

# *Datensicherheit*

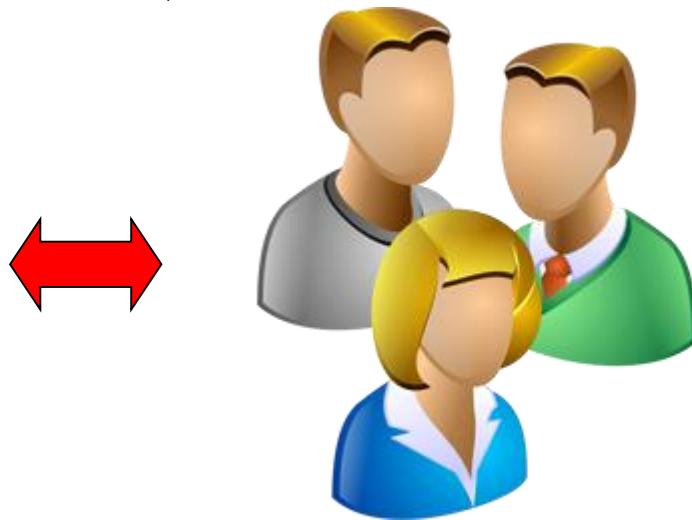
# *IT-Sicherheit*

# IT- Sicherheit und Datenschutz

*immer automatisiert*



*immer personenbezogen*



**IT Sicherheit**

**die DATEN  
müssen sicher  
sein**

**Datenschutz**

**die PERSONEN  
müssen sicher  
sein**

**IT Sicherheit:**

**Schutz von DATEN**

vor Beeinträchtigung bei der automatisierten Verarbeitung

**Datenschutz:**

**Schutz der Personen**

vor missbräuchlicher Verwendung der **personenbezogenen DATEN**  
Die Wahrung der schutzwürdigen Belange Betroffener

## Verlust der Verfügbarkeit

- IT-Systeme müssen funktionieren
  - Daten müssen verfügbar sein

## Verlust der Vertraulichkeit

- ➔ Unbefugte haben keinen Informationszugriff
  - ➔ Nur für einen beschränkten Empfängerkreis

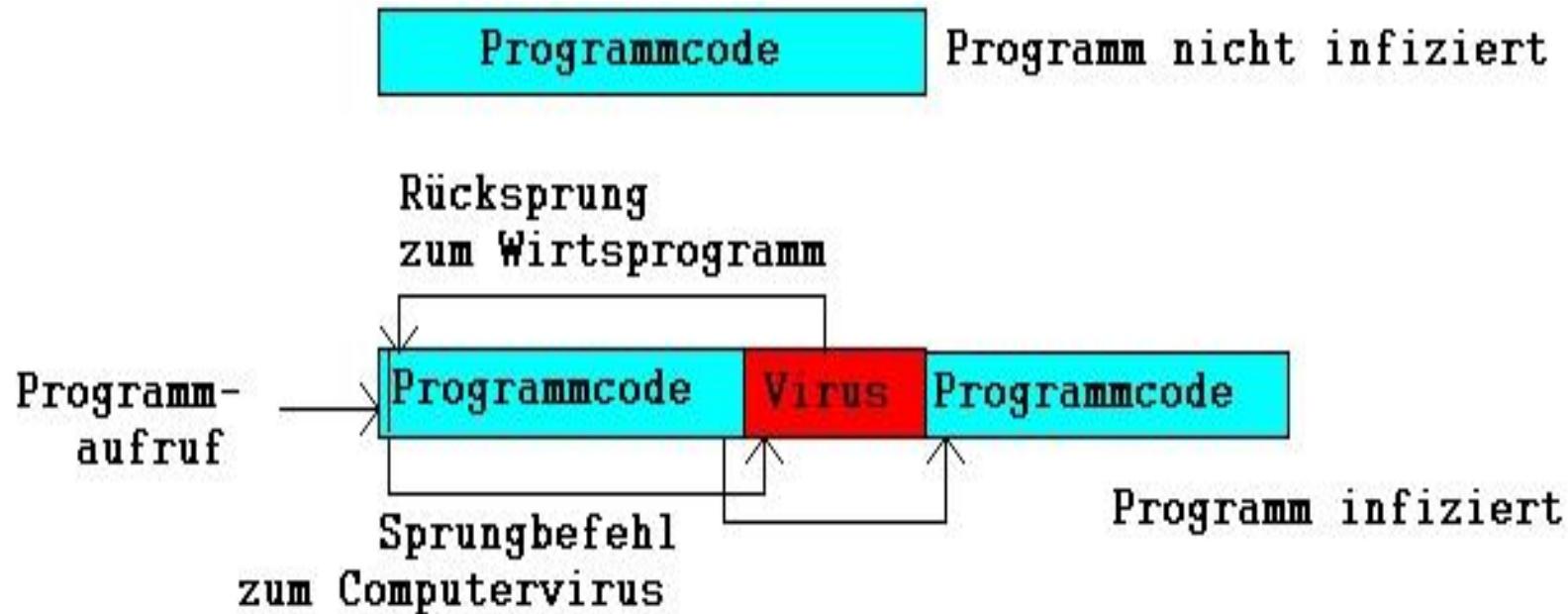
## Verlust der Integrität

- Daten sind vollständig
    - *absichtlich*
    - *unabsichtlich*
    - *technische Fehler*
  - Daten sind unverändert

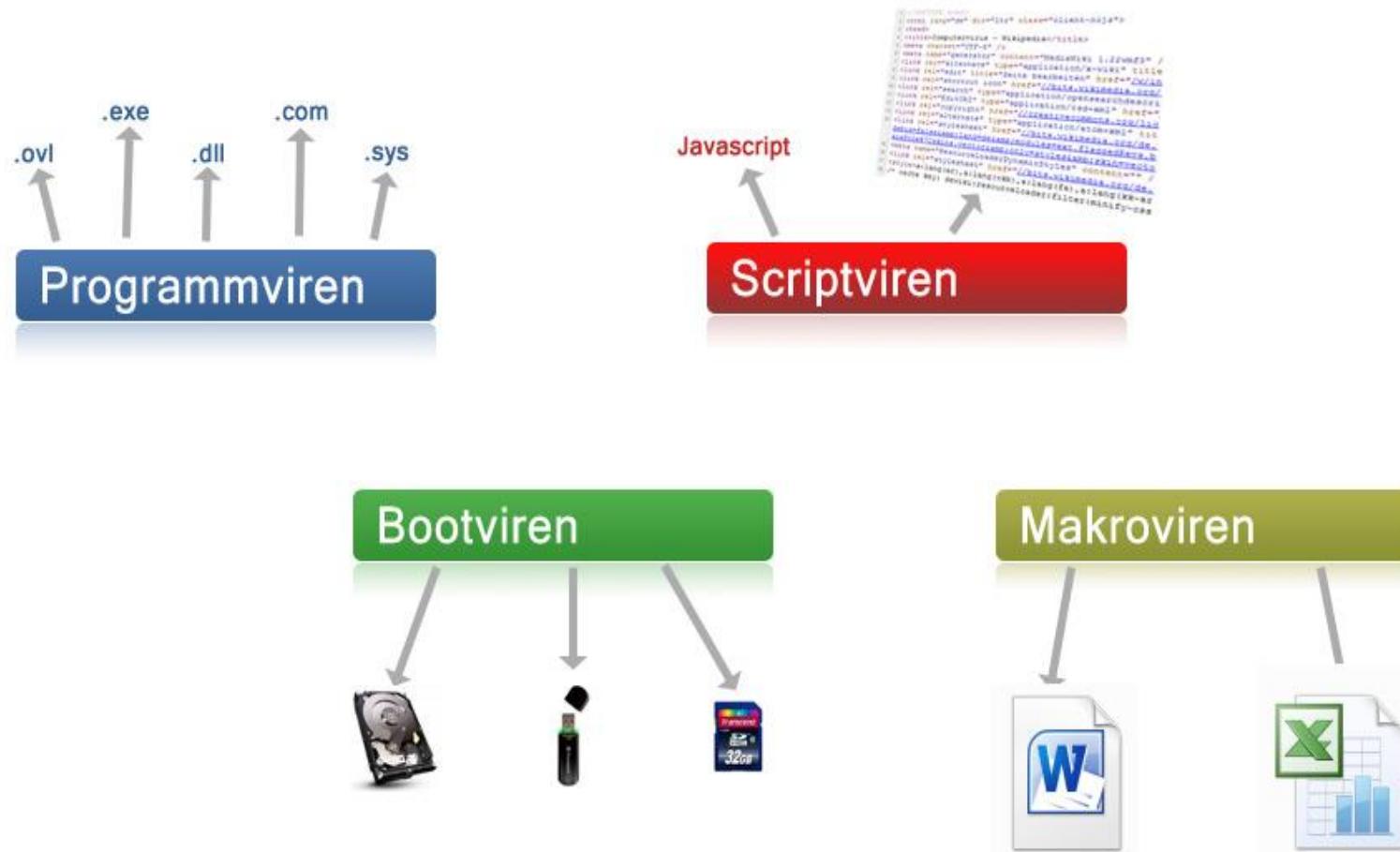
## Verlust der Authentizität

- Daten sind sicher einem Sender zuzuordnen
  - Daten sind unabstreitbar

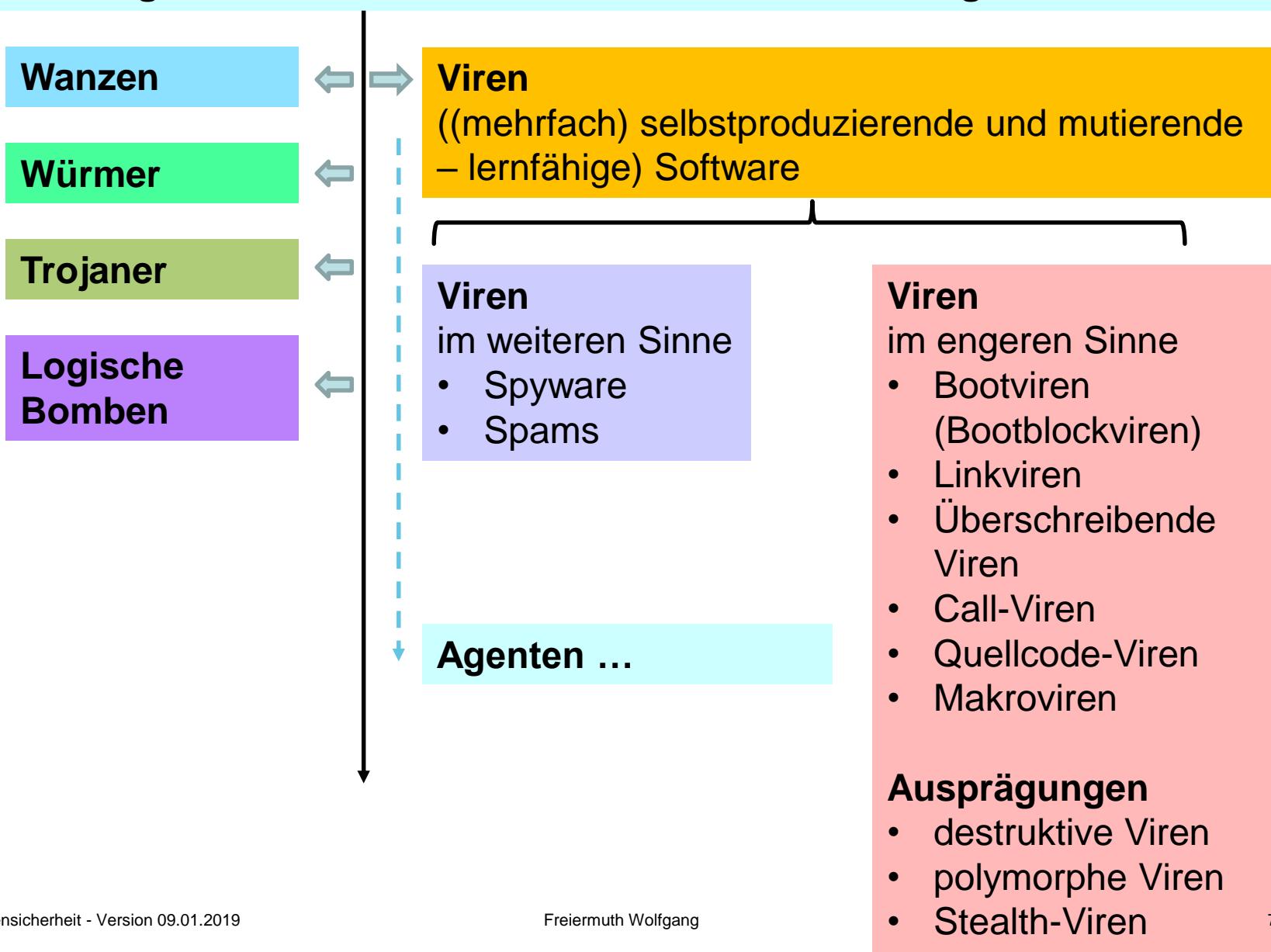
## Schädigende Software => unerwünschte Programmteile



## **Schädigende Software => unerwünschte Programmteile**



# Schädigende Software/Malware => unerwünschte Programmteile





- **malicious Software (Malware)**
- **Black Hat /White Hat, Hacker / Cracker**
- **Finanzagent Money Mule (vgl. Emule)**
- **Botnetze**
- **Spyware**
- **pornographische, gewaltverherrlichende extremistische Seiten**
- **Spam**
- **Warez, Gamez, Serialz**
- **Phishing / Pharming / Drive-by-Exploits**
- **(Werbe-) PopUp's / Windows Nachrichtendienst**
- **Abofallen**
- **Proxy, Ripper, Zero Day Exploit**
- **sonstige ungewollte Inhalte**



- malicious Software (Malware)
  - • Wanzen
    - Viren
    - Würmer
    - Trojanische Pferde, Sniffer, Keylogger, Backdoor
    - Rootkit, Bootkit, FUD „fully undetected“
    - Bomben
    - Dialer
    - sonstige Schadsoftware

# Gefahren für die IT-Sicherheit



## • Computerwanzen

- Sie können Software und Betriebssystem manipulieren.  
Auch das Umfunktionieren eines IP-Telefons in eine Wanze, das sogenannte Raumabhören, ist ein denkbare Angriffsszenario.  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi\\_voip\\_leitlinie\\_pdf.pdf?blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_voip_leitlinie_pdf.pdf?blob=publicationFile)



# Gefahren für die IT-Sicherheit



- **Viren**

- **biologisch:**

- **Erbsubstanz einer Proteinhülle**
- **benötigt Wirtszelle zur Vermehrung**
- **ändert die ursprüngliche Funktion der Wirtszelle**

- **Computer:**

- **Programmcode**
- **benötigt Wirtsprogramm zur Vermehrung**
- **ändert die ursprüngliche Funktion der befallenen Software**
- **nistet sich oft im Bootsektorenbereich ein**

# Gefahren für die IT-Sicherheit



## • Viren, polymorphe

- „**Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern.** Dazu gehört unter anderem der Austausch von Befehlssequenzen und zufallsgesteuertes Einstreuen von unsinnigen Befehlsgruppen. Diese sind in keiner Weise für das Funktionieren des Virus erforderlich. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.“

# Gefahren für die IT-Sicherheit



## • Viren, Stealth

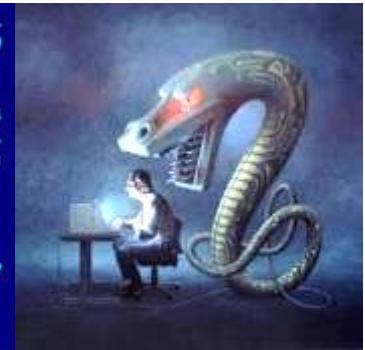
- „Stealth-Viren oder Tarnkappen-Viren besitzen spezielle Schutzmechanismen, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt werden. Sie täuschen dem Virensuchprogramm **einen nicht infizierten Zustand einer infizierten Datei vor**. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist. Einige Viren benutzen Teifunktionen von echten Stealth-Viren.“

## Gefahren für die IT-Sicherheit

### • Würmer

- Schadprogramm, gehören zu Malware, eine Virus im Netzwerk
- „kriechen“ durch Netzwerke, Wechselmedien, USB Sticks
- sind selbständig lauf- und reproduktionsfähig
- verbreitet sich im Gegensatz zu Viren **ohne** fremde Dateien (wird selbst aktiv) und infiziert auch Bootsektoren **nicht** mit seinem Code.

```
0 00 00-6D 73 62 6C          msbl
0 6A 75-73 74 20 77          ast.exe I just w
9 20 4C-4F 56 45 20          ant to say LOVE
0 62 69-6C 6C 79 20          YOU SAN!! billy
0 64 6F-20 79 6F 75          gates why do you
3 20 70-6F 73 73 69          make this possi
0 20 6D-61 6B 69 6E          ble ? Stop makin
E 64 20-66 69 78 20          g money and fix
7 61 72-65 21 21 00          your software!!
0 00 00-7F 00 00 00          à ð► H △
0 00 00-01 00 01 00          ð ð  ◉ ◉ ◉
0 00 00-00 00 00 46          á@ L F
C C9 11-9F E8 08 00          ♦ Jééù-ñññ
0 00 03-10 00 00 00          ►H ◉ à ▶
3 00 00-01 00 04 00          p v ð ◉ ◉ ◉
```



Robert T. Morris erlangte 1988 im Alter von 23 Jahren einen gewissen allgemeinen Bekanntheitsgrad durch die Programmierung des ersten Computerwurms, der sich im Internet weit ausbreitete und es nahezu komplett lahmlegte.  
Sein Vater war zu dieser Zeit Leiter des zur National Security Agency (NSA).

Morris wurde 1990 zu einer Bewährungsstrafe, 400 Stunden sozialer Arbeit und 10.000 US-Dollar Geldstrafe verurteilt.

Weiterhin trug Morris die Gerichtskosten in Höhe von etwa 150.000 US-Dollar.

Jetzt ist er Professor für Informatik am MIT.

# Gefahren für die IT-Sicherheit



## • Trojaner

- **Trojanisches Pferd, kurz Trojaner, wird ein Computerprogramm oder Skript bezeichnet, das als nützliche Anwendung getarnt ist. Im Hintergrund - aber ohne Wissen des Anwenders - eine andere Funktion erfüllt.**

Trojaner sind Schadprogramme, die vom Benutzer unbemerkt Aktionen auf dessen Computer ausführen. Zu diesen Aktionen gehören u. a.:

- Löschen von Daten
- Sperren von Daten
- Modifizieren von Daten
- Kopieren von Daten
- Beeinträchtigen der Funktionalität von Computern oder Computernetzwerken
- Im Gegensatz zu Computerviren und -würmern sind Trojaner **nicht** in der Lage, sich selbsttätig zu vervielfältigen.

# USB Keylogger

## Beschreibung

The screenshot shows a Windows desktop environment. In the center, a web browser window displays a 'Website gesperrt!' (Website blocked!) message from G Data InternetSecurity 2012. The message states: 'G Data InternetSecurity 2012 hat den Zugriff auf diese Webseite verweigert. Die Seite enthält infizierten Code.' (G Data InternetSecurity 2012 blocked access to this website. The page contains infected code.) Above the browser, a shopping cart window from 'Ihr Warenkorb' (Your shopping cart) shows 'Ihr Warenkorb ist leer!' (Your shopping cart is empty!). In the bottom right corner, a 'Virensicht' (Virus scan) window from G DATA is open, showing a scan result for 'Virus beim Laden von Web-Inhalten gefunden.' (Virus found while loading web content). The address listed is 'Adresse: http://www.spyfile.com/usb/key-logger.html' and the status is 'Der Zugriff wurde verweigert.' (Access was blocked). The desktop background features a person's face. The taskbar at the bottom shows various open applications including Internet Explorer, Microsoft Word, and Microsoft PowerPoint.

