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

Grundbedrohung der IT-Sicherheit

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

➔ Daten sind unverändert

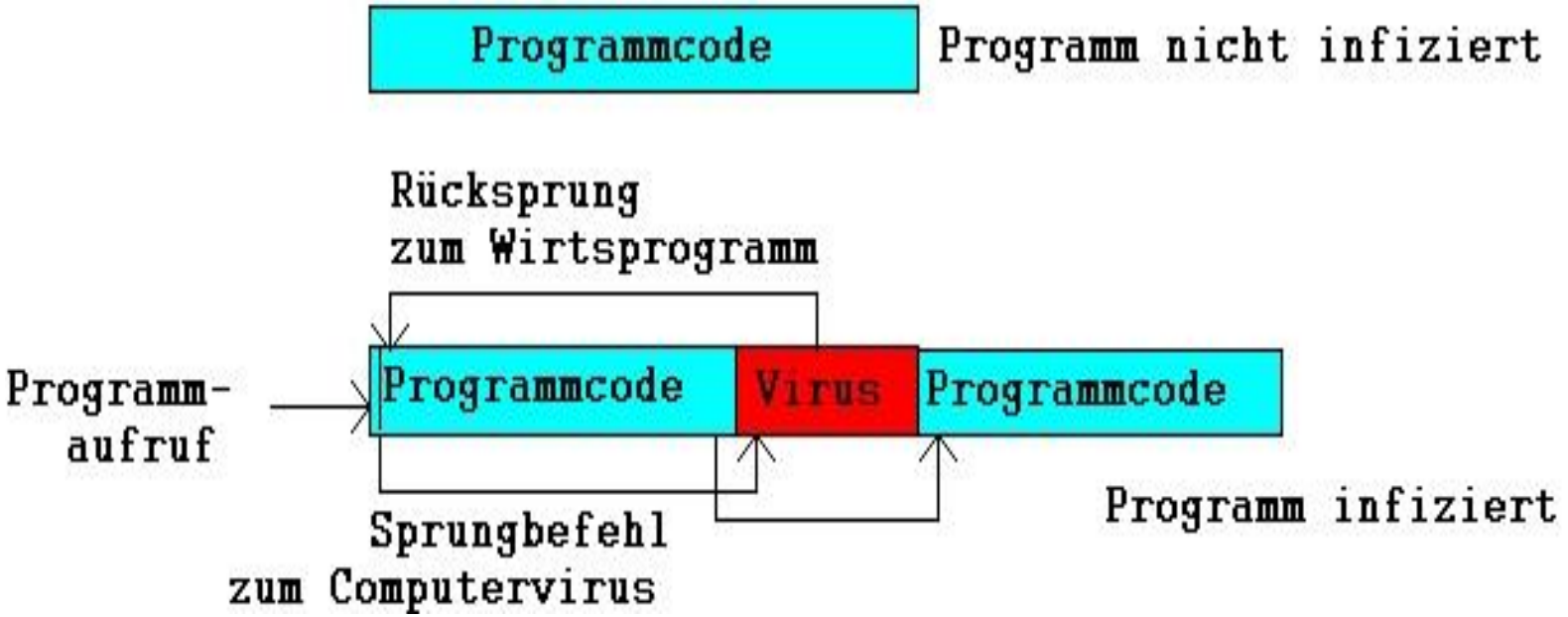
- absichtlich
- unabsichtlich
- technische Fehler

Verlust der Authentizität

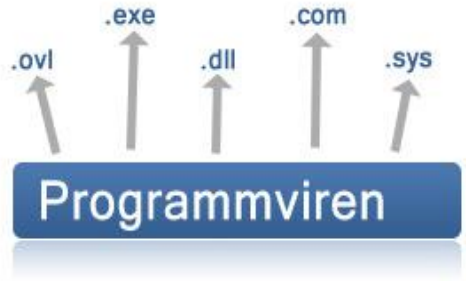
➔ Daten sind sicher einem Sender zuzuordnen

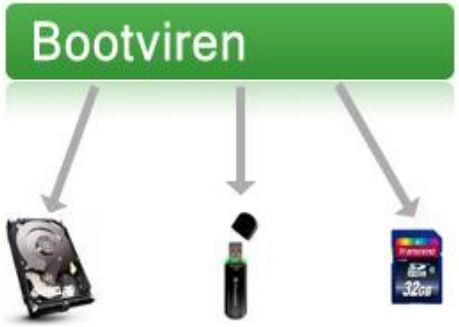
➔ Daten sind unabstreitbar

Schädigende Software => unerwünschte Programmteile

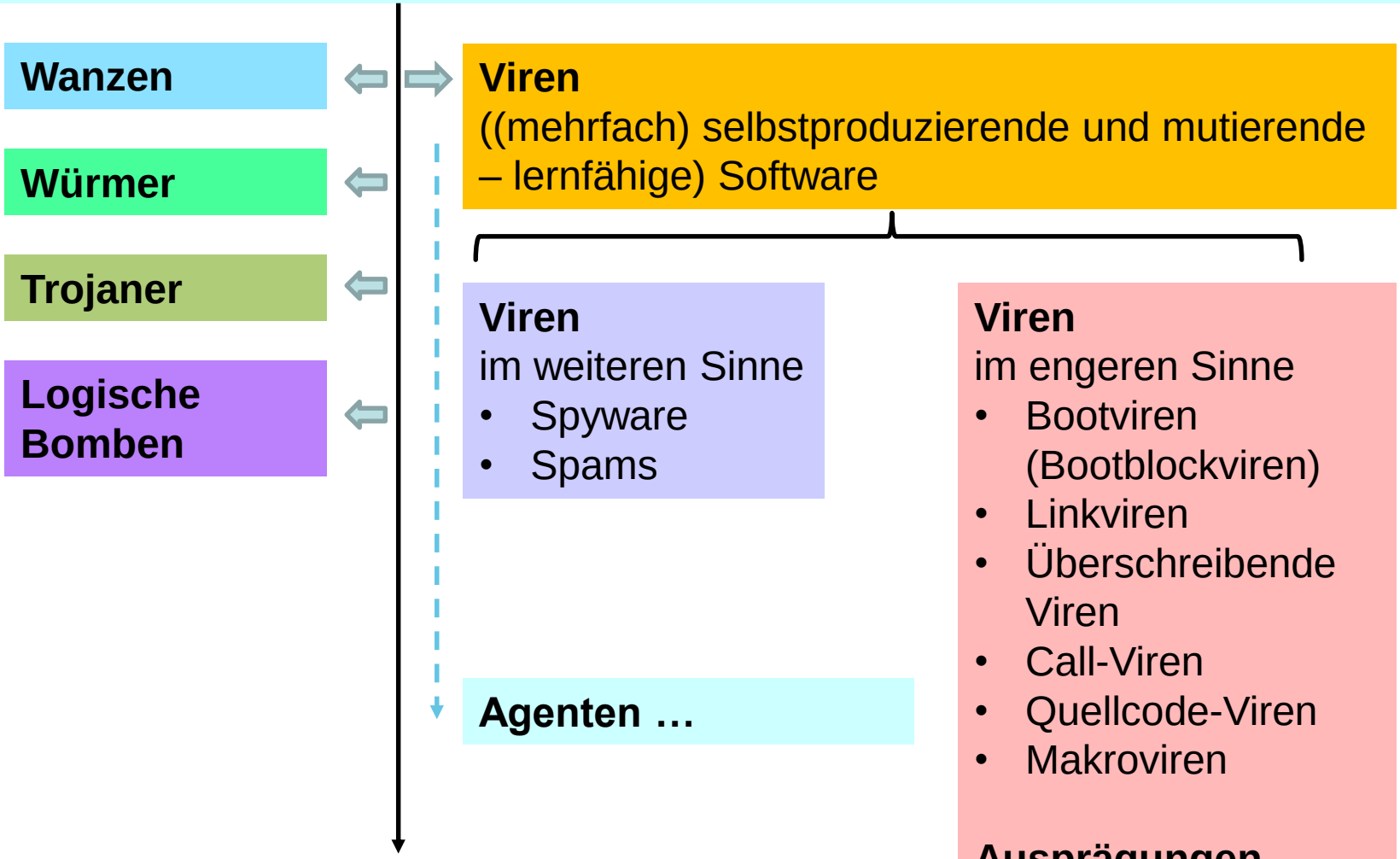


Schädigende Software => unerwünschte Programmteile





Schädigende Software/Malware => unerwünschte Programmteile



Gefahren für die IT-Sicherheit

- **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**

Gefahren für die IT-Sicherheit

- malicious Software (Malware)
  - Wanzen
  - Viren
  - Würmer
  - Trojanische Pferde, Sniffer, Keylogger, Backdoor
  - Rootkit, Bootkit, FUD „fully undedected“
  - 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 denkbares Angriffsszenario. 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 Teilfunktionen 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.**

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.

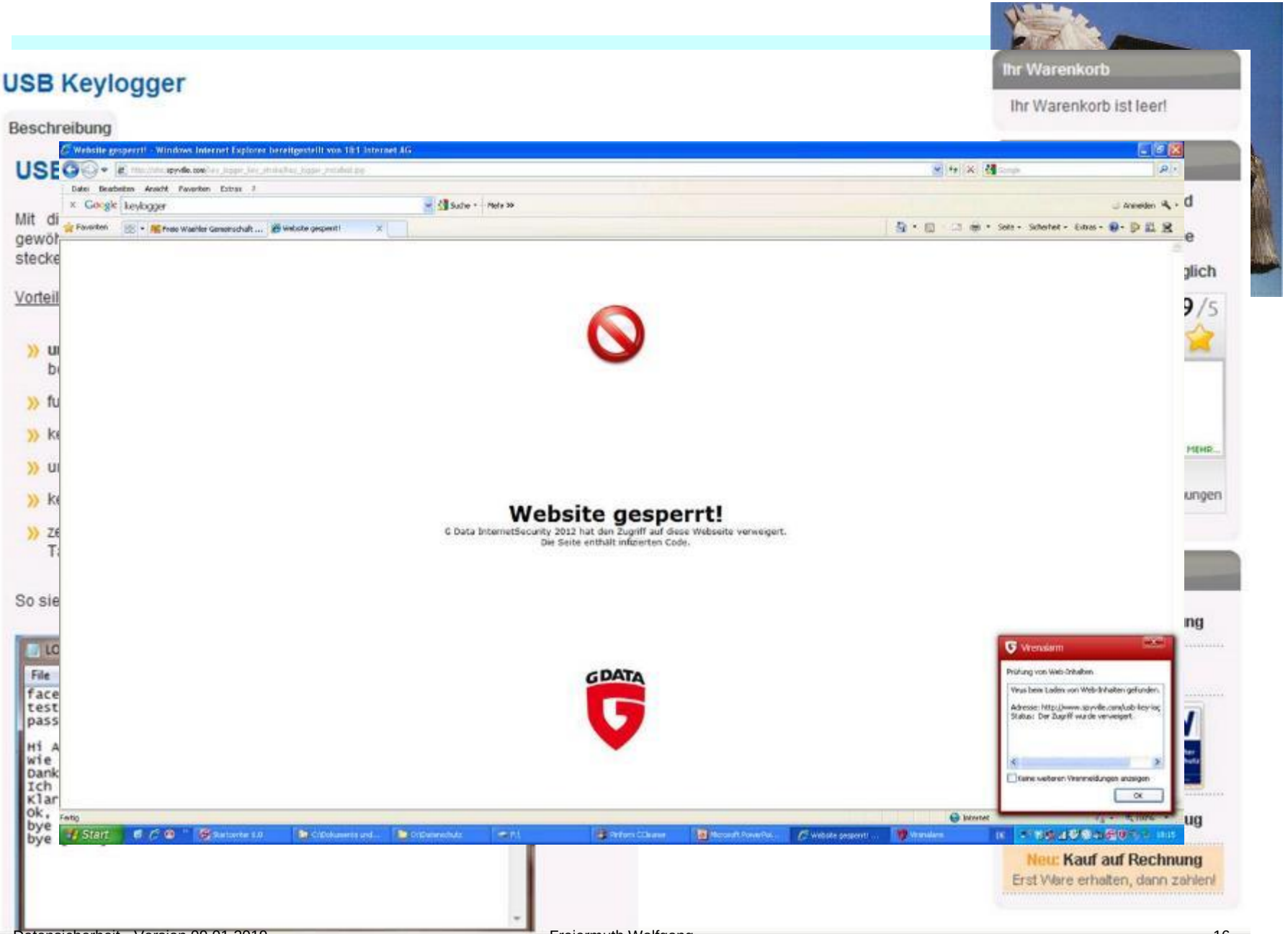
Gefahren für die IT-Sicherheit

- **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

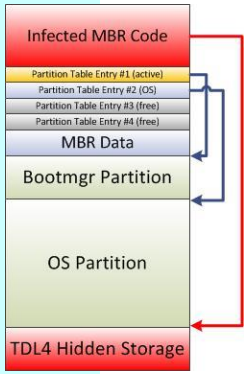


Gefahren für die IT-Sicherheit

- **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.



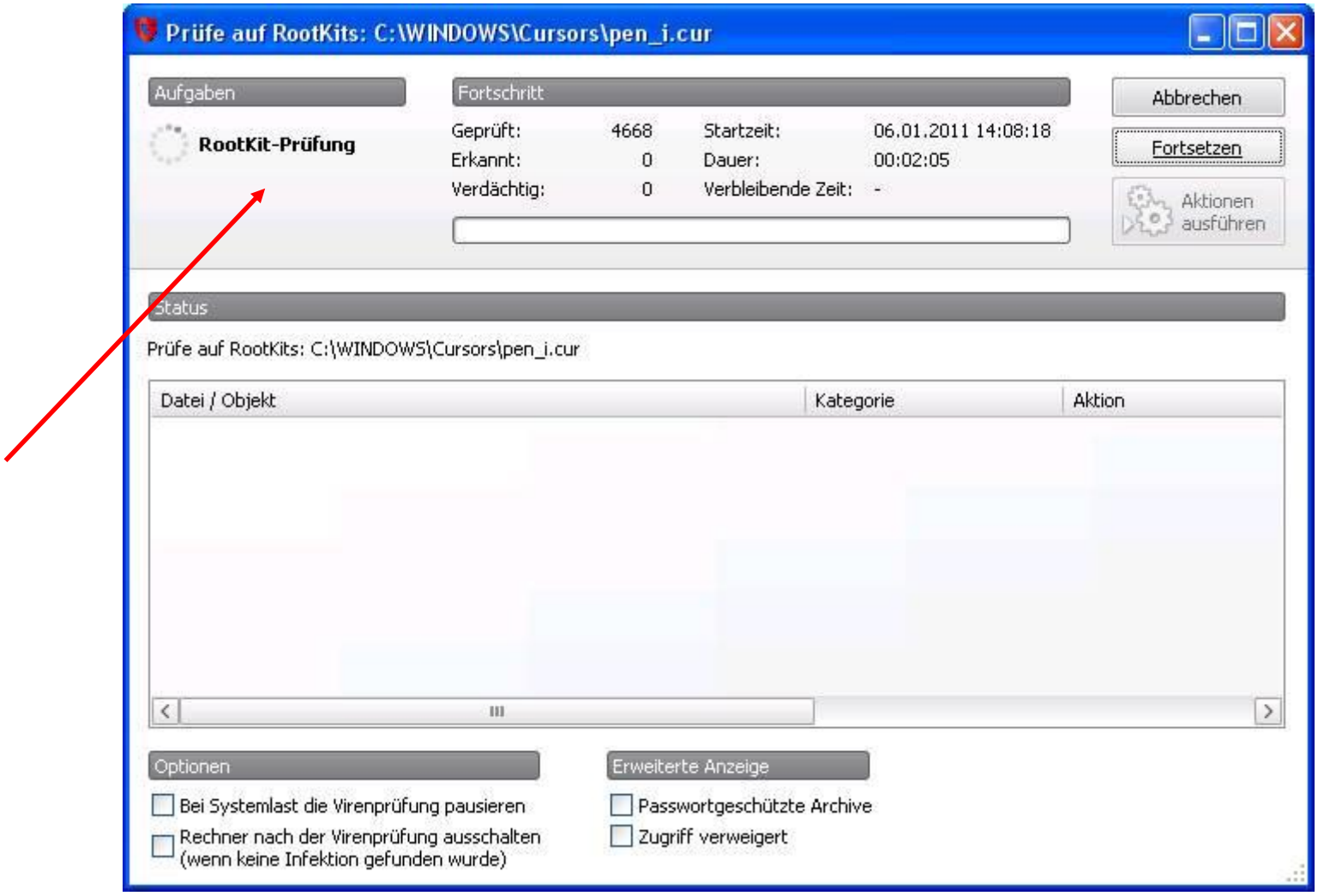
Ein Bootkit ist somit eine Mischung aus Bootsektorviren und Rootkits.
Wer die Hardware bereits unter seiner Kontrolle hat, kann auch die Software unter seiner Kontrolle haben.
Eine wirksame Absicherung gegen die Ausführung von unsigniertem Programmcode wird wohl erst mit dem Einsatz von TPM-Hardware 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

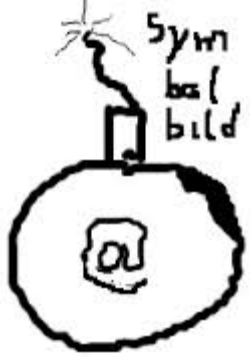
- **FUD „fully undetected“**

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

Gefahren für die IT-Sicherheit



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.

