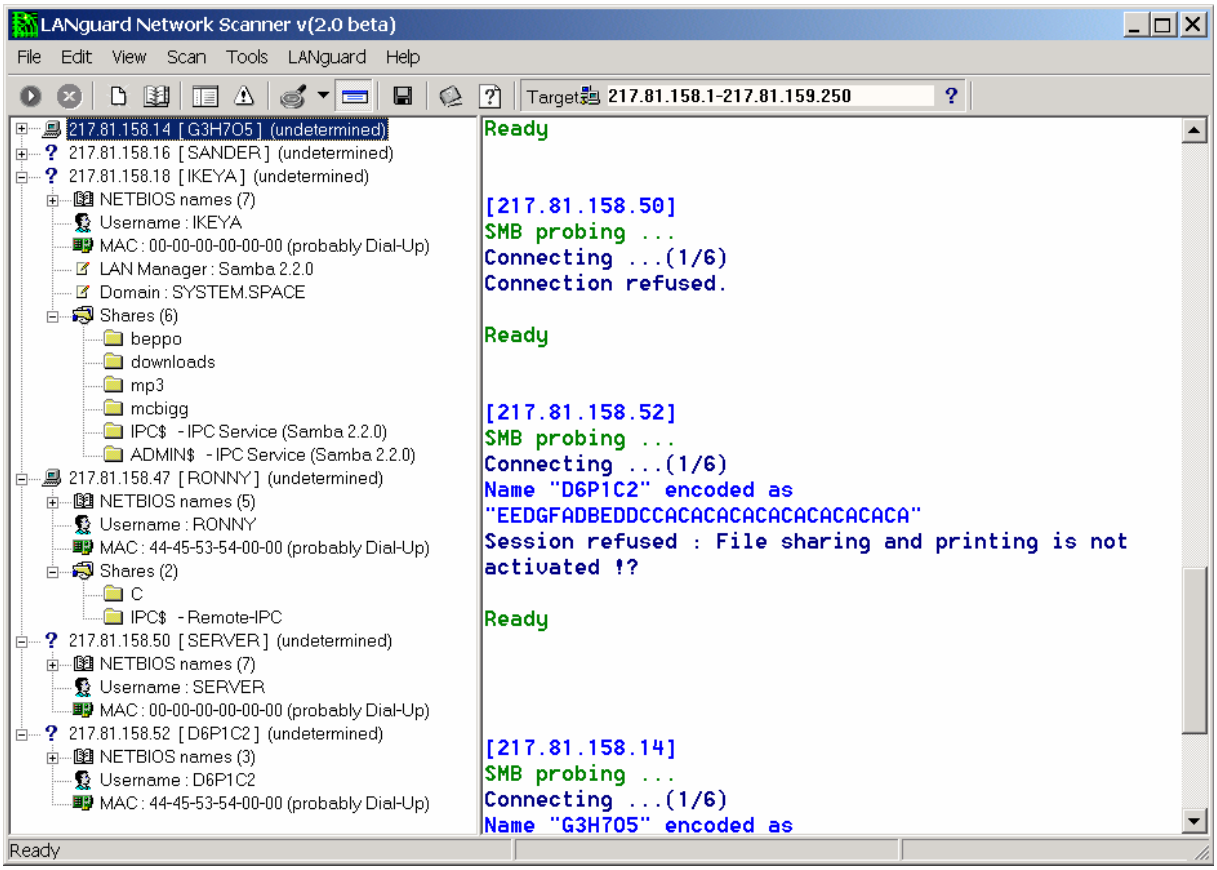
Live-Hacking: Sehen heißt verstehen!

Wer sich mit der Kunst der Verteidigung beschäftigt, muss auch mit Angriffstechniken vertraut sein. Im Rahmen einer Demonstration werden spannende Hackertechniken unter realistischen Umständen *live* durchgeführt und diskutiert. Trotz der kurzen Vortragszeit sollen folgende Angriffe live vorgeführt werden:

1) Offene Netbios-Shares/Windows-Freigaben[i] (***)

Viele Windowsbenutzer geben einzelne Verzeichnisse oder sogar ganze Festplatten frei, um über das Netzwerk darauf zuzugreifen. Man sollte erwarten, dass Rechner im Internet vor unerwünschtem Zugriffe geschützt sind, z.B. durch eine Firewall oder einen Router. Eine IP-Range wird nach Freigaben gescannt; es zeigt sich, dass eine Vielzahl von Rechnern ohne jeglichen Schutz direkt mit dem Internet verbunden ist und dass ein beträchtlicher Teil der Rechner ganze Festplatten freigeben. Einige haben sogar die gesamte C:\-Festplatte freigegeben:



Das eingesetzte Tool „LANGuard“ ist derart einfach zu bedienen, dass ein durchschnittlicher Anwender seine gesamte Funktionalität innerhalb fünf Minuten erfasst[1].

