



Mittwoch, 15. Oktober 2014, 18:30 Uhr  
Dr. André Hojka (Vater Gruppe)  
Prof. Dr. Walter Reimers

# Schutz der Privatsphäre am eigenen Rechner

*oder*

## *12 Dinge, die Sie beachten sollten*



**Hundertprozentigen Schutz gibt es nicht!**

**oder mit Joachim Ringelnatz:**

**Sicher ist, dass nichts sicher ist.**

**Selbst das nicht.**





12 

11 

10 

9 

8 

7 

6 

5 

4 

3 

2 

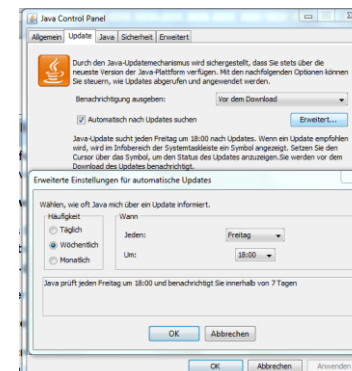
1 



# 1. Sicherheitsupdates



- Bei **Beseitigung von Sicherheitslücken** muss man schneller als der Cyberkriminelle sein.
- Prüfen, ob für Betriebssystem, Browser, Office-Pakete, Medienplayer, Dienstprogramme von Providern oder Virens Scanner **automatische Updates** durchgeführt werden.
- Update-Prüfprogramm z.B.: [http://www.chip.de/downloads/CHIP-Updater\\_70656452.html](http://www.chip.de/downloads/CHIP-Updater_70656452.html)
- **Hinweise auf Updates** zu beachten und nicht wegklicken
- Das Bürger-CERT des BSI bietet einen **Newsletter-Service über aktuelle Updates**. Softwareproduzenten und Brancheninformationsdienste wie [www.heise.de](http://www.heise.de) oder [www.golem.de](http://www.golem.de) stellen Warndienste ("Alert Services") per E-Mail und Newsticker zur Verfügung.
- Aber Vorsicht: Kriminelle können **gefälschte Updates** nutzen! Seriosität prüfen!
- **Automatisierung des Update Service z.B. bei Microsoft:** "[Microsoft Safety & Security Center](http://www.microsoft.com/scc/)"
- **Microsoft Patch-Day:** jeden zweiten Dienstag im Monat veröffentlicht Microsoft jüngste Aktualisierungen (durch Zeitverschiebung zu den USA bei uns meist spät abends).
- **Updatemechanismus von Java** auf regelmäßige Aktualisierungen einstellen:  
über den Reiter „Update“ im „Java Control Panel“ – Schaltfläche „Erweitert“ für Updateeinstellungen





## 2. Virenschanner

- Insbesondere unter Windows ist eine gute Antiviren-Software unerlässlich. Täglich erscheinen neue Viren: Kaspersky Lab 2013: **täglich 315.000 neue Viren!**
- Viren-Scanner überprüfen Dateien auf „**Fingerabdrücke**“ **bekannter Schadprogramme**. Deshalb muss die Software regelmäßig aktualisiert werden.
- Ein Virenschanner sollte **automatisch immer im Hintergrund** laufen (Icon in der Task-Leiste). Infizierte Dateien werden von der Antiviren-Software in einem **Quarantäneordner** gekapselt (ohne Verbindung zum Betriebssystem):



Im Quarantäneordner kann der Benutzer wählen:  
Infizierte Datei löschen / bereinigen und normal speichern / trotz Infektion ausführen

- **Kostenlose Virenschutzprogramme** mit deutschsprachiger Benutzeroberfläche:
  - Avira Free Antivirus (<http://free-av.de>)
  - avast! Free Antivirus (<https://www.avast.com/de-de/free-antivirus-download>)
  - AVG Anti-Virus Free (<http://free.avg.com/de-de/startseite>)
  - Microsoft Security Essentials (<http://microsoft.com/securityessentials>)
- Unter [http://www.heise.de/security/bilderstrecke/bilderstrecke\\_329610.html](http://www.heise.de/security/bilderstrecke/bilderstrecke_329610.html) findet man **Bildschirmbilder von falschen Virenschannern**.
- Virenschanner belasten das System und damit die **Performance**. Die mehrfache Prüfung des Dateiinhalts auf Virenbefall führt nach Meinung des BSI selten zu mehr Sicherheit.



