



MAX-PLANCK-GESELLSCHAFT

## Aktuelle Entwicklungen der IT-Sicherheit

Prof. Dr. Rainer W. Gerling  
Datenschutzbeauftragter der MPG

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

1



MAX-PLANCK-GESELLSCHAFT

## Was ist IT-Sicherheit?

- IT-Sicherheit ist ...  
... „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
  1. in informationstechnischen Systemen oder Komponenten oder
  2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.“

BSI-G § 2 Abs. 2

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

2



MAX-PLANCK-GESellschaft

## Patch-Management

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

3



MAX-PLANCK-GESellschaft

## Automated Web Patrol with Strider HoneyMonkeys

	Zahl der URLs	Zahl der Sites
• Total	752	287
• WinXP SP1 Unpatched	688	270
• WinXP SP2 Unpatched	204	115
• WinXP SP2 Partially Patched	17	10
• WinXP SP2 Fully Patched	0	0

	Zahl der URLs
• Total	752
• In Google Suchergebnissen	102 (13.6%)
• In Yahoo Suchergebnissen	100 (13.3%)

- Im Juli 2005 wurde der erste Zero-Day-Exploit entdeckt
- Erkenntnisse, dass die Web-Seiten Ihre Angriffe auf neue (bessere) Exploits updaten
- Quelle: <http://research.microsoft.com/HoneyMonkey/>

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

4



MAX-PLANCK-GESELLSCHAFT

## Sicherheitslücken aktueller Betriebssysteme

- Alle Betriebssysteme haben Sicherheitslücken!
  - OpenSource oder ClosedSource macht da keinen Unterschied
- Sicherheitssoftware hat Sicherheitslücken!
- Die breite Masse der Sicherheitslücken hat mit Pufferüberläufen zu tun
  - Der erste Pufferüberlauf war der Morris-Wurm am 2. November 1988  
(Pufferüberlauf im fingerd unter DEC/VAX mit BSD und SUN)
- Sobald Sicherheitslücken bekannt werden, müssen sie korrigiert (gepatcht) werden.
  - Schadsoftware, die die Sicherheitslücken ausnutzt, ist binnen Stunden verfügbar

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

5



MAX-PLANCK-GESELLSCHAFT

## Was muss getan werden?

- Zeitnahes einspielen der Updates ist unbedingt erforderlich
  - Test in einer Testumgebung vor dem Verteilen (muss schnell gehen)
- Alle Windows Klienten über WSUS
  - Microsoft Anwendungen wo immer möglich über WSUS
  - Alle Anderen Anwendungen über Softwareverteilung/Anwendungsmechanismen
- Linux/Unix über Distributionsspezifische Mechanismen
- Alle auf Servern exponierten Anwendungen (Login-Server, Web-Server, Name-Server usw.) müssen individuell aktualisiert werden.
- Updates wann immer verfügbar
- Virens Scanner: Mit den eigenen Mechanismen wann immer verfügbar
  - Klienten: mindestens alle zwei Stunden
  - Mail-Server, Web-Proxy: Bei Verfügbarkeit; mindestens alle 30 Minuten
- Mailing-Listen der Hersteller bzw. der Sicherheitsanbieter abonnieren
  - Z.B <http://www.heise.de/security>

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

6



MAX-PLANCK-GESELLSCHAFT

## P2P-Software/Skype

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

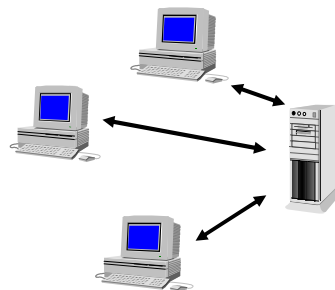
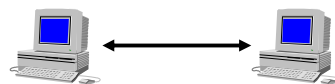
7



MAX-PLANCK-GESELLSCHAFT

## Filetransfer


- Klassischer Filetransfer zwischen zwei Rechnern
- Filetransfer zwischen einem Klienten und einem Server
  - ftp-Server
  - http-Server



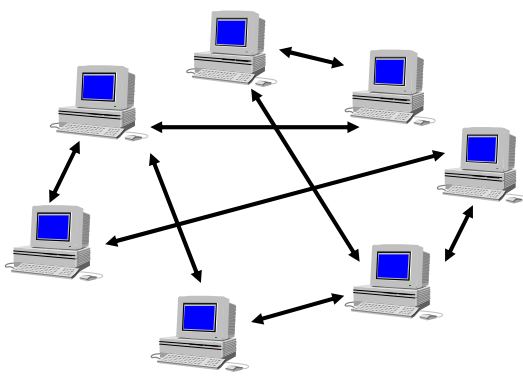
Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