# Gefahren für die IT-Sicherheit

- Rootkit, Bootkit

## Rootkit

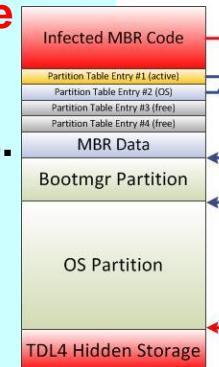
(root ist bei unixähnlichen Betriebssystemen der Benutzer mit Administrator-rechten) Eine **Sammlung von Softwarewerkzeugen**, die nach dem Einbruch in ein Softwaresystem installiert wird, um zukünftige **Logins des Eindringlings zu verbergen** und Prozesse und Dateien zu verstecken (tarnen) – auch vor dem Antivirenprogramm.

**Bootkit** ist eine Sammlung von Softwarewerkzeugen oder Bootloadern, die nach dem Einbruch in ein Computersystem installiert wird, um **weitere Sicherheitsmechanismen des Betriebssystems zu deaktivieren**.

**Ein Bootkit ist somit eine Mischung aus Bootsektorviren und Rootkits.**

Wer die Hardware bereits unter seiner Kontrolle hat, kann auch die Software unter seiner Kontrolle haben.

Eine wirksame Absicherung gegen die Ausführung von unsigniertem Programmcode wird wohl erst mit dem Einsatz von TPM-Hardware zu erreichen sein. Das Trusted Platform Module (TPM) ist ein Chip, der einen Computer oder ähnliche Geräte um grundlegende Sicherheitsfunktionen erweitert.



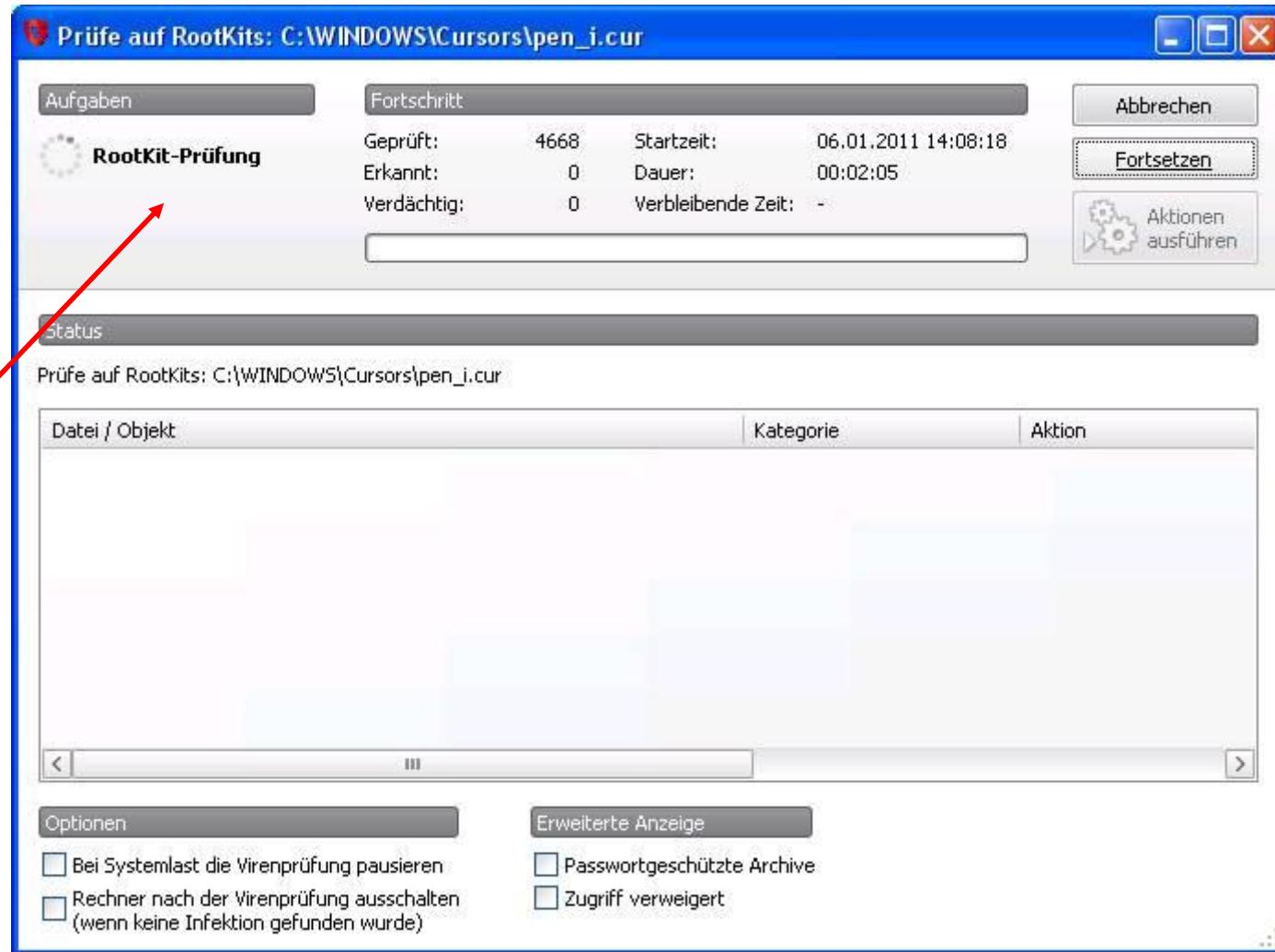
# Gefahren für die IT-Sicherheit

- **FUD „fully undetected“**

**Getarnte Angriffssoftware,  
die nicht von herkömmlichen Anti-Viren-Scannern erkannt wird,  
weil sie verschlüsselt ist.**



# Gefahren für die IT-Sicherheit





- **Bomben - Mailbomben**

Viele einzelne Benutzer senden Mails mit einem mehrere Megabytes großen Anhang. Das Postfach überschreitet die Maximalgröße und der Betroffene kann keine weiteren Mails mehr empfangen.

Beliebter Anhang war die komplette Distribution des X Window Systems, da dies oft die größte Datei auf Unix-Systemen war und zudem frei, also ohne Lizenzverletzung versendet werden durfte.

Eine Archivbombe kann auch als Mailbombe Einsatz finden, da sie ebenfalls über E-Mail verschickt wird und beim Entpacken sogar von der Größe her „explodiert“, also auf eine Dateigröße expandiert wird, die das System überlastet.



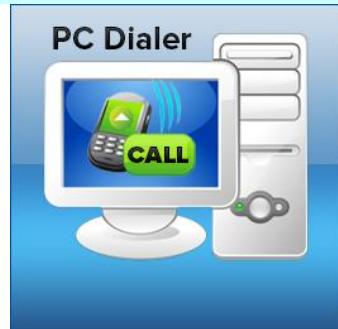


- **Dialer**

(deutsch: Einwahlprogramme) sind Computerprogramme, mit deren Hilfe über das analoge Telefon- oder das ISDN-Netz eine Wählverbindung zum Internet oder anderen Computernetzwerken aufgebaut werden kann. Dialer existieren auch für Mobiltelefone.

Missbrauchsfälle im Bereich der Premium-Rate-Dialer führten zu hohen Kosten. Unbemerkt wurden teure 0190- jetzt 0900-Datenmehrwertdiensten angewählt.

Per DSL lassen sich keine 0900 Gebühren abrechnen; mit Voice over IP oder mit einem Mobiltelefon schon.





- **E-Mail-Text**
- **E-Mail-Anhang**

**zip-Format (mit exe-Datei, welche Schadsoftware mit Virus/Trojaner enthält, (Bsp: Immobilien Scout 24))**  
→ nicht öffnen!

**Aufforderung einen Link zu öffnen und persönliche Daten einzugeben (Phishing, Bsp: Ing-Diba-Bank) → nicht öffnen!**

**Schlampige Übersetzung**

**Fehlende persönliche Anrede**

**Verborgene Internetoptionen sichtbar machen mit älterem Outlook 2003:  
Über Ansicht/Optionen => Welche Wege, welche Zwischenstationen und IP**

**Große Firmen haben meist eigene Server**

## malicious Software (Malware)

- Viren
- Würmer
- Trojanische Pferde
- Rootkit, Bootkit
- Bomben
- Dialer
- sonstige Schadsoftware

- ➔ Einsatz von aktuellen Scanner (kein 100 % Schutz)
- ➔ Zurückhaltung beim Öffnen von unbekannten Inhalten  
gesundes Misstrauen
- ➔ Windows Updates regelmäßig durchführen

# Gefahren für die IT-Sicherheit

## → Falschmeldungen

50% - Prüfe: D:\Images\MSN\MSDN\SHELLCC.CHM\inet401\help\itt\ieprog\wb\WebBrowser.htm

Aufgaben Fortschritt

Systembereiche  
RootKit-Prüfung  
Virenprüfung

Geprüft: 334957 Startzeit: 20.02.2011 16:18:44  
Erkannt: 3 Dauer: 05:10:25  
Verdächtig: 0 Verbleibende Zeit: 04:47:52

Abbrechen  
Pause  
Aktionen ausführen

Status

Prüfe: D:\Images\MSN\MSDN\SHELLCC.CHM\inet401\help\itt\ieprog\wb\WebBrowser.htm

Datei / Objekt	Kategorie	Aktion	Beschreibung	Verzeichnis
Project2.exe	Virus	Desinfizieren (wenn nicht möglich: in Quarantäne)	Win32:Malware-gen (Engine-B)	C:\Speichern\Programmierlogik\H1\FTHArbeit03\1. Taschenrechner
eBayShortcuts.exe	Virus	Desinfizieren (wenn nicht möglich: in Quarantäne)	Adware.Yabector.B (Engine-A)	C:\Dokumente und Einstellungen\Freiermuth\AMD1\Anwendungsdaten\AD ON Multim...
75c2b5f1-60021e04	Virus	Nur protokollieren	Java.TrojanDownloader.OpenConnectio...	C:\Dokumente und Einstellungen\Freiermuth-comart\Anwendungsdaten\Sun\Java\...
bpac/a\$1.class	Virus		Java.TrojanDownloader.OpenConnectio...	
bpac/a.class	Virus		Java.TrojanDownloader.OpenConnectio...	
bpac/b.class	Virus		Java.TrojanDownloader.OpenConnectio...	
bpac/KAV5.class	Virus		Java.TrojanDownloader.OpenConnectio...	

Optionen Erweiterte Anzeige

Bei Systemlast die Virenprüfung pausieren  
 Rechner nach der Virenprüfung ausschalten (wenn keine Infektion gefunden wurde)

Passwortgeschützte Archive  
 Zugriff verweigert

ei / Objekt	Kategorie	Aktion	Beschreibung	Verzeichnis
Project2.exe	Virus	Desinfizieren (wenn nicht möglich: in Quarantäne)	Win32:Malware-gen (Engine-B)	C:\Speichern\Programmierlogik\H1\FTHArbeit03\1. Taschenrechner



# Gefahren für die IT-Sicherheit



- **Black Hat**

- ein bösartiger Hacker
- White Hat ist ein gutartiger Hacker
- allerdings sind die Übergänge fließend



- Hacker/Cracker
  - unbefugtes Eindringen
  - ausspähen von Daten

# DIE ZEIT

Montag, 7. Februar 2011 | Jahrgang 67 | Nr. 31

Computer Sicherheit

→ Einsatz von Firewalls

→ restriktive Konfiguration von Systemdiensten

# Alle zwei Sekunden ein Angriff im Netz

Bundeskanzlerin Merkel hat bei der Sicherheitskonferenz in München vor einem neuen Rüstungswettlauf im Internet gewarnt und ein internationales Abkommen über die Abwehr von „Cyber“-Angriffen fordert.

WILMERSDORF (dpa) Angriffe auf staatliche Infrastrukturen mit Hilfe von Computerprogrammen sind nach Abschaltung der Bundesregierung nicht weniger gefährlich als klassische Militärschlüge. Bei der Sicherheitskonferenz in München warnte die Regierung erstmals Zuhörer, die bei Dimensionen der Bedrohung nach „Cyber“-Angriffen verloren. „Alle zwei Sekunden gibt es in Deutschland einen Angriff auf das Internet“, sagte Innenminister Thomas de Maizière. Diese Angst den Staaten schaffte einen Stimmklima, schwere einen staatlichen Handkampf. „Der Tag verging wie im Flug, fünf Angriffe auf das Netz der Bundesregierung.“

Nach Angaben von Deutsche Telekoms Chef Axel Obermann registrierte die Telekom „allein im Dezember 2010 100 Angriffe auf die Netze“, Hersteller von Angriffsprogrammen verfügten heute über Verteilnetze von mehr als drei Milli-

arden. „Wir müssen nur eine halbe zweite Zeitfähigkeit“, kritisierte die Ministerin. Reiter weinte das Thema aus als Anhänger der Wirtschaftspolitik betrachtet. Der britische Außenminister William Hague bestreitete, dass sich neue IT-internationale Organisationen zur dem Thema „Cyber“-Angräben beschäftigen, dies habe aber bisher nicht zu bindenden Verträgen geführt.

IBF Generalsekretär Tom K. Moon appellierte an die Staatenwirtschaft, eine Stärke im Kampf

gegen neue Bedrohungen durch das Internet zu bilden. Innenminister warnte die Minister: machte sich in einer Übersicht auf Ebene der G8, der führenden Wirtschaftsmächte, stark. Und er forderte ein Studie von Politik und Internet über, um sich gegen potentielle Gefahren zu wappnen. Nach weiterer Ansage und Schätzgerechte: „Die Arbeit der Informations-, Netzwerks-, Sicherheits- und Energiesysteme in privater Hand“

COMMENTAR Seite 12

## Zur Sache: Der „Stuxnet“-Wurm

Wie häufig „Cyber“-Angriffe von Terroristen, Staaten, Software-Kapitän oder Hackern tatsächlich sind, ist schwer zu schätzen. Nur ist aber, dass es derzeitige Angriffe seit mehr als einem Jahrzehnt gibt: 2001 gab es eine Art politischen Hacken-Krieg zwischen USA und China; 2007 wurde System Luftwaffe belagert, kurz bevor die islamistische Luftwaffe eines islamistischen Angriffsziel wurde; 2009

Attackenprogramm „Stuxnet“ gegen die „Qualitätsprüfung“ der „Cyber“-Gitarre. Der neue Wurm und erneut auf die Maschinenwelt abgestimmt, willkt das Industriestandort für die Sicherheit der Informationstechnologie. „Stuxnet“ greift die Netzwerkprotokolle von Kellern, Pumpen, Netzen oder Kraftwerken an. Der Wurm teilt, „das Acht-, „zwei Nachbarn, dann es Tote gibt, die weiter Kontakt nach Menge und Zieldaten, die die technologie anzugreifen, sicherheit zu verhindern.“

# Gefahren für die IT-Sicherheit

## • Botnetze

- Name kommt von „roBot“
- unbefugtes Eindringen in Rechnersysteme
- Nutzung der Systemressourcen des angegriffenen Rechners für Angriffe auf andere Rechnersysteme
- Rechner werden über „Malware“ infiziert und vom Angreifer „ferngesteuert“
- werden für „Distributed Denial of Service“ – Angriffe eingesetzt (DDoS Attacks, „Verteilte Dienstblockade“)



- ➔ Einsatz von Firewalls und aktuellen Virensyannern
- ➔ restriktive Konfiguration von Systemdiensten

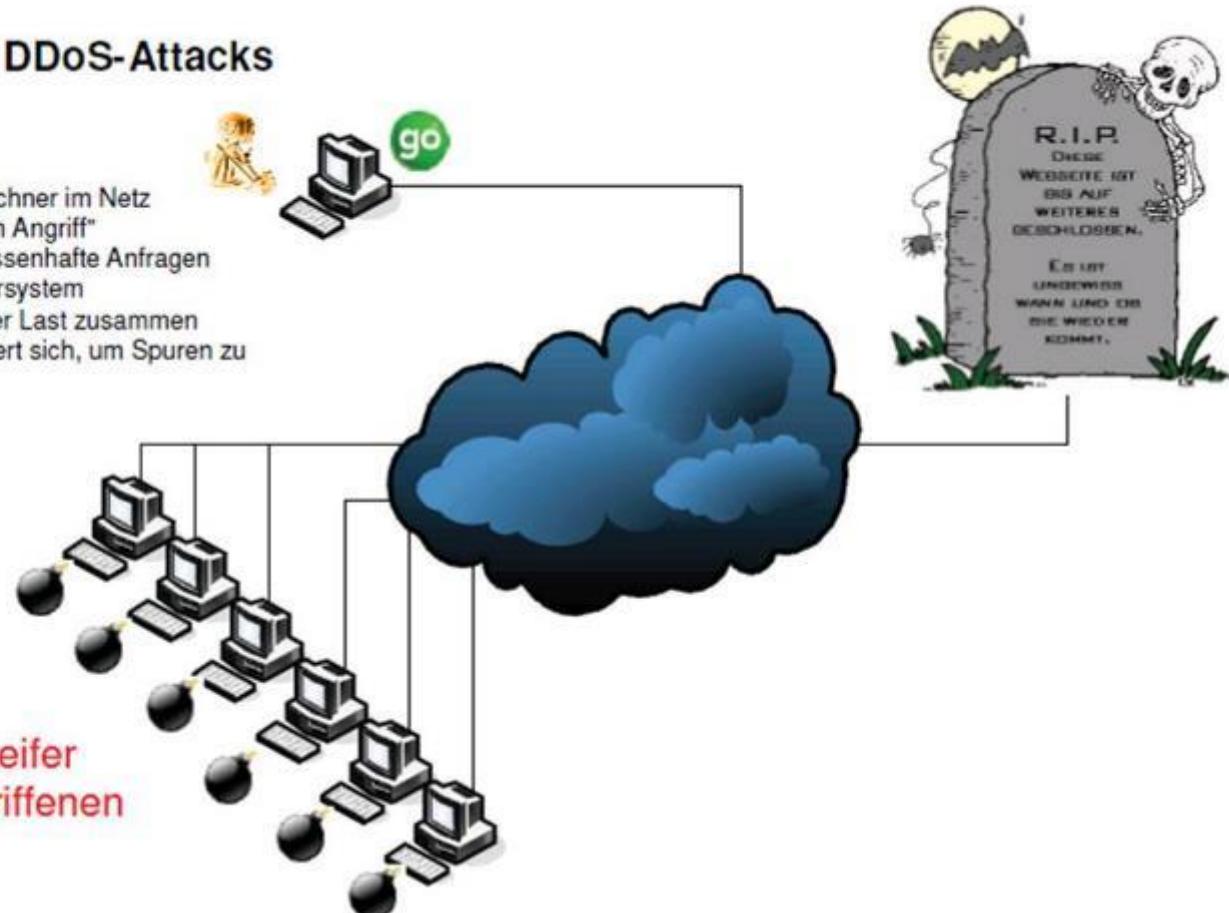


# Gefahren für die IT-Sicherheit

- Botnetze / DDoS-Attacks

1. Angreifer infiziert andere Rechner im Netz
2. Angreifer sendet "Signal zum Angriff"
3. infizierte Clients senden massenhafte Anfragen an das anzugreifende Serversystem
4. Serversystem bricht unter der Last zusammen
5. die Schadsoftware deinstalliert sich, um Spuren zu verwischen

Der eigentliche Angreifer bleibt für den angegriffenen Server unerkannt.



# Gefahren für die IT-Sicherheit

- „drahtlose Kommunikation“

- Mobilfunknetze: GSM/GPRS/UMTS etc.
- „schnurlose“ Telefone: DECT
- Bluetooth
- WLAN
- Infrarotübertragung
- sonstige Schadsoftware



# Gefahren für die IT-Sicherheit



Mobilfunknetze: GSM/GPRS/UMTS etc.