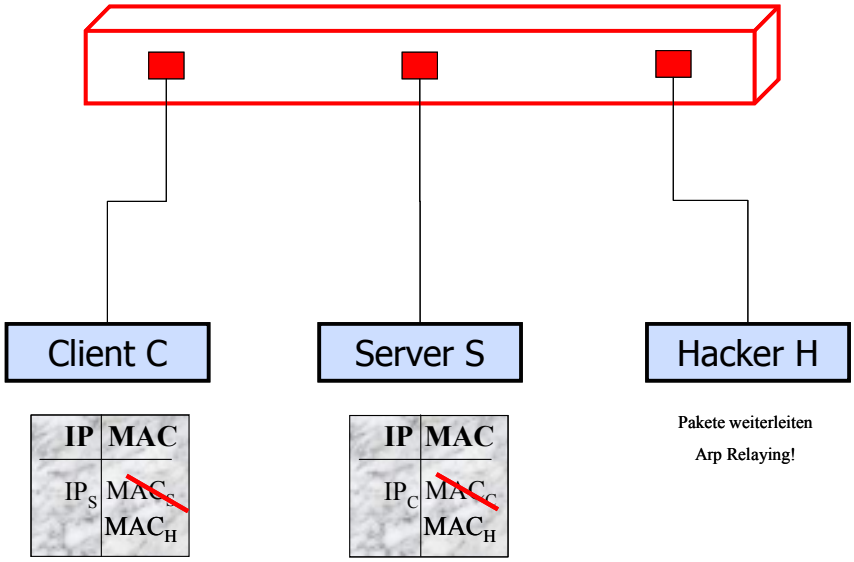
2) Sniffing auf dem LAN/Ethernet

Eine einfach Übung ist das Ausspähen von Daten, die über das LAN übertragen werden: TCP-Pakete, die von einem Rechner zu einem anderen übertragen werden sollen, liefert das Netzwerk (in der Regel der Hub) bereitwillig an beliebige andere Systeme aus. Ursächlich dafür ist das dem Ethernet zugrunde liegende Paradigma CSMA/CD.

3) Sniffing am Switch

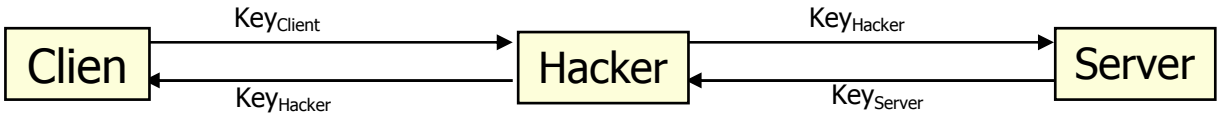
Administratoren vertrauen oft darauf, dass unerwünschtes *Sniffing* durch den Einsatz eines Switches vereitelt werden kann. Das Sniffing in geswitchten Netzen ist zwar anspruchsvoll, aber mit etwas Erfahrung einfach zu realisieren: Durch gespoofte ARP-Pakete manipulieren wir die ARP-Caches („*ARP Cache Poisoning*“) der einzelnen Systeme, sodass sämtliche Pakete an unseren Angriffslaptop ausgeliefert werden – welcher daraufhin die Pakete an den eigentlichen Empfänger weiterleitet. Es wird gezeigt, wie wir mühelos über das Netzwerk transportierte Informationen ausspähen können.

[1] Wir warnen vor dem spielerischen Umgang mit LANGuard, da einige der *per default* aktivierten Analysen gegen §202a StGB verstoßen; Verstöße werden mit bis zu 5 Jahren Haft bestraft.



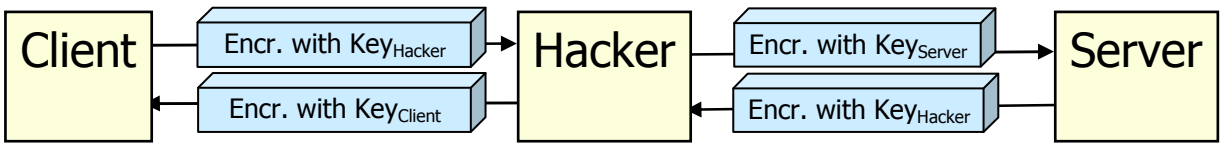
4) Sniffing von SSL-Verbindungen (***)

Beim Internetbanking/Broking verlassen sich Anwender oft auf verschlüsselte Verbindungen (SSL/HTTPS). Leider handelt es sich hierbei oft um eine trügerische Sicherheit: Verschlüsselung ist zwar ein Garant dafür, dass die versendeten Informationen von einem *passiven* Angreifer nicht ausgelesen werden können. Es wird aber keinesfalls sichergestellt, dass der Benutzer mit dem erwünschten Kommunikationspartner kommuniziert. Durch DNS-Spoofing leiten wir den Kunden einer Bank, auf unseren Server um. Um ihm seine gewohnte Weboberfläche zu bieten, leiten wir – ähnlich wie das ein Web-Proxy tut – auf den Server seiner Bank weiter. Da eine verschlüsselte SSL-Session etabliert wird, werden zunächst die Public-Keys ausgetauscht:



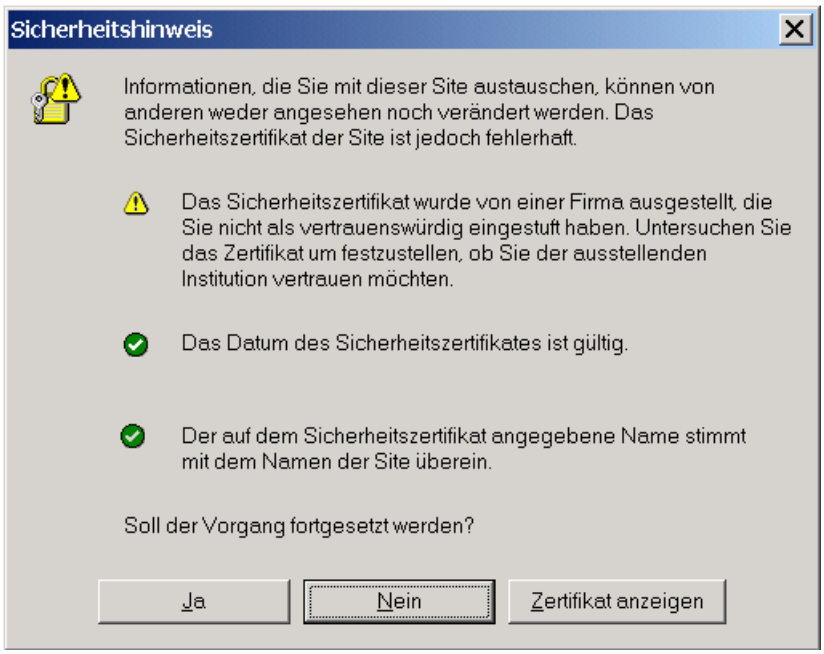
Unser Hacker-Rechner agiert als Man-in-the-Middle und sorgt dafür, dass Client und Server jeweils die Public-Keys des Hackers untergejubelt werden. Nun gibt unser Opfer beim Online-Broking eine Nutzinformation (im Beispiel seine Zugangsnummer und seine PIN) ein und schickt sie – verschlüsselt mit dem Key des Hackers – ab. Der Hacker entschlüsselt die PIN mit seinem eigenen Private-Key und verschlüsselt sie mit dem Public-Key der Bank.

Unser argloser Anwender kann nun wie gewohnt mit seiner Bank kommunizieren – aber der Hacker liest mit:



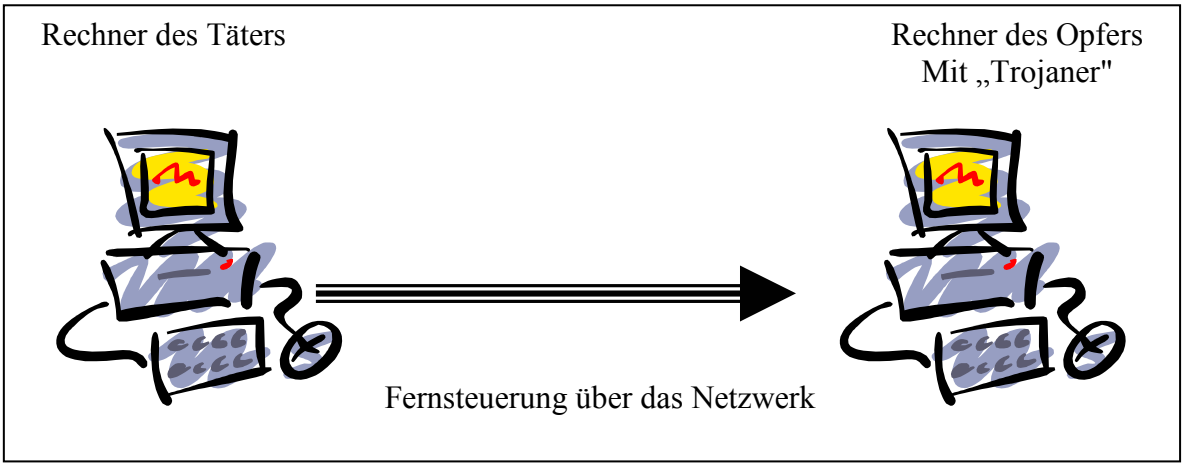
Die Man-in-the-Middle-Attack wird nur entlarvt, wenn der Benutzer seine Aufmerksamkeit auf das X.509-Zertifikat richtet, das die Identität des Webservers bestätigen soll. Dies erfordert aber die Erfüllung dreier Bedingungen:

1. Der Anwender benötigt komplexes Spezial-Know-How.
2. Das Zertifikat der CA (Zertifierungsstelle), die das Zertifikat der Bank ausgestellt hat, muss sich im Speicher vertrauenswürdiger Stammzertifizierungsstellen des Webbrowsers befinden.
3. Der CA muss vertraut werden.