8


  
MAX-PLANCK-GESELLSCHAFT

## Peer2Peer (P2P)



- Jeder Rechner ist Klient und Server
- Die Datei ist nirgends komplett
- Jeder hat nur Fragmente
  - Er lädt was ihm fehlt
  - Er bietet an was er hat
- Es werden Standard Protokolle benutzt


Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 9

  
MAX-PLANCK-GESELLSCHAFT

## P2P

- Typische Vertreter
  - KaZaA, Napster, Gnutella, Edonkey2000, Napigator, Limewire, Bearshare, WinMX, Aimster, Morpheus, BitTorrent, Emule, 1-Click Player
  - Napster war nur für den Austausch von MP3-Dateien gedacht.
  - BitTorrent z.B. für CD-Images (Linux, Knoppix)
  - Wie geht man damit im Unternehmen um?

Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 10




MAX-PLANCK-GESELLSCHAFT

## Skype

- P2P Internet Telefonie
  - Windows, Macintosh, Linux, PocketPC
  - SkypeOut: Telefonie ins Telefonnetz
  - SkypeIn: Telefonnumemr im Festnetz
  - Dateitansfer ist möglich
  - Klient kann Supernode werden und ist dann Server für andere
  - Wurde gerade an eBay verkauft!!!
- Wie geht man im Unternehmen damit um?

Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 11



MAX-PLANCK-GESELLSCHAFT

## Skype

- Blocken in der Firewall ist schwierig
  - Nutzt http/https
  - Nur Inhaltsfilter können das
- Inhaltskontrollen zwecklos
  - Verschlüsseltes Protokoll
  - Protokoll nicht dokumentiert

Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 12



MAX-PLANCK-GESELLSCHAFT

## JAP Anon Proxy

- **Datenschutztool**
  - Uni Dresden (Prof. Dr. Hannes Federrath)
  - Unabhängiges Landeszentrum für Datenschutz
- Mit **JAP** ist es möglich, anonym und unbeobachtbar im Internet zu surfen.
  - „Mit Hilfe der neuen AN.ON-Peer-To-Peer-Forwarding-Technologie können JAP-Nutzer nun eine bestimmte Bandbreite ihrer anonymen Internetverbindung für andere Internetsurfer freigeben und damit ihren Beitrag zur Freiheit des World Wide Web leisten.“

Der Datenschutzbeauftragte

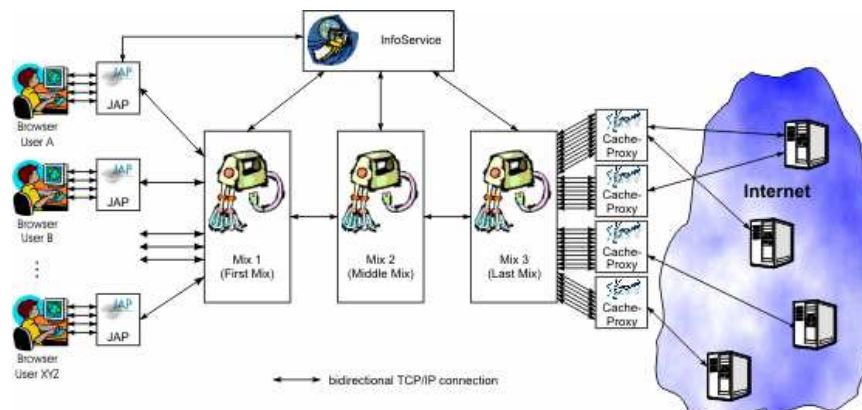
Aktuelle Entwicklungen der IT-Sicherheit

13



MAX-PLANCK-GESELLSCHAFT

## MIXe



Quelle: TU Dresden

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

14



MAX-PLANCK-GESellschaft

## JAP Anon Proxy

- **JAP** konnte gut geblockt werden, da Adressen der MIXe bekannt sind.
  - Mit der P2P Funktionalität ist blocken schwierig
    - Blockade der Infoserver
- Web-Seiten können Zugriffe über **JAP** blocken.
- Muss ich als Datenschützer gegen **JAP** sein?
  - Mitarbeiter umgehen Blockade von Web-Seiten mit Hilfe von **JAP**

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

15



MAX-PLANCK-GESellschaft

## Bot-Nets

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

16





MAX-PLANCK-GESELLSCHAFT

## Was sind Botnets?

- **Botnet** ist ein Fachausdruck für eine Sammlung von Softwarekomponenten, oder Bots, die autonom laufen. Der Besitzer des Botnets kann die Gruppe aus der Ferne administrieren. Gewöhnlich durch IRC, oder auch andere unauffällige Mechanismen.