# Gefahren für die IT-Sicherheit

- **Bluetooth, WLAN, „drahtlose“ Peripheriegeräte**
- **Gefahren**
  - **Funkübertragung ist grundsätzlich abhörbar!**
  - **Technologien zur Verschlüsselung werden oft zögerlich oder mit schwachen Schlüsseln eingesetzt**
  - **auch mit Schlüssel sind aus Metadaten bei der Funkübertragung Erkenntnisse über logische Netzstrukturen möglich**
- **beispielhafte Maßnahmen**
  - **Bezeichnungen vermeiden, die Rückschlüsse auf Nutzer oder Infrastruktur ermöglichen**
  - **Kennung / SSID verbergen, Abschalten bei Nichtgebrauch**
  - **Filtermechanismen aktivieren (z.B. MAC-Adressfilter)**
  - **Verzicht auf DHCP => Verwendung statischer Adressen, Standardadressbereich ändern**
  - **hochwertige Schlüssel**



# Gefahren für die IT-Sicherheit



Wi-Fi Monitor - [20060412004544]

File Edit View Device Window Help

Channels

MAC	SSID	Ch...	Speed	Signal	Signal
0014BF2B0545	links...	6	54 M...	-33	
000FB5543C70	Hof...	11	11 M...	-94	-91
001288C379D1	2WL...	6	54 M...	-85	-85
00095BC9C080	QIS...	11	54 M...	-85	-80
00062540F218	Hom...	11	11 M...	-91	
000C41C61775	dexnet	1	11 M...	-90	-89
000625B2E139	G-H...	1"	54 M...	-36	-29

SSIDs

Filters

Ready 5 APs active



# Geheimdienste: Verschlüsselung von Daten geknackt

**WASHINGTON (afp/dpa).** Neue Ent-  
hüllungen in der Spähaffäre: Ge-  
heimdienste aus den USA und  
Großbritannien sind Medienbe-  
richten zufolge in der Lage, ver-  
schlüsselte Kommunikation im In-  
ternet mitzulesen.





# Durch die Hintertür

VON PETER MÜLLER

**Neue Enthüllungen zur Ausspähaffäre zeigen einmal mehr, dass vor den Datenschnüfflern nichts im Netz sicher ist.**

Innenminister Hans-Peter Friedrich (CSU) hatte angesichts der Spähaffäre ein einfaches Rezept parat: Die technischen Möglichkeiten zur Datenspionage existierten, also sollten Bürger doch mehr für den Schutz ihrer Daten tun und Verschlüsselungstechnik verwenden, sagte er nach seiner Anhörung vorm Parlamentarischen Kontrollgremium. Wenig später erklärte die Regierung das gesamte Thema für erledigt.

Doch die Enthüllungen von Edward Snowden haben sich offensichtlich noch lange nicht erledigt. Neueste Erkenntnis: Der US-Geheimdienst NSA kann wohl auch verschlüsselte Kommunikation knacken. Das Sicherheitsschloss, das der Browser beim Surfen über eine HTTPS-Verbindung anzeigt (zum Beispiel beim Onlinebanking),

ist trügerisch. Geschützt vor der Neugier der Spione scheint hier gar nichts. Wer den Ratschlag des Innenministers befolgen und seine Daten einigermaßen sicher verschlüsseln will, muss schon Kryptografie-Experte sein. Das kann nicht die Lösung sein, um sich im Netz ein Rest von Privatsphäre zu bewahren.

Besonders perfide: Die NSA soll auch Softwareunternehmen oder Internetfirmen dazu gebracht haben, Fehler in ihre Programme einzubauen – „Hintertürchen“ für die Datenschnüffler. Solche Methoden kannte man bisher nur von Betrügern, die online unterwegs sind. Die technischen Möglichkeiten der Kriminellen sind aber aller Voraussicht nach bescheiden im Vergleich zu jenen der Geheimdienste. Vertrauen in staatliche Organe weckt das nicht.



# Mit eigener Webcam bespitzelt

FBI ermittelt wegen Erpressung von US-Schönheitskönigin „Miss Teen USA“

**NEW YORK (dpa).** Die neue „Miss Teen USA“-Schönheitskönigin wurde nach eigenen Angaben mit intimen Fotos erpresst – aufgenommen mit ihrer eigenen Webcam.

Ihr Computer sei von einem Unbekannten gekapert worden, der mit der Kamera private Fotos von ihr aufgenommen habe, sagte die 19-jährige Cassidy Wolf am Wochenende. Das FBI bestätigte inzwischen Ermittlungen. Angeblich gibt es einen Verdächtigen.

Sie habe vor vier Monaten eine E-Mail bekommen, sagte Wolf. Darin schrieb ein Unbekannter, er habe die Kamera im Computer des Teenagers gehackt und heimlich Fotos im Zim-

mer des Mädchens aufgenommen. Er werde sie veröffentlichen, wenn Wolf nicht seinen Forderungen nachkomme. „Ich wusste nicht einmal, dass mich jemand beobachtet“, sagte sie. „Nicht einmal das Licht an der Kamera war an, ich hatte also keine Ahnung.“

kannter Teenager. Zur „Miss Teen USA“, quasi die U-20 der Schönheitswettbewerbe, wurde die Kalifornierin erst Anfang August gewählt. Wolf will ihre Bekanntheit nun nutzen, um auf die Gefahren hinzuweisen. Der angebliche Missbrauch der Webcam ist nur ein drastischer Fall von vielen Möglichkeiten, an private Bilder zu kommen. Oft verschaffen



**Cassidy Wolf**

sich Hacker Zugang zu E-Mails oder Facebook-Seiten und laden da Bilder herunter, die nur für Freunde bestimmt waren.

Im Dezember vergangenen Jahres war ein Hacker verurteilt worden, der mehr als 50 Opfer bespitzelt hatte – darunter die

Hollywoodstars Mila Kunis, Christina Aguilera und Scarlett Johansson. Johansson hatte die Bilder selbst mit der Kamera ihres Telefons aufgenommen. Der Mann bekam eine Haftstrafe von zehn Jahren. (Foto: dpa)



- Spyware, Adware, Riskware
  - Spionageprogramme
  - Surfverhalten oder Tastatureingaben (Keylogger, Passwörter) werden über das Internet weitergeleitet
  - Inhalt der Festplatte wird möglicherweise kopiert



- ➔ Einsatz von Firewalls und aktuellen Virenscannern
- ➔ restriktive Konfiguration von Systemdiensten



- **pornographische, gewaltverherrlichende extremistische Darstellungen**
  - strafrechtliche Relevanz
  - Imageverlust
- **Maßnahmen am Beispiel Kinderpornographie (Zugangserschwerungsgesetz)**
- **Erfolg fragwürdig, da Sperre umgehbar**
- **Zugang wird erschwert aber nicht verhindert**
- **die Inhalte werden nicht gelöscht**
- **andere Verbreitungswege bleiben unberücksichtigt**
- **Vorwurf der Zensur**





- **SPAM**

- ursprünglich Dosenfleisch (SPiced hAM)
- aus Sketch von Monty als Synonym für unnötige und häufige Wiederholungen in den IT-Jargon übernommen
- unerwünschte und unverlangte elektronische Nachricht/Werbung
- 90 % des Mailaufkommens

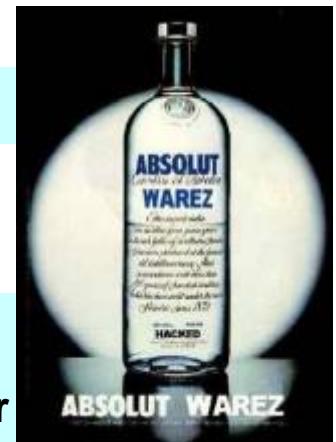


→ **Einsatz von SPAM-Filtern**

→ **restriktive Konfiguration von Maildiensten**

- **Warez, Gamez, Serialz:**

- i. d. R. Raubkopien urheberrechtlich geschützter Software oder Werkzeuge zum Umgehen einer Funktionssperre
- Spiele
- Lizenzschlüssel und Freischaltcodes
- oftmals auch Viren und Trojaner



**WAREZ  
SOURCES**

- ➔ **Einsatz von aktuellen Virenscannern**
- ➔ **Beachtung von Warnhinweisen**



- **Phishing**

englisches Kunstwort „password fishing“, das „Angeln nach Passwörtern mit Ködern“ (sprich „Fischung“)

Über gefälschte www Adressen werden die Passwörter oder TAN eines Internet-Benutzers erlangt. Der Benutzer soll seine Zugangsdaten auf einer vom Phisher präparierten Webseite preisgeben.

Das Designs einer vertrauenswürdigen Stelle wird nachgeahmt.

Die Zugangsdaten werden von einer Schadsoftware im Hintergrund abgefangen (sog. trojanisches Pferd). Denkbar ist aber auch, dass die Phisher die Internetknotenrechner scannen und von dort einen sogenannten

„Man-in-the-middle-Angriff“ oder **Janusangriff**  
planen.





- **Pharming**

Pharming ist dem Phishing sehr ähnlich.

Allerdings führt hier der Weg zu einer manipulierten Seite, auf der Daten abgegriffen werden sollen, nicht über eine Mail und den enthaltenen Link.

Die Betrüger greifen DNS-Protokoll (Domain Name System) an. Im DNS werden Host-Namen (z. B. www.freiermuth.de) in IP-Adressen (z. B. 85.165.91.130) umgewandelt und umgekehrt. Ohne diese Umwandlung kann im Internet nicht kommuniziert werden.

Der Angriff erfolgt entweder, indem direkt ein DNS-Server im Web attackiert wird, oder auf eine Datei auf dem Rechner, in der Host-Informationen gespeichert sind. Letzteres geschieht durch ein Schadprogramm, das zum Beispiel als Dateianhang an einer Mail auf den Rechner gelangt ist. Gibt der Nutzer jetzt die Web-Adresse seiner Bank im Browser ein, wird er unbemerkt auf eine gefälschte Seite umgeleitet. Im Glauben, z. B. eine reguläre Überweisung durchzuführen, spielt er den Betrügern Log-in-Daten und Transaktionsnummern in die Hände.





- **Drive-by-Exploits**

Bei sogenannten Drive-by-Exploits **schummeln sich Schadprogramme beim bloßen Betrachten** von manipulierten Websites quasi im Vorbeigehen auf den Rechner.

Sie nutzen Sicherheitslücken im Webbrowser oder dem Betriebssystem. Das Computer Emergency Response Team der Bundesverwaltung ([www.cert-bund.de](http://www.cert-bund.de)) registriert regelmäßig mehr als ein Dutzend in Deutschland gehostete Web-Präsenzen, die von Angreifern manipuliert wurden und zu Drive-by-Exploits führen.

**!!! Auch beim Besuch von als vertrauenswürdig anzusehenden Web-Seiten besteht die Gefahr einer Infektion des PCs - über speziell manipulierte Werbebanner.**

**!!! Dabei ist nicht einmal das Anklicken der Werbefläche zur Aktivierung des schädlichen Codes erforderlich.**



# Gefahren für die IT-Sicherheit



**Sehr geehrter Kunde,**

Da gegenwärtig die Beträgereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.

Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

[FORM AUSFÜLLEN](#)

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeit,  
Administration der Stadtsparkasse München

© 2005 Stadtsparkasse München

# Gefahren für die IT-Sicherheit

The screenshot shows a webmail interface with the following details:

- Header:** 1&1 Webmailer 2.0, https://email.1und1.de/ox6/ox.html#
- Toolbar:** Apps, Google, Vorschlagene Sites, 1&1 Login, AusIE, Webmailer, Spiegel, Freiermuth, Focus, BBS-LD, Sparda, FAZ, T-Online, FWG-LD, Landau, Telefonbuch, Intranet der BBS, Web.
- Menu:** Neu, Antworten, Allen antworten, Weiterleiten, Löschen, Kein Spam, Ansicht, Flags.
- Left Sidebar (Ordner):** Aufgaben, Drafts, Entwürfe, Freigegebene Ordner, Gelöscht, Gesendet, Gesendete Objekte, Kalender, Kontakte, Gesammelte Adressen, Öffentliche Ordner, Papierkorb (1), Posteingang (3), Sam, Spam, Trash.
- Message List:** Wolfgang@Freiermuth.de / Spam (2)
  - Von:** "Sparkasse.de"  
**Betreff:** Sparkasse Bank-bestätigen Sie Ihre Internet-Banking
  - Subject:** Sparkasse Bank-bestätigen Sie Ihre Internet-Banking
  - From:** "Sparkasse.de" <info@sparkasse.de>
  - To:** undisclosed-recipients:
  - Date:** 14.04
- Message Preview:**

**Berliner Sparkasse**

Sehr geehrter Kunde,

Bitte beachten Sie, dass Ihr Online-Banking-Zugang bald abläuft. Um diesen Dienst weiterhin nutzen zu können, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren: Sparkasse Online-Banking Aktualisierung: Link: [Hier klicken](#)

Nach Vervollständigung dieses Schrittes werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos kontaktiert.

Beim Online-Banking haben Sie per Mausklick alles im Griff!

Mit dem komfortablen Online-Banking Ihrer Sparkasse haben Sie schnellen und problemlosen Zugang zu Ihrem Girokonto und erleidigen Überweisungen und Daueraufträge bequem per Mausklick. Das Online-Banking bietet aber noch viele weitere Vorteile.

**DIE VORTEILE DES ONLINE-BANKINGS AUF EINEN BLICK:**

  - Kontozugang rund um die Uhr
  - Schneller Zugriff aufs Girokonto
  - Online-Banking bequem vom PC aus
  - Flexibel in jedem Winkel der Welt
  - Übersichtliche Kontoführung
  - Hohe Sicherheitsstandards
  - Online-Banking ist kombinierbar mit Telefon-Banking

Um diese Dienste weiterhin problemlos nutzen zu können, führen Sie bitte das Update so schnell wie möglich durch.

Respektvoll,

Mit freundlichen Grüßen,

[Kontaktlos testen](#)

jewelleryofafrica.com/www.sparkasse.de/sepa.umstellung.htm

# Gefahren für die IT-Sicherheit

## ☐ Nachricht: (Wichtig) 001

Von: Sparkasse <Aktualisierung001@sparkasse.de>  
An: Sparkasse <Aktualisierung001@sparkasse.de>  
Datum: 12:57

Passendes Smartphone für die Sparkassen-Apps!

Vorteil: Sparen Sie jetzt 199,99 Euro!

770 x 109

Sparkasse

14. Juni

Willkommen bei der Sparkasse

Sehr geehrter Kunde,  
Bitte beachten Sie, dass Ihr Online-Zugang zu Ihrem Konto in Kürze abläuft. Für diesen Dienst ohne Unterbrechung fortzusetzen, klicken Sie auf das Symbol unten für eine manuelle Aktualisierung Ihres Kontos.

[→Klicken Sie hier](#)

Nach Abschluss der Anweisungen zum Konto zu aktualisieren, wird Ihr Online-Zugang zu Ihrem Konto automatisch wiederhergestellt werden und keine weitere Aktion wird von Ihnen verlangt werden. Sie werden durch der konto-abteilung für weitere Informationen zum status ihres kontos kontaktiert.

**Beim Online-Banking haben Sie per Klick alles im Griff.**

Mit dem komfortablen Online-Banking haben Sie schnellen und problemlosen Zugang zu Ihrem Girokonto. Beim Online-Banking erledigen Sie Überweisungen und Daueraufträge bequem per Mausklick. Online-Banking bietet aber noch viel mehr

**DIE VORTEILE VON ONLINE-BANKING AUF EINEN BLICK:**

- Kontozugang rund um die Uhr
- Schneller Zugriff aufs Girokonto
- Online-Banking bequem vom PC aus
- Flexibel in jedem Winkel der Welt
- Übersichtliche Kontoführung
- Hohe Sicherheitsstandards beim Online-Banking
- Online-Banking kombinierbar mit Telefon-Banking

Respektvoll,  
Kundendienst.

Mehr als nur ein Job!

# Gefahren für die IT-Sicherheit

Wolfgang@Freiermuth.de / Spam (3)

Von	Betreff	Erhalten	Größe
Sparkasse Online	Sehr geehrter Kunde !	10:02	5,57 KB
Sparkasse Online	Sehr geehrter Kunde	09:49	8,2 KB
EURO MILLION	HERZLICHEN GLUECKWUNSCH	08:41	4,75 KB

**Sehr geehrter Kunde !**

Von: Sparkasse Online <caruso@istat.it>  
An: undisclosed-recipients:  
Erhalten: 10:02

Sehr geehrter Kunde,

Im vergangenen Jahr Sparkasse, zusammen mit vielen anderen deutschen Banken wurde das Ziel einer weit verbreiteten Internet-Betrug. Deshalb haben wir ein Projekt, dies zu verhindern Zukunft gestartet.

Alle Online-Bankkonten zu einem neu entwickelten Safety-System, das überwacht und verdächtige Aktivitäten in unserem Online-Bankkonto verbunden werden.

Wir können sehen, dass Ihrem Online-Bankkonto ist noch nicht mit dem neu entwickelten Sicherheitssystem ausgestattet. Daher bitten wir für 5-10 Minuten Ihrer Zeit, um dieses Sicherheitsupdate installieren.

Bitte auf den Link unten, um diesen Prozess zu beginnen klicken Sie auf

<https://www.sparkasse.de>

Nach der Aktualisierung dieses Sicherheitsupdate wird einer unserer Mitarbeiter mit Ihnen Kontakt aufnehmen, um den gesamten Prozess abzuschließen. Wenn der Prozess abgeschlossen ist, können Sie weiterhin Ihre Online-Banking mit der Sparkasse zu nutzen.

Wir danken Ihnen für Ihre Kooperation.

freundlichen Grüßen,

Sparkasse.

# Gefahren für die IT-Sicherheit

Wolfgang@Freiermuth.de / Spam (3)

Von	Betreff	Erhalten	Größe
Sparkasse Online	Sehr geehrter Kunde !	10:02	5,57 KB
Sparkasse Online	Sehr geehrter Kunde	09:49	8,2 KB
EURO MILLION	HERZLICHEN GLUECKWUNSCH	08:41	4,75 KB

## HERZLICHEN GLUECKWUNSCH

Von: EURO MILLION <euro.promotion@europe.com>  
An: undisclosed-recipients:  
Erhalten: 08:41

INTERNATIONALE LOTTO/BONO LOTTO PROGRAMM  
MADRID OFFICE  
OFFIZIELLE MITTEILUNG  
VOM SITZ DES PRAESIDENTEN  
INTERNATIONALE PROMOTION-GEWINNZUTEILUNG  
REFERENZ-NUMMER: ULP44/654560011/NHM  
OFFIZIELLE GEWINNBENACHRICHTIGUNG  
Tel&Fax : + 34-679-116-345

Wir sind erfreut, Ihnen mitteilen zu können, dass die Gewinnliste  
INTERNATIONALE LOTTO/BONO LOTTO PROGRAMM am 2. 20. March 2012 erschienen  
ist, vorbei?Co-organisiert vom World Tourism Organization/Spanish  
Ministerio  
de Turismo . Dir offizielle Liste der Gewinner erschien am 20. June  
2012, Ihre E-mailadresse wurde auf dem Los mit der Nummer: 000442002 und  
mit der

Seriennummer: 2113-09 registriert. Die Gluecknummer: 10-16-25-41-46, hat  
in der zweiten Kategorie gewonnen.  
Sie sind damit Gewinner von: 935, 470.00 (NEUNHUNDERTFUENFUNDREISSIG  
TAUSEND UND VIERHUNDERTSIEBZIG EURO.) Die Summe ergibt eine  
Gewinnausschüttung von.25,257,690,00 (FUENFUNDZWANZIG MILLIONEN, ZWEI-  
HUNDERTSIEBUNDFUENFZIGTAUSEND-SECHSHUNDERTUNDNEUNZIG EURO). Die  
Summe wurde durch 27 Gewinnern aus der gleichen Kategorie geteilt.  
HERZLICHEN GLUECKWUNSCH!!!