5) Trojanische Pferde (***)

Ein simples und dennoch eindrucksvolles Werkzeug, um Zugriff auf fremde Systeme zu erhalten, ist die Installation von trojanischen Pferden. Gerne zeigen wir, wie man mit Tools wie NetBus oder Cafeini die Verfügungsgewalt über einen Windows-PC erlangt. Beide Tools stehen im Internet zum kostenlosen Download bereit und repräsentieren eine ganze Klasse



von Trojanischen Pferden. Ist der Rechner unseres Opfers bereits trojanisiert, so können wir aus der Ferne damit allerlei Schabernack treiben, den wir zur Freude unseres Publikums gerne demonstrieren: So öffnen wir auf dem befallenen Rechner über das Internet die CD-Schublade. Daraufhin sperren wir einzelne Tasten des Opferrechners, steuern den Mauszeiger

fern und führen dann Änderungen in einem geöffneten Word-Dokument durch. Den Webbrowser des Opfers schicken wir auf Knopfdruck auf die Webseite des Playboy-Magazins, was einen Anwender - insbesondere bei der Anwesenheit seines Vorgesetzten - in Erklärungsnöte bringen kann.

Doch außer zu solchen Streichen lassen sich die Trojaner auch zu handfester Industriespionage einsetzten: Per Mausklick lassen wir uns den Bildschirminhalt des Opfers anzeigen, spionieren seine Tastatureingaben aus – und fertigen uns Kopien von vertraulichen Dateien an. Verfügt der Rechner des Opfers über ein Mikrophon, so lässt sich dieses als Wanze einsetzen, die über das Netzwerk abgehört werden kann.

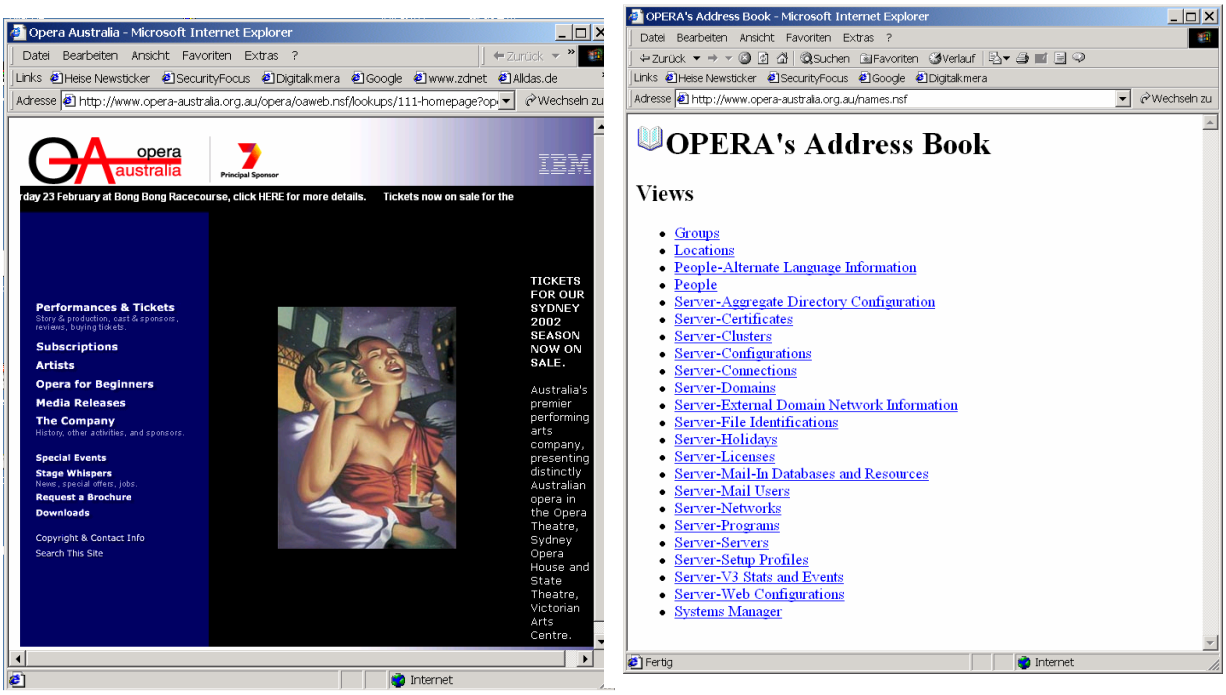
Im Internet stehen neben über eintausend von Trojanern auch praktische Tools zum Download bereit, mit denen sich ein Trojaner unauffällig mit einer beliebige EXE-Datei verschmelzen lässt.

Vor Experimenten mit dem Cafeini-Trojaner warnen wir besonders: er verfügt über ein undokumentiertes „Feature“: Vertrauliche Informationen werden unaufgefordert vom Cafeini-Server zu einer polnischen E-Mail-Adresse geschickt. Darüber hinaus werden von einem polnischen Webserver EXE-Dateien heruntergeladen – und ausgeführt. Der Trojaner ist also selbst trojanisiert.