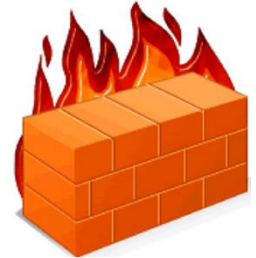


## 2. Virens Scanner - Infektionsbeseitigung

- **Sofortige Erstmaßnahmen:** Passwörter und Zugangsdaten von einem sauberen Rechner aus ändern und gegebenenfalls Kontoauszüge falsche Buchungen überprüfen.
- Bei Verdacht Vireninfektion: Internetnutzung vermeiden; von CD/DVD oder USB-Stick mit **unverseuchtem System und aktuellem Virens Scanner booten** und die infizierte Platte durch Antiviren-Software bereinigen lassen
- **Rechner säubern bei geringerem Befall:**
  - Computer ausschalten und Expertenrat einholen
  - [Bootreihenfolge](#) im BIOS ändern und von viren-freie System- beziehungsweise Boot-CD oder entsprechendem USB-Stick starten
  - PC mit aktuellem Viren-Schutzprogramm prüfen
  - Noch nicht gesicherte Daten sichern
  - Viren durch Anti-Viren-Programm entfernen lassen
  - Festplatte und alle anderen Datenträger noch einmal überprüfen
  - Boot-Reihenfolge des Rechners wieder zurückstellen auf Festplatte und System neu starten
  - Rekonstruktion von veränderten oder gelöschten Daten aus den Datensicherungen und den Sicherungskopien der Programme
  - Je nach Ursache der Vireninfektion Hersteller/Ersteller/Absender der Infektionsquelle und BSI informieren. Wurden Daten vom infizierten Rechner verschickt, Empfänger der Daten warnen.
- **System neu aufsetzen bei größerer Bedrohung:**  
Rechner aus vertrauenswürdigen Backup wiederherstellen



## 3. Firewall



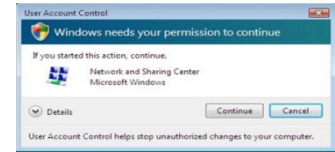
- Die Firewall überprüft wie eine Brandschutzmauer anhand der Adresse des Rechners (IP-Adresse), ob ein Datenpaket, das in ein Netzwerk hinein oder aus dem Netzwerk heraus will, dazu berechtigt ist. Dazu werden Listen mit erlaubten IP-Adressen für bestimmte Verbindungsfunktionen (ports) erstellt.
- Eine **normale** Firewall schützt viele Rechner gegenüber der Umwelt. Eine **Personal** Firewall dient dem Schutz des Rechners, auf dem sie installiert ist.
- Funktionalitäten der Personal Firewall:
  - **Paket Filter**: Kontrolle der Datenpakete auf vom Benutzer festgelegte Regeln
  - **Sandboxing**: Sperrung von Programmen/Dateien in eine abgeschottete Umgebung und Ausführung in diesem Bereich; so kann eventuelle Schadsoftware durch die Isolation vom eigentlichen System dort keinen Schaden anrichten.
- Enge Filterregeln gestatten nur wirklich notwendigen Zugriffe. Nicht benötigte Ports sollten gesperrt sein.
- Zur Konfiguration und zum Verstehen von Warnungen einer Firewall muss man allerdings die Bedeutung von IP-Adressen, Rechnernamen und Ports kennen.
- Mehrere Firewalls belasten die Performance des Rechners zumeist mehr als sie Nutzen stiften, da sie mehrmals das gleiche prüfen.



## 4. Benutzer mit eingeschränkten Rechten

4

- **Nicht mit Administratorenrechten arbeiten**
- **Unterschiedliche Benutzerkonten einrichten (für jeden Nutzer eines)**
- **Stets aktuelle Software einsetzen – Warnfenster für angebotene Updates ernst nehmen**
- **Nutzungsberechtigungen einschränken – z.B. Dateiberechtigungen erteilen**
- **Nutzungsmöglichkeiten für Kinder einschränken**
- **Sensible Daten auf separaten Geräten bearbeiten – bei gemeinsamer PC-Nutzung keine Passwörter auf dem Rechner speichern**
- **Verlauf löschen – andere Nutzer können dann virtuelle Reisen nicht nachvollziehen**





## 5. Vorsicht und Misstrauen gegenüber Link und Absender

ENISA, European Network  
and Information Security Agency:  
„Social Engineering: Exploiting the  
Weakest Links 08-2008“

“... attackers are readily able to exploit  
psychological factors and human behaviour,  
as well as users' (mis)understanding of the  
technology that they are required to use ...

... However, the key to success ultimately lies in  
improving the awareness of the people who may be targeted ...”