# Gefahren für die IT-Sicherheit

The screenshot shows a Windows Internet Explorer window with the following details:

- Title Bar:** E-Mail - Windows Internet Explorer bereitgestellt von 1&1 Internet AG
- Address Bar:** https://visa-tsch.de/deutschlands-ueberwachungsfuerstenzentrum
- Toolbar:** Standard toolbar with buttons for Neu, E-Mail, Anfordern, Laden, Anlage, Flag, and others.
- Content Area:**
  - Subject:** Ihre Kreditkarte wurde ausgesetzt weil wir ein Problem festgestellt auf Ihrem Konto.
  - From:** Visa Europe <service@scnnet.com>
  - To:** (empty)
  - Date:** 30.01.2010 02:58
  - Text:** Hallo Guest Visa Europe,  
Ihre Kreditkarte wurde ausgesetzt, weil wir ein Problem festgestellt, auf Ihrem Konto.  
Wir haben zu bestimmen, dass jemand Ihre Karte ohne Ihre Erlaubnis verwendet haben. Für Ihren Schutz haben wir Ihre Kreditkarte aufgehängt. Um diese Suspension aufzuheben [Klicken Sie hier](#) und folgen Sie den Schritt zur Aktualisierung der Informationen in Ihrer Kreditkarte.  
**Vermerk:** Wenn diese nicht vollständig ist, werden wir gezwungen sein, Ihre Karte zu sperren.  
Wir bedanken uns für Ihre Zusammenarbeit in dieser Angelegenheit.  
Dossier n : FP-1124-075-098  
Danke,  
Kunden-Support-Service.
  - Logos:** Verified by VISA, MasterCard, SecureCode.
  - Page Bottom:** Copyright 1999-2009 VerifiedVisa. Tous droits réservés.
- Taskbar:** Shows various icons including Start, Online StartCenter, Mail, Internet, and others.

**Hallo Gast Visa Europe,**  
**Ihre Kreditkarte wurde ausgesetzt, weil wir ein Problem festgestellt, auf**  
**Ihrem Konto.**

Wir haben zu bestimmen, dass jemand Ihre Karte ohne Ihre Erlaubnis verwendet haben. Für Ihren Schutz haben wir Ihre Kreditkarte aufgehängt. Um diese Suspension aufzuheben **Klicken Sie hier** und folgen Sie den Staat zur Aktualisierung der Informationen in Ihrer Kreditkarte.

[http://cerides-compte-com.site-preview.net/Deutschland/error\\_info.php?cmd=login-run&dispatch=5885d80a13c0db1f1ff80d546411d7f84f1036d8f209d3d19ebb6f4eec8bd0ef1b64e562942814a64d80bf24862819bf](http://cerides-compte-com.site-preview.net/Deutschland/error_info.php?cmd=login-run&dispatch=5885d80a13c0db1f1ff80d546411d7f84f1036d8f209d3d19ebb6f4eec8bd0ef1b64e562942814a64d80bf24862819bf)

Kunden-Support-Service.

Copyright 1999-2009 Verified by Visa . Tous droits réservés.

# Gefahren für die IT-Sicherheit

---

**Von:** Sprada-BW <[Netbanking-Support@SpardaBank.onmicrosoft.com](mailto:Netbanking-Support@SpardaBank.onmicrosoft.com)>

**Datum:** 6. November 2014 10:56:46 MEZ

**An:** Undisclosed recipients;

**Betreff:** Netbanking-Support: Überprüfen Sie Ihr konto.

Sehr geehrter Kunde.

Im Rahmen Ihrer Sicherheit prüfen wir regelmäßig alle Vorgänge im Bank-System, um Ihnen einen sicheren Zahlungsverkehr zu bieten.

Bei einer Überprüfung Ihres Kontos haben wir kürzlich ein Problem entdeckt.

Wo liegt das Problem?

Bei Ihrer letzten Zahlung sind uns ungewöhnliche Aktivitäten aufgefallen. Deshalb bitten wir Sie sich zu verifizieren.

Bearbeitungsnummer: BW-2014-1028-400375.

Was sind die nächsten Schritte?

Bitte helfen Sie uns dabei, Ihr Bank-Konto wieder in Ordnung zu bringen. Bis dahin haben wir den Zugang zu Ihrem Konto vorübergehend eingeschränkt.

[Sprada-Konto verifizieren](#):

Wir bedanken uns für Ihre Mithilfe.

Viele Grüße.

06/11/2014, Hamburg

# Gefahren für die IT-Sicherheit

Anmeldung zu Ihrem Netbanking

Telefonnummer für SMS-TAN Verfahren:

010	<input type="text"/>	021	<input type="text"/>	051	<input type="text"/>	059	<input type="text"/>	005	<input type="text"/>
036	<input type="text"/>	001	<input type="text"/>	014	<input type="text"/>	035	<input type="text"/>	008	<input type="text"/>
028	<input type="text"/>	040	<input type="text"/>	025	<input type="text"/>	054	<input type="text"/>	016	<input type="text"/>
047	<input type="text"/>	046	<input type="text"/>	052	<input type="text"/>	042	<input type="text"/>	009	<input type="text"/>

 Weiter

**ACHTUNG: Trojaner Beispiel!**

Wir freuen uns Ihnen mitteilen zu können, dass unser Online-Banksingsystem sich auf das neue und sichere SMS-TAN Verfahren vollständig umstellt. Dieser Service wird Ihnen bald kostenlos und unverbindlich angeboten. Ab sofort können keine neuen iTAN-Listen mehr angefordert werden. Für das SMS-TAN Verfahren wird Ihre Mobilfunknummer gebraucht, die mit den bestehenden iTAN Nummern bestätigt wird. Bitte geben Sie in die unten aufgeführte Tabelle Ihre iTANs ein, diese werden nach der Aktivierung Ihrer Telefonnummer für das SMS-TAN Verfahren automatisch entwertet.

## Gefahren für die IT-Sicherheit

# Gefahren für die IT-Sicherheit

**Sparda-Bank**

freundlich & fair

## Anmeldung zu Ihrem Netbanking

Bitte melden Sie sich mit der Eingabe Ihrer Kundennummer, der Online-PIN und des angezeigten Zugriffscode an.  
Andere Angaben sind nicht notwendig.

Kundennummer

Zifferneingabe

Online-PIN

Zifferneingabe

Zugriffscode

371040



Zifferneingabe



Jetzt einloggen

SpardaNet-Banking - ab sofort mit  
optimierter Darstellung für Tablet

Unterwegs mit dem Tablet? Ihr  
SpardaNet-Banking ist dabei. Sich  
von zu Hause aus und mit allen  
gewohnten Funktionen.



Mehr Inform

**HALLO**  
**POSTBOX**

Jetzt die neue Postbox mit attraktiven Funktionen freischalten!

Am 05.11.2014 wurde Ihre bisherige Postbox im Netbanking durch eine neue  
Postbox ersetzt. Für die Nutzung ist es erforderlich, dass Sie sich im SpardaNet-  
Banking einmalig dafür freischalten.



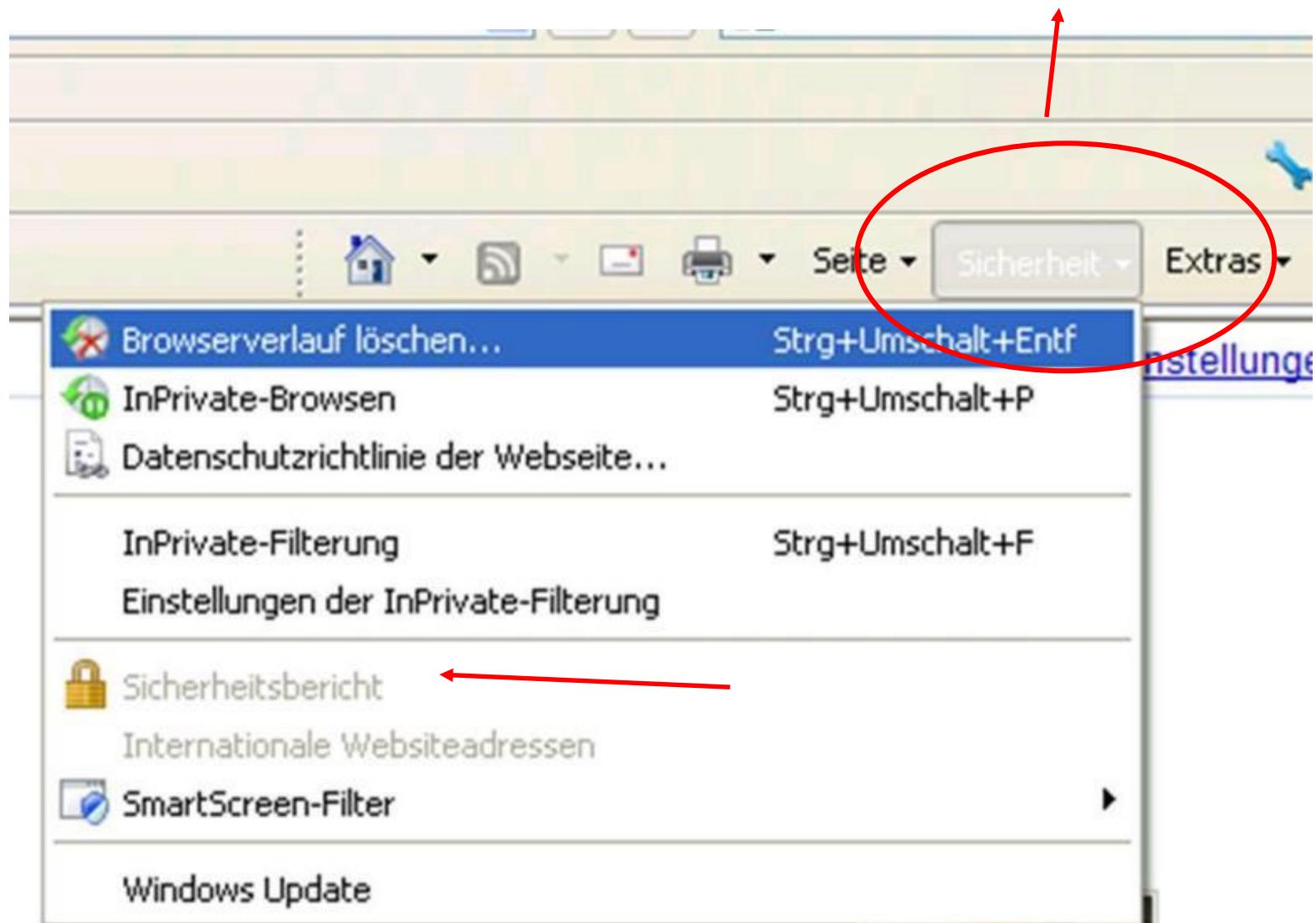
Mehr Informationen

[Impressum](#) [Nutzungsbedingungen](#) [Datenschutz](#) [Preisverzeichnis](#) [Sicheres Banking](#)

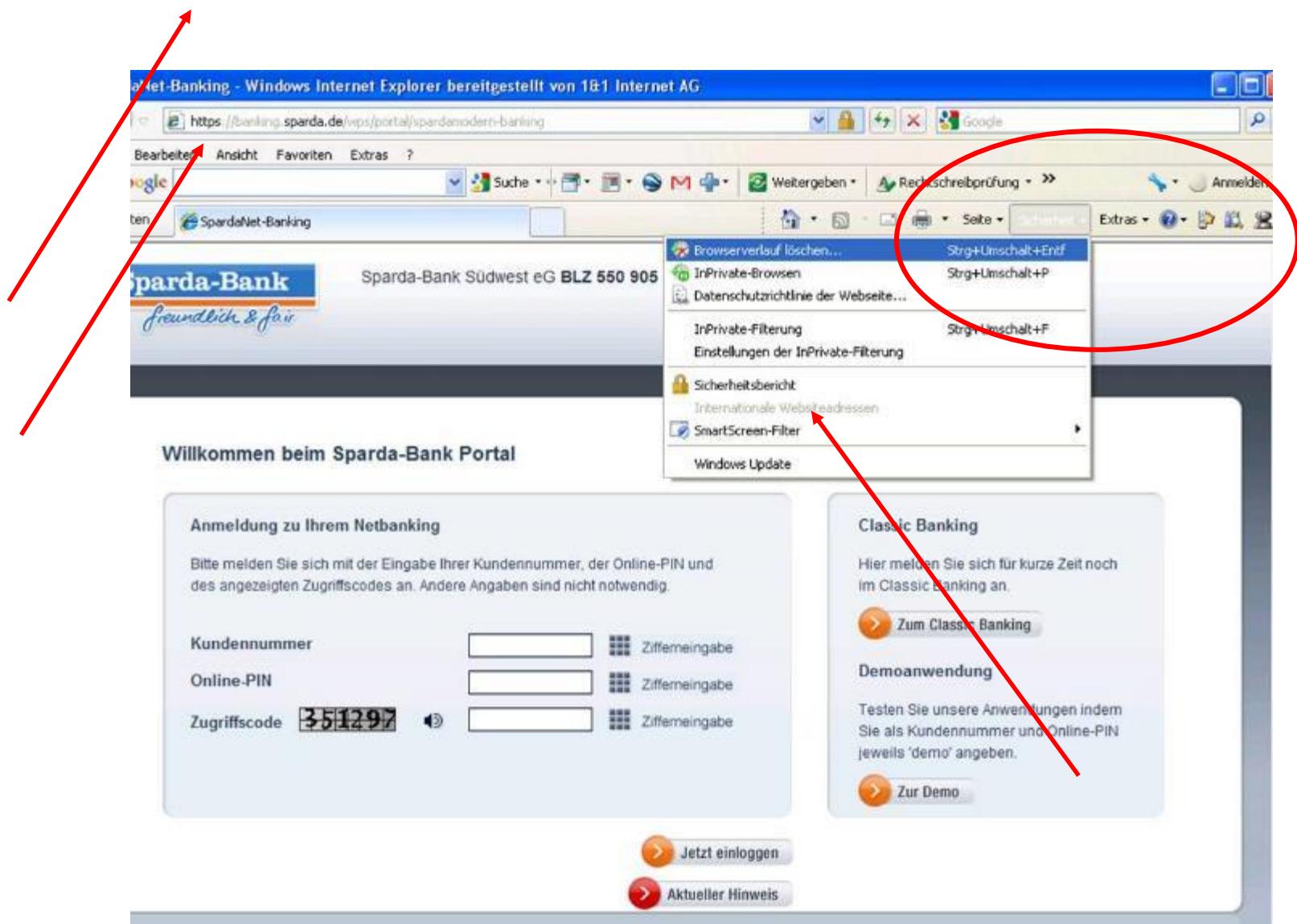
# Gefahren für die IT-Sicherheit

Von	Betreff
 Sparkasse Online-Banking	e-Banking Aktualisierung.
 "rechnungonline@mail.vodafone.de"	Ihre Festnetz-Rechnung für November 2014
 Vodafone D2	Ihre Rechnung 340590572 vom 20.11.2014
 "support@t-online.de"	Ihre Rechnung 417557744159 vom 19.11.2014
 Fiducia	code / 3700518839854004 / 18.11.2014 / 12:48:01

- ➔ **Einsatz von aktuellen Browsern**
- ➔ **Beachtung von Warnhinweisen**
- ➔ **Nutzung von verschlüsselter Verbindung, Prüfung der Zertifikate**



<https://banking.sparda.de/wps/portal/spardamodern-banking>



# Gefahren für die IT-Sicherheit

The image shows a composite screenshot. On the left, a portion of an email client interface is visible, showing a folder structure with 'SPAM' and 'TRASH' and a list of emails. On the right, a detailed view of an email message is shown. The email subject is 'Dringend Maßnahmen erforderlich!' and the 'From' field is highlighted with a red box, showing 'Sparkasse <nilton@idt.org.br>'. The message body starts with 'Sehr geehrter Kunde,' and discusses a project to combat a recent scam. It ends with a link to 'https://Sparkasse.de' and a note to 'Mit freundlichen Grüßen Ihre Sparkasse'. Below the email, a browser window is shown with a red box highlighting a link in the address bar: 'hail.or.kr/bbs/data/secure/sparkasse/sparkasse.de.htm'. A red arrow points from this link to a red box on the left side of the browser, which contains the text 'Kostenlos testen...'.

Dringend Maßnahmen erforderlich!

Von: Sparkasse <nilton@idt.org.br>

An: undisclosed recipient(s),

Erhalten: 15.03.2013 13:54

Sehr geehrter Kunde,

im vergangenen Jahr wurde die Sparkasse zusammen mit vielen anderen Deutschen Kre Betruges. Daher haben wir ein Projekt zur Bekämpfung gestartet.

Auf allen Online-Girokonten soll nun ein neu entwickeltes Sicherheitssystem installiert wer Transaktionen schnell aufspüren und lösen kann.

Wir haben festgestellt, dass Ihr Girokonto noch nicht mit diesem Sicherheitssystem ausge um dieses Sicherheitsupdate/Maßnahmen zu vervollständigen.

Nach dem Update wird sie einer unserer Mitarbeiter kontaktieren, um den gesamten Pro: Girokonto wieder einwandfrei gesichert und Sie können es wie gewohnt nutzen.

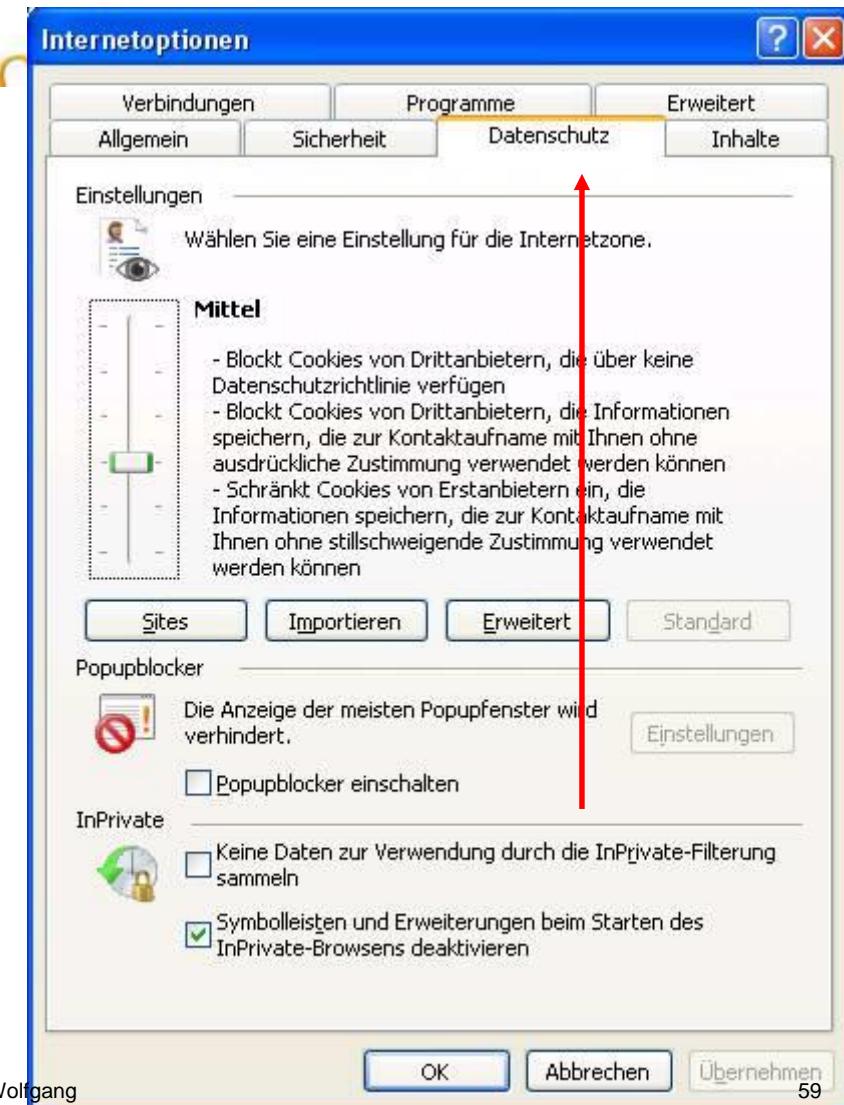
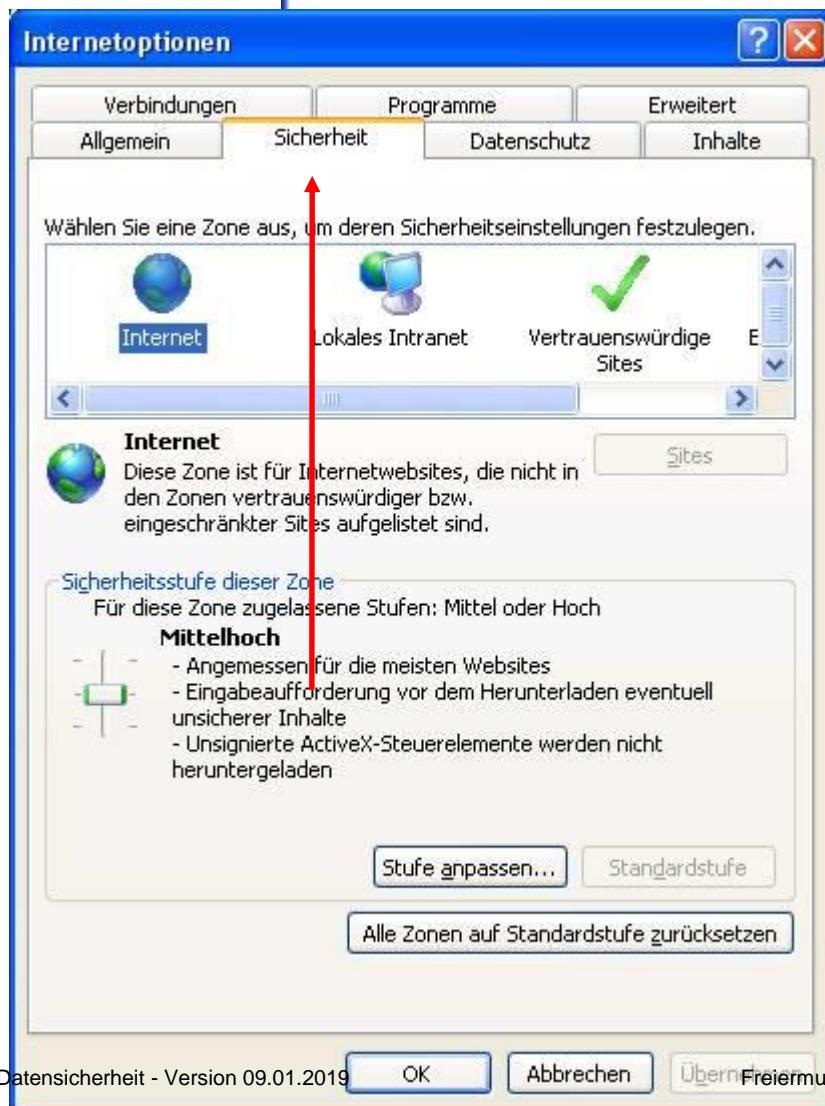
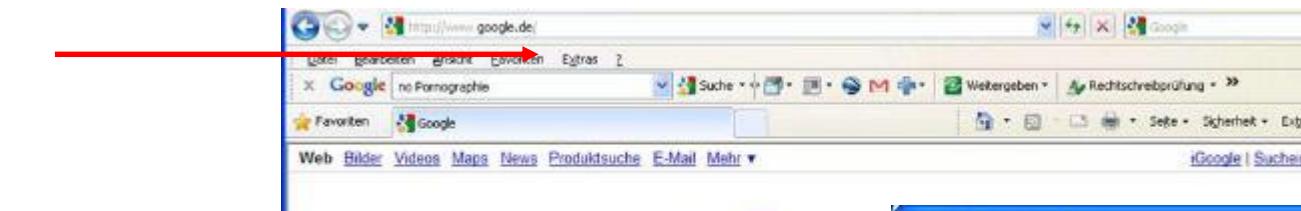
Wir wollen Ihnen im Voraus für Ihre Mitarbeit danken.