Der Datenschutzbeauftragte

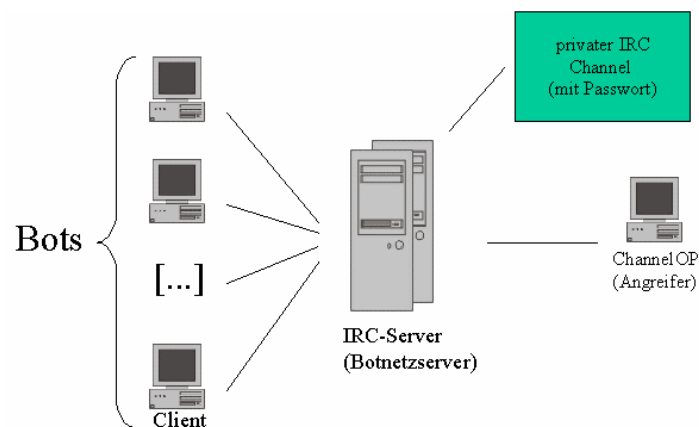
Aktuelle Entwicklungen der IT-Sicherheit

17



MAX-PLANCK-GESELLSCHAFT

## Was sind Botnets?



Quelle: Cert Uni Stuttgart

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

18



MAX-PLANCK-GESELLSCHAFT

## Deutsche Honeynet Projekt

- Gegenwärtig Benutzung von nur drei Sensoren
- Quantitative Ergebnisse (November 2004 Februar 2005):
  - Mehr als 150 Botnets
  - Mehr als 230.000 verschiedene IP-Adressen
  - Typische Größe einige Hundert bis 50.000 Rechner
  - Mehr als 320 DDoS-Angriffe
- Mehr als 80% des Angriffe auf Ports 445, 139, 137, 135.

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

19



MAX-PLANCK-GESELLSCHAFT


## Was tut man damit?

- Vermieten
  - DDoS Angriffe
  - Spammen
- Datenverkehr belauschen
- Keylogger
- Phishing
- ....

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

20



MAX-PLANCK-GESELLSCHAFT

# Phishing, Viren & Co.

Der Datenschutzbeauftragte
Aktuelle Entwicklungen der IT-Sicherheit
21



MAX-PLANCK-GESELLSCHAFT

# Sober-Wurm



**FUSSBALL-WM 2006**

**Computerwurm gaukelt Fans WM-Karten vor**

Experten warnen vor einem gefährlichen Computerwurm, der dem Empfänger vorgaukelt, Karten für die Fußball-WM gewonnen zu haben. Die verdächtige Post tarnt sich als offizielle Nachricht des Weltfußballverbands FIFA, enthält aber eine Form des Sober-Wurms. [mehr]

► Thema WM 2006



**WM Ticket Verlosung - Nachricht (Plain Text)**

Von: FIFA@ok2006.de  
 An: [redacted]  
 Cc: [redacted]  
 Betreff: WM Ticket Verlosung

Herzlichen Glueckwunsch,

beim Run auf die begehrten Tickets für die 64 Spiele der Weltmeisterschaft 2006 in Deutschland sind Sie dabei. Weitere Details ihrer Daten entnehmen Sie bitte dem Anhang.