## 5. Vorsicht und Misstrauen gegenüber Link und Absender

ENISA, European Network and Information Security Agency:  
 „Social Engineering: Exploiting the Weakest Links 08-2008“

	Correctly classified	Incorrectly classified	Don't Know
Legitimate messages	36%	37%	27%
Illegitimate messages	45%	28%	26%
Overall	42%	32%	26%



Subject: Contribute to the Tsunami Disaster Relief Effort  
 From: Contribute Paypal



[Sign Up](#) | [Log In](#) | [Help](#)

### Contribute to the Tsunami Disaster Relief Effort

We at PayPal wish to express our profound sorrow over the suffering and loss of life resulting from the earthquakes and tsunami in South Asia and Africa. You can help those affected by this disaster by donating directly to UNICEF's Tsunami Disaster Relief effort using your PayPal account.

**Make a donation to the Tsunami Relief Effort through PayPal**

[Donate now](#)

UNICEF works to bring relief to all disaster victims, particularly women and children who are the most vulnerable. The organization is working closely with the governments in all the countries affected by this disaster to combat the spread of disease and ensure that the victims have immediate access to fresh water, food, shelter, medical care and supplies. Visit [www.unicefusa.org](http://www.unicefusa.org) to learn more about UNICEF's Tsunami Disaster Relief efforts.



UNICEF is rushing relief assistance to the countries hardest hit by massive ocean flooding following the earthquake on 12/26. UNICEF is working to meet the needs of hundreds of thousands of people who survived the tsunamis but now need shelter, water, medical supplies and other urgent assistance.


Privacy Notice: If you donate \$250 or more, PayPal will provide your name, billing address, email and donation amount to UNICEF so that UNICEF can provide you with a receipt for your donation. Other than this, PayPal will not share your information with UNICEF. PayPal will waive all fees in relation to the donation, so that UNICEF will receive 100% of the amount you donate.

Total Collected: \$731,481.18 USD  
 contributed by 15568 donors



## 6. Internet-Browser



- Internet-Browser sind die **zentrale Komponente** für die Internet-Nutzung und daher beliebte **Ziele für Cyber-Angriffe** z.B. über den Adobe Flash Player oder Java-Programme.
- Sicher sind Browser mit **Sandbox-Technologie**, wie z. B. in Google Chrome (<https://www.google.com/chrome>) mit integriertem/aktuellem Adobe Flash Player.  
Alternativ: Freie Software wie z.B. „Sandboxie“ (<http://www.sandboxie.com/>) verwenden und beliebigen Browser nur in einem isolierten Bereich öffnen.
- Versuche zur Verführung zum Download schädlicher Programme („Social Engineering“) sowie „Drive-by-Download“-Angriffe können mit Aktivieren der Filtermechanismen im Browser durch Kooperation bei der Bewertung von Seiten durch den Browserhersteller abgewehrt werden:
  - **SmartScreen-Filter im Internet Explorer** (unter [Extras/](#)  [Sicherheit](#) Smartscreen-Filter ein/aus)
  - **Phishing- und Malwareschutz im Mozilla Firefox und in Google Chrome**

Durch die enorme Dynamik bei der Entwicklung neuer Angriffsmethoden können solche Filter schnell aufgeweicht werden.

- Die Java-Laufzeitumgebung ermöglicht die Ausführung neuer Programme also auch von Schadprogrammen. **Verzicht auf Java erhöht die Sicherheit.**  
Wenn bestimmte Anwendungen Java benötigen, wird der Benutzer darauf hingewiesen.  
Empfehlung: Java-Unterstützung in den Einstellungen Ihres Webbrowsers abschalten. Einschalten erst wenn es von einer vertrauenswürdigen Website benötigt wird.
- Nach Installation von Java unbedingt die automatische Updatefunktion aktivieren (siehe Folie 4).



# 6. Internet-Browser

## Sicherheitseinstellungen der gängigen Browser



6

- **Internet Explorer:**
  - Sicherheitseinstellungen: <http://windows.microsoft.com/de-DE/internet-explorer/ie-security-privacy-settings>
  - Blockieren aktiver Inhalte: <http://windows.microsoft.com/de-AT/windows7/How-to-use-Tracking-Protection-and-ActiveX-Filtering>
  - **Empfehlung: Blockieren der ActiveX-Steuerelemente, neueste Version des Internet Explorers verwenden**
- **Chrome:**
  - Sicherheitseinstellungen: <http://support.google.com/chrome/?hl=de#topic=14666&rd=1>
  - Blockieren aktiver Inhalte: <http://support.google.com/chrome/bin/answer.py?hl=de&answer=142064>
  - **Empfehlung: Unter "Plugins blockieren" die Funktion "Click-to-Play,, wählen**
- **Firefox:**
  - Sicherheitseinstellungen: <http://support.mozilla.org/de/kb/Einstellungen-Fenster%20-%20Sicherheits-Abschnitt>
  - **Empfehlung: Standard-Einstellungen von Firefox verwenden, "Passwörter speichern,, deaktivieren, beim Speichern von Passwörtern im Browser ein Master-Passwort festlegen,**  
Hinweise für sicheres Passworte: <https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter.html>
- **Opera:**