<https://Sparkasse.de>

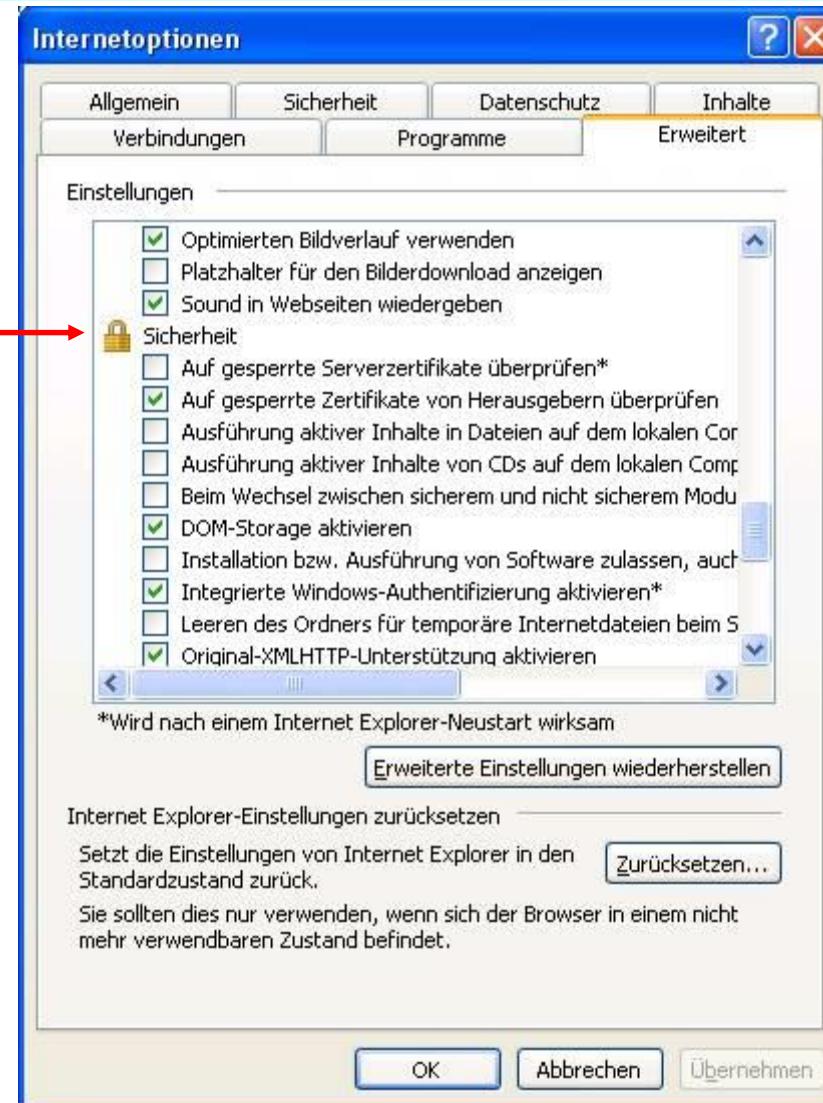
Mit freundlichen Grüßen  
Ihre Sparkasse

Kostenlos testen...

hail.or.kr/bbs/data/secure/sparkasse/sparkasse.de.htm



# Gefahren für die IT-Sicherheit



# Gefahren für die IT-Sicherheit



- **(Werbe-) PopUp's**

- Einblendungen in Bildschirmfenstern
- sind oftmals lästig und werden „einfach weggeklickt“
- das „Wegklicken“ löst möglicherweise ungewollte Aktionen aus

## Auszug aus dem Inhalt eines Werbefenster:

„Mit dem Schließen dieses Fensters bestätigen Sie Ihre Einwilligung zum Installieren einer Softwarekomponente, durch die kostenpflichtige Verbindungen zum Anbieter der Webseite XY aufgebaut werden. Gleichzeitig verzichten Sie auf Ihr Widerspruchsrecht.“

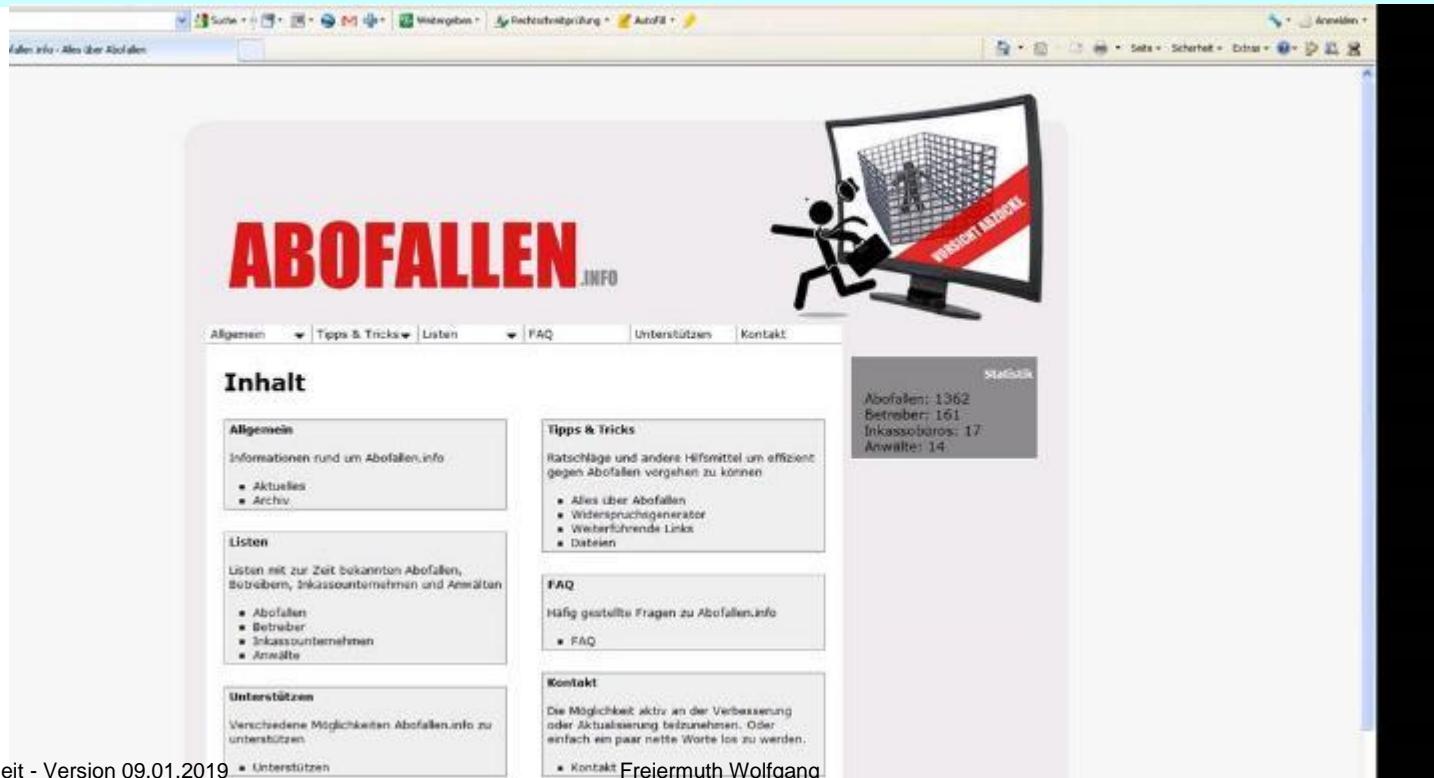
- **Windows Nachrichtendienst**

- Im Windows Betriebssystem enthalten (LAN Messenger, „WinPopUp“)
- dient der Kontaktaufnahme zwischen den Nutzern innerhalb eines Windowsnetzwerkes
- wird gerne von Administratoren eingesetzt, um Nutzer zu informieren
- kann bei falscher Konfiguration auch über das Internet erreicht werden und möglicherweise für Irritationen sorgen



## • Abofallen

- bieten den Internetnutzern Downloadmöglichkeiten für diverse Software
- bieten teilweise kostenlose Software im Rahmen sogenannter „Supportverträge“



# Gefahren für die IT-Sicherheit

## • Abofallen

- führen möglicherweise zum Abschluss von Abo-Verträgen mit hohen Kosten und langen Laufzeiten (<http://www.opendownload.de>)



# Gefahren für die IT-Sicherheit

Apache OpenOffice - Deutsche Startseite - Windows Internet Explorer

http://www.openoffice.org/de/?utm\_source=OoO3\_3\_de&utm\_medium=Client&utm\_campaign=Upgrade

Datei Bearbeiten Ansicht Favoriten Extras ?

Google Suche Teilen AutoFill Mehr >

Favoriten Das Örtliche für Landau-Pfal... Stadt Landau - Das Telefonbuch Deutschla... Freie Wähler Gemeinschaft... FOCUS Online - Nachrichten 1&1 Webmailer 2 SPIEGEL ONLINE - Nachrichten 1&1 Hilfe-Center Amazon Google

Google Apache OpenOffice - Deu... Apache OpenOffice - Deu...

 Apache OpenOffice™ | The Free and Open Productivity Suite

## Announcing Apache OpenOffice 3.4

home » de

Wir suchen Verstärkung für unser Team. Mehr Informationen unter <http://www.openoffice.org/de/mithelfen.html>

**Neu hier?**  
[Download](#) · [Kurzinfo](#) · [Features](#) · [PrOo-Box](#) · [Sitemap](#)

**Probleme?**  
[FAQ](#) · [Dokumentation](#) · [Mailinglisten](#) · [Foren](#) · [Oo-Wiki](#) · [Ansprechpartner](#) · [Das Team](#)

**Mithelfen?**  
[EIS](#) · [BugZilla](#) · [Wiki](#) · [TCM](#) · [Tools](#) · [IRC](#) · [Blogs](#) · [Glossar](#) · [QATrack](#)

**Marketing & Presse**  
[Marketing-Material](#) · [Pressebereich](#) · [Referenzen](#) · [Präsentationen](#)

Apache OpenOffice - die freie Bürossoftware

Apache OpenOffice ist sowohl eine [Office Suite](#), die auf vielen [Betriebssystemen](#) und in zahlreichen [Sprachen](#) verfügbar ist, als auch ein [Open-Source](#) Projekt, bei dem ehrenamtliche Mitglieder das Produkt immer weiter verbessern und unterstützen. Für diese Gemeinschaft suchen wir ständig neue Mitglieder.

  
Writer Math Calc Draw Impress Base

 **Download**  
[Die aktuelle Version von Apache](#)  
[Die aktuelle Portable-Version](#)  
(externer Link zu winPenPack)

**Warnung vor Download-Abofallen**

A red arrow points from the text "Warnung vor Download-Abofallen" to the "Download" section.

# Comeback der Internet-Abofallen

## Gefahren für d

von BERRIT GRABER

**MÜNCHEN.** Vor zwei Jahren sollte ein Gesetz der Online-Abzocke mit Routenplanern und Kochrezepten einen Riegel vorschieben. Doch die Gauner sind zurück. Und bitten noch frecher zur Kasse.

Am 1. August 2012 trat die sogenannte Buttonlösung EU-weit in Kraft. Das Gesetz versprach Millionen Internet-Surfern Schutz vor Kostenfallen, vor unerwünschten Abonnements zu Intelligenztests oder Softwareprogrammen und vor monatelangem Inkassoräger. Doch zu früh gefreut. Die Internet-Gauner sind zurück. Und sie versuchen, noch dreister abzukassieren, Gesetz hin oder her. Eine unbedachte Registrierung auf vermeintlich kostenfreien Service-Seiten wie zum Beispiel einem Routenplaner – und schon kommt eine Rechnung ins Haus über ein Jahr „Mitgliedschaft“ für stolze 249 Euro. „Die Internet-Abzocke erlebt eine Renaissance“, warn Martina Totz von der Verbraucherzentrale Rheinland-Pfalz.

Zurzeit melden sich unzählige Verbraucher bei den Verbraucherzentralen. Sie sind verärgert und entnervt, weil sie aus heiterem Himmel Rechnungen und Mahnungen von Anwäl-

ten oder Inkassobüros am Hals haben. Die meisten hatten lediglich nach kostenlosen Kochrezepten für Mittagessen und anderen Service-Angeboten gesucht. Gelandet sind sie aber auf den Seiten fragwürdiger Anbieter wie routenplaner-24.net, rezepte-portal-24.net, horoskop-portal-24.net oder tattoo-vorlagen-24.net. Nur, weil sie ihre E-Mail-Adresse eintippten, um sich beim Portal anzumelden, sollen sie jetzt die einmalige Jahresgebühr von 249 Euro zahlen.

Es werden Gebühren in Höhe von 249 Euro verlangt und falsche Gerichtsurteile zitiert.

Die totgegläubte Abkassier-Masche sei wieder „quiklebding“, hat auch Anne-Katrin Wiesemann von der Verbraucherzentrale Sachsen beobachtet. Vor 2012 hatten sich die Betrüger allerdings noch auf Forderungen von meist 96 Euro im Jahr beschränkt. Jetzt wollen sie weit mehr als das Doppelte.

Seit August 2012 müssen Anbieter ihre Internets Seiten so gestalten, dass der Verbraucher die kostenpflichtige Bestellung ausdrücklich bestätigt. Ein Button mit der Aufschrift „zahlungspflichtig bestellen“ muss deutlich auf

die Kosten hinweisen, die beim Anklicken fällig werden. Doch der Betreiber der neuen dubiosen Seiten, eine Firma mit Sitz im mittelamerikanischen Belize und einem europäischen Servicecenter in Wien, scheint sich nicht um die gesetzlichen Vorgaben zu scheren. Der Bestellbutton ist nur mit der Aufschrift „Registrieren“ versehen. Außerdem gilt die Widerrufsbelehrung als fehlerhaft.

„Bloß nicht zahlen“, warnt Verbraucherschützerin Wiesemann. Weil der Online-Anbieter die gesetzlichen Vorschriften nicht einhalte, komme auch kein Vertrag zustande. Und wer keinen Vertrag abgeschlossen habe, müsse auch nichts bezahlen. Am besten sei, sich gleich nach der ersten unberechtigten Geldforderung aktiv zu wehren, per Einwurfeinschreiben zu antworten und den angeblichen Vertrag zu bestreiten, so Totz. Kostenlose Musterbriefe gibt es unter anderem online unter [www.vz-rlp.de/musterbriefe-internet-telefonie](http://www.vz-rlp.de/musterbriefe-internet-telefonie) oder in den örtlichen Beratungsstellen der Verbraucherzentralen.

Neu ist, dass die heutigen Betrüger offenbar gezielt falsche Gerichtsurteile zur Rechtslage im Internet streuen, wie die Verbraucherzentrale Sachsen-Anhalt warnt. Die Urteile seien frei erfunden.



Freiermuth Wolfgang

# Gefahren für die IT-Sicherheit



Liebe Winzerinnen und Winzer,

heute sind wir von einem Pfälzer Weingut informiert worden, dass er per Post ein Schreiben erhalten hat, welches den Eindruck einer Datenaktualisierung für die Pfälzer Wein- und Sektmesse in Bad Dürkheim suggeriert.

Dieses Schreiben ist weder von Pfalzwein e.V. noch von der Landwirtschaftskammer in Neustadt versendet worden.

Wir möchten Sie warnen, dass Sie dieses Auftragsformular nicht ausfüllen. Der Inhaber dieses ~~Expo-Guides~~ hat seinen Sitz in Mexiko und mit der Unterschrift wird ein Jahresbeitrag von 1181 Euro fällig.

Wir wissen nicht, ob es so ein Schreiben auch mit einer Datenaktualisierung für die andere Weinmessen gibt. In diesem Fall gilt das Gleiche.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Viele Grüße

**Susanne Breiling**

# Gefahren für die IT-Sicherheit

## • Bewertungsportale

**Schauen Sie sich mal diese Sauerei an - Das Hörbuch zum SPIEGEL-Bestseller: 23 wahre Geschichten vom Lebenretten** von Jörg Nießen (1. Oktober 2011) - Audiobook

**EUR 19,95 Audio CD**

Bestellen Sie in den nächsten **11 Stunden**, um den Artikel am Mittwoch, 28. November zu erhalten.

**Die Mütter-Mafia** von Kerstin Gier (14. Mai 2012)

**EUR 7,99 Taschenbuch**

Bestellen Sie in den nächsten **11 Stunden**, um den Artikel am Mittwoch, 28. November zu erhalten.

Andere Angebote - Taschenbuch

**EUR 5,99 neu** (98 Angebote)

**EUR 1,58 gebraucht** (96 Angebote)

**der lachenden Engel** von Jörg Nießen

Andere Angebote - Audio CD

**EUR 3,90 neu** (38 Angebote)

**EUR 2,90 gebraucht** (1 Angebot)

**Fitzek**

**503 Rezensionen**

Sterne	Anzahl
5 Sterne:	(391)
4 Sterne:	(48)
3 Sterne:	(34)
2 Sterne:	(11)
1 Stern :	(19)

› [Alle 503 Kundenrezensionen anzeigen...](#)

› [Alle Diskussionen](#)

- **Bewertungsportale**

- Reisen
- Autos/Werkstätten
- Ärzte/Gesundheit
- Restaurants
- usw.