Viele Benutzer fühlen sich bezüglich Trojaner-Attacken sicher, weil sie Antiviruslösungen oder Personal Firewalls im Einsatz haben. Leider identifizieren Antiviruslösungen nur altbekannte Trojaner. Personal Firewalls sorgen dafür, dass Installierte Applikationen nur über definierte Ports kommunizieren dürfen (z.B. ist Outlook nur der Zugriff auf Port 110 (POP-3) und 25 (SMTP) gestattet). Um Zugriff auf das Internet zu erhalten, führen Trojaner Personal Firewalls oft aufs Glatteis, und nennen ihre aktiven Prozesse einfach Outlook.exe. Besonders kritisch ist, wenn Personal Firewalls automatisch auf Angriffe reagieren[ii]

6) „Knacken“ von Domino-Servern[iii]

Viele Unternehmen setzen Lotus Domino als Webserver ein. Zum Domino-Server sind im letzten Jahr zahllose Sicherheitslücken (Buffer Overruns, D.o.S, etc.) bekannt geworden, die wir allerdings nicht demonstrieren. Default-Installationen des Domino-Servers sind schon seit Jahren mit Fehlern versehen: Domino-Datenbanken wie names.nsf, catalog.nsf oder log.nsf sind oft von jedermann lesbar. Wir zeigen, wie man durch die Eingabe einer einfachen URL an vertrauliche Notes-Datenbanken gelangen kann; zum Beispiel, wie man auf das Mitarbeiteradressbuch der „Opera Australia“ zugreift (die Sicherheitslücke wurde vor Veröffentlichung dieses Papers behoben.):



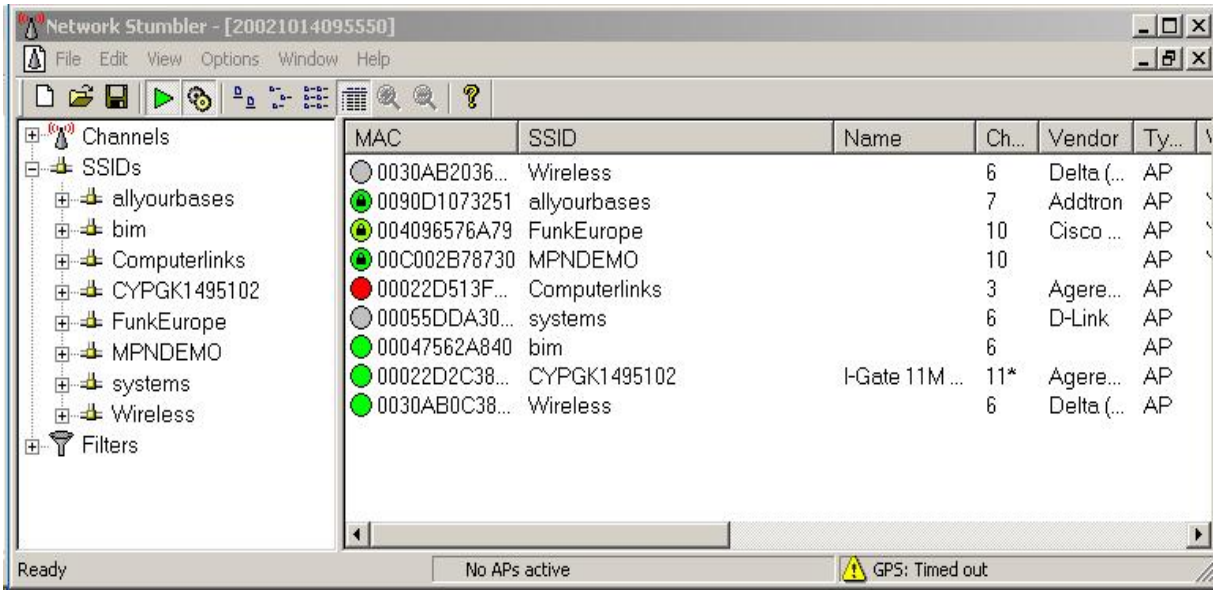
Auf der Webseite der Opera Australia ist das IBM-Logo zu sehen – scheinbar liegt ein Sponsoring vor. Ob der Server auch von IBM gewartet wird, ist unbekannt.

7) D.o.S. gegen Windows 2000 und Windows XP (***)