Gefahren für die IT-Sicherheit

- **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.

Gefahren für die IT-Sicherheit

- **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

Gefahren für die IT-Sicherheit

malicious Software (Malware)

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

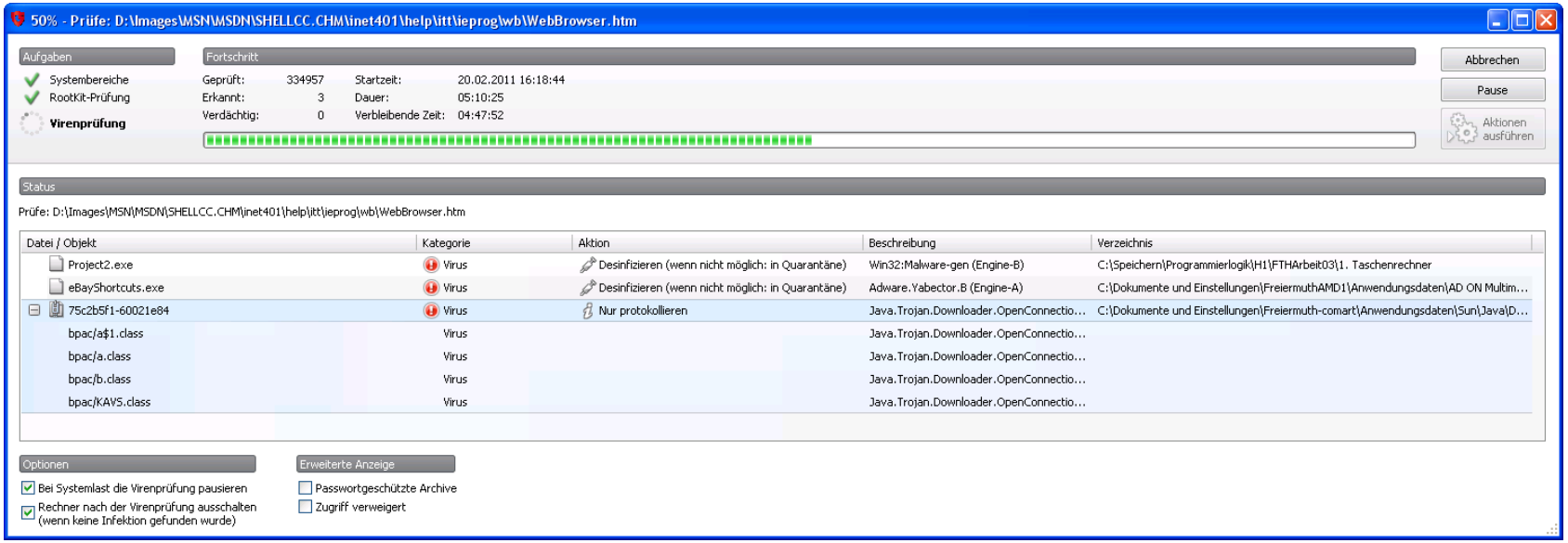
➔ **Einsatz von aktuellen Scanner (kein 100 % Schutz)**

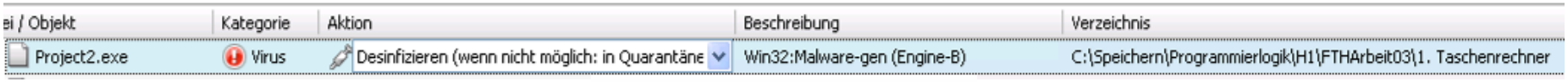
➔ **Zurückhaltung beim Öffnen von unbekannten Inhalten gesundes Misstrauen**

➔ **Windows Updates regelmäßig durchführen**

Gefahren für die IT-Sicherheit

➔ Falschmeldungen





Gefahren für die IT-Sicherheit

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

Gefahren für die IT-Siche

- **Hacker/Cracker**
  - **unbefugtes Eindringe**
  - **ausspähen von Daten**
  - **verändern von Daten**
  - **sonstige Schadsoftw**


DIE

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


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 gefordert.

Zur Sache: Der „Stuxnet"-Wurm

➔ **Einsatz von Firewalls**

➔ **restriktive Konfiguration von Systemdiensten**

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“)**

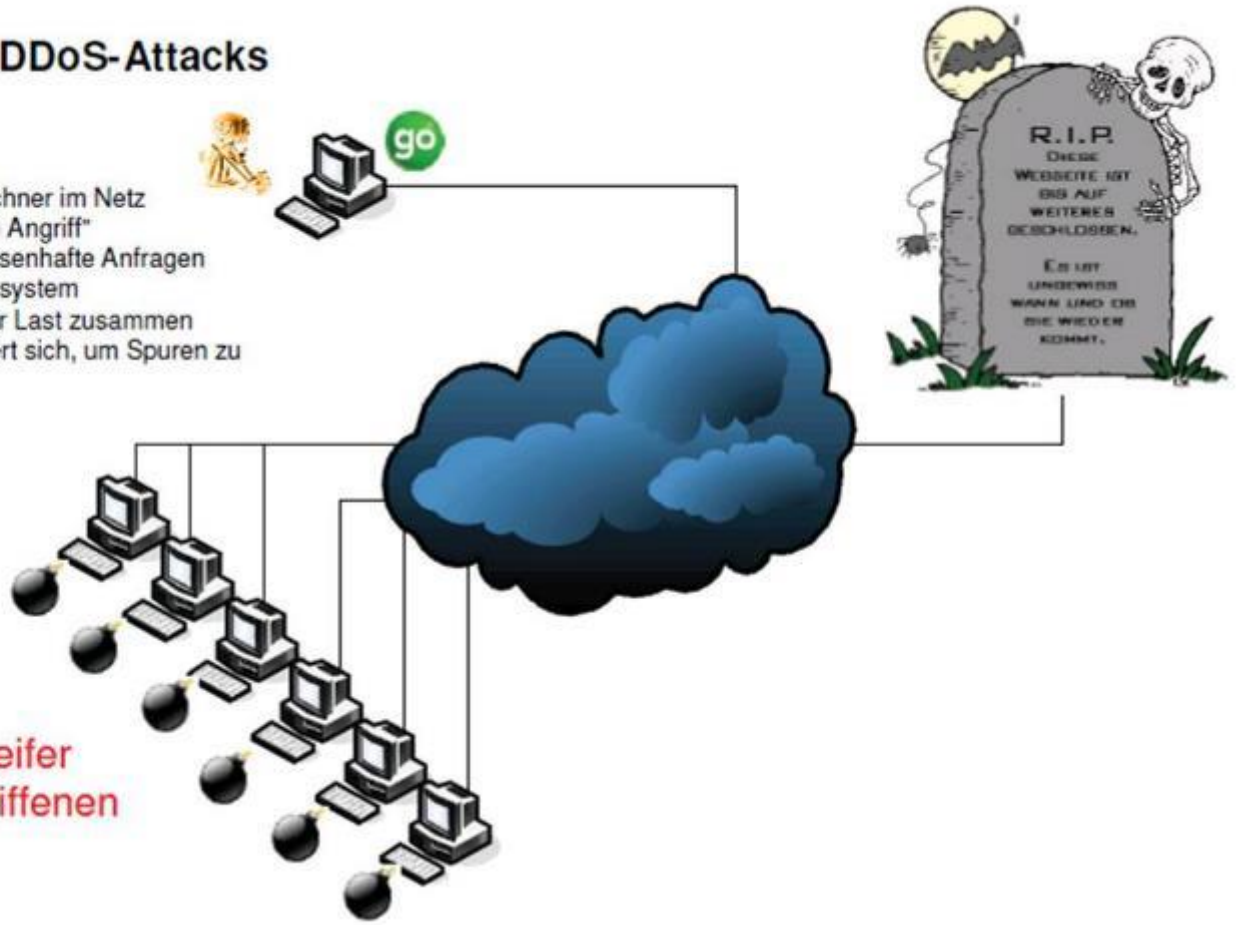
➔ **Einsatz von Firewalls und aktuellen Virensyannern**

➔ **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



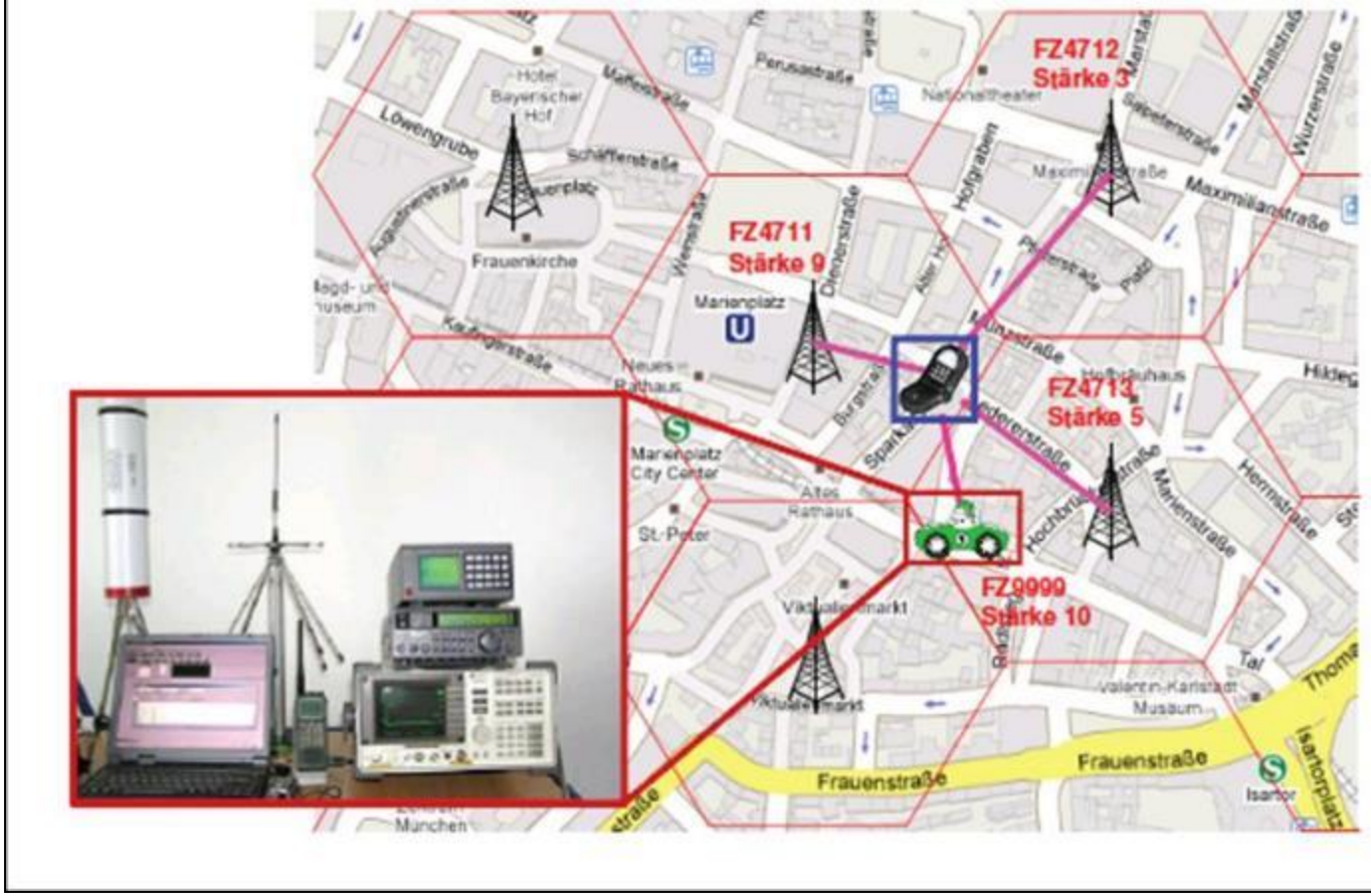
Der eigentliche Angreifer bleibt für den angegriffenen Server unerkannt.

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

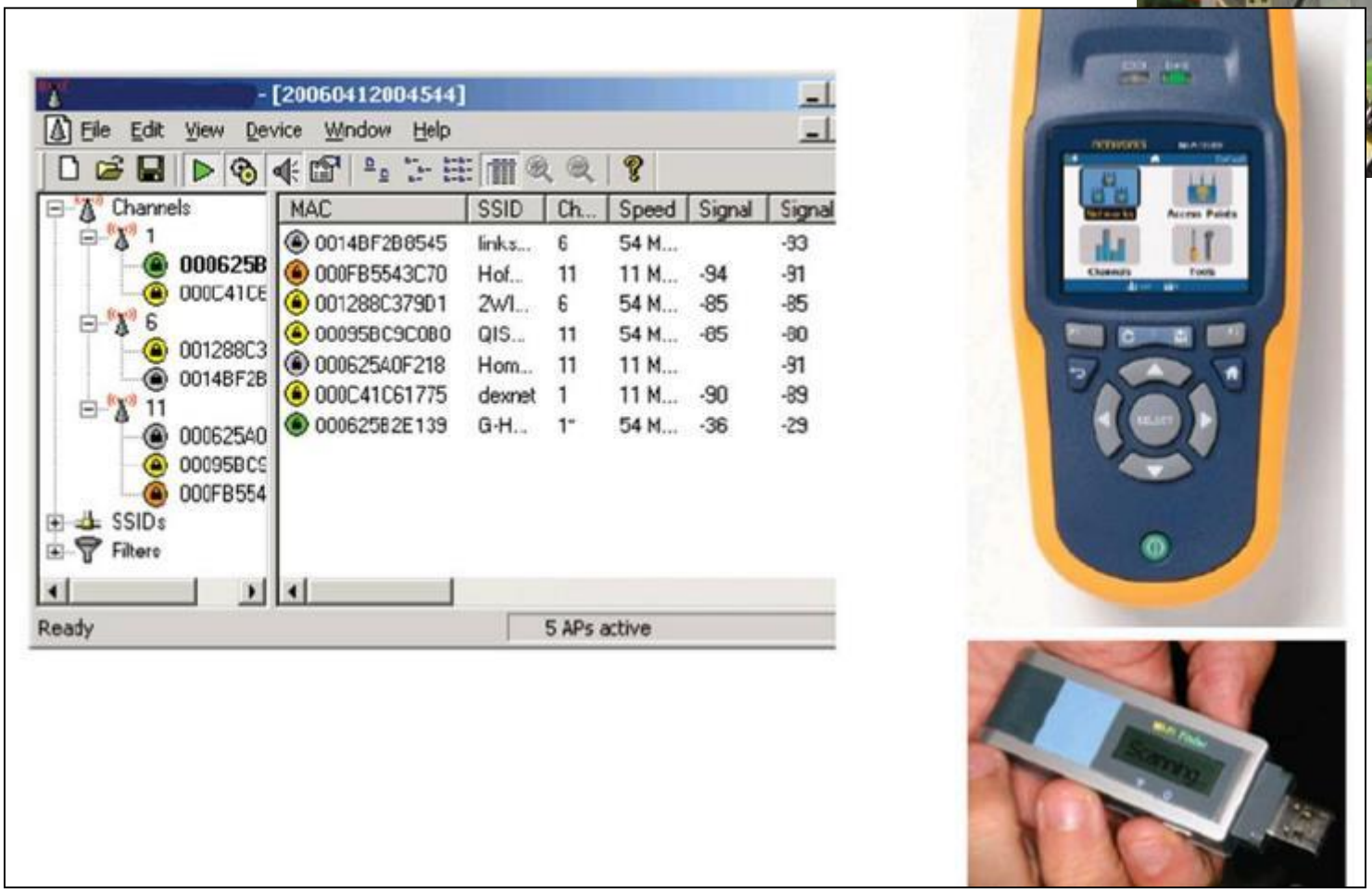
Mobilfunknetze: GSM/GPRS/UMTS etc.