„**Falsche**“ Infos im Netz:  
Umweltplakette Frankreich

- **positive Bewertung**
- **negative Bewertung**
- **konstruktive Bewertung**
- **destruktive Bewertung**
- **Selbstbewertung**

[Umweltplakette.pdf](#)

- **Bewertungsportale**

**Frei nach Churchill (?):**

**„Traue keiner Statistik, die du nicht selbst gefälscht hast..“**

**Frei nach Computerzeitschrift „CHIP“:**

**„5-Sterne-Mafia“ ==> Agenturen bieten Dienstleistungen an**

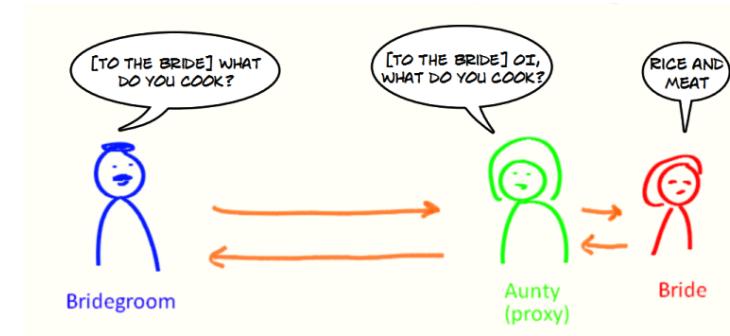
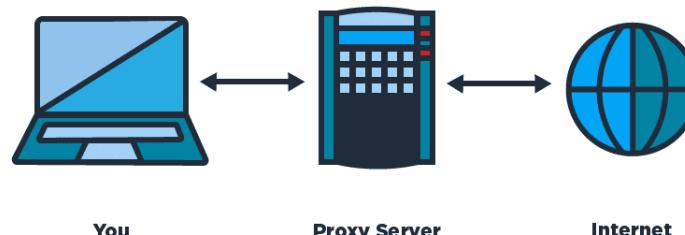
- ✓ **Große Portale bevorzugen**
- ✓ **Möglichst viele Bewertungen zu einem Produkt**
- ✓ **Wer hat bewertet**
- ✓ **Achten Sie auf die Sprache**
- ✓ **Suchen Sie gezielt nach negativen Bewertungen**
- ✓ **Prüfen Sie auf mehreren Portalen**



- **Proxy**

Ein Proxy ist eine Kommunikationsschnittstelle/Netzrechner in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.

Ist der Netzrechner entsprechend manipuliert, kann er Datenpakete nicht von A nach B leiten, sondern „über Bande“. D.h., Dritten wird ermöglicht, über die Adresse des Proxys im Internet zu agieren.



Bräutigam

Tante=Manipulator

Braut



## • Ripper

sind Betrüger, die an Schwarzmärkten Geld verdienen, aber dann die Ware nicht liefern.

Auch bezahlte und nicht ausgeführte Hackerdienste  
→ auch Cyberkriminelle werden hinters Licht geführt



## • Zero Day Exploit



Eine Sicherheitslücke, für die es noch keine Schutzmaßnahmen gibt, wird von Hacker entdeckt und ausgenutzt.



## • Verborgene Befehle

Unhörbare Manipulation:

Die Spracherkennung von Alexa, Cortana, Siri und Co kann ein Einfallstor für subtile Manipulation sein, wie deutsche IT-Forscher festgestellt haben. Denn über für uns unhörbare Kanäle – beispielsweise versteckt in einem Radiosong – können geheime Befehle an die Assistenten gesendet werden. Diese manipulativen Botschaften bringen das System dann dazu, eine Tür zu öffnen oder online Waren zu kaufen.

# Gefahren für die IT-Sicherheit

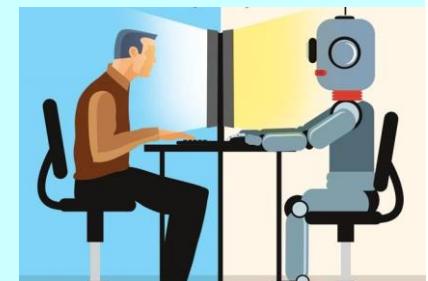
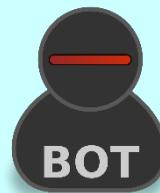
- **Deepfakes**

Audio- und Videodateien,  
in denen die Stimme und Gesichter von z.B.  
Politikern täuschend echt manipuliert werden.  
Jede beliebige Aussage wird  
in den „Mund gelegt“ und alles sieht  
echt aus und hört sich echt an.



- **Bots**

automatisierte Computerprogramme,  
die politische Botschaften verbreiten.  
Ihr Einfluss ist „besorgniserregend“;  
sie befeuern die Verbreitung von Desinformationen.



# WHAT DOES **DOXING**

„Bei einem Hacker-Angriff auf hunderte deutsche Politiker wurden zahlreiche personenbezogene Daten geklaut und veröffentlicht.  
Dieser Vorgang hat einen Namen: Doxxing.“  
(FAZ, 04.01.2019)

- **Doxing**

**dox**, Abkürzung für documents, auch **doxxing**, ist das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, zumeist mit bösartigen Absichten gegenüber den Betroffenen.



## Zum „Die Insel der Gutgläubigen“

Die meisten Menschen gehen noch immer viel zu sorglos mit ihren persönlichen Daten im Internet um – oft aus Unwissenheit. Dabei ist das Internet schon lange kein Neuland mehr. Aber kennen Sie etwa den Unterschied zwischen Doxing und Hacking?“  
etwa (FAZ, 08.01.2019)

Personen, die vom Doxing betroffen sind, sind oft Folgeattacken ausgesetzt, basierend auf den veröffentlichten Daten.

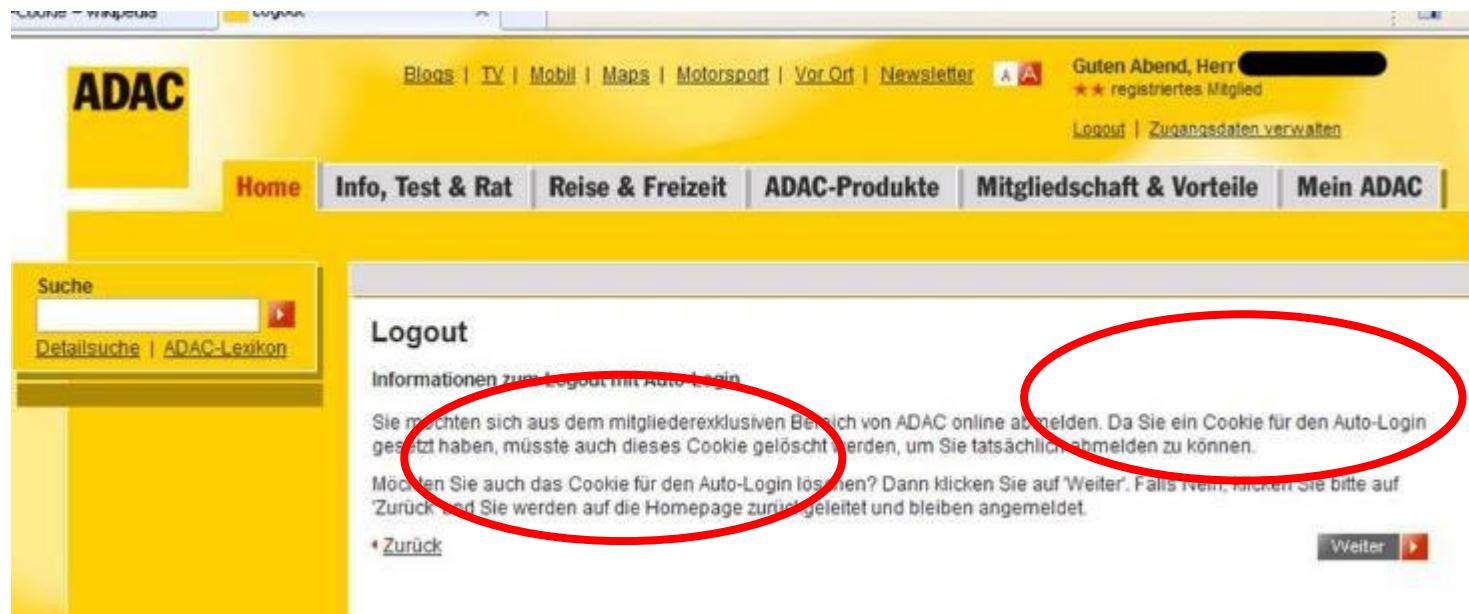


## • Cookies (auf Deutsch: Plätzchen, Kekse)

- **S** Normalerweise darf jeder Betreiber eines Internetplatzes nur **sein** **Cookie** auslesen.
- **U** So darf Online-Shop A nicht den Cookie von Online-Shop B auslesen.
- **I** ABER:
  - **R** Setzt ein sogenannter **Drittanbieter** ein Werbebanner auf A und
  - **R** auch ein Werbebanner auf B, dann wird mit Hilfe dieser Cookies
    - **V** doch ein Surfverhalten des Verbrauchers erhalten - bis das Cookie
- **I** gelöscht wird.
- **V** Es gibt dauerhafte Cookies (evtl. über Jahre auf dem PC) und
- **S** Session- Cookies (werden nur für den Zugriff gesetzt, wie bei Online-Banking, und dann gelöscht, wenn der Browser geschlossen wird).



Beim Suchen nach einem Bild für Mini Tower für mein Script  
kam diese Meldung!



Guten Abend, Herr ██████████  
★★ registriertes Mitglied

Logout | Zugangsdaten verwalten

Home | Info, Test & Rat | Reise & Freizeit | ADAC-Produkte | Mitgliedschaft & Vorteile | Mein ADAC

**Logout**

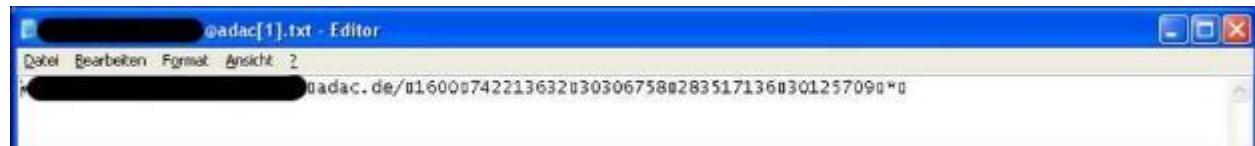
Informationen zum Logout mit Auto-Login

Sie möchten sich aus dem mitgliederexklusiven Bereich von ADAC online abmelden. Da Sie ein Cookie für den Auto-Login gesetzt haben, müsste auch dieses Cookie gelöscht werden, um Sie tatsächlich abmelden zu können.

Möchten Sie auch das Cookie für den Auto-Login löschen? Dann klicken Sie auf 'Weiter'. Falls Nein, klicken Sie bitte auf 'Zurück' und Sie werden auf die Homepage zurückgeleitet und bleiben angemeldet.

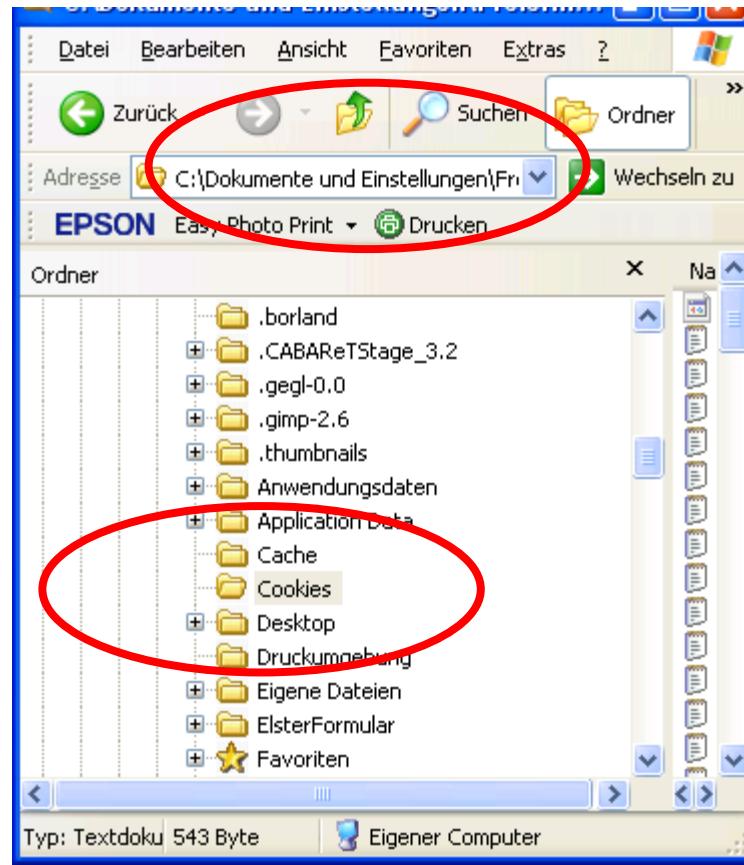
[Zurück](#) [Weiter](#)

name@www.adac[1].txt

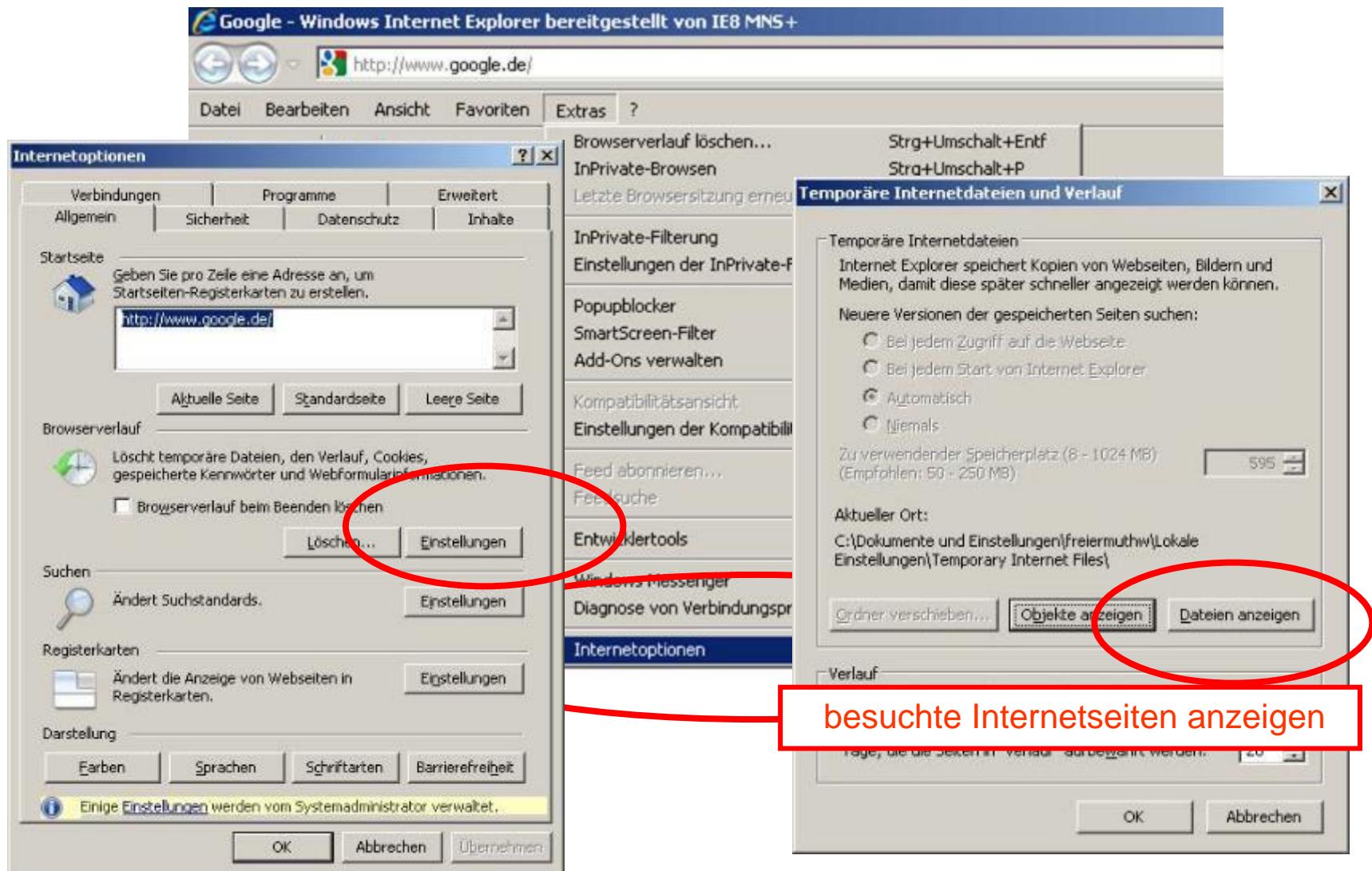


- Cookies dienen der Wiedererkennung des Benutzers
- stellen einfache Informationsspeicherung am Client ohne aufwändige Programmierung am Server dar

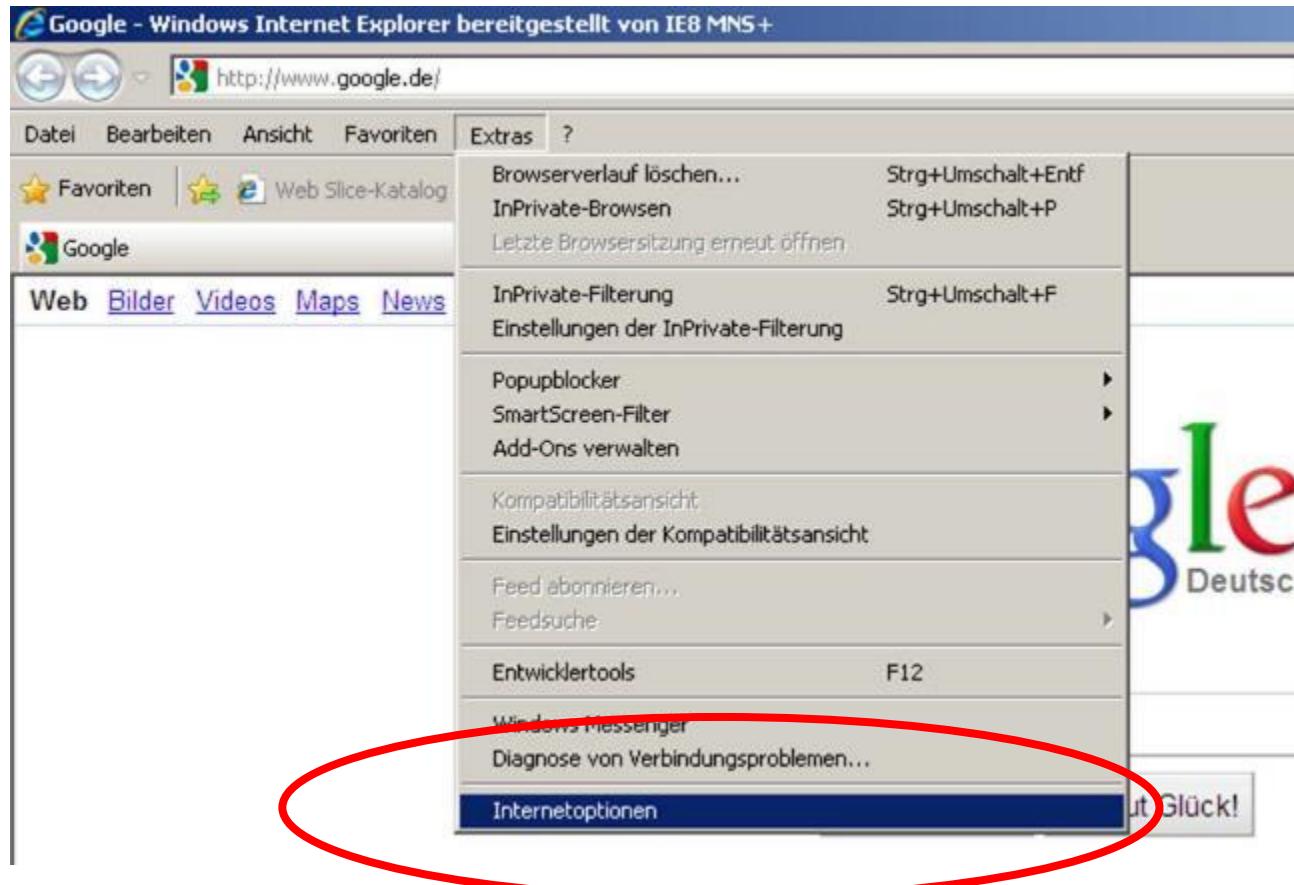
**Der Browser speichert besuchten Webseiten im „Cache“, um schneller zugreifen zu können.**



