



Sicherer als sicher

Sicherheit in IT und Internet – Handlungsmöglichkeiten

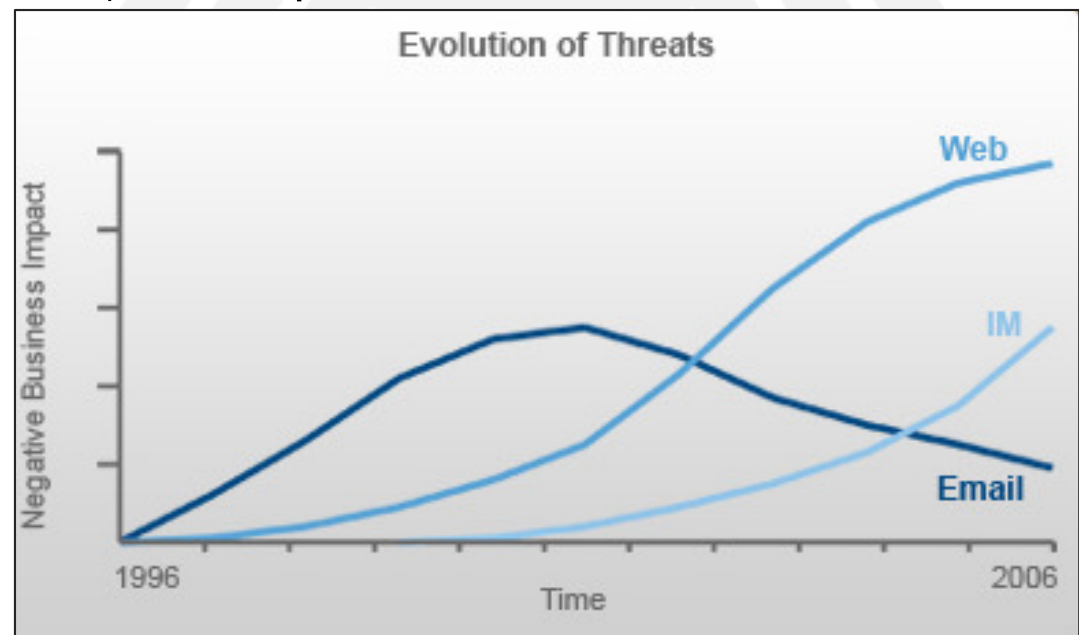
Horst Flätgen
Bundesamt für Sicherheit in der
Informationstechnik (BSI), Bonn

Berlin, 29. Oktober 2009



Angriffstechniken werden immer intelligenter

- ➔ Angriffe über Schwachstellen im Internet-Browser und seinen Hilfsprogrammen („Drive-by-Downloads“)
- ➔ Schadprogramme klinken sich in die Kommunikation ein („Man-in-the-Middle-Attacken“)
- ➔ Computer werden unbemerkt „gekapert“ und zu Botnetzen zusammengeschaltet. Mit diesen werden Server lahm gelegt (DDoS) oder Spam-Mails versandt.



Schadprogramm-Angriffe

- ➔ „Conficker“-Wurm befällt Windows-Systeme und gefährdet Sicherheitsmechanismen
- ➔ Angebliche Antiviren-Programme (Scare ware) sind auf dem Vormarsch: Sie bieten nicht nur keinen Schutz, sondern laden oft auch Schadsoftware nach
- ➔ Mobile Geräte werden immer häufiger angegriffen.

Computer: Conficker -Wurm befällt Bundeswehr-Rechner

Der seit Wochen weltweit grassierende Computer-Wurm namens Conficker hat auch mehrere hundert Bundeswehr-Rechner befallen.

Einzelne betroffene Dienststellen wurden vom Bundeswehr-Netzwerk getrennt, um eine weitere Ausbreitung der Schadsoftware zu verhindern, sagte ein Sprecher des Bundesverteidigungsministeriums am Samstag in Berlin. Derzeit gebe es aber keine weiteren Einschränkungen. Spezialisten eines Computer-Notfall-Teams der Bundeswehr und des Unternehmens BWI Informationstechnik GmbH hätten Maßnahmen zur Entfernung der Schadsoftware und Wiederherstellung der vollen Funktionsfähigkeit der Computersysteme der Bundeswehr eingeleitet.