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



Gefahren für die IT-S

Geheimdienste: Verschlüsselung von Daten geknackt

WASHINGTON (afp/dpa). Neue Enthüllungen in der Spähaffäre: Geheimdienste aus den USA und Großbritannien sind Medienberichten zufolge in der Lage, verschlüsselte Kommunikation im Internet mitzulesen.

großer Technik- und Internetfirmen an die verschlüsselten Daten. Die NSA stecke jährlich 250 Millionen Dollar in ein Programm, das unter anderem zum Ziel hat, verdeckt Einfluss auf die Produkte von Firmen zu nehmen. Genannt werden die Unternehmen nicht. Um welche Verschlüsselungstechnik es genau geht, ist ebenfalls nicht beschrieben.

Das Bundesinnenministerium erklärte, man habe keine Anhaltspunkte dafür, dass die Behauptungen zutreffend sind. Es werde wei-
/erschlüsselung geraten.

KOMMENTAR SEITE 2

Gefahren für die IT-Sic

„Die Rheinpfalz“
07.09.2013

KOMMENTAR

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.

Gefahren für die IT-Sicherheit

„Die Rheinpfalz“
August 2013

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

Cassidy Wolf

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)

Gefahren für die IT-Sicherheit

- **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**

Gefahren für die IT-Sicherheit

- **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**

Gefahren für die IT-Sicherheit

- **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**

Gefahren für die IT-Sicherheit

- **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**

➔ **Einsatz von aktuellen Virenscannern**

➔ **Beachtung von Warnhinweisen**

Gefahren für die IT-Sicherheit

- **Phishing**

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

Gefahren für die IT-Sicherheit

- **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.

Gefahren für die IT-Sicherheit

- **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) 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

Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien 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.

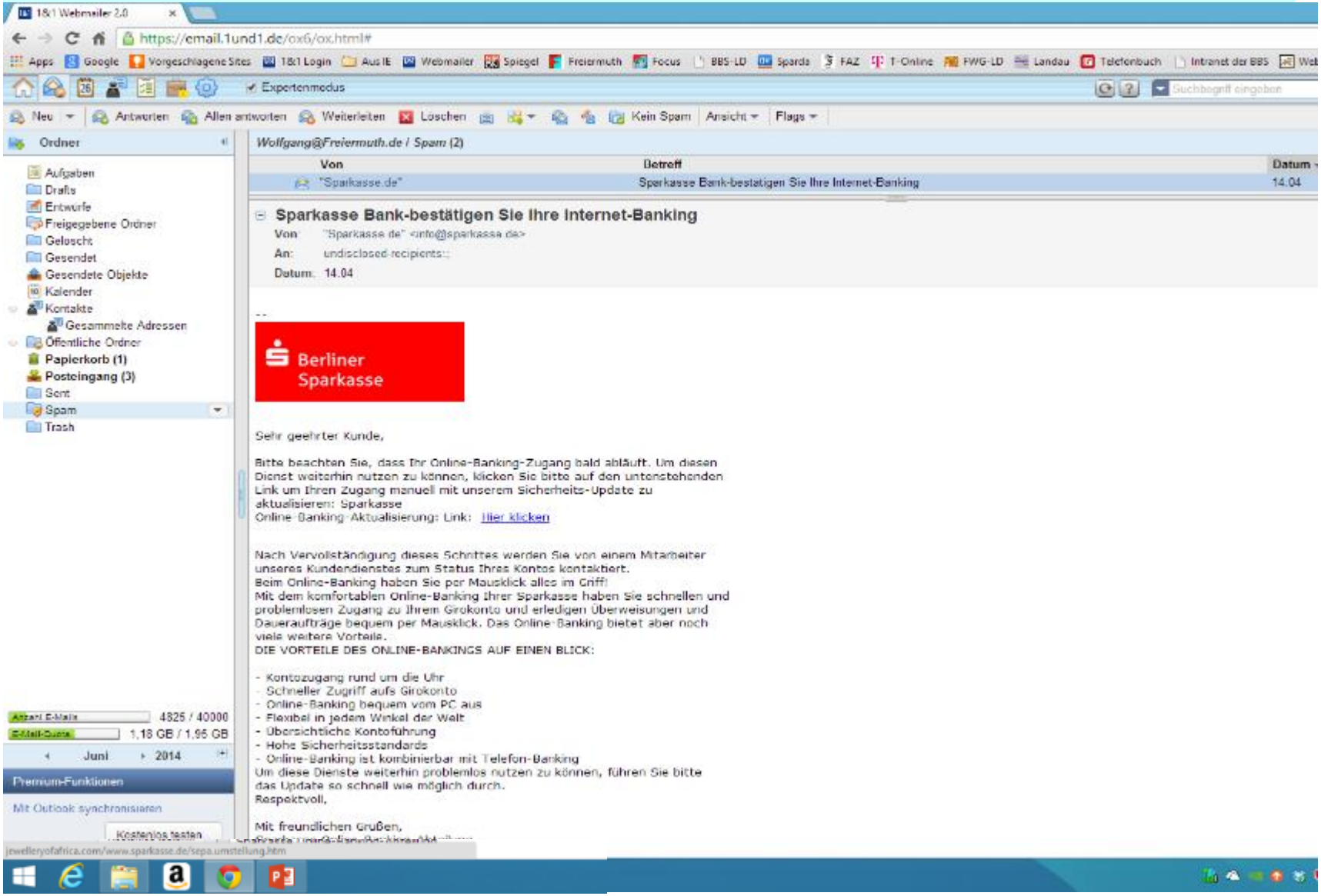
Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

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

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

Gefahren für die IT-Sicherheit



Gefahren für die IT-Sicherheit

Nachricht: (Wichtig) 001

Von: Sparkasse <Aktualisierung001@sparkasse.de>

An: Sparkasse <Aktualisierung001@sparkasse.de>

Datum: 12:57

770 x 109

Sparkasse

Passendes Smartphone für die Sparkassen-Apps!

Vorteil: Sparen Sie jetzt 199,99 Euro!

Enabled by Vodafone

→ mehr

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 kontakiert.

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:

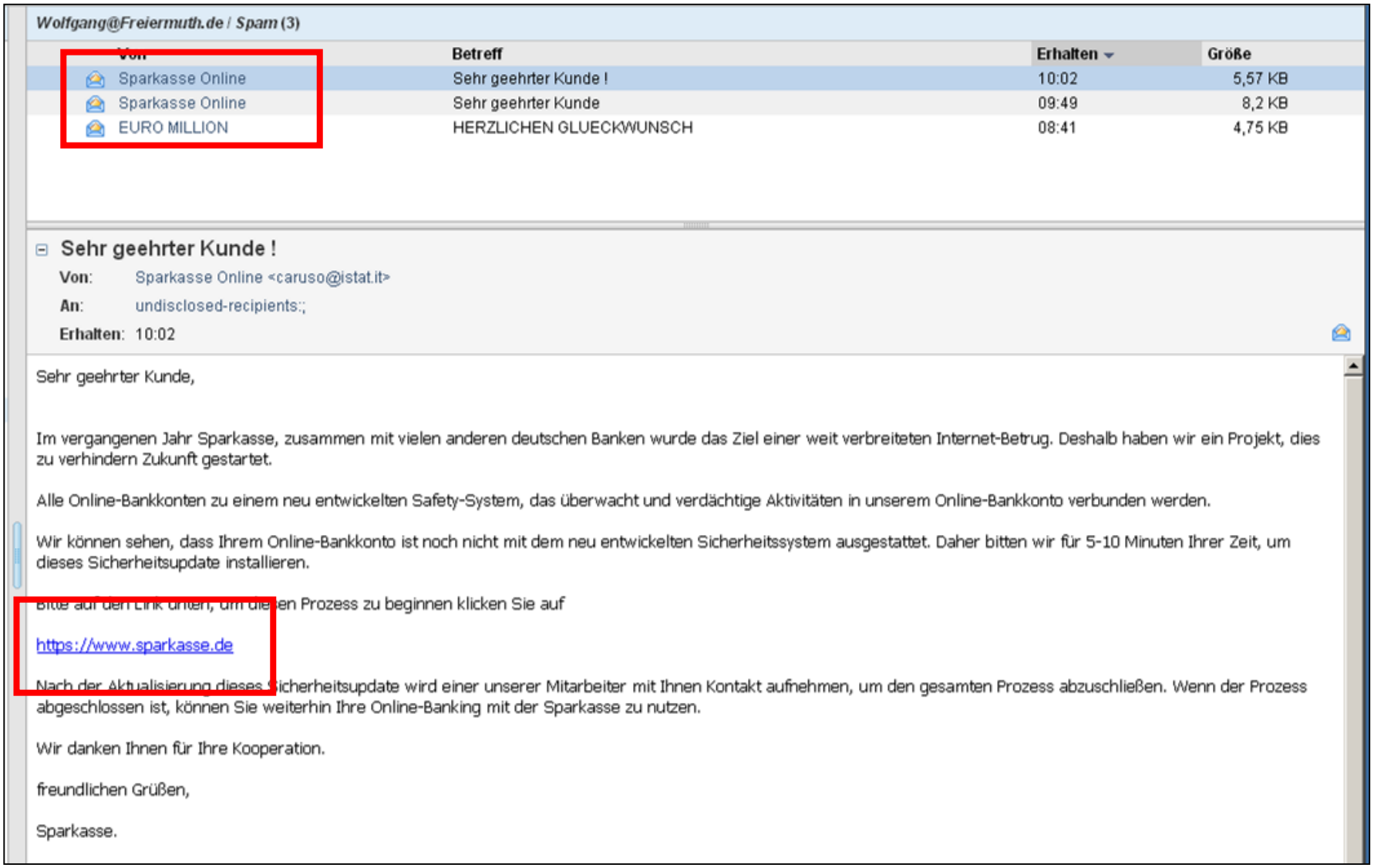
- **Kontozugang rund um die Uhr**
- **Schneller Zugriff aufs Girokonto**
- **Online-Banking bequem vom PC aus**
- **Flexibel in jedem Winkel der Welt**
- **Übersichtliche Kontoführung**
- **Hohe Sicherheitsstandards beim Online-Banking**
- **Online-Banking kombinierbar mit Telefon-Banking**

Respektvoll,
Kundendienst.

Mehr als nur ein Job!

Part_2.2.gif (34 KB) Part_2.3.png (3 KB) Part_2.4.png (1 KB) Part_2.5.png (15 KB) Part_2.6.jpeg (17 KB) Part_2.7.gif (4

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

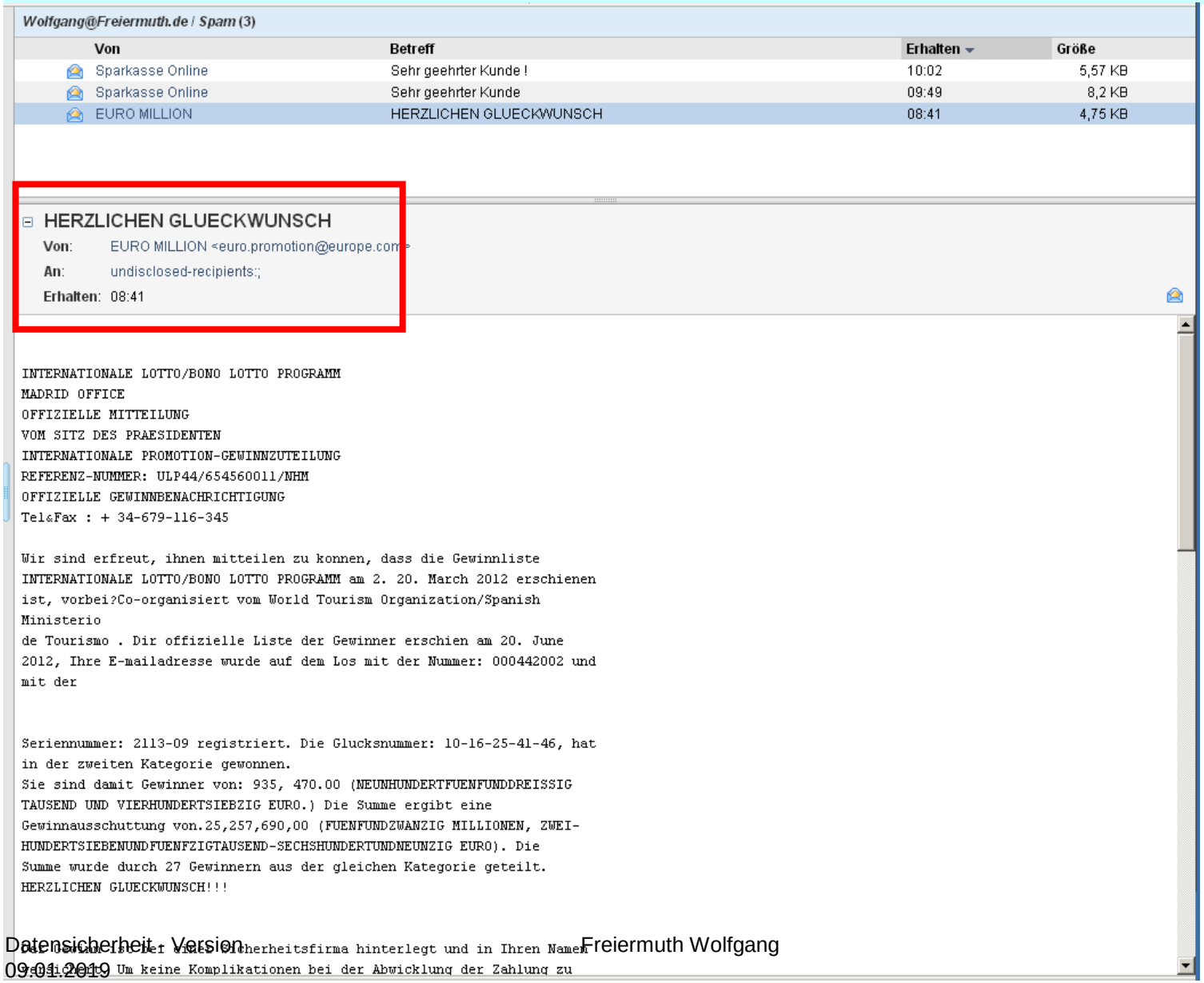
Nach der Aktualisierung dieses Sicherheitsupdate wird einer unserer Mitarbeiter mit Ihnen Kontakt aufnehmen, um den gesamten Prozess abzuschließen. Wenn der Prozess abgeschlossen ist, können Sie weiterhin Ihre Online-Banking mit der Sparkasse zu nutzen.