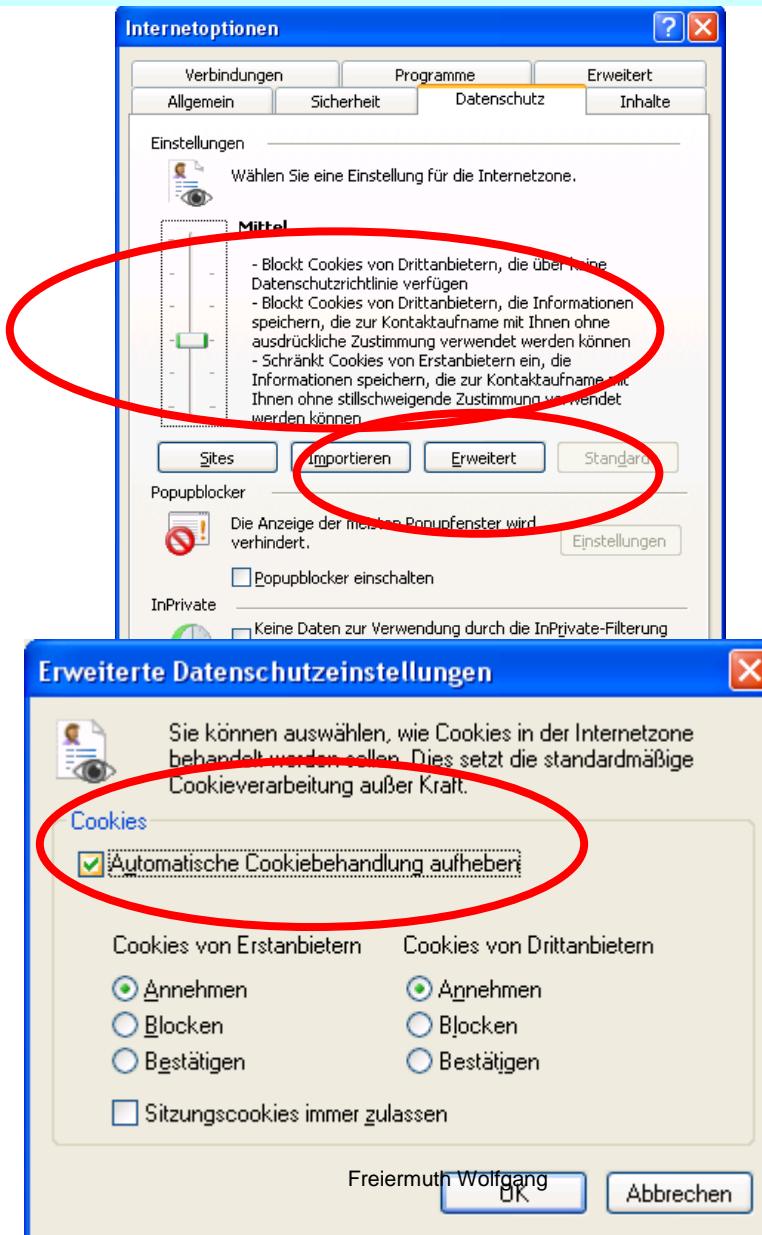
# IT-Sicherheit und Datenschutz



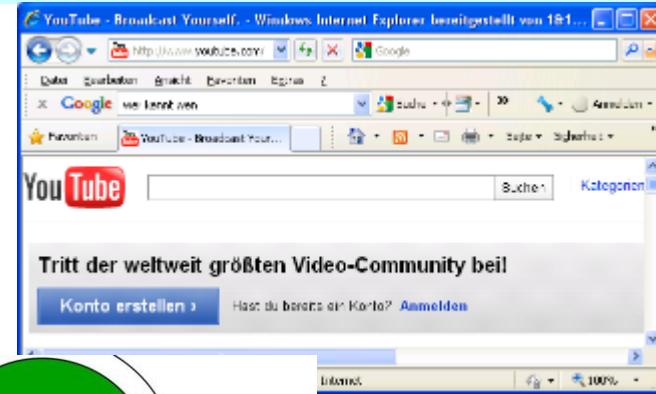
# IT-Sicherheit und Datenschutz



# IT-Sicherheit und Datenschutz



## virtueller Exhibitionismus



## WhatsApp





- **Tracker oder Tracking-Cookies**

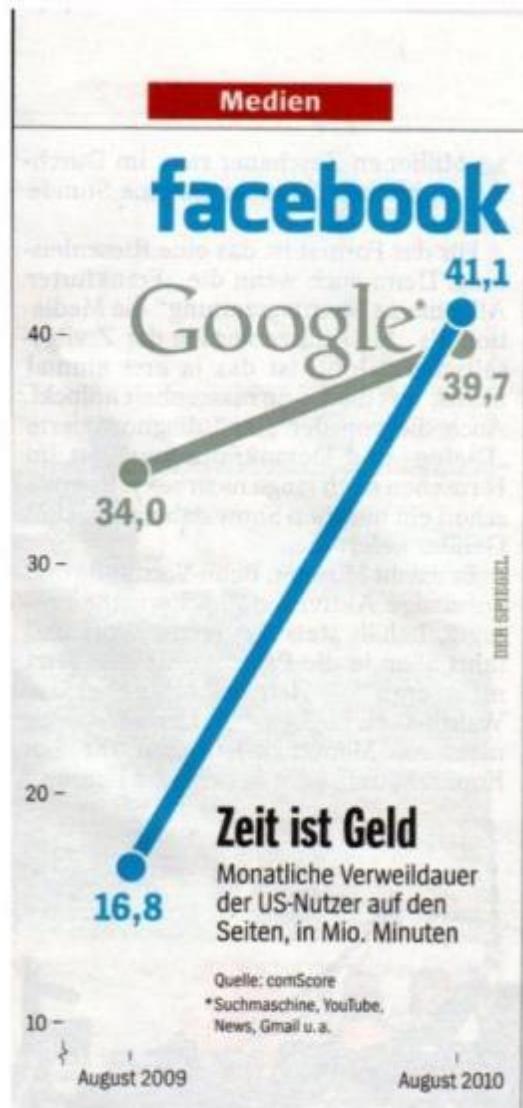
- sind eine besondere Form der Cookies (Cookies: kleine Dateien, mit denen Webseitenbetreiber sofort merken, wenn ein bereits bekannter User erneut auf die Webseite geht).
  - Tracker oder Tracking-Cookies informieren nicht nur den Webseitenbetreiber. Sie verfolgen den Nutzer über mehrere Webseiten hinweg. Daher auch der Name „Cross Domain Tracker“.
  - So bekommen die Absender der Tracker sehr genaue Infos über das Surfverhalten, die Interessen und die Kaufgewohnheiten.
  - => Profile des Users können erstellt und gegen Gebühr weitergereicht werden.
  - Tracking unterbinden mit:  
Browsererweiterung wie NoScript  
Programm Ghostery  
Download der Trackinglisten vom Fraunhofer Institut für Sichere Informationsverarbeitung (für den Internet Explorer, müssen ständig aktualisiert werden)

# IT-Sicherheit und Datenschutz

"Zusammenführen" von Informationen:



## IT-Sicherheit und Datenschutz



Was der Firma noch gefährlich werden kann, ist ihr notorisch salopper Umgang mit den Nutzerdaten. Schon der neue E-Mail-Dienst geht ein hohes Risiko ein: Versprochen ist, dass Facebook die gesamte Kommunikation auf ewig speichert – Löschen ist, gelinde gesagt, umständlich. Aber werden die Mitglieder ihre gesamte Lebensgeschichte, aufgefädelt in zahllosen Konversationen über Jahre und Jahrzehnte, diesem unberechenbaren Konzern anvertrauen?

Der Spiegel 47/2010



## Teilen deiner Inhalte und Informationen

Dir gehören alle Inhalte und Informationen, die du auf Facebook postest. Zudem kannst du mithilfe deiner Privatsphäre- und App-Einstellungen kontrollieren, wie diese geteilt werden. Außerdem gilt:

Alles was du wissen musst an einem Platz.

1. Für Inhalte wie Fotos und Videos, die unter die Rechte am geistigen Eigentum fallen (sog. „IP-Inhalte“), erteilst du uns durch deine Privatsphäre- und App-Einstellungen die folgende Erlaubnis:  
Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz“). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löscht, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.

2. Wenn du IP-Inhalte löscht, werden sie auf eine Weise entfernt, die dem Leeren des Papierkorbs auf einem Computer gleichkommt. Allerdings sollte dir bewusst sein, dass entfernte Inhalte für eine angemessene Zeitspanne in Sicherheitskopien fortbestehen (die für andere jedoch nicht zugänglich sind).

### Mein Konto löschen

Falls du glaubst, dass du Facebook nicht noch einmal verwenden und dein Konto löschen möchtest, können wir uns darum kümmern. Denke daran, dass du dein Konto weder reaktivieren noch die von dir hinzugefügten Informationen oder Inhalte erneut abrufen kannst.

Wenn du dein Konto immer noch löschen möchtest, klicke auf „Mein Konto löschen“.

[Erfahre mehr zur Kontolösung](#)

[Mein Konto löschen](#) [Abbrechen](#)

[Seite erstellen](#) [Entwickler](#) [Karrieren](#) [Datenschutz](#) [Cookies](#) [Impressum/Nutzungsbedingungen](#)

4. Wenn du die Einstellung „öffentlich“ bei der Veröffentlichung von Inhalten oder Informationen verwendest, können alle Personen, einschließlich solcher, die Facebook nicht verwenden, auf diese Informationen zugreifen, sie verwenden und sie mit dir (d. h. deinem Namen und Profilbild) assoziieren.

## 17. Besondere Bestimmungen für Nutzer außerhalb der USA

Du bist damit einverstanden, dass deine persönlichen Daten in die USA weitergeleitet und dort verarbeitet werden.

## Neue Nutzungsbedingungen: Was sich ab Februar 2015 bei Facebook ändert

„Die Nutzer müssen sich damit abfinden, mehr Daten preiszugeben - oder das Netzwerk verlassen.,, (Spiegel.de)

Video:

<http://www.spiegel.de/video/facebook-aendert-nutzungsbedingungen-ein-video-kommentar-video-1552330.html>

aus: Spiegel-Online 30.01.2015

## Das Wichtigste aus den neuen Nutzungsbedingungen in 5 Stichworten:

1. **Sichtbarkeit:** Facebook will es Nutzern leichter machen, zu entscheiden, wer ihre Inhalte sieht. Viele Einstellungen zum Datenschutz müssen die Nutzer aber in der Regel selbst mit ein paar Klicks aktivieren. Dabei ist es wichtig zu beachten, dass auch Daten, die für andere Nutzer unsichtbar sind, noch immer von Facebook gesehen werden könnten.
2. **Standortdaten:** Künftig kann Facebook anhand der Standortdaten gezielte Werbeanzeigen schalten - zum Beispiel von Restaurants in der Nähe. Facebook kann auch gezielt Neuigkeiten von Freunden aus der Umgebung anzeigen. Wer das nicht möchte, sollte wenn möglich der Facebook-App auf seinem Smartphone den Zugriff auf das GPS-Modul verbieten - und die GPS-Verbindung nur anschalten, wenn er sie wirklich braucht.

aus: Spiegel-Online 30.01.2015

3. **Kaufen-Button:** Das Netzwerk will diese neue Schaltfläche zunächst nur in einigen Regionen testen. Mit dem Kaufen-Button können Kunden direkt über das Facebook-Konto Waren bestellen. Damit kann das Unternehmen neben Nutzungsdaten auch an Einkaufsgewohnheiten und Zahlungsdaten der Kunden kommen. Durch Zusammenführung dieser Daten könnten umfassende Personenprofile erstellt werden.
4. **Werbung:** Facebook darf nun auch auswerten, welche anderen Websites die Nutzer im Netz besucht haben und welche Apps sie verwenden. So will das Unternehmen Werbung noch genauer auf den Einzelnen zuschneiden. Wer dann etwa online ein Paar Sportschuhe kauft, könnte beispielsweise Anzeigen für Sportkurse oder andere Trainingskleidung sehen. Bislang wurden die Inhalte der Werbeanzeigen nur aus "Gefällt mir"-Angaben und anderen Aktivitäten im Netzwerk generiert. Die Nutzer können sogar freiwillig dabei helfen, die Werbung zu optimieren, indem sie selbst die Relevanz der Anzeigen bewerten.
5. **Interessenprofil:** Nutzer können nun mit einem Klick auf die rechte obere Ecke der Werbeanzeigen herausfinden, warum sie genau diese Werbeanzeige sehen. Facebook gewährt ihnen also einen Einblick in ihre auf gesammelten Daten basierende Anzeigenpräferenz.

aus: Spiegel-Online 30.01.2015

## Protokolldaten

### Beispiel 1: Mailserververlogdatei

Jan 24 05:57:05 gateway sendmail[14510]: m004v9UM014510: **to=XXX@mail.XXXXXXXXXXXXXX**, **from=<www-data@media.XXXXXXXX>**, **size=1780**, **class=0**, **arcpts=1**, **msgid=<20080124045621.58EF81C31FD@media.XXXXXXXX>**, **proto=ESMTP**, **daemon MTA**, **relay=mail.XXXXXXXX [XXXXXXXXXX]**

Jan 24 05:57:09 gateway amavis[13611]: (m004v9UM014510) AMCL /var/spool/amavis/amavis-milter-0004v9UM014510: <www-data@media.XXXXXXXX> -> <XXX@datenschutz.rlp.de>

Jan 24 05:57:09 gateway amavis[13611]: (m004v9UM014510) Checking: <www-data@media.XXXXXXXX> -> <XXX@datenschutz.rlp.de>

Jan 24 05:57:21 gateway amavis[13611]: (m004v9UM014510) spam\_scan: hits=-4.901 tests=BAYES\_00

Jan 24 05:57:21 gateway amavis[13611]: (m004v9UM014510) **Passed** <www-data@media.XXXXXXXX> -> <XXX@datenschutz.rlp.de>, Message-ID: <20080124045621.58EF81C31FD@media.XXXXXXXX>, Hits: -4.901

Jan 24 05:57:21 gateway sendmail[14510]: m004v9UM014510: Milter change: header X-Virus-Scanned: from amavisd-new at media.XXXXXXXX to by amavisd-new

Jan 24 05:57:21 gateway amavis[13611]: (m004v9UM014510) TIMING [total 12501 ms] - got data: 0 (0%), body hash: 2 (0%), mkdir parts: 1 (0%), mime\_decode: 30 (0%), get-file-type: 19 (0%), decompose\_part: 3 (0%), parts: 0 (0%), AV-scan-1: 11481 (92%), SA msg read: 5 (0%), SA parse: 5 (0%), SA check: 939 (8%), unlink-1-files: 10 (0%), rmdir: 0 (0%), unlink-1-files: 0 (0%), rmdir: 0 (0%), rundown: 2 (0%)

Jan 24 05:57:22 gateway sendmail[14516]: m004v9UM014510: **to=XXX@mail.XXXXXXXXXXXXXX**, **delay=00:00:13**, **xdelay=00:00:00**, **mailer=smtp**, **pri=31988**, **relay=[XXXXXXXXXXXX] [XXXXXXXXXXXX]**, **dn=2.0.0**, **stat=Sent** ( <20080124045621.58EF81C31FD@media.XXXXXXXX> ) **Queued mail for delivery**

wie groß?  
wann?  
von wem?  
an wen?  
OK!

## Protokolldaten

### Beispiel 2: Webserververlogdatei

von wo? 1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET / HTTP/1.1" 200 259 "http://www.google.de/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

wann? 1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /rlp.ico HTTP/1.1" 200 318 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

welche Seite? 1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /cgi-bin/index.cgi" HTTP/1.1" 200 6342 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

wie groß? 1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /format.css HTTP/1.1" 200 3923 "http://www.lverwamt.rlp.de/cgi-bin/index.cgi" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

Verweis von? 1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /images/logo.png HTTP/1.1" 200 10706 "http://www.lverwamt.rlp.de/cgi-bin/index.cgi" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /images/blaubutton.gif HTTP/1.1" 200 79 "http://www.lverwamt.rlp.de/intra.css" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /images/external.png HTTP/1.1" 200 267 "http://www.lverwamt.rlp.de/cgi-bin/index.cgi" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

1X2.1X.33.251 - - [24/Jan/2008:07:49:46 +0100] "GET /images/icon\_acrobat.gif HTTP/1.1" 200 1023 "http://www.lverwamt.rlp.de/intra.css" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11"

## Protokolldaten

### Beispiel 4: Proxyserververlogdatei

von wo?

```
1201268023.656 1020 1X2.1X.2X4.253 TCP_MISS/200 1244 GET http://www.datenschutz.rlp.de/i
noext.html - DIRECT/195.145.244.51 text/html
1201268023.770 113 1X2.1X.2X4.254 TCP_MISS/200 4274 GET http://www.datenschutz.rlp.de/n
avi/head-0.html - DIRECT/195.145.244.51 text/html
1201268023.860 181 1X2.1X.2X4.254 TCP_MISS/200 6279 GET http://www.datenschutz.rlp.de/k
ontrolle/ds_in_rp.html - DIRECT/195.145.244.51 text/html
```

wann?

```
1201268023.936 75 1X2.1X.2X4.254 TCP_MISS/200 414 GET http://www.datenschutz.rlp.de/im
ages/listbutton.gif - DIRECT/195.145.244.51 image/gif
1201268024.095 419 1X2.1X.2X4.254 TCP_MISS/200 5664 GET http://www.datenschutz.rlp.de/n
avi/nav-2.html - DIRECT/195.145.244.51 text/html
1201268025.897 843 1X2.1X.2X4.254 TCP_MISS/200 30131 GET http://www.datenschutz.rlp.de/
kontrolle/oefentlich.html - DIRECT/195.145.244.51 text/html
1201268032.877 688 1X2.1X.2X4.254 TCP_MISS/302 527 GET http://www.datenschutzzentrum.de
/ - DIRECT/213.178.69.184 text/html
1201268033.767 115 1X2.1X.2X4.254 TCP_MISS/302 549 GET http://www.datenschutzzentrum.de
/favicon.ico - DIRECT/213.178.69.184 text/html
1201268049.496 15795 1X2.1X.2X4.254 TCP_MISS/200 15350 CONNECT www.datenschutzzentrum.de:
443 - DIRECT/213.178.69.184 -
1201268049.526 16639 1X2.1X.2X4.254 TCP_MISS/200 48508 CONNECT www.datenschutzzentrum.de:
443 - DIRECT/213.178.69.184 -
1201268093.620 230 1X2.1X.2X4.254 TCP_MISS/200 5340 GET http://sb.google.com/safebrowsi
ng/update? - DIRECT/209.85.135.91 text/html
1201268109.324 15409 1X2.1X.2X4.254 TCP_MISS/200 10186 CONNECT www.datenschutzzentrum.de:
443 - DIRECT/213.178.69.184 -
```

welche Seite?

## Lösungsansätze:

### Firewall

Eine Firewall ist eine Software, die den Zugriff auf ein Netzwerk beschränkt.



Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.

Es wird unterschieden zwischen einer:

- **Personal Firewall** (auch Desktop Firewall) und einer
- **externen Firewall** (auch Netzwerk- oder Hardwarefirewall genannt).

Die Software einer externen Firewall läuft auf einem separaten Gerät und nicht auf dem zu schützenden System selbst.