Angriffspunkt für Hacker: Rechenzentrum eines Internet-Dienstleisters (Archivfoto vom 19.4.2006). dpa



MILLIONEN PCS INFIZIERT

Abzocke mit gefälschtem Virenschutz

von Alfred Krüger

Virens Scanner sind wichtig. Das wissen auch cyberkriminelle Internetbetrüger. Immer öfter bieten sie im Netz gefälschte Schutzprogramme an - auch auf seriösen Seiten. Die Verbreitung solcher Software habe epidemische Ausmaße erreicht, sagen Experten. [\[mehr\]](#)



Malwarenetzwerk „Ghostnet“


- ➔ Ghostnet wird Ende März 2009 bekannt
- ➔ Weltweit Rechner mit hohem Informationswert infiziert
 - Außenministerien
 - Botschaften
 - Internationale Organisationen
 - Nachrichtenorganisationen
- ➔ Infektion der Rechner über manipulierte Office-Dokumente (PDF, Word, Powerpoint, Excel)
- ➔ Anwendung besonders ausgefeilter Methoden des Social Engineering

"Ghostnet" spioniert weltweit Regierungscomputer aus | tagesschau.de

tagesschau.de®

09.04.2009 [tagesschau.de ▶ Ausland ▶ Computerspionage]

Ausland



Rund 1300 Rechner weltweit infiziert
"Ghostnet" spioniert Computer aus

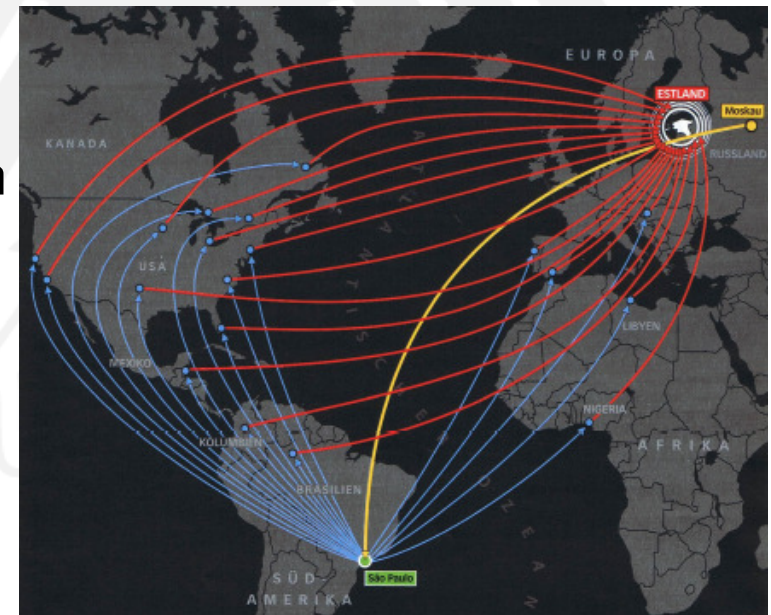
Kanadische Forscher haben ein riesiges Spionagenetzwerk entdeckt, das offenbar in Computer in aller Welt eingedrungen ist. Das Munk Centre for International Studies in Toronto geht davon aus, dass mindestens 1295 Rechner in 103 Staaten infiltriert worden sind.

Bis zu 30 Prozent der Computer seien "hochrangige Ziele" wie die Rechner von Außenministerien, Botschaften, internationalen Institutionen und Medien, heißt es in einem Bericht des Zentrums. Auch Computer der NATO und des Dalai Lama seien ausspioniert worden.



Botnetz-Angriffe

- ➔ 2007: DDoS-Angriff auf die Bundesverwaltung durch 350 Bots, die die 1000-fache Last erzeugten und den externen Internet-Zugang von zehn Bundesbehörden gestört haben.
- ➔ 2007: DDoS-Attacke auf Webseiten in Estland
- ➔ 2008: Cyberwar in Georgien im Zusammenhang mit dem Krieg in Südossetien: DDoS-Attacken legen Regierungs-Server in Georgien lahm
- ➔ 2009: Botnetz mit 1,9 Millionen Computern wird entdeckt. Angriffe auf Regierungsnetze der USA und U.K.