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

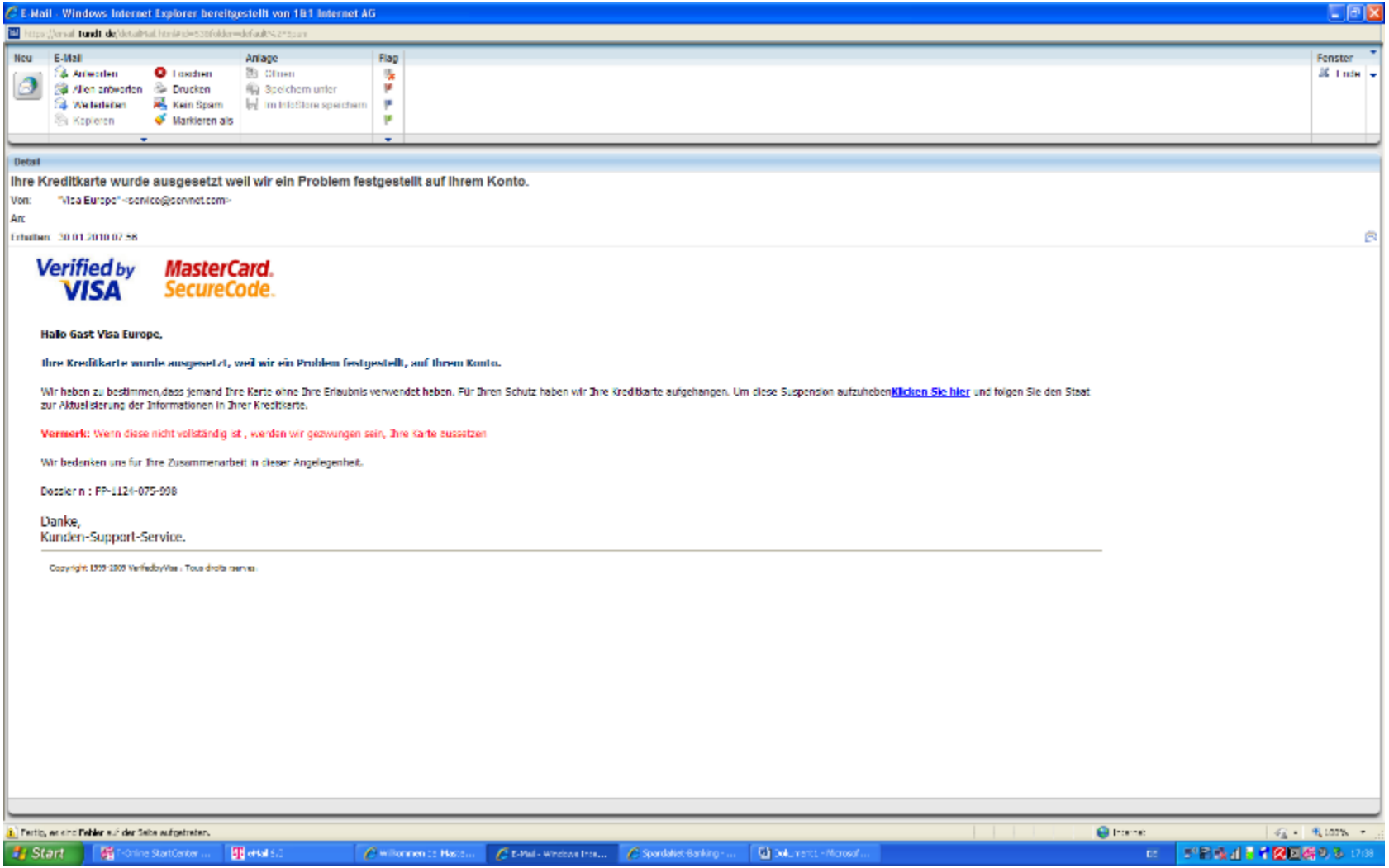
INTERNATIONALE LOTTO/BONO LOTTO PROGRAMM
MADRID OFFICE
OFFIZIELLE MITTEILUNG
VOM SITZ DES PRAESIDENTEN
INTERNATIONALE PROMOTION-GEWINNZUTEILUNG
REFERENZ-NUMMER: ULP44/654560011/NHM
OFFIZIELLE GEWINNBENACHRICHTIGUNG
Tel&Fax : + 34-679-116-345

Wir sind erfreut, ihnen mitteilen zu konnen, 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 Tourismo . 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 Glucksnummer: 10-16-25-41-46, hat
in der zweiten Kategorie gewonnen.
Sie sind damit Gewinner von: 935, 470.00 (NEUNHUNDERTFUENFUNDDREISSIG
TAUSEND UND VIERHUNDERTSIEBZIG EURO.) Die Summe ergibt eine
Gewinnausschuttung von.25,257,690,00 (FUENFUNDZWANZIG MILLIONEN, ZWEI-
HUNDERTSIEBENUNDFUENFZIGTAUSEND-SECHSHUNDERTUNDNEUNZIG EURO). Die
Summe wurde durch 27 Gewinnern aus der gleichen Kategorie geteilt.
HERZLICHEN GLUECKWUNSCH!!!

Der Betrag ist der Bank Sicherheitsfirma hinterlegt und in Ihren Namen
[illegible] Um keine Komplikationen bei der Abwicklung der Zahlung zu

Gefahren für die IT-Sicherheit



Gefahren für die IT-Sicherheit

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 aufgehangen. 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=5885d80a13c0db1f1ff80d546411d7f84f1036d8f209d3d19ebb6f4eeec8bd0ef1b64e562942814a64d80bf24862819bf1b64e562942814a64d80bf24862819b

Kunden-Support-Service.

Gefahren für die IT-Sicherheit

Von: Sprada-BW <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:

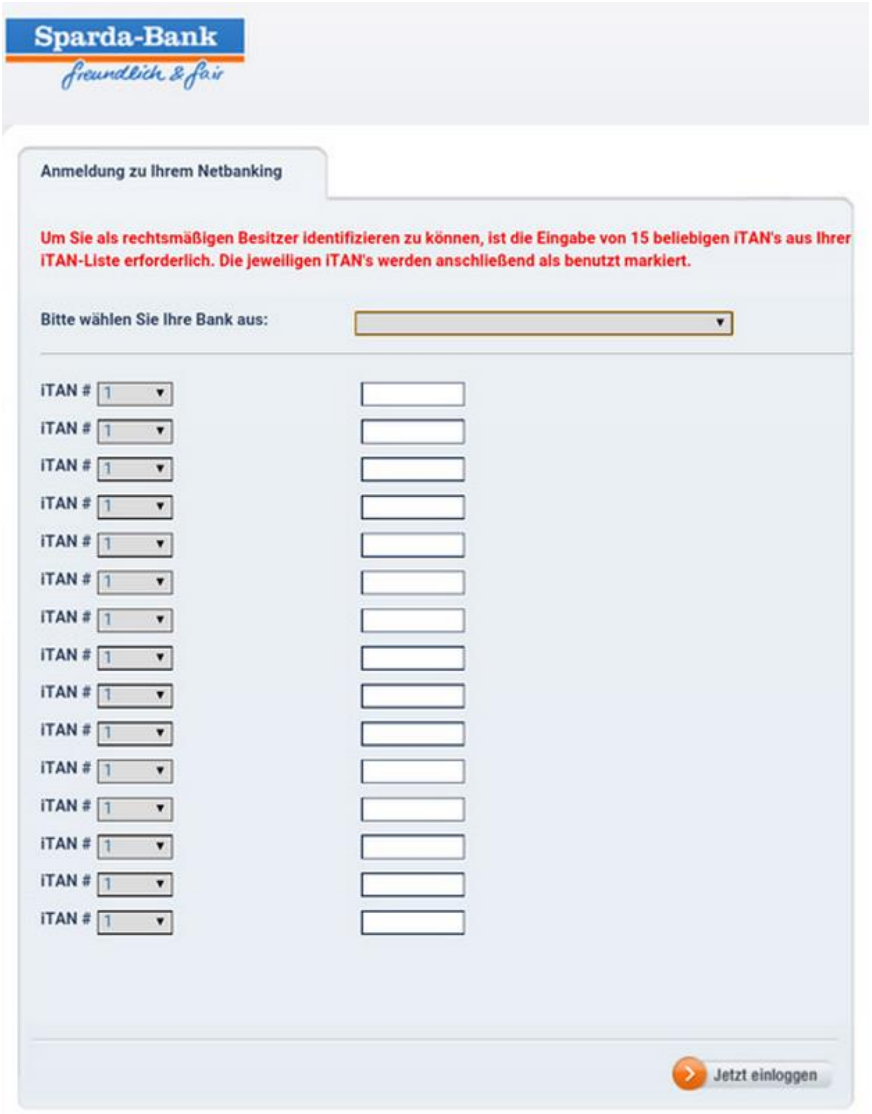
Wir bedanken uns für Ihre Mithilfe.
Viele Grüße.

06/11/2014, Hamburg

Gefahren für die IT-Sicherheit

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

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

Gefahren für die IT-Sicherheit

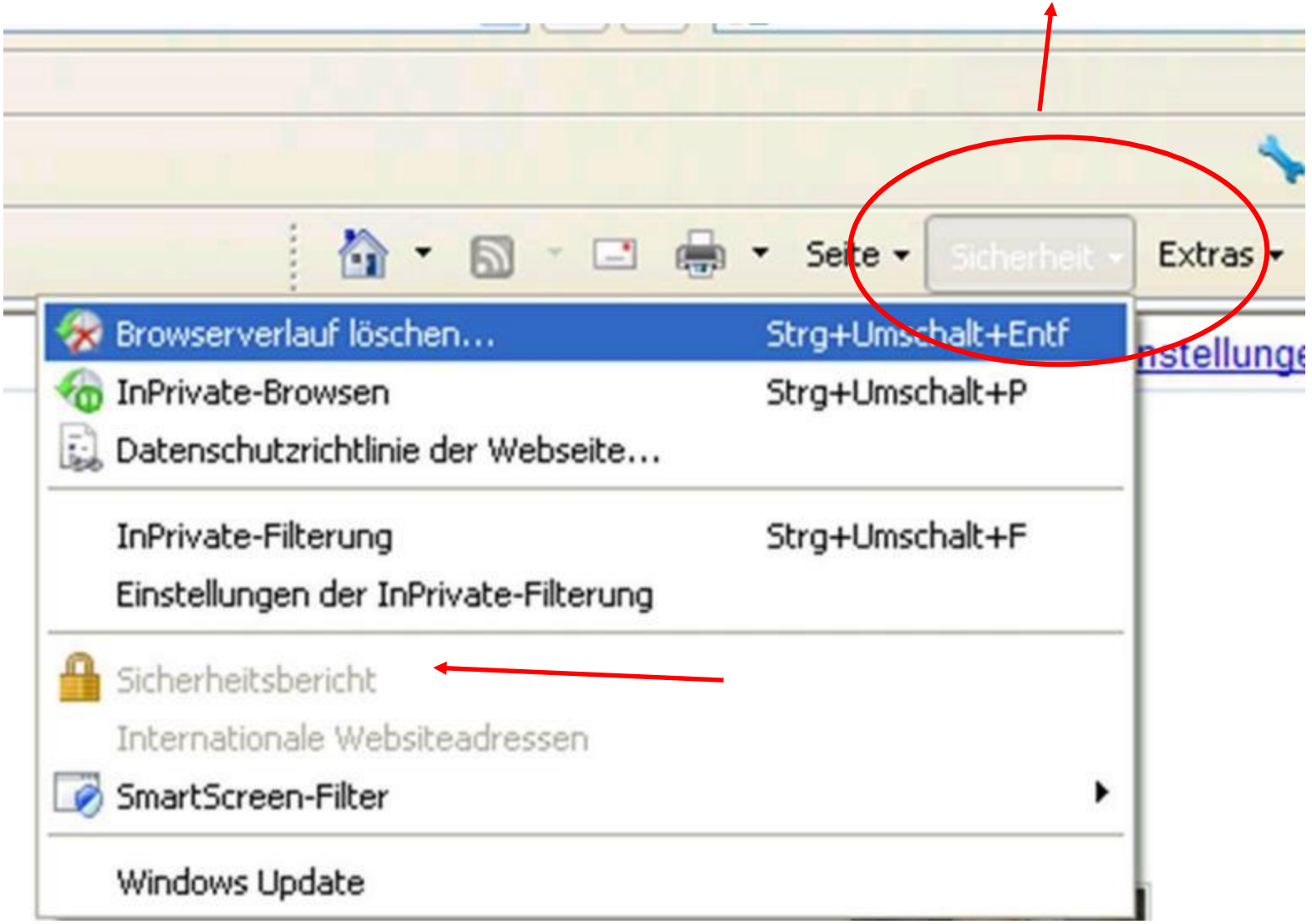
➔ **Einsatz von aktuellen Browsern**

➔ **Beachtung von Warnhinweisen**

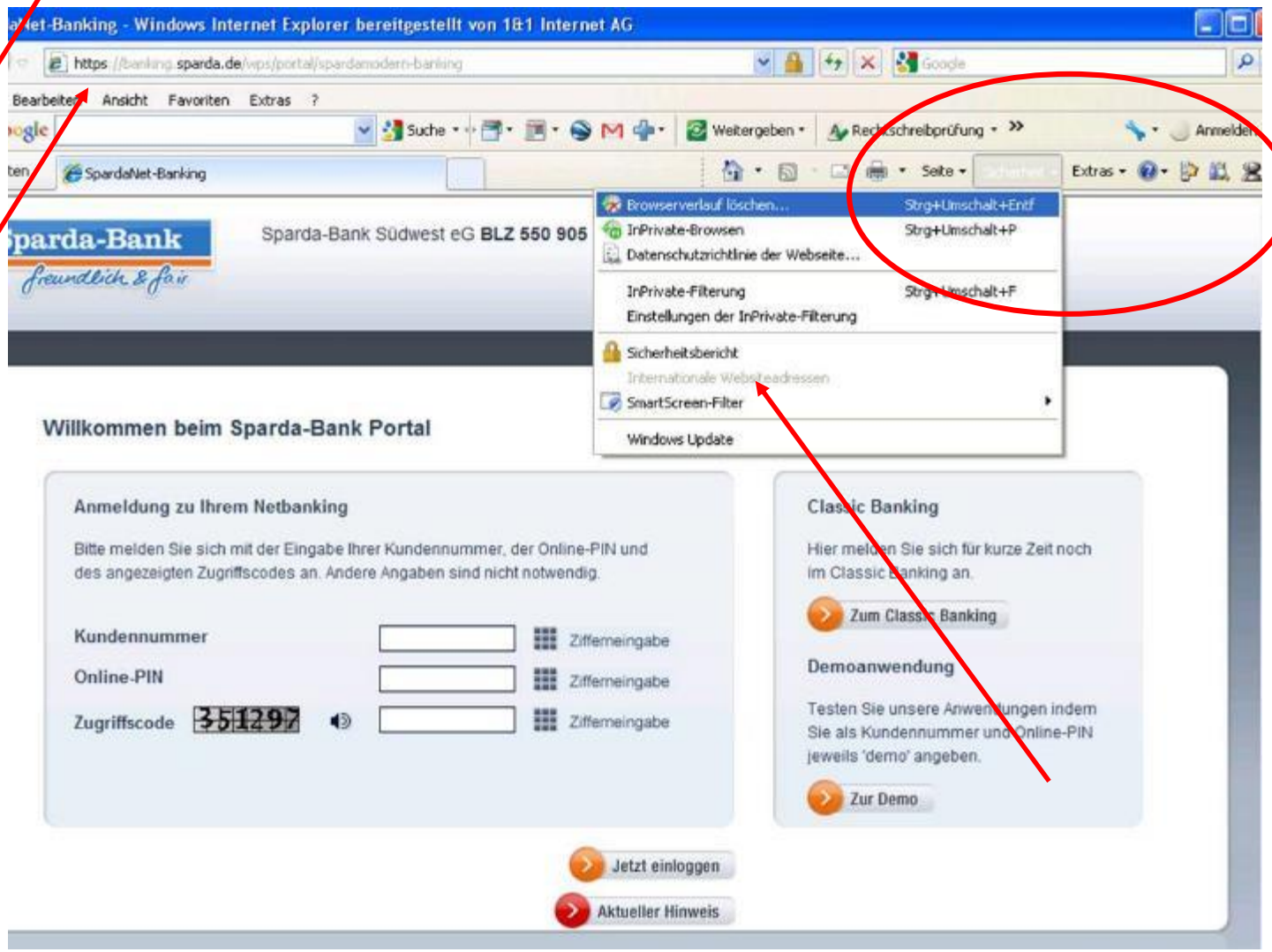
➔ **Nutzung von verschlüsselter Verbindung, Prüfung der Zertifikate**