Ihr "ok2006" Team

--- FIFA-Presskontakt:  
 --- Pressesprecher [redacted]  
 --- FIFA Fussball-Weltmeisterschaft 2006  
 --- Organisationskomitee Deutschland  
 --- [redacted]

okTicketInfo.zip (52KB)

Der Datenschutzbeauftragte
Aktuelle Entwicklungen der IT-Sicherheit
22



## E-Mail

(Quelle: PC-Welt)

MAX-PLANCK-GESELLSCHAFT

Sehr geehrter Sparkassen Kunde,  
wie sie vielleicht in den letzten Wochen und Monaten mitbekommen haben werden Deutsche Online Banken immer häufiger Opfer von sogenannten "Hoax-Attacken", dies bedeutet das fremde Personen versuchen die notwendigen Bankdaten(Kontonummer,pin usw.) über Viren, Keylogger oder Trojaner zu erhalten.  
Leider müssen wir Ihnen mitteilen das seit 2 Tagen auch die bundesweiten Sparkassen Opfer dieser Attacken wurden und bereits mehrere Benutzer einen Verlust einer großen Geldmenge hinnehmen mußten,wir bedauern dies aufrichtig. Wir sind verpflichtet alles was in unsere Macht steht zu tun um Ihre Sicherheit zu gewährleisten.  
Mit dieser Email möchten wir nun Ihre Kontoinformation überprüfen und damit bestätigen das Sie und nicht eine dritte Person Zugang zu ihrem Konto haben. Wir bitten um Ihr Verständnis das dies eine reine Vorsichtsmaßnahme ist und nur zu Ihrer Sicherheit beitragen wird. Bitte besuchen Sie unsere neu eingerichtete Sicherheitsseite zur Prävention(Vorbeugung) von Online Betrug.  
Außerdem werden wir von Ihnen 2 Tan nummer anfordern Diese beiden Tan nummern dienen als Schutz vor unbefugten Überweisungen dritter Personen.Sollte eine Ihrer nächsten beiden Überweisungen nicht mit den angegebenen Tan nummern durchgeführt werden,wird Ihr Konto blockiert und es werden keine Zahlungen mehr angenommen bzw. überwiesen da sich hiermit für uns der Verdacht bestätigen würde das eine dritte unbefugte Person Online Zugang zu Ihrem Konto hat. Wir bitten Sie deshalb die beiden von Ihnen angegebenen Tan nummern bei Ihren nächsten beiden Online Überweisungen aus dem oben genannten Grund zu verwenden.  
Nochmals vielmals um Entschuldigung für diese Unregelmäßigkeit und bedanken uns im Voraus für Ihre Kooperation. Alle Daten werden verschlüsselt gesendet und vertraulich behandelt.  
Nachdem Sie die erforderlichen Informationen an unseren Server übermittelt haben, wird ein Mitarbeiter die Daten überprüfen und sich mit Ihnen im Falle von Unregelmäßigkeiten oder Unklarheiten in den nächsten 24-48 Stunden telefonisch oder per E-mail in Verbindung setzen.  
Notieren Sie sich bitte folgende Nummer: 0847264817640  
Dies ist ihre persönlichen Sicherheitsidentifikations Nummer ,die Sie in Zukunft nutzen sollten um schnellstmöglichen Service per Email oder Telefon zu erhalten.  
Wichtig: Sollte ein Mitarbeiter Ihrer örtlichen Sparkasse Sie bereits telefonisch kontaktiert haben, können Sie diese E-mail ignorieren  
Vielen Dank  
Ihr Sparkassen Team

Der Datenschutzbeauftragte
Aktuelle Entwicklungen der IT-Sicherheit
23



## Die zugehörige Web-Seite

(Quelle: PC-Welt)

MAX-PLANCK-GESELLSCHAFT




Willkommen beim Online-Banking

**Überprüfung Ihrer Homebanking Daten.** Sie haben die Hilfe Seite der Sparkasse aufgerufen. Geben Sie bitte Ihre Kontonummer,BLZ,PIN und 2 Tan Nummern ein. Sie werden innerhalb der nächsten 24 Stunden von einem Sparkassen Mitarbeiter kontaktiert.

Ihre Zugangsdaten:

\* Konto-Nr.:

\* BLZ:

\* PIN:

\* TAN1:

\* TAN2:

Hiermit bestätige ich, dass ich die nachfolgenden Hinweise zur Kenntnis genommen habe und akzeptiere:

- ▶ Nutzungsbedingungen
- ▶ Sicherheitshinweis

Der Datenschutzbeauftragte
Aktuelle Entwicklungen der IT-Sicherheit
24



MAX-PLANCK-GESELLSCHAFT

## Netzkonfiguration

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

25



MAX-PLANCK-GESELLSCHAFT

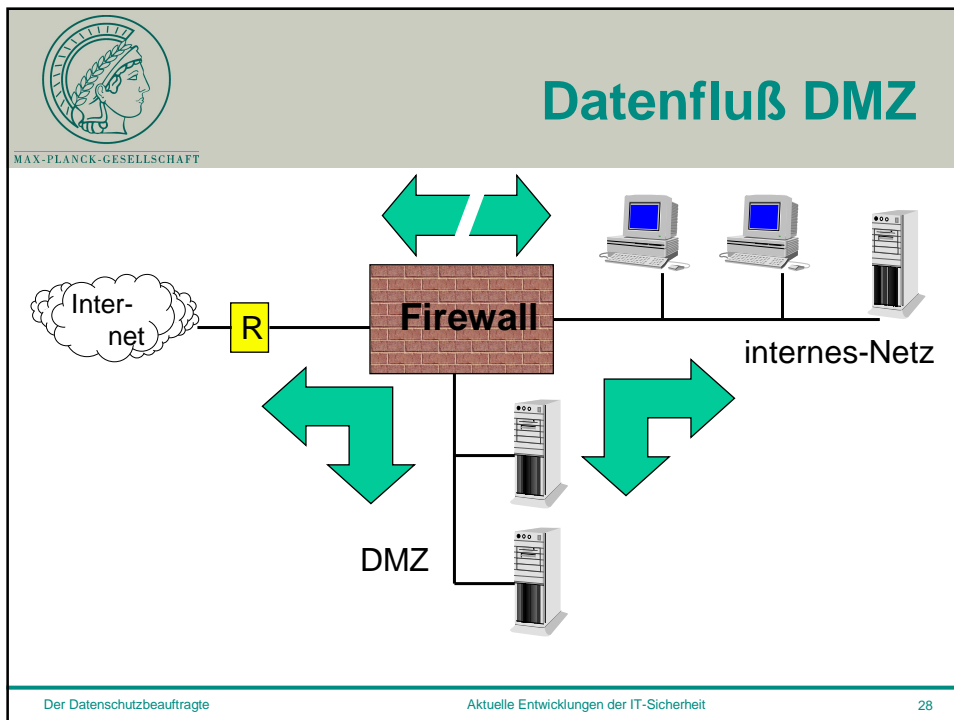
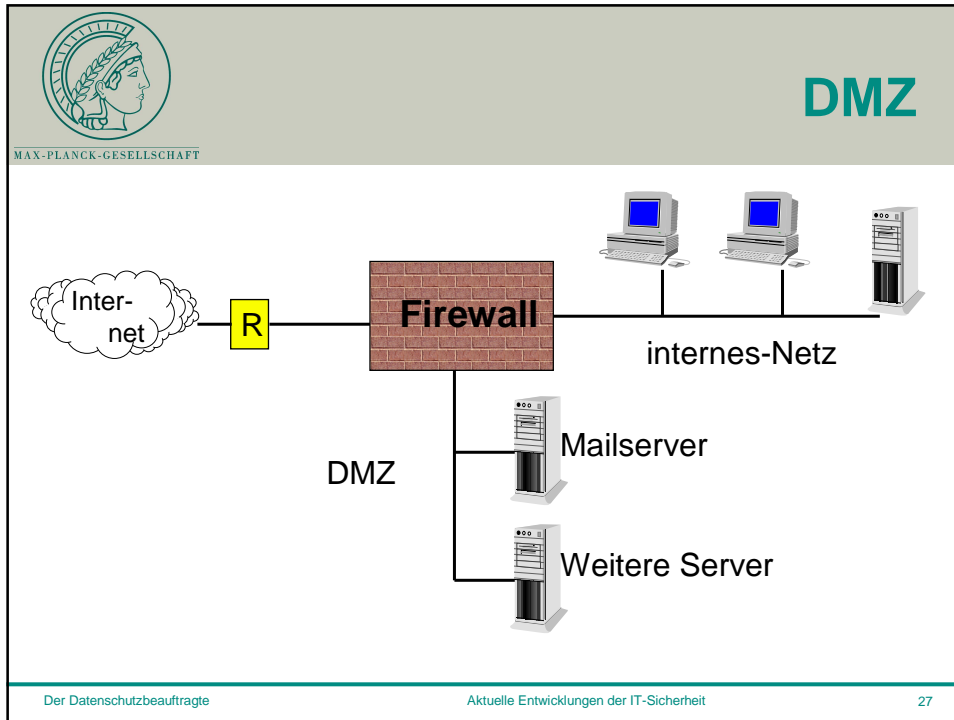
## Grundregeln