Elektronische Identitäten

- ➔ 2009: Die Zugangsdaten von 10.000 Kunden des E-Mail-Dienstes MS Hotmail tauchen im Internet auf. Die Passwörter wurden mit Phishing-Angriffen gesammelt.
- ➔ Das Beispiel zeigt, dass die Nutzer noch mehr sensibilisiert werden müssen. Microsoft sperrt die betroffenen Konten.
- ➔ Nach Microsoft bestätigten auch Yahoo und Google, dass Hacker E-Mail-Konten geknackt haben.

The screenshot shows a news article from FOCUS DIGITAL dated 06.10.2009. The article title is "Angriff auf Hotmail-Konten: Die Tricks der Phishing-Betrüger". The sub-headline reads: "Die Daten von 10 000 Kunden des Microsoft-E-Mail-Dienstes Hotmail sind im Internet aufgetaucht. Doch wie sind die Betrüger darangekommen?". The author is identified as Claudia Frickel. The article text states that thousands of Hotmail users in Europe cannot access their email accounts because their login data and passwords were leaked. Microsoft has locked the affected accounts and requires users to complete a security form. The article also mentions that users can check the date and time of their last successful login to see if they are affected.

The second screenshot shows a Windows Live Hotmail interface. The account name is "Hotmail" and the email address is "nordreport@live.de". The inbox shows 3 messages, with the top one being "Posteingang (3)". There are also links for "Junk-E-Mail", "Entwürfe", and "Gesendet".

Lagebericht IT-Sicherheit

Bedrohungen steigen an: quantitativ und qualitativ

- ➔ Professionalisierung der Internetkriminalität schreitet weiter voran
- ➔ Wirtschaftskriminalität zur Erlangung von Wettbewerbsvorteilen nimmt zu
- ➔ Schadprogramme verursachen Schäden in Milliardenhöhe



https://www.bsi.bund.de/cln_164/DE/Publikationen/Lageberichte/lageberichte_node.html

IT-Sicherheit durch gemeinsame Vernetzung und Verantwortung

IT-Sicherheit

- ➔ als Verantwortung des Staates
- ➔ als Verantwortung der IT-Wirtschaft
- ➔ als Verantwortung der Forschung
- ➔ als Verantwortung der Bürger



Das BSI bietet Unterstützung und ist kompetenter Ansprechpartner

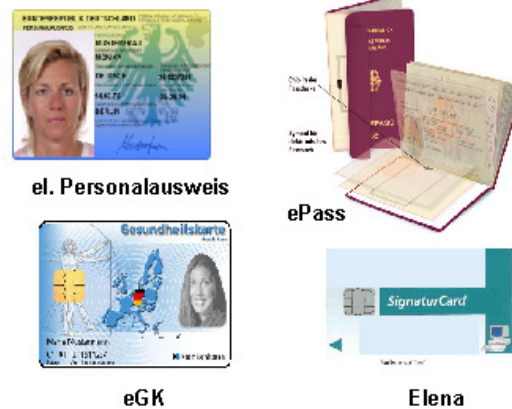
informationssichernde Systeme



sichere Infrastrukturen



Hoheitliche Dokumente



militärische Kommunikationssysteme Waffensysteme



IT-Sicherheit muss praktikabel sein!

Unterstützung für Privatanwender:

- ➔ BSI für Bürger
- ➔ Bürger CERT
- ➔ Deutschland sicher im Netz
- ➔ Weitere Bürgerportale...



Startseite | DsiN

Deutschland sicher im Netz e.V.
Gemeinsam für mehr IT-Sicherheit

Kinder & Jugendliche | Privatanwender | Unternehmen | Trainer & Berater | Wir über uns | Infos & Downloads

MesseCampus auf der it-a

DsiN brachte auf dem MesseCampus am 15.10.2009 Studierende, Professoren und Vertreter der IT-Wirtschaft zusammen. Kurze Vortragsveranstaltungen und ein anschließender Besuch bei ausgewählten Ausstellern zum Thema IT-Sicherheit standen auf dem Programm.
[weitere Informationen](#)

neue Filmkampagne

Unsere Filme **Sicheres Passwort, Datensparsamkeit und Sicherer Online-Einkauf** sowie weitere Informationen finden Sie neu auf unserer Website.
Zur Kampagne [with english subtitles](#)