Gefahren für die IT-Sicherheit

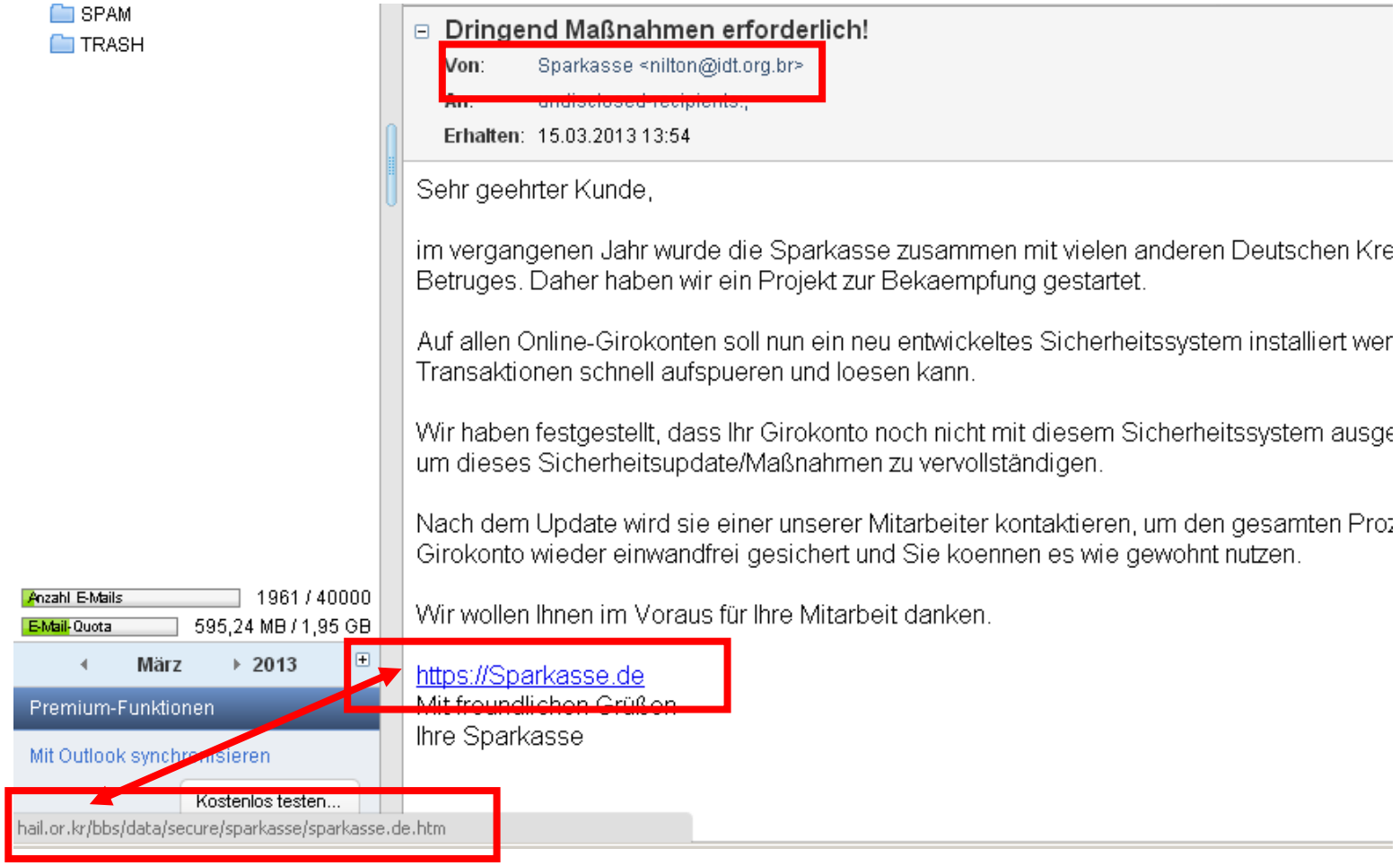
http://www.google.de/



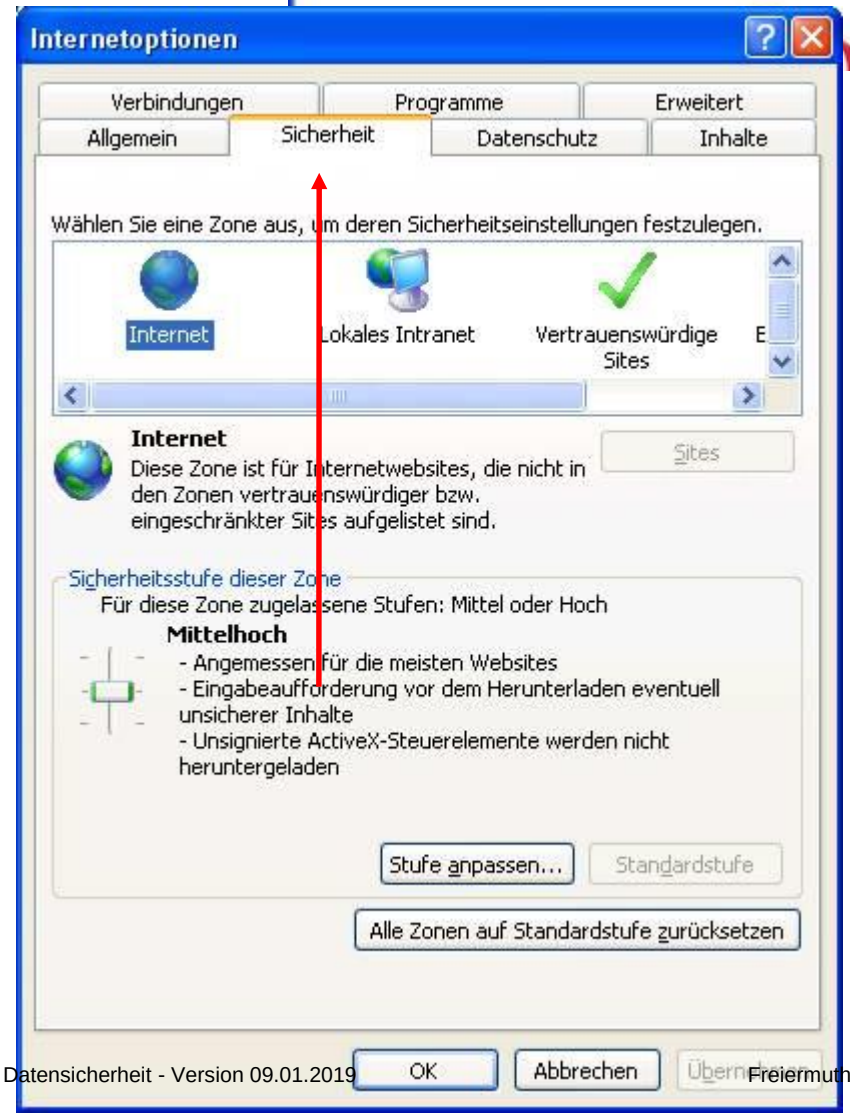
https://banking.sparda.de/wps/portal/spardamodern-banking

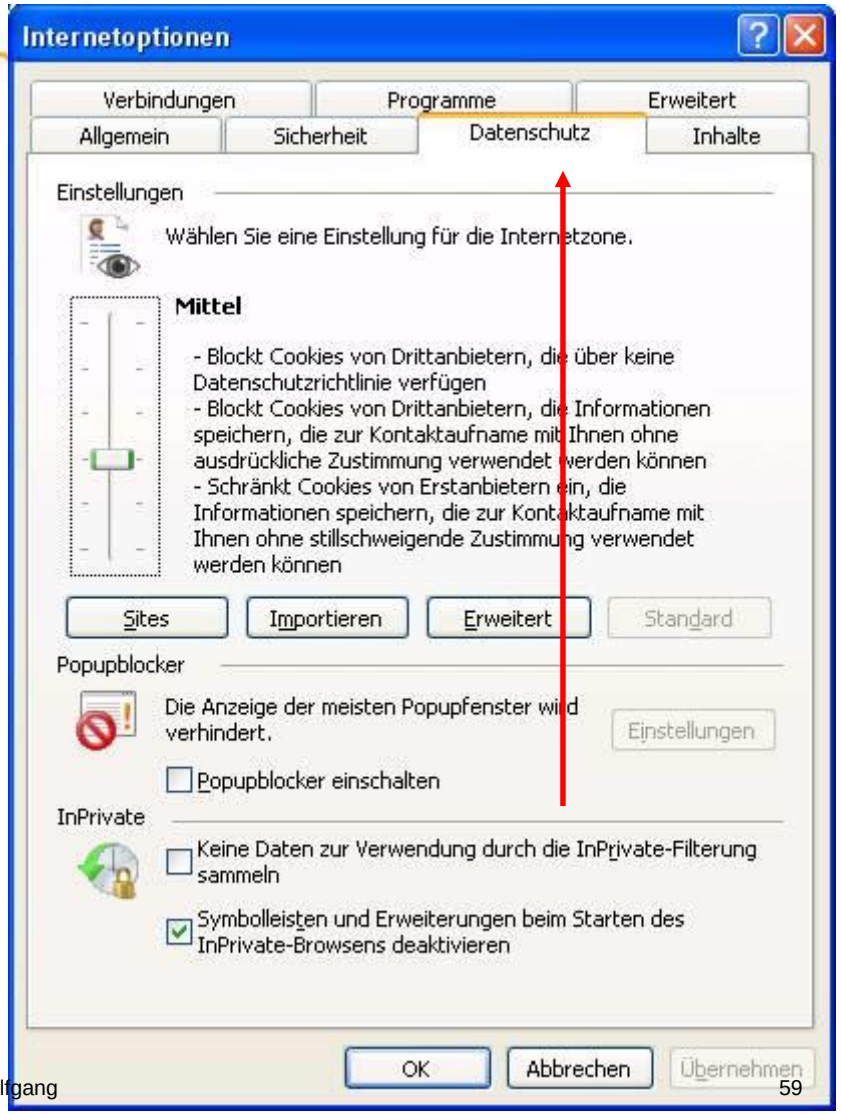


Gefahren für die IT-Sicherheit

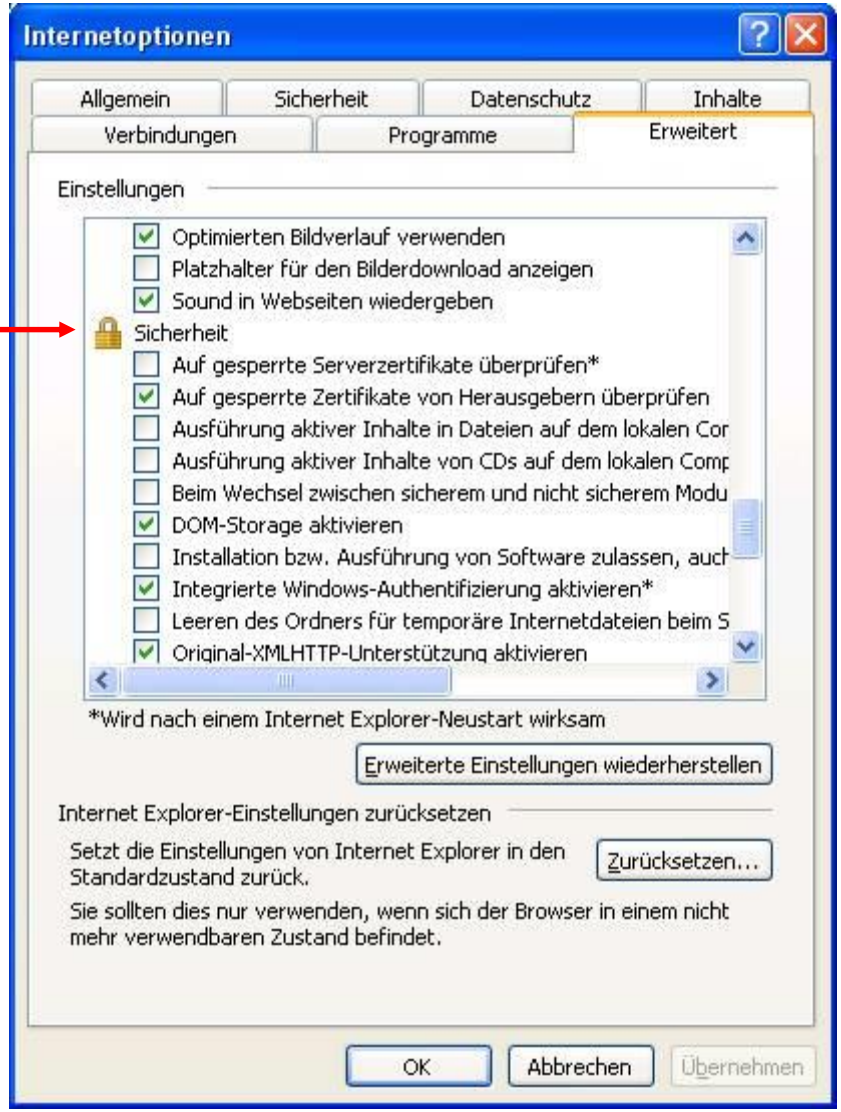



Web Bilder Videos Maps News Produktsuche E-Mail Mehr


Internetoptionen
Verbindungen
Programme
Erweitert
Allgemein
Sicherheit
Datenschutz
Inhalte
Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen.
Internet
Lokales Intranet
Vertrauenswürdige Sites
Internet
Diese Zone ist für Internetwebsites, die nicht in den Zonen vertrauenswürdiger bzw. eingeschränkter Sites aufgelistet sind.
Sites
Sicherheitsstufe dieser Zone
Für diese Zone zugelassene Stufen: Mittel oder Hoch
Mittelhoch
- Angemessen für die meisten Websites
- Eingabeaufforderung vor dem Herunterladen eventuell unsicherer Inhalte
- Unsignierte ActiveX-Steuerelemente werden nicht heruntergeladen
Stufe anpassen...
Standardstufe
Alle Zonen auf Standardstufe zurücksetzen
OK
Abbrechen


Internetoptionen
Verbindungen
Programme
Erweitert
Allgemein
Sicherheit
Datenschutz
Inhalte
Einstellungen
Wählen Sie eine Einstellung für die Internetzone.
Mittel
- Blockt Cookies von Drittanbietern, die über keine Datenschutzrichtlinie verfügen
- Blockt Cookies von Drittanbietern, die Informationen speichern, die zur Kontaktaufname mit Ihnen ohne ausdrückliche Zustimmung verwendet werden können
- Schränkt Cookies von Erstanbietern ein, die Informationen speichern, die zur Kontaktaufname mit Ihnen ohne stillschweigende Zustimmung verwendet werden können
Sites
Importieren
Erweitert
Standard
Popupblocker
Die Anzeige der meisten Popupfenster wird verhindert.
Einstellungen
Popupblocker einschalten
InPrivate
Keine Daten zur Verwendung durch die InPrivate-Filterung sammeln
Symbolleisten und Erweiterungen beim Starten des InPrivate-Browsens deaktivieren
OK
Abbrechen
Übernehmen

Gefahren für die IT-Sicherheit



Gefahren für die IT-Sicherheit

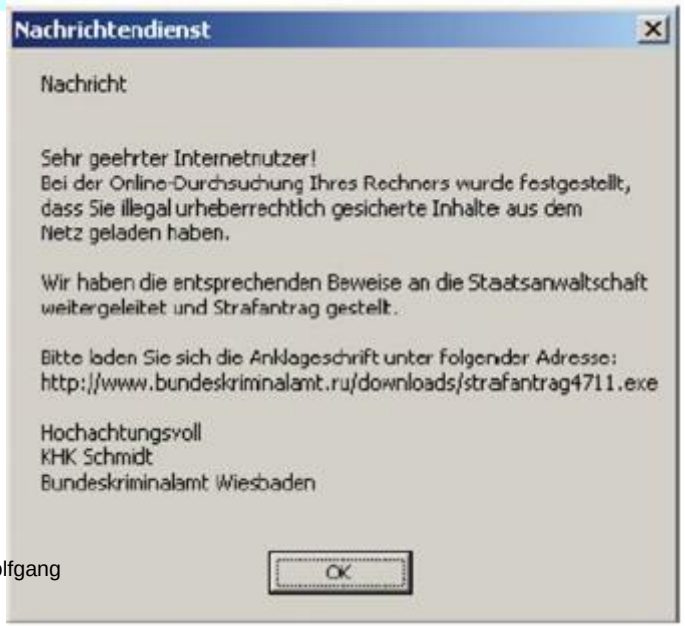
- **(Werbe-) PopUp‘s**
  - **Einblendungen in Bildschirmfenstern**
  - **sind oftmals lästig und werden „einfach weggeklickt“**
  - **das „Wegklicken“ löst möglicherweise ungewollte Aktionen aus**