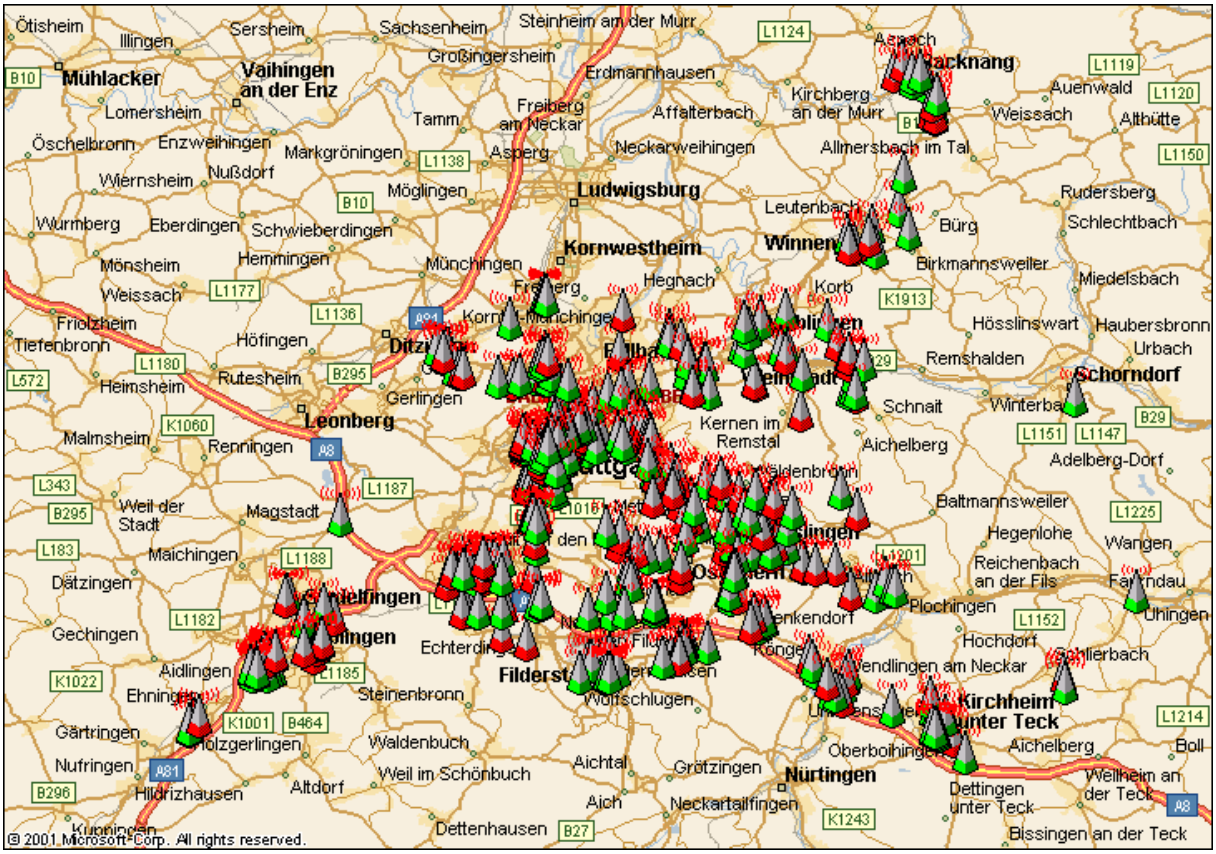
Unter D.o.S.-Attacken (Denial-of-Sevice) versteht man Angriffe auf die Verfügbarkeit eines Systems. Der Angreifer bringt das System zum Absturz oder sorgt dafür, dass sämtliche Ressourcen aufgezehrt werden. Im Internet existieren eine Vielzahl kleiner Programme, mit deren Hilfe man Applikationsserver oder sogar das darunterliegende Betriebssystem zum Absturz bringen kann. Manche Attacken basieren auf fragmentierten Paketen – andere rufen durch unerwartete Eingaben einen Buffer-Overrun hervor – wieder andere legen mit geschickt formatierten Mails den Mailclient des Benutzers lahm. Es wird gezeigt, wie das Linux-Programm Smbnuke aktuelle Versionen von Windows 2000 oder Windows XP zum Absturz bringt.

8) Attacken auf WLAN

WLANs sind komfortabel und preisgünstig; teilweise werden „wilde“ WLANS ohne Wissen der IT-Abteilung installiert. Es wird gezeigt, wie WLANs identifiziert werden und welche Schwächen gängige Schutzmassnahmen aufweisen. Mit einer Spezialantenne von Cisco werden eine große Reichweite und eine hohe Empfangsleistung sichergestellt.



Fährt man mit einem KFZ und einer entsprechenden Ausrüstung nur wenige Kilometer durch München, identifiziert man Duzende von WLANs - von denen ca. ein Drittel völlig ungeschützt ist.
Hier eine durch SySS erstellte Landkarte mit geschützten und ungeschützten WLANs im Großraum Stuttgart

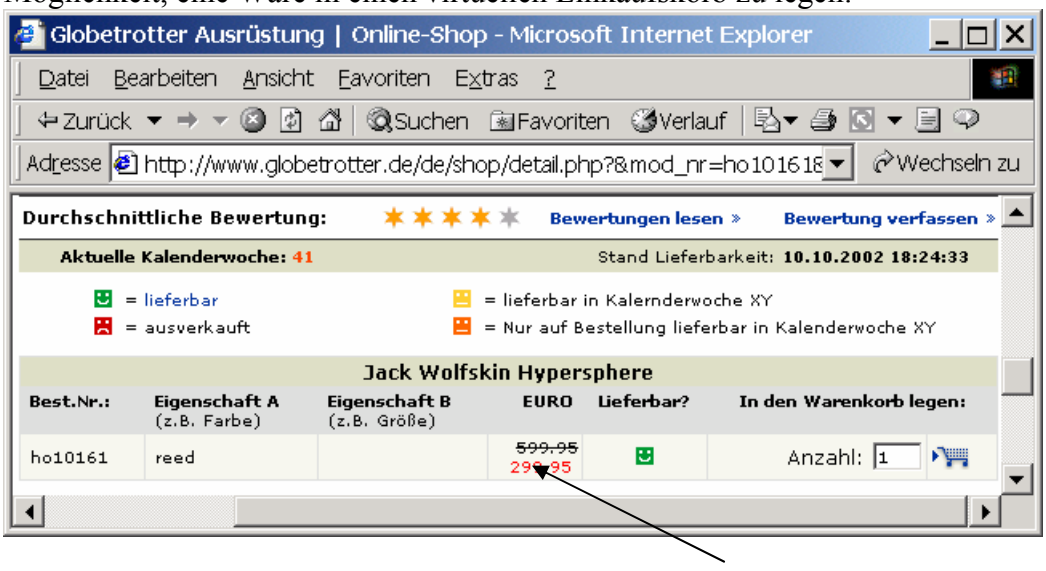


9) Attacken auf Webshops[iv] (***)