Sicherheitseinstellungen: <http://www.opera-tutorial.de/sicherheit.php>
- **Safari:**

Siehe „ Sicherheitseinstellungen in Safari“ im Online-Portal "VERBRAUCHER SICHER ONLINE" unter <http://www.verbraucher-sicher-online.de/anleitung/sicher-surfen-mit-dem-browser-safari>



# 6. Internet-Browser

## Einstellungen für den Internet Explorer 11



### Datenschutzeinstellungen

- **Cookies**

- speichern Informationen und Einstellungen eines Benutzers, die das Browsen angenehmer gestalten können.
- gefährden aber eventuell die Privatsphäre z.B. durch Speicherung der besuchten Websites zur Nachverfolgung.
- Einstellungen im Menüpunkt Sicherheit unter Datenschutzrichtlinien der Webseite...
- löschen und verwalten siehe unter: <http://windows.microsoft.com/de-de/internet-explorer/delete-manage-cookies>

- **Do Not Track**

- Bei Aktivierung sendet der Internet Explorer an besuchte Websites und an Drittanbieter auf diesen Websites die Info, dass der Benutzer keine Nachverfolgung wünscht.
- Websites können diese Anforderung entweder respektieren oder ungeachtet der Anforderung Aktivitäten ausführen, die als Nachverfolgung gelten.
- **Einstellung** unter „Sicherheit“ im Browsermenü
- Näheres siehe: <http://windows.microsoft.com/de-de/internet-explorer/ie-do-not-track>



## 6. Internet-Browser

### Einstellungen für den Internet Explorer 11



6

#### Datenschutzeinstellungen (Forts.)

- **InPrivate-Browsen**
  - Bei Aktivierung werden Kennwörter, Suchverlauf und Seitenverlauf beim Schließen der Registerkarte gelöscht.
  - Einstellung unter „Sicherheit“ im Browsermenü
  - Näheres siehe: <http://windows.microsoft.com/de-DE/internet-explorer/ie-security-privacy-settings>
- **Positionsfreigabe**
  - hilft Websites mit dem Standort des Benutzers zur Optimierung der Benutzerfreundlichkeit.
  - Aktivieren/Deaktivieren unter: → Internetoptionen → Datenschutz → Standort
- **Popupblocker**
  - beschränkt oder blockiert Popups von Websites.
  - Einstellen der Blockierungsebene:
    - Extras → Popupblocker oder → Internetoptionen → Datenschutz



# 6. Internet-Browser

## Einstellungen für den Internet Explorer 11



6

P

### Sicherheitszonen

- Ziel: Schutz vor potenziell schädlichen Webinhalten
- Internet Explorer ordnet alle Websites automatisch einer Sicherheitszone zu:
  - **Internet**
  - **Lokales Intranet**
  - **Vertrauenswürdige Sites**
  - **Eingeschränkte Sites**
- Sicherheitsstufen definieren, welche Arten von Inhalt für die Website in einer Zone blockiert werden.
- ActiveX-Steuerelemente (kleine Apps für das Bereitstellen von Inhalten auf Websites.) werden bei entsprechender Einstellung nicht automatisch ausgeführt.



# 7. Möglichst sichere Passwörter

## Zeit um Passwörter zu hacken



Stand 2005	Passwortlänge				
Passwortzusammensetzung	5	6	7	8	9
A-Z	2 min.	1 Std.	1 Tag	24 Tage	2 Jahre
A-Z, a-z, 0-9	10 Min.	6 Std.	9 Tage	1 Jahr	32 Jahre
A-Z, a-z, 0-9, - [ ] = \ ; , , . / ` ~ ! @ # \$ % ^ & * ( ) _ + { }   : „ < > ?	4 Std.	11 Tage	2 Jahre	144 Jahre	9857 Jahre

Stand 2009	Passwortlänge							
Passwortzusammensetzung	5	6	7	8	9	10	11	12
A-Z	3,7 ms	0,2 sec.	10 sec.	9 min.	7,6 Std.	16,4 Tage	2,4 Jahre	122 Jahre
A-Z, a-z, 0-9, - [ ] = \ ; , , . / ` ~ ! @ # \$ % ^ & * ( ) _ + { }   : „ < > ?	41ms	3,4 sec.	4,8 min.	6,7 Std.	23,2 Tage	5,4 Jahre	454 Jahre	38.147 Jahre