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.“

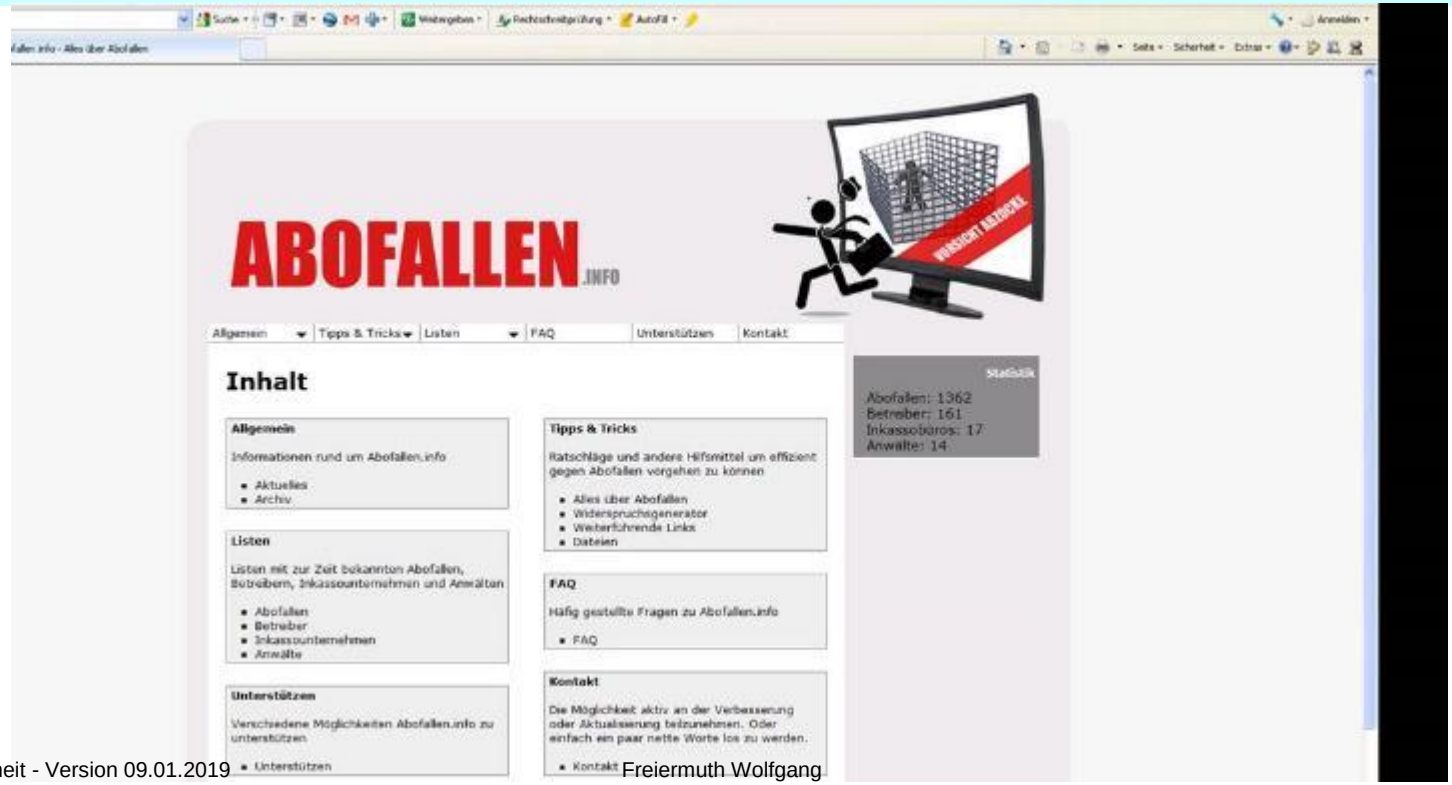
Gefahren für die IT-Sicherheit

- **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**



Gefahren für die IT-Sicherheit

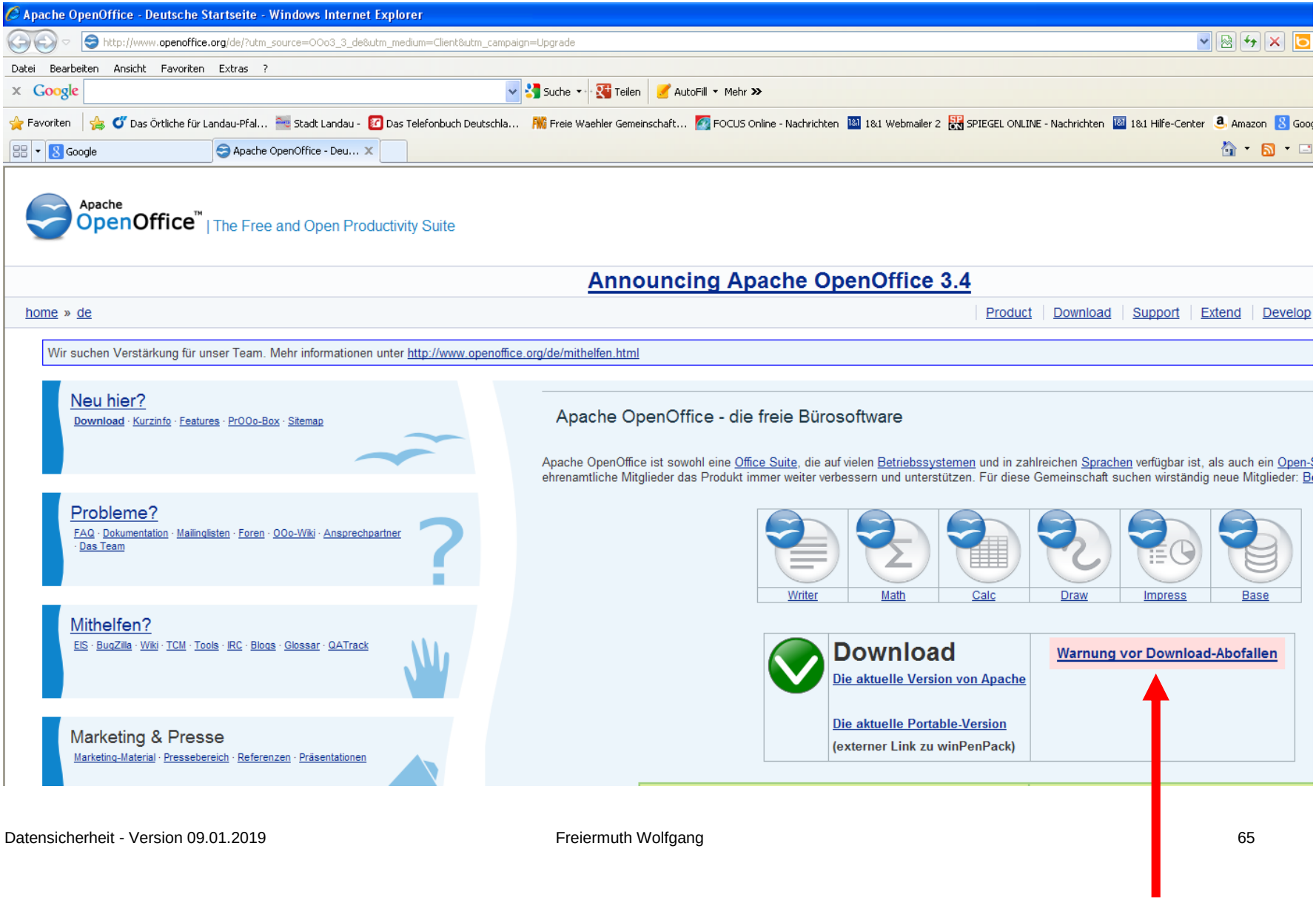
- **Abofallen**
  - **bieten den Internetnutzern Downloadmöglichkeiten für diverse Software**
  - **bieten teilweise kostenlose Software im Rahmen sogenannter „Supportverträge“**



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



Gefahren für d

VORSICHT IM NETZ

Comeback der Internet-Abofallen

VERBRAUCHER-TIPP: Von Online-Abzockversuchen nicht einschüchtern lassen

VON BERRIT GRÄBER

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 Inkasso-Ärger. 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 zu Beispiel einem Routenplaner – und schon kommt eine Rechnung ins Haus über ein Jahr „Mitgliedschaft" für stolze 249 Euro. „Die Internet-Abzocke erlebt eine Renaissance", warnt 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 Anwälten oder Inkassobüros am Hals haben. Die meisten hatten lediglich nach kostenlosen Kochrezepten fürs 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 totgeglaubte Abkassier-Masche sei wieder „quicklebendig", 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 Internetseiten 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 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.

Eine dubiose Firma mit Sitz in Mittelamerika steckt hinter den neuen Internet-Abofallen. FOTO: IMAGO

Rheinpfalz-Zeitung
August 2014

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**

Gefahren für die IT-Sicherheit

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

„Falsche“ Infos im Netz:
Umweltplakette Frankreich

Umweltplakette.pdf

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

Gefahren für die IT-Sicherheit

- **Bewertungsportale**

Frei nach Churchill (?):

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

Frei nach Computerzeitschrift „CHIP:

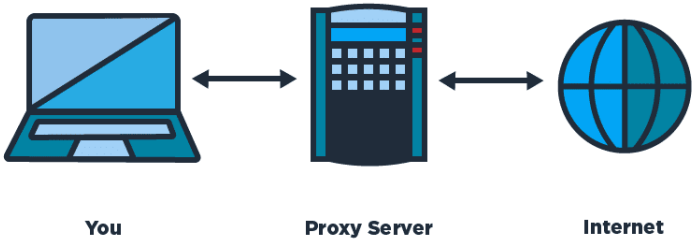
„5-Sterne-Mafia“ == > Agenturen bieten Dienstleistungen an

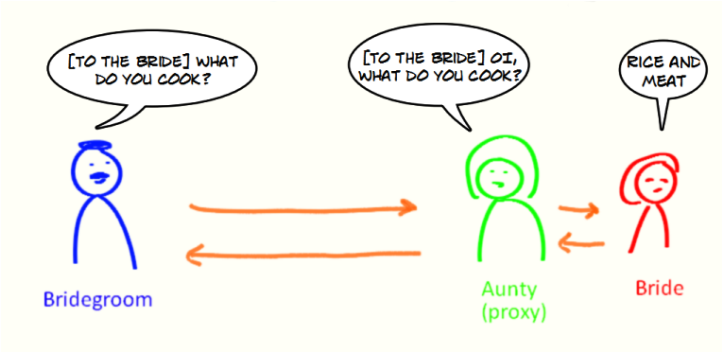
- ✓ **Große Portale bevorzugen**
- ✓ **Möglichst viele Bewertungen zu einem Produkt**
- ✓ **Wer hat bewertet**
- ✓ **Achten Sie auf die Sprache**
- ✓ **Suchen Sie gezielt nach negativen Bewertungen**
- ✓ **Prüfen Sie auf mehreren Portalen**

Gefahren für die IT-Sicherheit

- **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

Gefahren für die IT-Sicherheit

- **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.

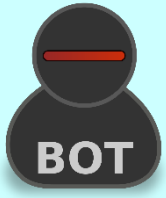
Gefahren für die IT-Sicherheit

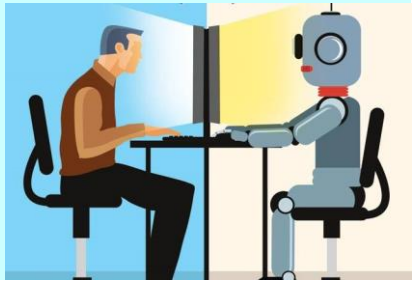
- **Deepfakes**

  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.

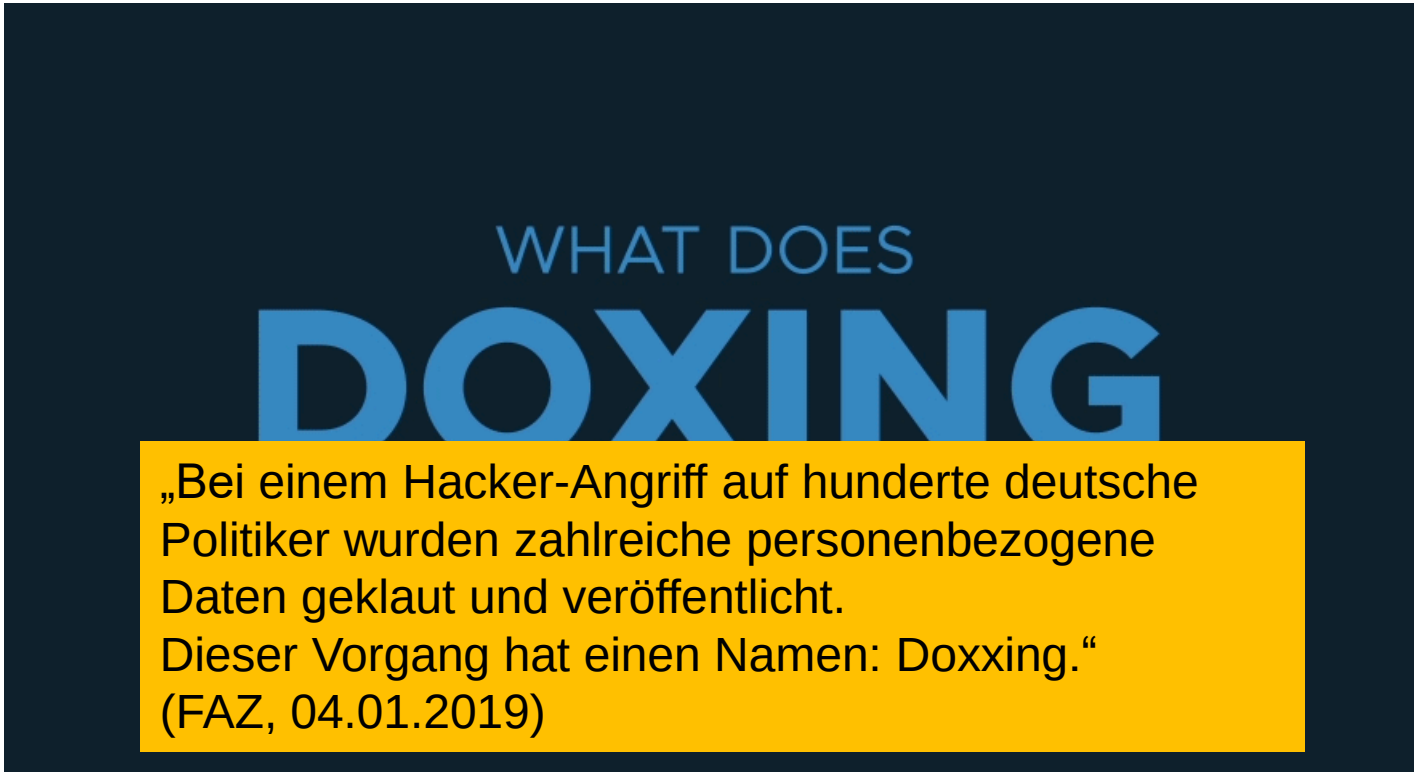
- **Bots**

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





Gefahren für die IT-Sicherheit



„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)

Gefahren für die IT-Sicherheit

- **Doxing**

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

Zum her.

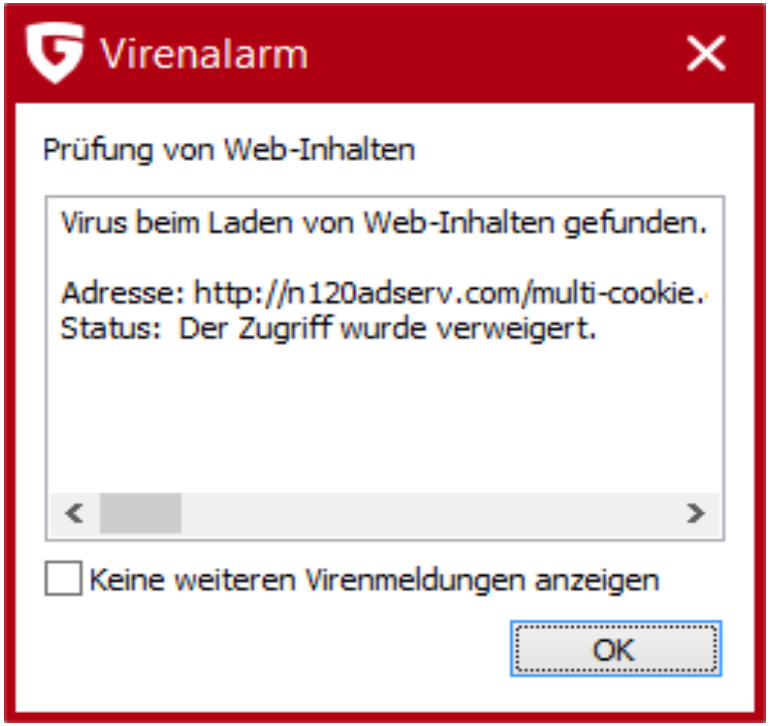
„Sc
Kor **nit**
sch
Die er
etwa

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

“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?“
(FAZ, 08.01.2019)

- **Cookies (auf Deutsch: Plätzchen, Kekse)**

Normalerweise darf jeder Betreiber eines Internetplatzes nur **sein Cookie** auslesen.
So darf Online-Shop A nicht den Cookie von Online-Shop B auslesen.
ABER:
Setzt ein sogenannter **Drittanbieter** ein Werbebanner auf A und auch ein Werbebanner auf B, dann wird mit Hilfe dieser Cookies doch ein Surfverhalten des Verbrauchers erhalten - bis das Cookie gelöscht wird.
Es gibt dauerhafte Cookies (evtl. über Jahre auf dem PC) und 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!