Schirmherrschaft:
Bundesministerium des Innern

Aktuelle Meldungen

Innovative Software für mehr Sicherheit bei der Internetkommunikation
02.10.2009
Für DsiN stellt die Deutsche Telekom das neue Computerprogramm Sicherheitsprofil @home zur Verfügung. Mit



BSI für Bürger

Suchbegriff eingeben

IT-Sicherheit

- Das Internet
- Der Browser
- Datensicherung
- Viren & andere Tiere
- Abzocker & Spione
- Infiziert - und nun?
- Schützen - aber wie?

Themen

- Kinderschutz
- Computerspiele
- Chat - aber sicher?
- Der Staat online
- Online-Banking
- Einkaufen im Internet
- WLAN
- Phishing
- Benutzerkonten / Netzwerk

Startseite

Ins Internet - mit Sicherheit

Im Internet surfen ist wie Autofahren - reinsetzen und starten. Doch halt: Auch auf der Datenautobahn besteht Unfallgefahr! Um einen Zusammenstoß mit Würmern, Viren oder anderen Störenfriedern zu vermeiden, sollten Sie Ihren Computer schützen. Wie, das erfahren Sie auf dieser Internetseite.

Mobile Banking

Bankgeschäfte auch von unterwegs erledigen, ohne jederzeit den Laptop im Gepäck haben zu müssen - Mobile Banking macht's möglich. Mit diesem Dienst können Nutzer über Mobiltelefone, PDA und Smartphones (bekannteste Beispiele sind das iPhone und der BlackBerry) ihren Kontostand abfragen, Überweisungen ausführen, Daueraufträge einrichten und vieles mehr. Doch aufgepasst! Alle Gefahren, die Sie vom Online-Banking mit dem Computer kennen, bestehen auch beim Mobile Banking. Hinzu kommen die Sicherheitsrisiken mobiler Endgeräte. Mit welchen Schutzmaßnahmen Sie sich vor den Gefahren

Schnelleinstieg

Die 10 wichtigsten Tipps

Warn- und Informationsdienst

BÜRGERCERT
Ins Internet - mit Sicherheit

Bundesamt für Sicherheit in der Informationstechnik



Bürger-CERT - Ins Internet - mit Sicherheit

Links | Presse | Impressum | Kon

BÜRGERCERT

Ins Internet - mit Sicherheit

Startseite

Über uns

Fragen und Antworten

Hilftexte

Glossar

Archiv

Abonnieren

Nutzerdaten

Sie sind hier: Startseite

Das Bürger-CERT informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen - kostenfrei und absolut neutral. Unsere Experten analysieren für Sie rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf Warnmeldungen und Sicherheitshinweise per E-Mail. Das Bürger-CERT ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik. Wenn auch Sie auf Nummer Sicher gehen wollen, abonnieren Sie unsere Dienste.

Ein Projekt von

Bundesamt für Sicherheit in der Informationstechnik

Aktuelle Sicherheitsinformation

14.10.2009: Microsoft Patchday Oktober 2009:
Im Oktober 2009 schließt Microsoft mithilfe von 13 Sicherheitsupdates insgesamt 34 Sicherheitslücken. Das Bürger-CERT empfiehlt, die zugehörigen Sicherheitsupdates möglichst zeitnah zu installieren.

Im Bürger-CERT suchen

Technische Warnungen

Newsletter "Sicher • Informiert"

Extraausgabe "Sicher • Informiert"



IT-Sicherheit muss praktikabel sein

Unterstützung für Behörden:

- ➔ Umsetzungsplan Bund

Unterstützung für die Wirtschaft:

- ➔ IT-Grundschutz
- ➔ Zertifizierung
- ➔ Empfehlungen



IT-Sicherheitsmaßnahmen müssen auch für normale Nutzer praktikabel sein – sonst werden sie aus Bequemlichkeit einfach umgangen