Quelle: DuD Datenschutz und Datensicherheit 10/2009







## 8. Persönliche Daten im Internet über verschlüsselte Verbindungen

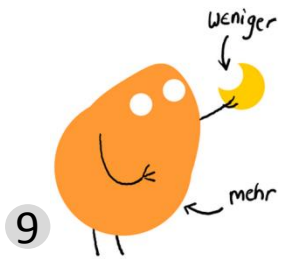


8

### Verschlüsselungstechniken

Unabhängig vom Online-Shop und der gewünschten Zahlungsmethode gilt: Achten Sie immer darauf, dass alle Daten verschlüsselt werden, die Sie an einen Online-Shop übermitteln. Dies erkennen Sie bei an Meldungen wie "Sie haben ein geschütztes Dokument angefordert..." oder "Sie sind im Begriff, sich Seiten über eine sichere Verbindung anzeigen zu lassen...". Außerdem erscheint bei einer verschlüsselten Datenverbindung ein "s", hinter den Buchstaben "http" in der Adresszeile des Browsers. Ein weiterer Hinweis auf die Verschlüsselung: Bei vielen Browsern erscheint im unteren Bereich oder in der Adresszeile ein kleines, geschlossenes Vorhängeschloss.





## 9. Wenige Anwendungen

**Deinstallieren Sie nicht benötigte Programme.** - Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.

### Programm deinstallieren oder ändern

Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.

oder [Secunia Personal Software Inspector \(PSI\)](#)  
o.ä.

Organisieren ▾ Deinstallieren/ändern

Name	Herausgeber	Installiert am	Größe	Version
Lenovo Warranty Information	Lenovo	14.03.2012	861 KB	1.0.0005.00
GPL Ghostscript	Artifex Software Inc.	20.04.2012		9.05
Mobile Broadband Drivers	Ericsson AB	20.04.2012		6.5.1.5
Intel® HD-Grafiktreiber	Intel Corporation	20.04.2012	74,2 MB	8.15.10.2538
7-Zip 9.22 (x64 edition)	Igor Pavlov	20.04.2012	4,75 MB	9.22.00.0
RapidBoot	Lenovo	20.04.2012	949 KB	1.12
Microsoft Visual C++ 2008 Redistributable - KB2467174 - x86 9.0.30729.5570	Microsoft Corporation	20.04.2012	598 KB	9.0.30729.5570
Global Safe Disk 1.93.1	PrimeWorx GmbH	20.04.2012	6,19 MB	1.93.0001
Microsoft Report Viewer Redistributable 2008 SP1	Microsoft Corporation	23.04.2012		
Microsoft Report Viewer Redistributable 2008 SP1 Language Pack - DEU	Microsoft Corporation	23.04.2012		
Microsoft SQL Server Compact 3.5 SP2 DEU	Microsoft Corporation	23.04.2012	3,69 MB	3.5.8080.0
Microsoft SQL Server Compact 3.5 SP2 Query Tools DEU	Microsoft Corporation	23.04.2012	5,42 MB	3.5.8080.0
Microsoft SQL Server 2008 R2-Richtlinien	Microsoft Corporation	23.04.2012	0,99 MB	10.50.1600.1
Microsoft Visual Studio Tools for Applications 2.0 Language Pack - DEU	Microsoft Corporation	23.04.2012	91,1 MB	9.0.35191
Microsoft SQL Server 2008 R2-Setup (Deutsch)	Microsoft Corporation	23.04.2012	38,7 MB	10.51.2500.0
Microsoft SQL Server 2008 R2 Native Client	Microsoft Corporation	23.04.2012	6,82 MB	10.51.2500.0
Microsoft Visual Studio Tools for Applications 2.0 - ENU	Microsoft Corporation	24.04.2012	235 MB	9.0.35191
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation	24.04.2012	788 KB	9.0.30729.6161
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	24.04.2012	298 KB	8.0.61001
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	24.04.2012	600 KB	9.0.30729.6161





## 10. Sicherheitskopien

**Erstellen Sie regelmäßig Sicherheitskopien ("Backups") Ihrer Daten, um vor Verlust geschützt zu sein.**

**Hierzu können Sie beispielsweise eine externe Festplatte nutzen.**

- Möglichkeit 1: Bordmittel von Windows oder Apple
- Möglichkeit 2: Backup mit Open Source SW (z.B. „Areca“)
- Möglichkeit 3: Kostenlose SW: z.B. „Backup & Recovery“ od. „Ocster“), Kostenpflichtige Ergänzungen bieten Vollverschlüsselung o.ä.