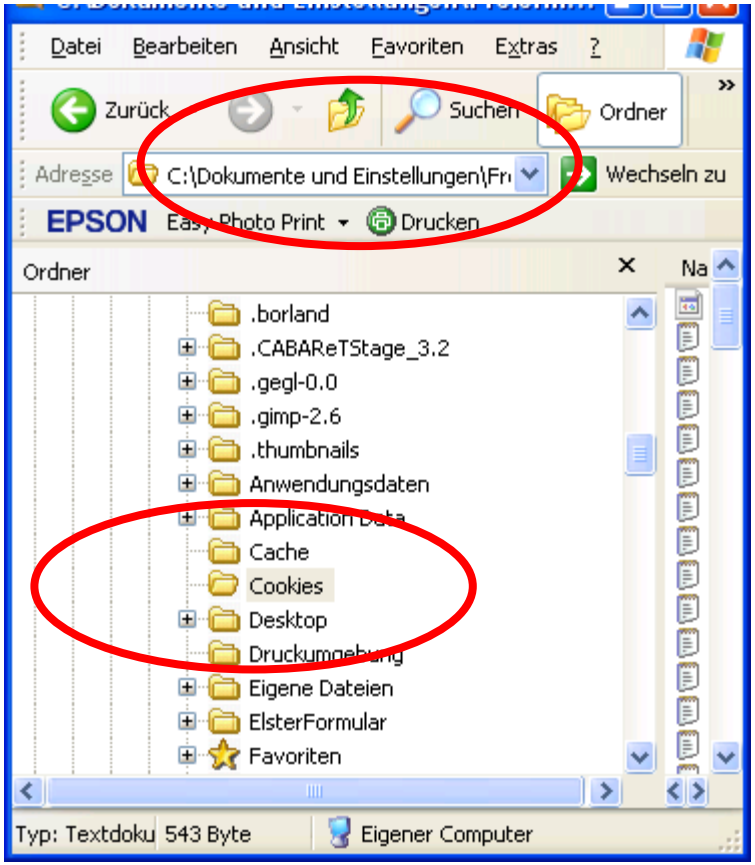
IT-Sicherheit und Datenschutz

name@www.adac[1].txt

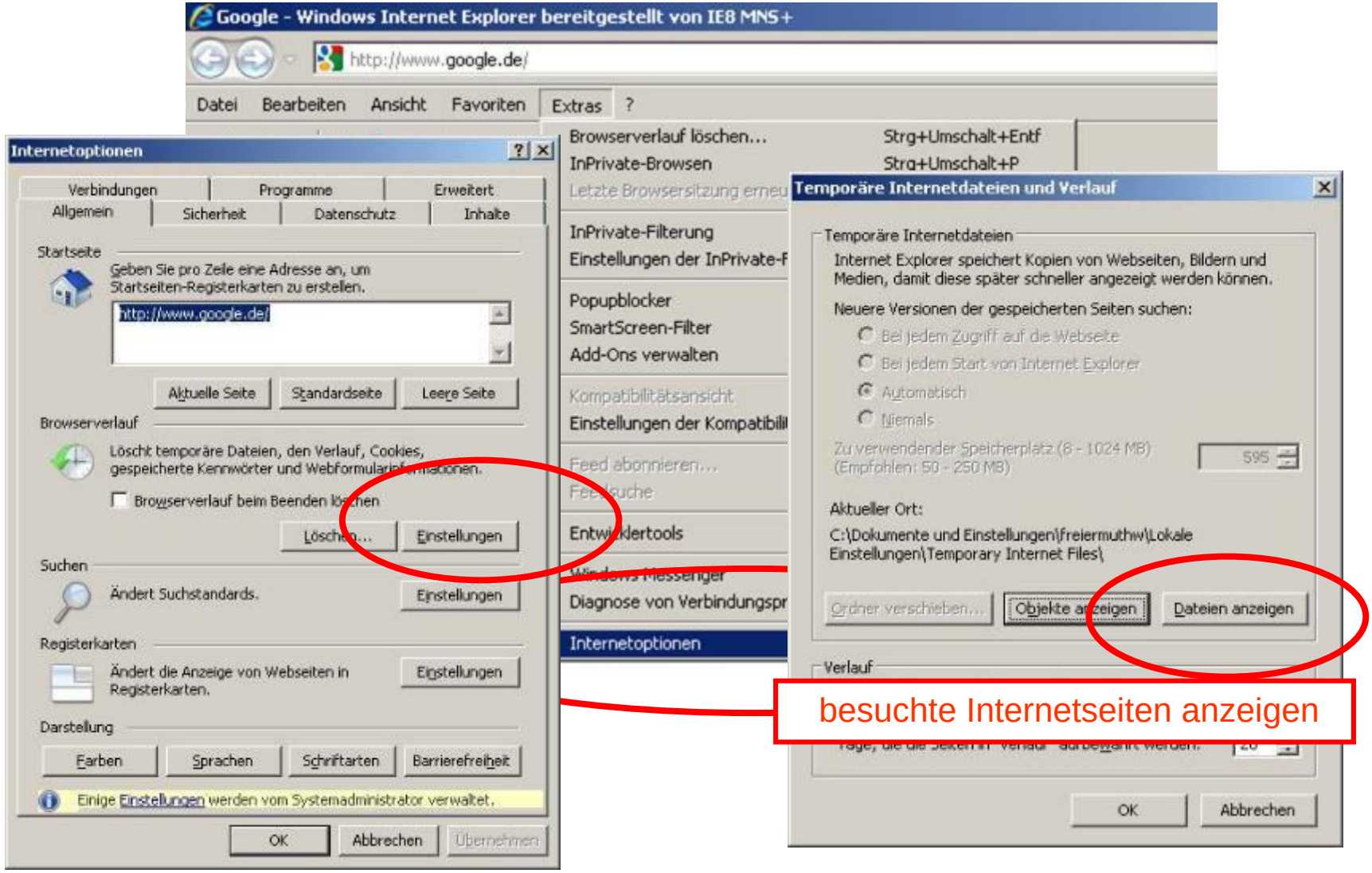
➔ **Cookies dienen der Wiedererkennung des Benutzers**

➔ **stellen einfache Informationsspeicherung am Client ohne aufwändige Programmierung am Server dar**

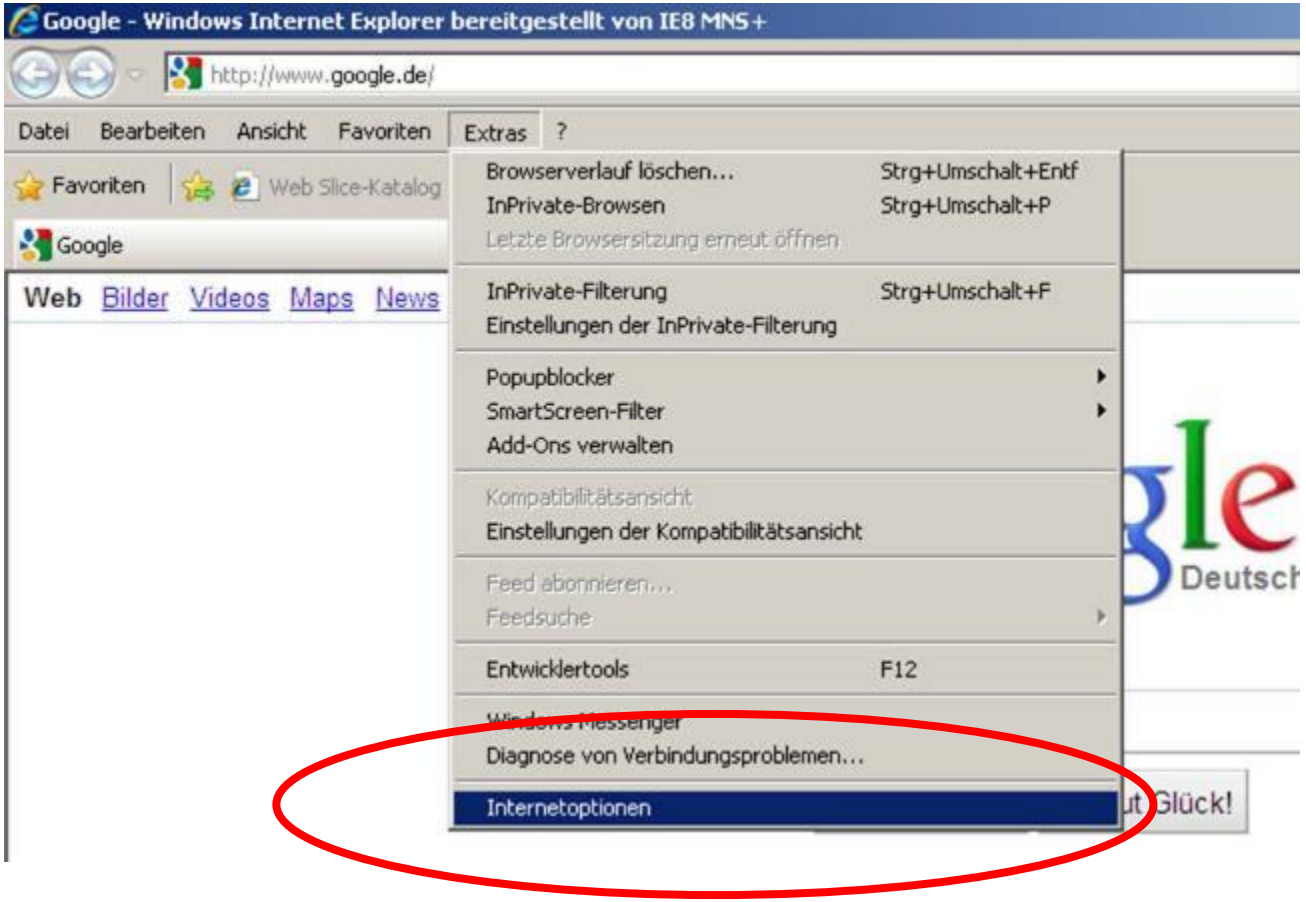
Der Browser speichert besuchten Webseiten im „Cache“, um schneller zugreifen zu können.



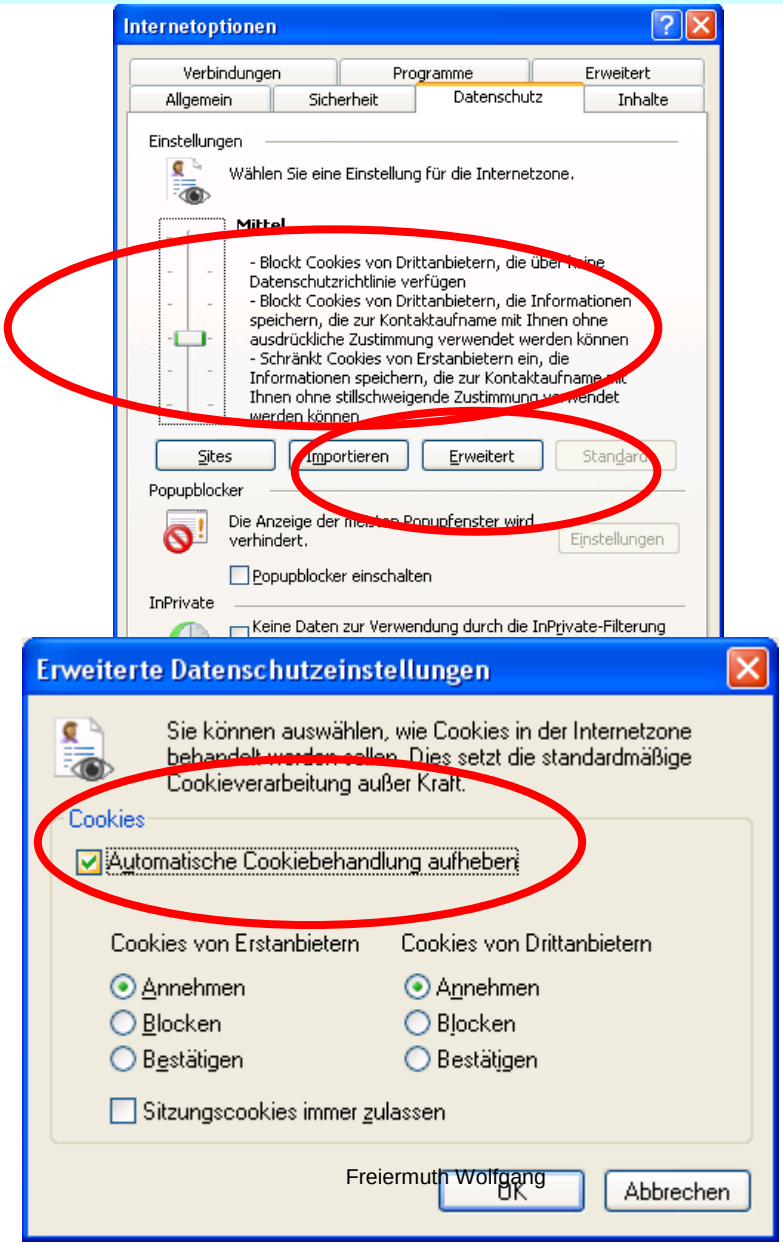
IT-Sicherheit und Datenschutz



IT-Sicherheit und Datenschutz



IT-Sicherheit und Datenschutz



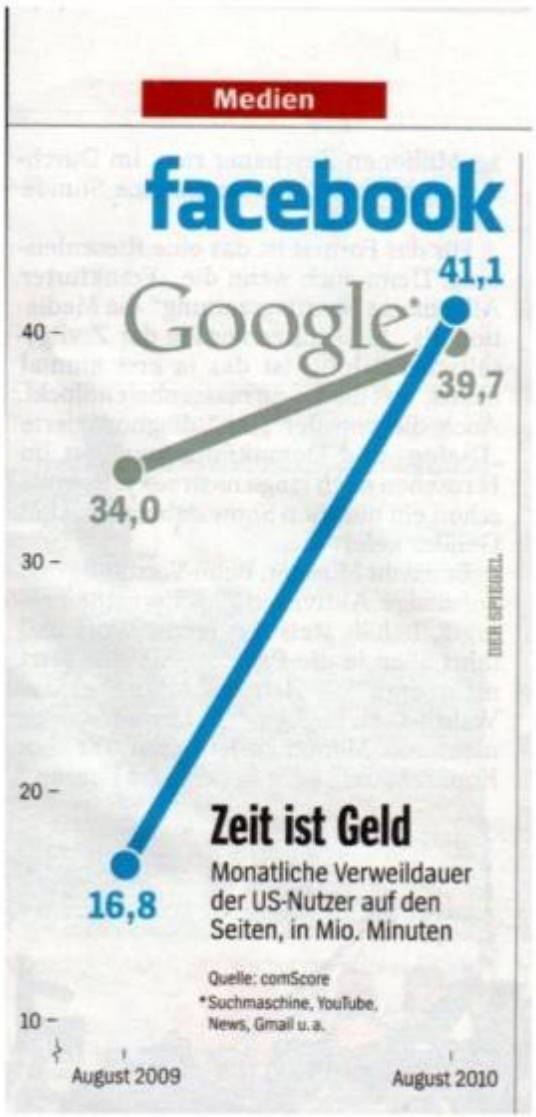
IT-Sicherheit und Datenschutz

virtueller Exhibitionismus

- **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)


"Zusammenführen" von Informationen:
Google
flickr
Benutzer
amazon
Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz
'gläserner User"

IT-Sicherheit und Datenschutz



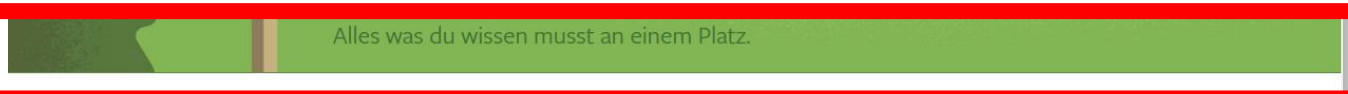
Was der Firma noch gefährlich werden kann, ist ihr notorisch salopper Umgang mit den Nutzerdaten. Schon der neue E-Mail-Dienst geht ein hohes Risiko ein: Versprochen ist, dass Facebook die gesamte Kommunikation auf ewig speichert – Löschen ist, gelinde gesagt, umständlich. Aber werden die Mitglieder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

Der Spiegel 47/2010

IT-Sicherheit und Datenschutz

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:



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 löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.

2. Wenn du IP-Inhalte löschst, 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).

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.