Angriffe auf Web-Applikationen sind von Natur aus anspruchsvoll; da es sich meist um Individuallösungen handelt, ist Erfahrung und Phantasie gefragt. Automatisierte Scanner sind nicht geeignet, solche Applikationen zu testen. Es zeigt sich, dass die Entwickler der Weblösungen oftmals viel zu wenig Augenmerk auf IT-Security legen. Oft lassen sich fremde

Sitzungen übernehmen („Session Hijacking“) oder unter Anwendung von Meta-Charakter Attacks Verzeichnisse ausspähen.
Auf dem Markt verfügbare Webserver (Apache, IIS, Domino, IPlanet, Websphere etc.) haben oft selbst Schwächen oder sind unzureichend konfiguriert.
Es wird demonstriert, wie Warenkorbkonzepte ausgehebelt werden - durch eigene Techniken funktioniert dies sogar bei SSL/HTTPS-Verbindungen:

Der naivste und - aus der Perspektive eines Angreifers erfolgsversprechendste - Fehler besteht darin, dass den Eingabedaten des Anwenders blind vertraut wird. Hierfür ein Beispiel aus der Praxis, dessen Verständnis Grundkenntnisse von HTTP voraussetzt. Ein Kunde einer Online-Bank kann verschiedene Konten verwalten. Jedes Konto wird durch eine eindeutige Konto-Nummer identifiziert. Meldet sich der Kunde über Web bei seiner Bank an, so werden ihm die Namen und Nummern seiner Konten aufgelistet. Per Mausklick kann der Kunde eines seiner Konten auswählen, zu dem ihm dann Details angezeigt werden. Beim Klick auf eines der Konten, wird per HTTP einfach die Kontonummer des Kontos zur Bank geschickt. Arbeitet der Kunde mit einem gewöhnlichen Webbrowser, so ist es ihm nicht möglich, Zugriff auf ein fremdes Konto zu erlangen. Modifiziert ein böswilliger Kunde aber die HTTP-Kommunikation, so ist er in der Lage, eine fremde Kontonummer zur Bank zu schicken - und erhält so Zugriff auf ein fremdes Konto. Voraussetzung ist eine schlampig erstellt Webapplikation, bei der die Auswahl des Anwenders nicht überprüft wird. Das leider nur selten befolgte Paradigma lautet: "*Never trust input data*". Hier ein weiteres Beispiel, wie Ladendiebe in Webshops einbrechen. Eins ist bei jedem Webshop gleich: der Kunde hat die Möglichkeit, eine Ware in einen virtuellen Einkaufskorb zu legen:



Bei der Analyse dreier Webshops wurde festgestellt, dass beim Klick auf den Button mit der Bedeutung "diesen Gegenstand in den Einkaufskorb legen" nicht nur die Produkt-ID, sondern auch der Preis vom Anwender zum Webserver geschickt wird. Beim führenden Outdoor-Versender Globetrotter (www.globetrotter.de) sieht das etwa so aus:

```
POST /de/cart/cart.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/msword, application/vnd.ms-
powerpoint, */*
Referer:
http://www.globetrotter.de/de/shop/detail.php?&mod_nr=ho10161&artbez=Jack+W
olfskin+Hypersphere&k_id=06&h_kat=Zelte%2C+Campingm%F6bel
Accept-Language: de,en-us;q=0.5
Content-Type: application/x-www-form-urlencoded
```