- Alles was nicht verboten ist, ist erlaubt
  - d.h. unerwünschte und gefährliche Ports werden gesperrt, der Rest ist offen
  - Die Firewall erst offen betreiben und dann langsam „zudrehen“
- Alles was nicht erlaubt ist, ist verboten
  - Einige Dienste werden explizit erlaubt, dann kommt das große Deny-Statement

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

26





## Was wird gesperrt?

MAX-PLANCK-GESELLSCHAFT

- Alles, was nicht benötigt wird!
- Ausgehend:
  - http, https für alle
  - smtp für den Mailserver  
(bei externem Mailserver: alle auf Mailserver)
- Eingehend:
  - smtp zum Mailserver
  - http, https zum Webserver

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

29



## Check Point Firewall 1

MAX-PLANCK-GESELLSCHAFT

local - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - VPN | Address Translation - VPN | Bandwidth Policy - VPN | Compression Policy - VPN

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Name-Server	Any	dns	accept		Gateways	Any	Nur interner DNS-Server darf DNS-Anfragen nach außen machen
	Any	SAP-Server	SAP	accept		Gateways	Any	SAP-Fernwartung wird bei Bedarf freigeschaltet
3	Any	E-Mail-Server	smtp	accept		Gateways	Any	
4	E-Mail-Server	Any	smtp	accept		Gateways	Any	
5	Local_Net	Any	http https	accept		Gateways	Any	
6	Any	Intranet-Server	https	accept	Short	Gateways	Any	
7	Any	Login-Server	SSH	accept	Short	Gateways	Any	
8	Any	Any	Any	drop	Log	Gateways	Any	Der gesamte Restverkehr ist verboten

For Help, press F1

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

30



MAX-PLANCK-GESELLSCHAFT

## Verschlüsselung

- Darf man verschlüsselte Informationen durch eine Firewall lassen?
  - **Kein Inhaltsfilterung und Kontrolle**
  - IPsec, pptp, https, ssh, PGP
- Verschlüsselungs-Gateway mit Kontrolle nötig
  - Ersetzt fehlende Kontrolle der Firewall
  - eventuell auf der Firewall

Der Datenschutzbeauftragte

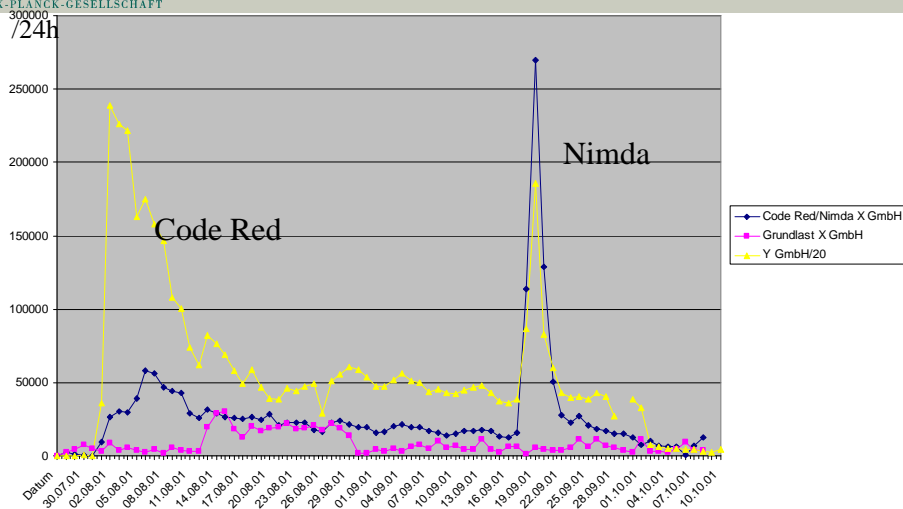
Aktuelle Entwicklungen der IT-Sicherheit

31



MAX-PLANCK-GESELLSCHAFT

## Code Red und Nimda



Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

32





MAX-PLANCK-GESELLSCHAFT

## Zugriffe ins Firmen-Netzwerk

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

33



MAX-PLANCK-GESELLSCHAFT

## Beispiel: Web-Portal

- Zugriff nur über https
- Möglichst nur Standards
- Authentisierung
  - über Zertifikate
    - Softwarebasiert oder mit Chipkarten
  - Über Einmalpassworte
    - TAN-Listen oder Hardware