# 11. WLAN über Verschlüsselungsstandards

11



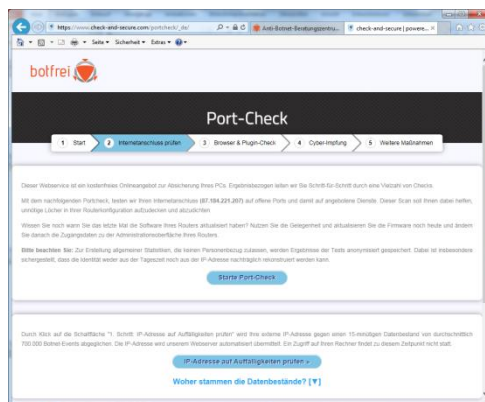
- **Halten Sie sich an die BSI-Empfehlungen für Router!**
  - **Ändern Sie das Passwort!**
  - **Gehen Sie vom Netz, wenn Sie den Router konfigurieren!**
  - **Nutzen Sie https!**
  - **Halten Sie die Firmware aktuell!**
  - **Löschen oder ersetzen Sie den Login-Banner!**
  - **Richten Sie den MAC-Filter ein!**
  - **Deaktivieren sie nicht benötigte Funktionen ihres Routers!**
  - **Deaktivieren Sie den Fernzugang ihres Routers!**
  - **Ändern Sie Einstellungen an der Firewall nur bei entsprechender Kenntnis!**
- **Konfigurieren Sie Ihren Access Point über sichere Wege!**
- **Ändern Sie den Netzwerknamen!**
- **Sorgen Sie für Verschlüsselung! → WPA2 ( ) ein komplexes Passwort mit mindestens 20 Zeichen**
- **Deaktivieren Sie das WPS-PIN Verfahren!**
- **Schalten Sie Ihr WLAN nur bei Gebrauch ein.**





## 12. Regelmäßige Überprüfung des Sicherheitsstatus

- eco - Verband der deutschen Internetwirtschaft e.V.
  - **Anti-Botnet Beratungszentrum „botfrei“**  
unter  
<https://www.botfrei.de>
  - **Port-Check und Auffälligkeitsprüfung der IP-Adresse, Internet-Browser- und Plug-In-Check, Second-Opinion Antiviren-Scanner**  
sowie **Härtung des Systems** (kostenfreie Impfung)  
unter  
<https://www.check-and-secure.com/start/>



System härten: Cyber-Impfung durchführen!

Download Impfstoff





## 12. Überprüfung des Sicherheitsstatus

- Überblick über die allgemeine IT-Sicherheitslage wie z.B. aktuelle oder neuartige Angriffsmethoden sowie Betrugsmaschinen

- Aktuelle IT-Sicherheitslage dargestellt z. B. in der **Schwachstellenampel des BSI** unter

<https://www.cert-bund.de/schwachstellenampel>

- Kostenloses Abonnement der BSI-Meldungen des **Bürger-CERT-Newsletters** unter

<https://www.buerger-cert.de/subscription-new-request>

Produktname	geschlossene Schwachstellen		offene Schwachstellen		BSI Bewertung
	insgesamt	davon kritisch	insgesamt	davon kritisch	
Chrome	137	84	0	0	<span style="color: green;">●●●●●</span>
<b>Gesamtbewertung offener Schwachstellen</b>			0	0	<span style="color: green;">●●●●●</span>

Informationen zum Hersteller Google  
 Die letzten drei Security Bulletins  
<http://googlechromesaves.blogspot.de/2014/03/>  
<http://googlechromesaves.blogspot.de/2014/02/>  
<http://googlechromesaves.blogspot.de/2014/01/>  
 Suchen Sie im WID-Portal zum Hersteller [Google](#)  
[WID Suchseite Chrome](#)

Informationen zu weiteren offenen, kritischen Schwachstellen:  
 • Keine offenen kritischen Schwachstellen vorhanden.

Produktname	geschlossene Schwachstellen		offene Schwachstellen		BSI Bewertung
	insgesamt	davon kritisch	insgesamt	davon kritisch	
Kernel	103	16	1	1	<span style="color: red;">●●●●●</span>
<b>Gesamtbewertung offener Schwachstellen</b>			1	1	<span style="color: red;">●●●●●</span>

Informationen zum Hersteller Linux Kernel  
 Die letzten drei Security Bulletins  
<http://www.kernel.org/pub/linux/kernel/v3.x/>  
 Suchen Sie im WID-Portal zum Hersteller [Linux](#)  
[WID Suchseite Kernel](#)

Informationen zu weiteren offenen, kritischen Schwachstellen:  
 • <http://www.mitre.org/cve/bv/cvname.cve?name=CVE-2014-4271>  
 • <http://www.mitre.org/cve/bv/cvname.cve?name=CVE-2014-7169>

**BÜRGERCERT** Ins Internet – mit Sicherheit

---

Startseite

Über und Fragen und Antworten

Hilfeseite

Glossar

Archiv

**Abonnieren**

Nutzerdaten

Sie sind hier: Startseite > Abonnieren

### Abonnieren

Das Bürger-CERT bietet Ihnen drei unterschiedliche Informationsdienste im Abonnement an, für die Sie sich hier kostenlos registrieren können.