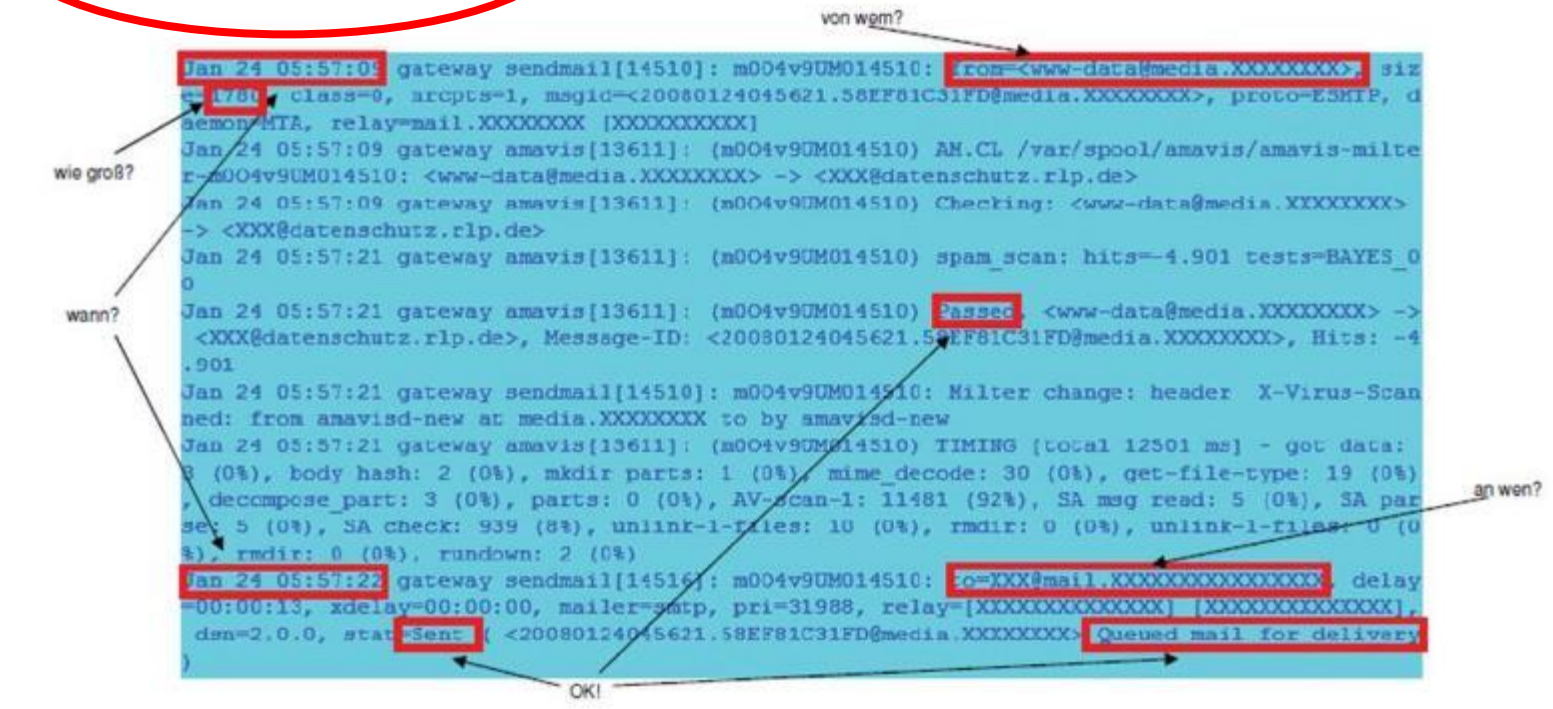
aus: Spiegel-Online 30.01.2015

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

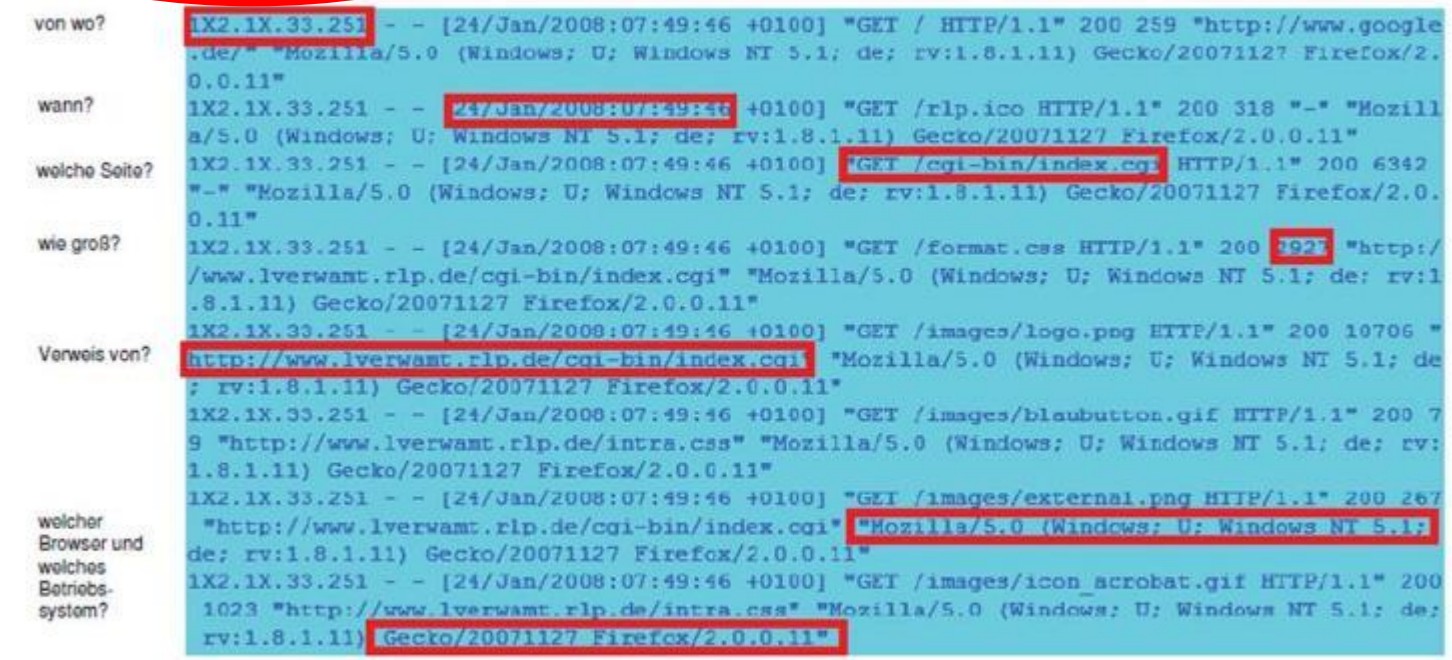
Beispiel 1: Mailserverlogdatei



Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

Protokolldaten

Beispiel 2: Webserverlogdatei



Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

Protokolldaten

Beispiel 4: Proxyserverlogdatei

von wo?

wann?

welche Seite?

```
1201268023.656    1020 1X2.1X.2X4.25 TCP_MISS/200 1244 GET http://www.datenschutz.rlp.de/i
ndex2.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
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/oeffentlich.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 -
```

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

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:

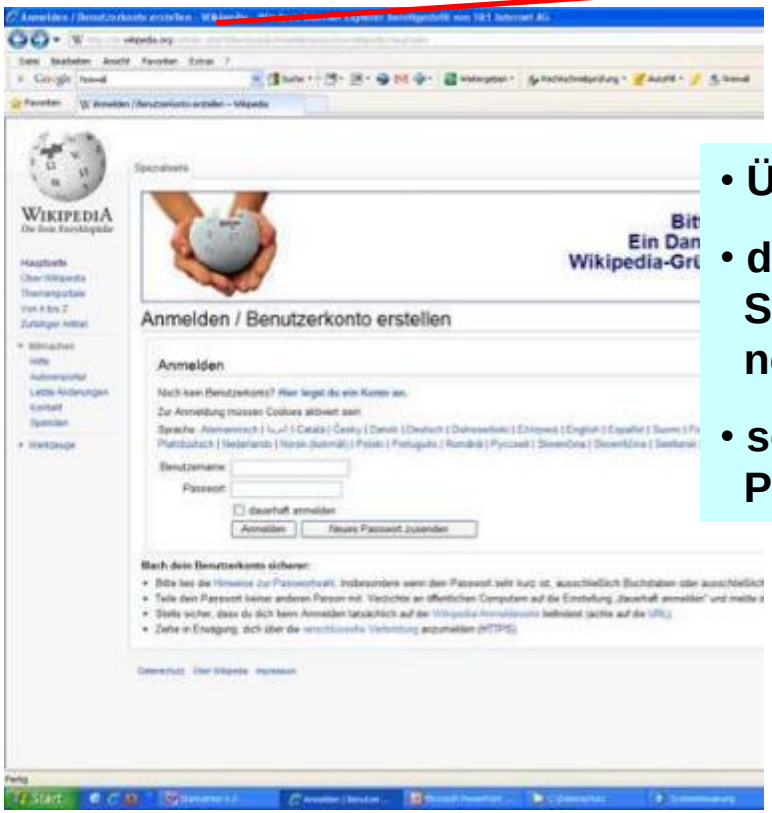
Passwortsicherheit

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

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

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**

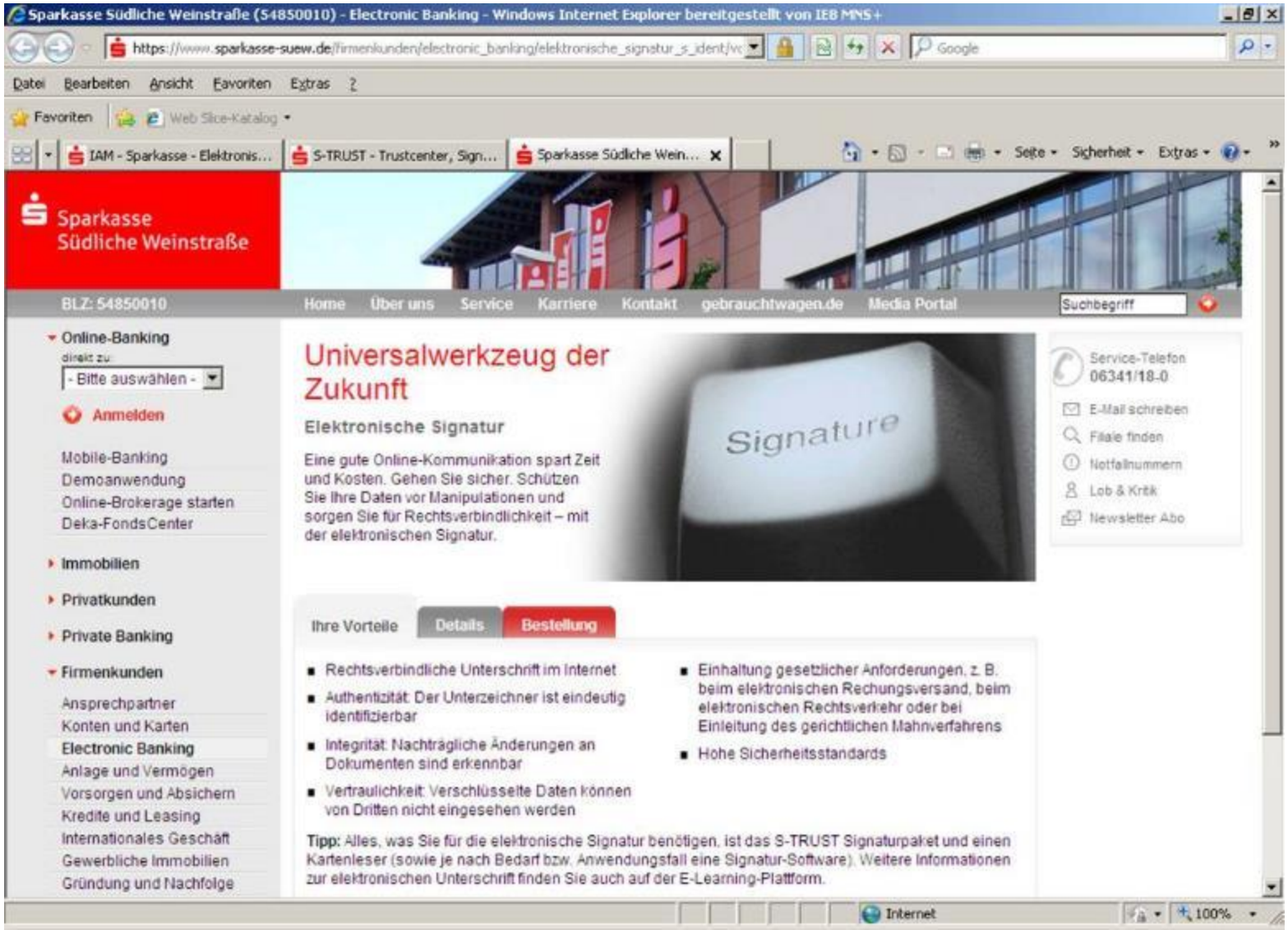
Lösungsansätze:

Authentizität im Emailverkehr

- **Einsatz der elektronischen Signatur**
  Die elektronische Signatur erfüllt technisch gesehen den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten (≠ digitale Signatur)
- **Verschlüsselung und elektronische Signatur**
- **Einsatz kryptographischer Verfahren**

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

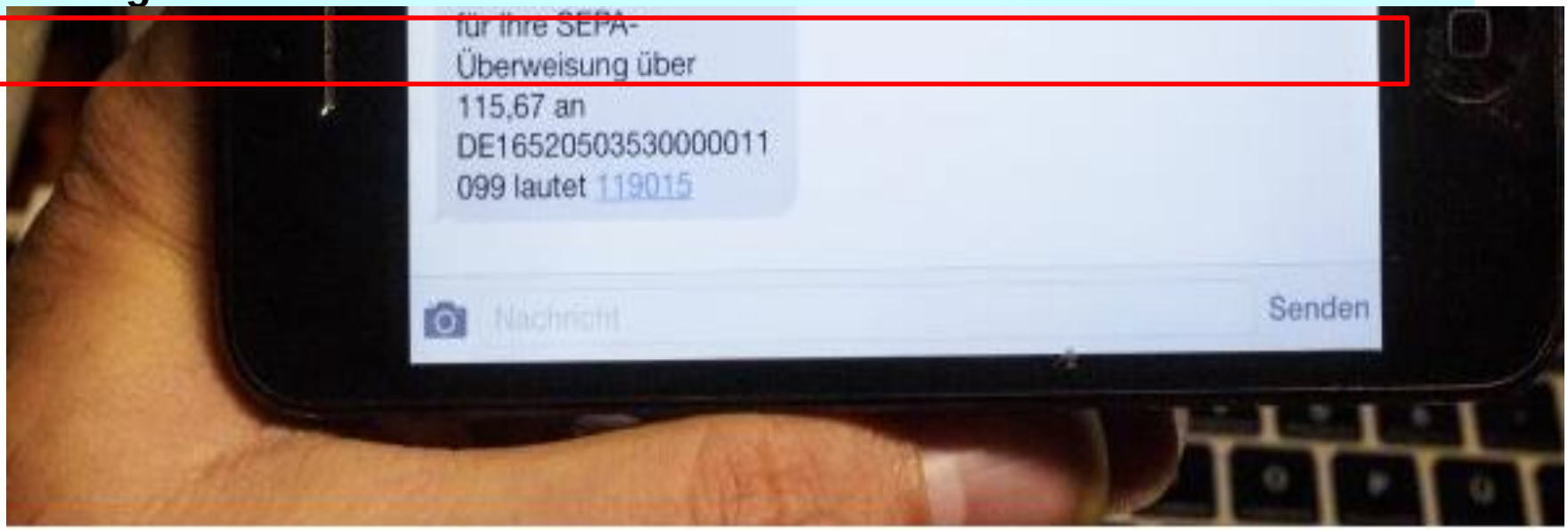
Lösungsansätze:



Lösungsansätze:

Lösungsansätze:

Lösungsansätze:



sverfahren mit mTan: Kriminelle spionieren Smartphone aus

i Online-Bankgeschäften: Wer sich sogenannte mTan aufs Handy schickten lä
werden. Im neuen SPIEGEL raten Experten zu anderen, sichereren Verfahre

8.05.2014 – 12:01 Uhr

enden | Merken

Hamburg - Experten warnen vor Onlinebanking
sind Einmalpasswörter, die den Kunden auf ihr H
"Über manipulierte Handy-Apps können Internet
Smartphones ausspionieren", sagt Christian Fur

Lösungsansätze:

Lösungsansätze:

Aus: Rheinpfalz-Zeitung vom 26. März 2013

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 Stiftung 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.

Grundbedrohung der IT-Sicherheit

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

➔ Daten sind unverändert

- absichtlich
- unabsichtlich
- technische Fehler

Verlust der Authentizität

➔ Daten sind sicher einem Sender zuzuordnen

➔ Daten sind unabstreitbar

Grundbedrohung und Lösungsmöglichkeiten bei der IT-Sicherheit

Verlust der Verfügbarkeit — **Schaffung von Ausfallsicherheit**; **Datensicherung**

Verlust der Vertraulichkeit — **Verschlüsselung**

Verlust der Integrität

Verlust der Authentizität

} **Elektronische Signatur**

➔ **Aufklärung und Sensibilisierung aller beteiligten Personen**

Vielen Dank
für Ihre Aufmerksamkeit!