Quelle: Kobil

Quelle: RSA

Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

34



MAX-PLANCK-GESELLSCHAFT

## Beispiel: Netzwerkzugriff

- IPsec muss installiert und konfiguriert sein
- Authentisierung mit Passwort oder Zertifikat
- Gateway-Lösungen möglich
  - Beispiel: Cisco VPN
    - Klassisches VPN mit IPsec
    - WebVPN: Sicherer Zugriff auf interne Web-Seiten
      - VPN mit Browser als Client
    - Integration mit Firewall



Quelle: Cisco

Der Datenschutzbeauftragte

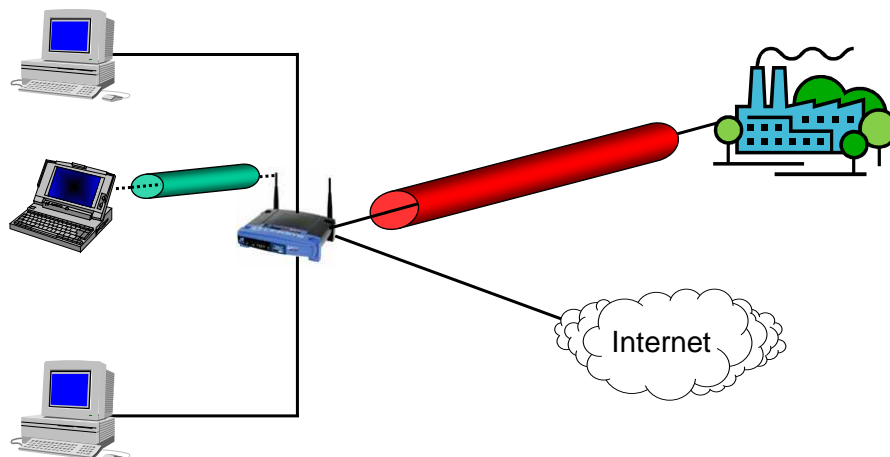
Aktuelle Entwicklungen der IT-Sicherheit

35



MAX-PLANCK-GESELLSCHAFT


## VPN-Gateway auf Router



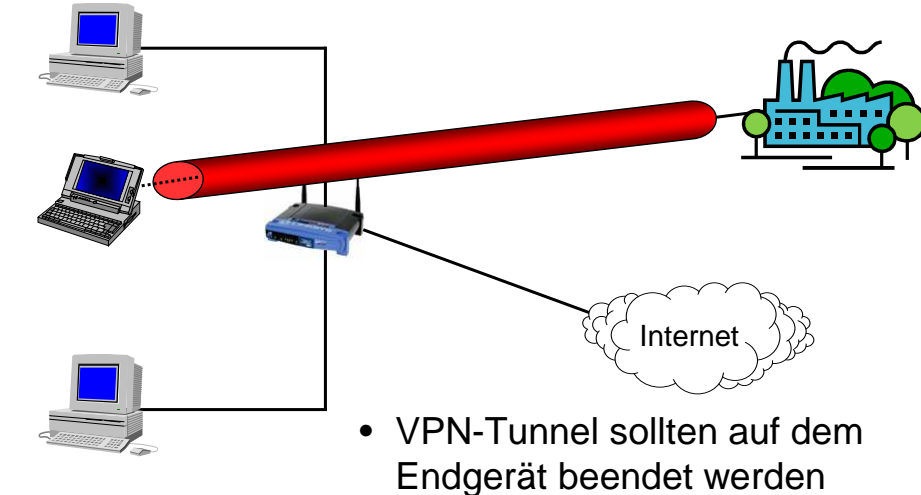
Der Datenschutzbeauftragte

Aktuelle Entwicklungen der IT-Sicherheit

36

 **VPN-Gateway auf Router**

MAX-PLANCK-GESELLSCHAFT



- VPN-Tunnel sollten auf dem Endgerät beendet werden

Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 37

 **Kontrollen**

MAX-PLANCK-GESELLSCHAFT

- E-Mail
  - Viren-Scanner, Datei-Anhänge
- Web-Portal
  - Filtern von Eingaben
  - Kontrolle des Eingehenden Datenstroms
- Netzzugang
  - Volle Kontrolle durch Firewall nach Entschlüsselung/vor Verschlüsselung

Der Datenschutzbeauftragte Aktuelle Entwicklungen der IT-Sicherheit 38