Falls Sie zukünftig keine oder andere Informationen vom Bürger-CERT erhalten möchten, können Sie unter dem Menüpunkt "Nutzerdaten" die entsprechenden Funktionen "Abonnement ändern" und "Abonnement kündigen" finden. Sollten dabei Probleme auftreten, schicken Sie uns bitte eine E-Mail an [offentlich@cert-bund.de](mailto:offentlich@cert-bund.de).

**Technische Warnungen**

Sie kennen sich mit Computern aus und wollen mehr Informationen? Mit den Technischen Warnungen werden Sie einmal pro Woche über Sicherheitslücken und andere Bedrohungen informiert. Zusätzlich benachrichtigen wir Sie per E-Mail sofort, wenn kritische Gefahren auftauchen.

**Ich möchte diesen Dienst abonnieren**

**Newsletter "Sicher + Informiert"**

Der aktuell-informative Bürger-CERT Newsletter "Sicher + Informiert" berichtet alle zwei Wochen über Wissenswertes und Tipps zur Computersicherheit. Hiermit versorgen Sie keine wichtige Information, werden regelmäßig auf dem Laufenden gehalten und sind stets "Sicher + Informiert".

**Ich möchte diesen Dienst abonnieren**

**Extrausgabe "Sicher + Informiert"**

Was tun wenn's brennt? Mit der Extrausgabe des Newsletters "Sicher + Informiert" werden Sie über kritische Gefahren für Ihren Computer sofort per E-Mail informiert. In leicht verständlicher Form erfahren Sie hier umgehend, wie Sie sich und Ihre Daten bei akuten Gefahren schützen können.

**Ich möchte diesen Dienst abonnieren**

**Jetzt abonnieren – weitere Informationen unter [Fragen und Antworten](#)**

E-Mail eingeben \*

Bürger-CERT-Wort \*

Signatur-Optionen

Für die Signatur-Optionen "PGP" und "S/MIME" benötigen Sie ein Zusatzprogramm (Plug-In) für Ihr Mailprogramm. Die erforderlichen Schlüssel finden Sie in unserem [Impressum](#).

Die mit einem \* gekennzeichneten Felder sind Pflichtfelder.