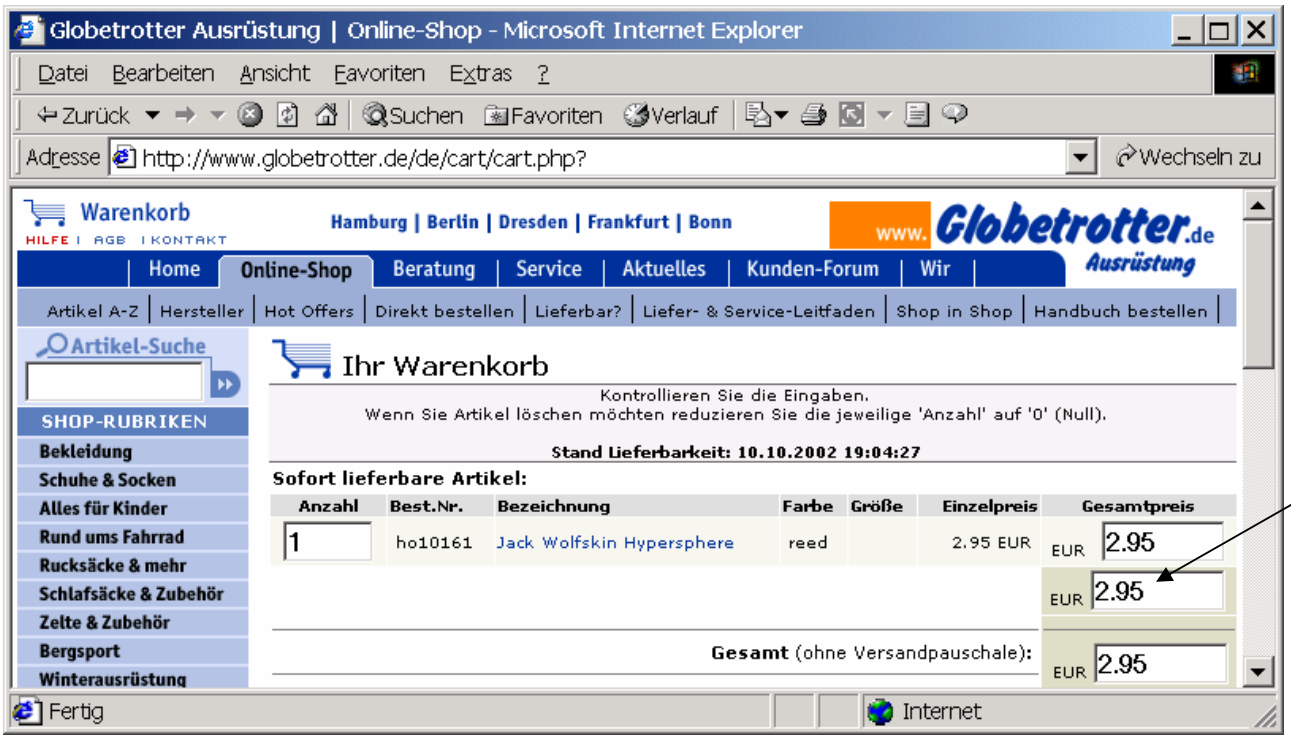
```
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: www.globetrotter.de
Content-Length: 256
Connection: Keep-Alive
Cache-Control: no-cache

amount=1&mod_nr=ho10161&art_nr=ho10161&artbez=Jack+Wolfskin+Hypersphere&vpr
eis=299.95&farbe=reed&groesse=&l_status=0&mwst=2&rabatt=&detail=1&follow_pa
ge=%2Fde%2Fcart%2Fcart.php%3F&cart_type=globe&put=1&In+den+Warenkorb+legen.
x=19&In+den+Warenkorb+legen.y=7GET /media/korrektur.gif HTTP/1.1
```

Zu sehen ist also, wie ein Produkt (genauer: ein Zelt zu 299,95 Euro) in den Warenkorb gelegt wird. In einer simulierten Attacke wurde die HTTP-Anfrage wie folgt modifiziert:

```
amount=1&mod_nr=ho10161&art_nr=ho10161&artbez=Jack+Wolfskin+Hypersphere&vpr
eis=2.95&farbe=reed&groesse=&l_status=0&mwst=2&rabatt=&detail=1&follow_page
=%2Fde%2Fcart%2Fcart.php%3F&cart_type=globe&put=1&In+den+Warenkorb+legen.x=
19&In+den+Warenkorb+legen.y=7GET /media/korrektur.gif HTTP/1.1
```

Wie unschwer zu erkennen ist, wurde die Anfrage nur in einem Punkt verändert: der Preis beträgt nun nicht mehr 299,95 Euro - sondern nur noch 2,95 Euro. Ein Blick in den Einkaufskorb beweist, dass das Täuschungsmanöver erfolgreich ist.



Bei Sicherheitsüberprüfungen - auch im Banken und Finanzsektor - zeigt sich, dass ein Großteil der Webapplikationen anfällig gegen solche Manipulationen ist. (Anm.: Der Webshop-Betreiber wurde vor Veröffentlichung dieses Artikels auf die Schwäche aufmerksam gemacht und hat sie mittlerweile behoben.)

10) Fazit und Ausblick

Laut der Statistik des CERT (www.cert.org) werden pro Tag etwa 12 neue Sicherheitsschwächen in Softwareprodukten bekannt. Täglich knacken meist jugendliche Täter Dutzende von Webserver und manipulieren deren Inhalte. Softwarehersteller befriedigen die nimmersatte Nachfrage von Kunden, indem sie neue Features – und damit oft auch neue Sicherheitslücken – in ihre Software einbauen. Und hat man sein Betriebssystem endlich so gut im Griff, dass man glaubt, sicher zu sein – dann wird es wohl in den nächsten Tagen obsolet und durch ein neues ersetzt.
Eins wird klar: die Gefahr durch Hackerattacken ist aktuell wie nie zuvor.

Dipl. Inform. Sebastian Schreiber ist Gründer und Geschäftsführer der SySS und unter schreiber@SySS.de zu erreichen.

---

[i] Siehe auch „*Security-Tipp*“ Network World 09/2002, von Sebastian Schreiber.
[ii] Siehe „*Gefährliche Blockade*“, C’t 26/2001 von Sebastian Schreiber und Jürgen Schmidt, http://www.heise.de/ct/01/26/038
[iii] Siehe „*Keine harte Nuss*", Notes Magazin 1/2002 von Sebastian Schreiber
[iv] Siehe „*Virtueller Ladendiebstahl*“ C’t 26/2002, S.92f von Sebastian Schreiber