Die Funktion einer Firewall besteht nicht darin, Angriffe zu erkennen. Sie soll ausschließlich Regeln für die Netzwerkkommunikation umsetzen.

**Lösungen über Filtersysteme:**

**Proxy-Server filtert aus:**

**zum Beispiel das Wort**

**SEX**

## Lösungen über Filtersysteme:

Proxy-Server filtert aus:

zum Beispiel das Wort

zweites juristisches  
**STAATSEXAMEN**

- Reine Wortfilter sind ungeeignet
- Intelligentere Filter sind notwendig aber schwierig zu realisieren

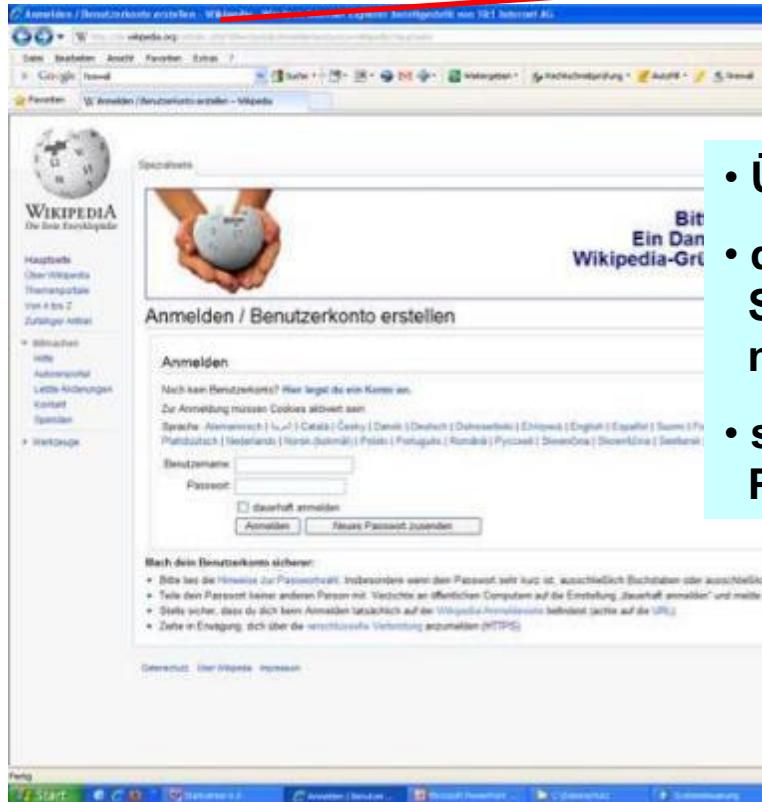
# Lösungsansätze:

## Passwortsicherheit

Stellen	Zeichenvorrat	Anzahl der Zeichen	Möglichkeiten	Dauer	manuell ≈1/10s	Netz ≈150/s	lokaler Rechner ≈10.000/s	Super- Computer ≈1.000.000/s
					Tage	Minuten	Sekunden	Sekunden
4	0-9	10	10.000		1,16	1,11	1,00	0,01
6	a-z,0-9	36	2.176.782.336	Dauer	Jahre 690,25	Tage 167,96	Tage 2,52	Stunden 0,60
8	a-z,A-Z,0-9	62	218.340.105.584.896	Dauer	Jahre 69.235.193,30	Jahre 46.156,80	Jahre 692,35	Jahre 6,92
8	a-z,A-Z,0-9, ,-, #+*!\$%&/()=?<>{}[];:_	76	1.113.034.787.454.980	Dauer	Jahre 352.941.015,81	Jahre 235.294,01	Jahre 3.529,41	Jahre 35,29

# Lösungsansätze:

## Vertraulichkeit im www



- Übertragung mittels **http://** erfolgt **unverschlüsselt**
- damit kann jede an der Übertragung beteiligte Stelle die inhaltliche Information zur Kenntnis nehmen
- somit können **Daten, Zugangswörter und Passwörter abgefangen werden**

## Lösungsansätze:

### Vertraulichkeit im www



- Übertragung mittels **https://** erfolgt **verschlüsselt**
- jede an der Übertragung beteiligte Stelle kann die inhaltliche Information **nicht(?)** zur Kenntnis nehmen

### Vertraulichkeit im Emailverkehr

- Umwandlung in **PDF Dokumente**
- Sicherung mit **Passwort zum Öffnen/Ändern**

## Lösungsansätze:

### Authentizität im Emailverkehr

- **Einsatz der elektronischen Signatur**

Die elektronische Signatur erfüllt technisch gesehen den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten ( $\neq$  digitale Signatur)

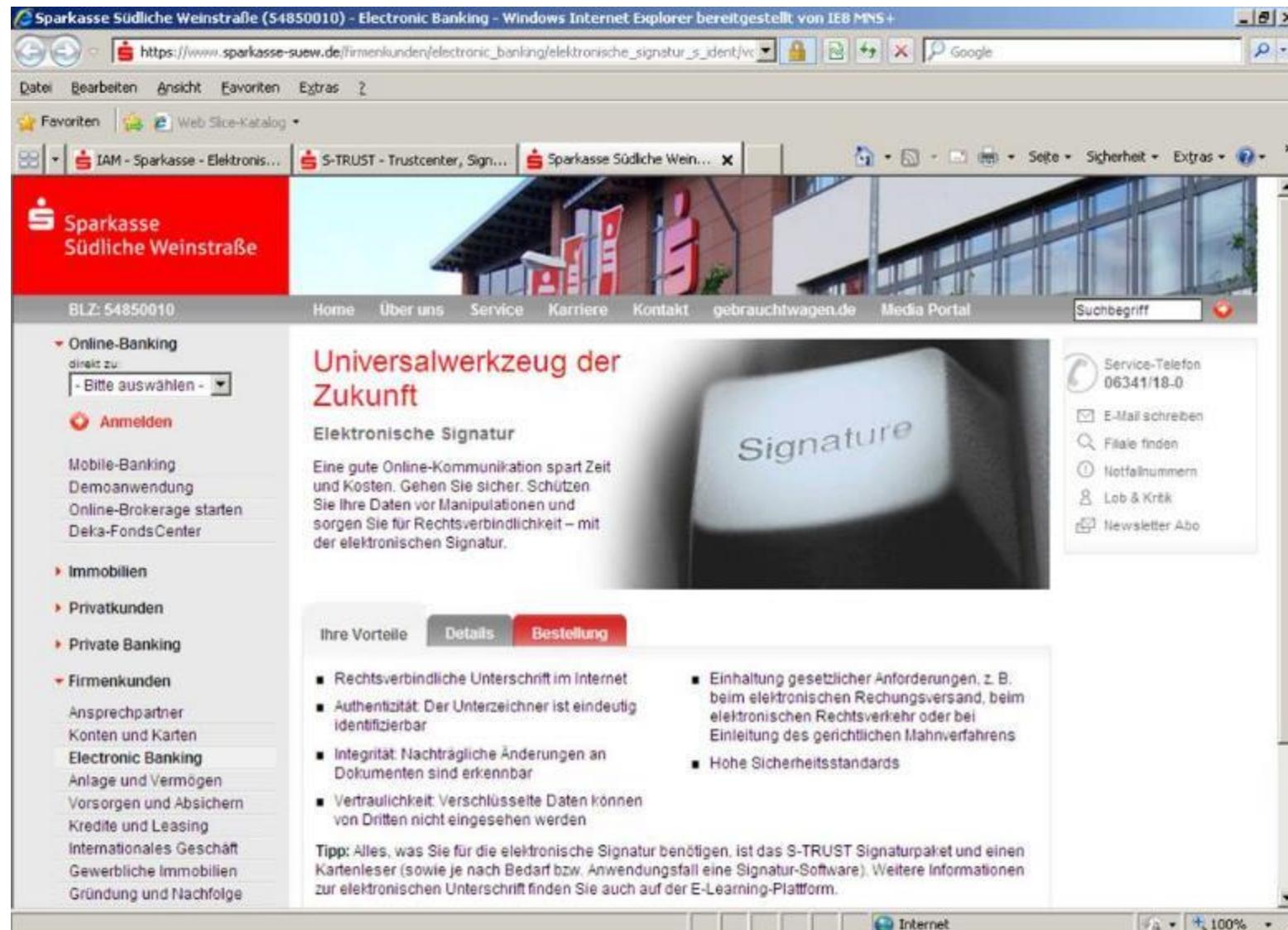
- **Verschlüsselung und elektronische Signatur**

- **Einsatz kryptographischer Verfahren**

<http://www.signatur.rlp.de/>



# Lösungsansätze:



Sparkasse Südliche Weinstraße (54850010) - Electronic Banking - Windows Internet Explorer bereitgestellt von IEB MNS+

https://www.sparkasse-suew.de/firmenkunden/electronic\_banking/elektronische\_signatur\_s\_ident/vs

Datei Bearbeiten Ansicht Favoriten Extras ?

Favoriten Web Side-Katalog

IAM - Sparkasse - Elektronische Signatur S-TRUST - Trustcenter, Signatur-Software

Sparkasse Südliche Weinstraße

BLZ: 54850010 Home Über uns Service Karriere Kontakt gebrauchtwagen.de Media Portal Suchbegriff

Online-Banking direkt zu  
- Bitte auswählen -

Anmelden

Mobile-Banking  
Demoanwendung  
Online-Brokerage starten  
Deka-FondsCenter

Immobilien  
Privatkunden  
Private Banking

Firmenkunden  
Ansprechpartner  
Konten und Karten  
Electronic Banking  
Anlage und Vermögen  
Vorsorgen und Absichern  
Kredite und Leasing  
Internationales Geschäft  
Gewerbliche Immobilien  
Gründung und Nachfolge

Universalwerkzeug der Zukunft

Elektronische Signatur

Eine gute Online-Kommunikation spart Zeit und Kosten. Gehen Sie sicher. Schützen Sie Ihre Daten vor Manipulationen und sorgen Sie für Rechtsverbindlichkeit – mit der elektronischen Signatur.

Service-Telefon 06341/18-0  
 E-Mail schreiben  
 Filiale finden  
 Notfallnummern  
 Lob & Kritik  
 Newsletter Abo

Ihre Vorteile Details Bestellung

- Rechtsverbindliche Unterschrift im Internet
- Authentizität: Der Unterzeichner ist eindeutig identifizierbar
- Integrität: Nachträgliche Änderungen an Dokumenten sind erkennbar
- Vertraulichkeit: Verschlüsselte Daten können von Dritten nicht eingesehen werden
- Einhaltung gesetzlicher Anforderungen, z. B. beim elektronischen Rechnungsversand, beim elektronischen Rechtsverkehr oder bei Einleitung des gerichtlichen Mahnverfahrens
- Hohe Sicherheitsstandards

Tipp: Alles, was Sie für die elektronische Signatur benötigen, ist das S-TRUST Signaturpaket und einen Kartenleser (sowie je nach Bedarf bzw. Anwendungsfall eine Signatur-Software). Weitere Informationen zur elektronischen Unterschrift finden Sie auch auf der E-Learning-Plattform.

## Lösungsansätze:

IAM - Sparkasse - Elektronische Signatur - Windows Internet Explorer bereitgestellt von IE8 MNS+

http://www.s-trust.de/eLearning\_DSV/

Datei Bearbeiten Ansicht Favoriten Extras ?

Favoriten Web Slice-Katalog

IAM - Sparkasse - Elektro... S-TRUST - Trustcenter, Sign... Sparkasse Südliche Weinstra...

Seite Sicherheit Extras ? >

# ELEKTRONISCHE SIGNATUR

Version 1.1

**Startseite**

- Einleitung
- Meine Signatur
- Beispiele
- Signaturprozess
- Technische Details

Herzlich willkommen!

Sicherheit und Rechtsverbindlichkeit im digitalen Zeitalter.

Die rasante Verbreitung des Internets in allen Lebensbereichen und der sprunghafte Anstieg der Nutzerzahlen erfordern eine grundlegende Neudefinition des Aspektes Sicherheit: Wo immer persönliche, geschäftliche und sonstige vertrauliche Daten via Internet übermittelt werden, müssen besonders hohe Sicherheitsstandards angelegt werden, um dem Missbrauch dieser Daten vorzubeugen.



Der Gesetzgeber hat deshalb im deutschen Signaturgesetz die Grundlage für die sichere, rechtsverbindliche Unterschrift für die Online-Kommunikation geschaffen: die **qualifizierte elektronische Signatur**.

Die Sparkassen-Finanzgruppe bietet nun als erste Bankengruppe Zahlungsverkehrskarten an, mit denen gleichzeitig diese rechtsverbindliche elektronische Unterschrift erzeugt werden kann.

Wie das funktioniert, wollen wir Ihnen in dieser Anwendung vermitteln.

Bitte klicken Sie auf die "weiter"-Schaltfläche.

Seite drucken Impressum

Auf http://www.s-trust.de/eLearning\_DSV/ wird gewartet...

Internet 100% 100%

# Lösungsansätze:

S-TRUST - Trustcenter, Signaturkarten, elektronische Signatur, digitale Signatur, PKI-Lösungen - Windows Internet Explorer bere

http://www.s-trust.de/service\_support/FAQs/grundlegende\_fragen/index.htm

Datei Bearbeiten Ansicht Favoriten Extras ?

Favoriten Web Slice-Katalog

IAM - Sparkasse - Elektron... S-TRUST - Trustcenter, 5... Sparkasse Südliche Weinstra...

Seite Sicherheit Extras ?

**Unternehmen**

- Produkte & Leistungen
- Lösungen
- Service & Support
- Anwendungssupport
- Kartenleser
- Zertifikatsmanagement
- Registrierungsmitarbeiter
- Software und Treiber
- Download
- FAQ
- Attribute und Pseudonyme
- Beantragung
- Download des Zertifikates
- Grundlegende Fragen zur elektronischen Signatur und Verschlüsselung
- Hardware
- Kartenverlust
- Probleme
- Rechtliches
- Spernung des Zertifikates
- S-TRUST Sign-it
- S-TRUST Zertifikat
- Technisches
- Umlaufs

**Grundlegende Fragen zur elektronischen Signatur und Verschlüsselung**

Allgemeine Fragen zur elektronischen Signatur werden auf dieser Seite beantwortet



- Was wird benötigt, um eine elektronische Signatur einzusetzen?
- Gibt es eine Liste der am Markt funktionierenden Anwendungen mit der qualifizierten Signatur?
- Wofür wird die elektronische Signatur benötigt?
- Wie funktioniert die elektronische Signatur?
- Welche Arten von Signaturen werden unterschieden?
- Was bedeutet "fortgeschrittene Signatur"?
- Was ist die qualifizierte elektronische Signatur?
- Was ist eine akkreditierte Signatur und wie unterscheidet sich diese von der qualifizierten Signatur?
- Was ist ein digitales Zertifikat?
- Was zeichnet ein qualifiziertes Zertifikat aus?
- Welche Dokumente können mit dem qualifizierten Zertifikat signiert werden (z.B. PDF)?
- Kann man ein Dokument mehrfach signieren?

**Suche**

suchen

Erweiterte Suche

**Kontakt**

- Anfrage an den Vertrieb
- Hotline und Support
- Informationen für Institute der Sparkassen-Finanzgruppe

**Elektronische Signatur**



**Zertifikatsmanagement**

- Download qualifizierter Zertifikate
- Sperren
- Zertifikatssuche u.-prüfung
- Support- und Sperroffline
- CSA-Passwort entsperren

## Lösungsansätze:



verfahren mit mTan: Kriminelle spionieren Smartphone aus

**i Online-Bankgeschäften: Wer sich sogenannte mTan aufs Handy schickten lässt, kann leicht betrogen werden. Im neuen SPIEGEL raten Experten zu anderen, sichereren Verfahren**

8.05.2014 - 12:01 Uhr

[Teilen](#) | [Merken](#)

Hamburg - Experten warnen vor Onlinebanking mit mTans. Sie sind Einmalpasswörter, die den Kunden auf ihr Handy gesendet werden. "Über manipulierte Handy-Apps können Internetdiebe Smartphones ausspionieren", sagt Christian Fuchs, Experte für Sicherheitstechnik an der Universität Hamburg.

# Lösungsansätze:



# Virenschutz mit Schwächen

**PC-TIPP:** Warentester bewerten weniger als die Hälfte der Sicherheitspakete mit gut

VON HANS PETER SEITEL

**LUDWIGSHAFEN.** Etliche Schutzprogramme für den Computer lassen zu wünschen übrig. Nur sechs von 14 untersuchten Sicherheitspaketen für private Windows-Rechner bewertet die Stiftung Warentest in einer neuen Studie als gut.

Hauptschwachpunkt der Programme: Sie spüren neue Viren nicht immer zuverlässig auf. Neben der Wirksamkeit des Virenschutzes und der Firewall überprüften die Tester, ob die Software einfach zu handhaben ist und wie stark sie den Rechner belastet. Die beste Gesamtnote gut erhielten die Programme von Eset, G Data, Avira, Avast, F-Secure und Kaspersky mit jährlichen Lizenzkosten für einen einzelnen PC zwischen etwa 35 und

50 Euro. Eine gute Virenabwehr bieten dem Test zufolge auch die zwei kostenlosen Programme von Avira und Avast. Sie beinhalteten jedoch keine Firewall und auch keine Extras wie Kindersicherung, Phishing-Schutz oder Spam-Filter. Wer sie nutzt, sollte entweder die Windows-Firewall eingeschaltet lassen oder eine andere Firewall installieren, empfiehlt das Stiftungsmagazin „Test“ (Heft 4/2013).

Nur als ausreichend bewerten die Tester die kostenpflichtigen Programme von Trend Micro, Norton und Panda. Ein Grund für die schlechte Note ist, dass diese Sicherheitspakete die Listen der neuesten Virensignaturen statt auf dem Rechner auf sogenannten Cloudservern im Internet speichern. Die Folge: Der Schutz vor neuen Schädlingen funktioniert laut Stif-

tung nur, solange eine Internetverbindung besteht, nicht aber, wenn die Schadsoftware einen nicht mit dem Netz verbundenen Rechner angreift, zum Beispiel von einem verseuchten Stick aus.

Die Stiftung rät, den PC selbst mit dem besten Schutzprogramm „stets mit Bedacht und Misstrauen“ zu verwenden. So sollten die Nutzer nicht nur das Antivirenprogramm sowie die übrige Software aktuell halten, sondern auch dubiose Internetseiten meiden, von denen etwa aktuelle Kinofilme kostenlos zum Download angeboten werden. Externe Speicher sollten gescannt werden, nachdem sie an einem fremden PC angeschlossen waren, und Fotos in Geschäften nur von schreibgeschützten Speicherkarten gedruckt werden, so die Testexperten.

## Grundsätzlich gilt:

**Virenschutzprogramme lohnen sich allein schon aus juristischen Gründen!**

**Sollte das Bankkonto geplündert werden, dann verlangen die Banken häufig den Beweis, dass der Kunde sich geschützt hat!**

**Beim Online-Shopping bieten größere Portale oft eine größere Sicherheit.**

**Ein absurd niedriger Preis ist verdächtig.**

**Überweisungen per Vorkasse sind bei unbekannten Anbietern leichtsinnig.**

**Bei kleinen Anbieter kann ein Blick ins Impressum und ein Testanruf Klarheit schaffen.**

## Verlust der Verfügbarkeit

→ IT-Systeme müssen funktionieren

→ Daten müssen verfügbar sein

## Verlust der Vertraulichkeit

→ Unbefugte haben keinen Informationszugriff

→ Nur für einen beschränkten Empfängerkreis

## Verlust der Integrität

→ Daten sind vollständig      - *absichtlich*

→ Daten sind unverändert      - *unabsichtlich*

    - *technische Fehler*

## Verlust der Authentizität

→ Daten sind sicher einem Sender zuzuordnen

→ Daten sind unabstreitbar

**Verlust der Verfügbarkeit**

**Schaffung von Ausfallsicherheit**

**Verlust der Vertraulichkeit**

**Datensicherung**

**Verlust der Integrität**

**Verschlüsselung**

**Verlust der Authentizität**

**Elektronische Signatur**

→ **Aufklärung und Sensibilisierung aller beteiligten Personen**

**Vielen Dank  
für Ihre Aufmerksamkeit!**