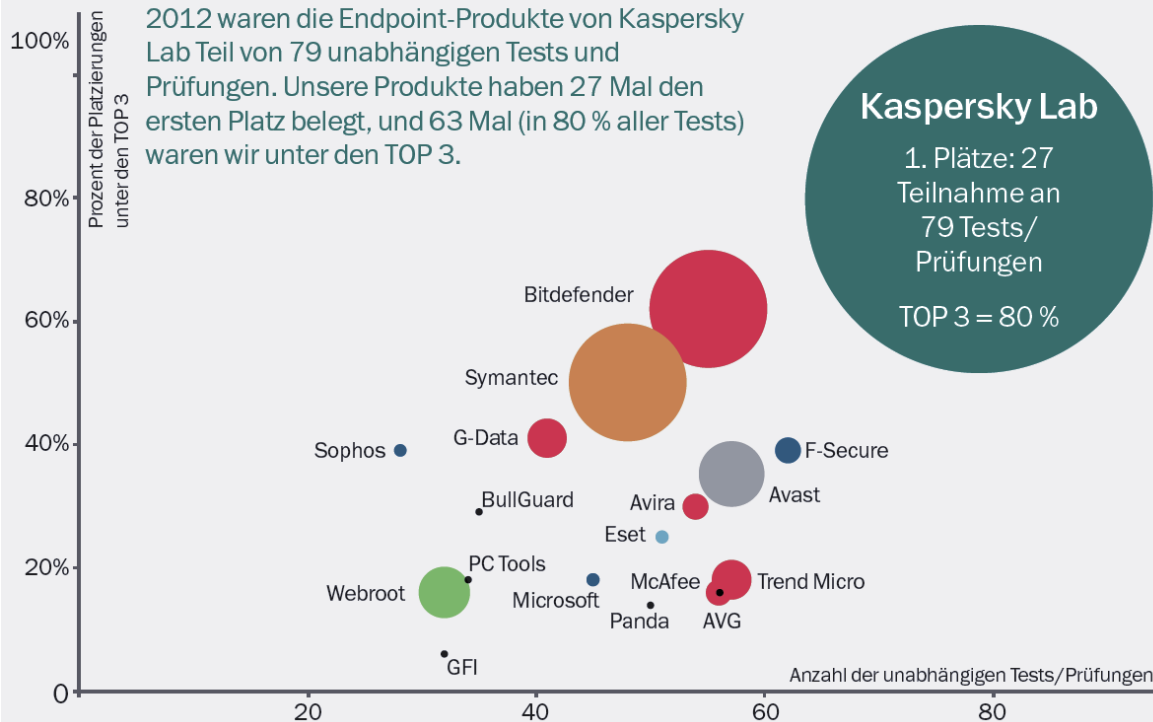




## 12. Überprüfung des Sicherheitsstatus Produkte zum Schutz vor Malware

### Werbung von Kaspersky

#### KASPERSKY LAB BIETET BRANCHENWEIT BESTEN SCHUTZ\*:



\*

Anmerkungen:

- Gemäß Zusammenfassung der Ergebnisse eines unabhängigen Tests aus dem Jahr 2012 für Unternehmens-, Verbraucher- und mobile Produkte.
- Die Zusammenfassung umfasst Tests, die von den folgenden unabhängigen Testlaboren und Magazinen durchgeführt wurden:
  - Testlabore: AV-Test, AV-Comparatives, VB100, PC Security Labs, Matousec, Anti-Malware.ru, Dennis Technology Labs
  - Magazine: CHIP Online, PC Advisor, PC Magazine, TopTenREVIEWS, CNET, PCWorld, ComputerBild, PC-Welt
- Die Größe der Kreise entspricht der Anzahl der ersten Plätze.







# Wie mache ich meinen PC sicher?

## Ausführliche Infos:



Bundesamt  
für Sicherheit in der  
Informationstechnik

[https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/meinPC\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/meinPC_node.html)

The screenshot shows the website interface for 'Wie mache ich meinen PC sicher?'. The main navigation bar includes links for 'Service', 'Gebärdensprache', 'Leichte Sprache', 'Datenschutz', and 'Kontakt & Impressum'. Below the navigation, there are four main categories: 'Wie mache ich meinen PC sicher?', 'Welche Gefahren begegnen mir im Netz?', 'Wie bewege ich mich sicher im Netz?', and 'Wie bewege ich mich sicher im mobilen Netz?'. The 'Wie mache ich meinen PC sicher?' category is selected, showing a list of sub-topics: 'Basisschutz für den Computer', 'Passwörter', 'Benutzerkonten / Netzwerk', 'Schutz- und Hilfsprogramme', 'Update- und Patchmanagement', 'Datenverschlüsselung', 'Datensicherung', 'Daten richtig löschen', 'Infektionsbeseitigung', and 'Open Source Software'. A 'Weitere Themen' section lists: 'Basisschutz für den Computer', 'Passwörter', 'Benutzerkonten / Netzwerk', 'Schutz- und Hilfsprogramme', 'Update- und Patchmanagement', 'Datenverschlüsselung', 'Datensicherung', 'Daten richtig löschen', 'Infektionsbeseitigung', and 'Open Source Software'. The 'Themenübersicht' section provides an overview of the most important tips for protecting the PC and safe surfing habits.



## Nächster Vortrag in dieser Vortragsreihe

**Mittwoch, 19. November 2014, 18:30 Uhr**

**Pierre Lukas und Swer Rieger (Consist Software Solutions GmbH)**

**Big Data– Ich sehe was, was du nicht siehst...**

*Hörsaal 7, Großes Hörsaalgebäude, Sokratesplatz 6*

Mit frei verfügbarer Technologie kann mittlerweile jedermann Big Brother oder NSA spielen. Spannend ist es jedoch zu verstehen, wie Unternehmen hieraus Mehrwerte und besseres Services erzielen können. Außerdem wollen wir einmal einen Blick in den Grenzbereich zwischen technisch Möglichem und moralisch/rechtlich Zulässigem werfen. Angereichert wird dies durch tatsächliche Anwendungsbeispiele und einer Live Demo.



# Veranstaltungshinweis zum Thema IT-Security

**Mittwoch 29. Oktober 2014**

**DiWiSH-Fachgruppe IT-Security**

Ort: IHK zu Kiel - Haus der Wirtschaft - Raum Ostsee - Bergstraße 2 24103 Kiel

**14:30 Uhr Live Hacking – so brechen Hacker in IT-Netze ein**  
**Sebastian Schreiber, SySS GmbH**

**16:15 Uhr Überwachung durch die NSA – Hat die moderne Kryptographie etwas entgegenzusetzen?** Prof. Dr. Thomas Wilke, CAU zu Kiel

**17:30 Uhr Die Antwort Europas auf die US-amerikanische Missachtung des Datenschutzes** Dr. Thilo Weichert, ULD Schleswig-Holstein