Vertrauen schaffen

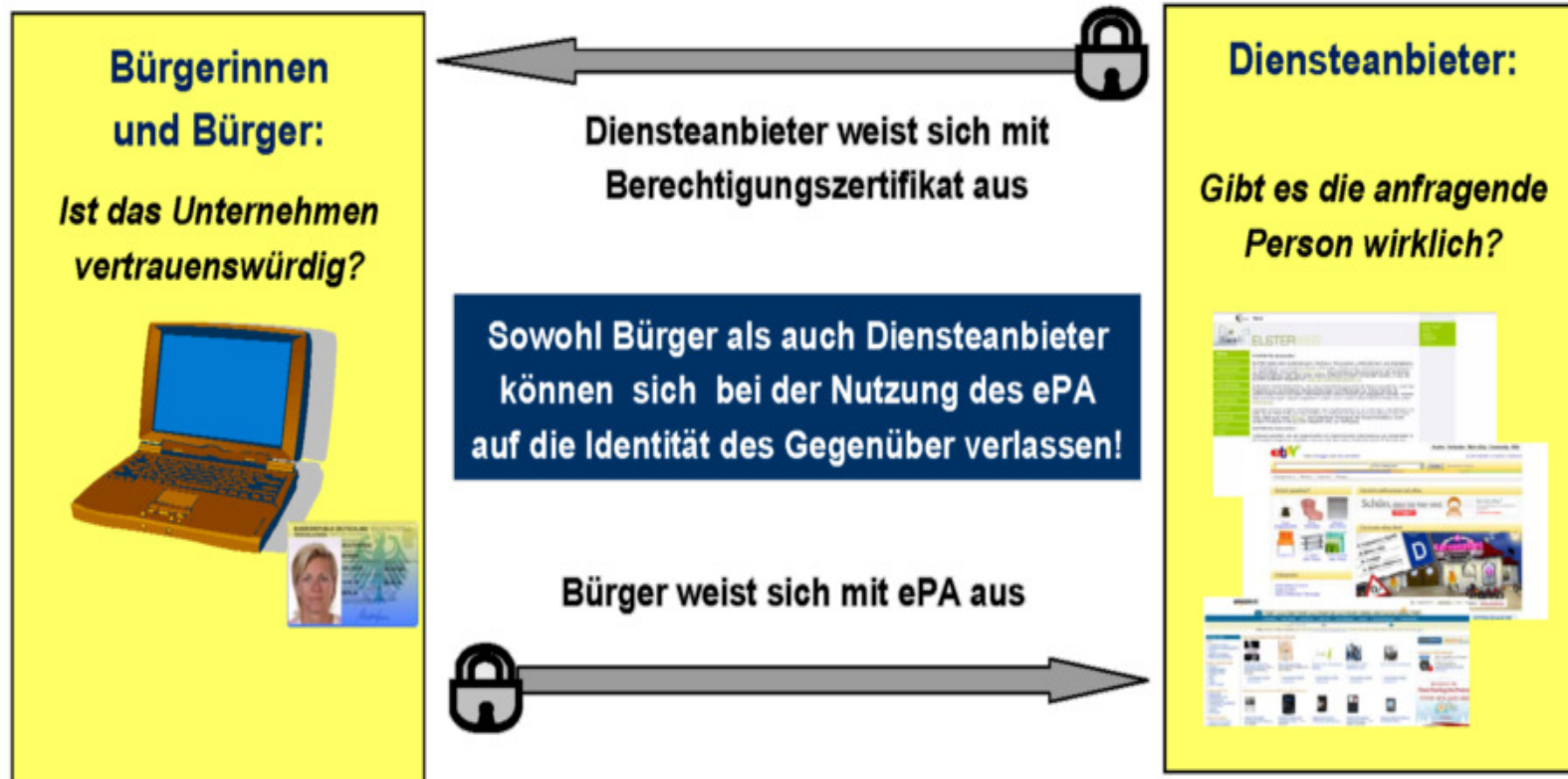
Geschäftsprozesse und Verwaltungsakte im Internet setzen IT-Sicherheit voraus: Nur dann haben Anbieter und Kunden das nötige Vertrauen.

Wege dahin: Sichere Online-Identifizierung und verbindliche elektronische Unterschrift

Beispiele:

- ➔ elektronischer Personalausweis
- ➔ DE-Mail

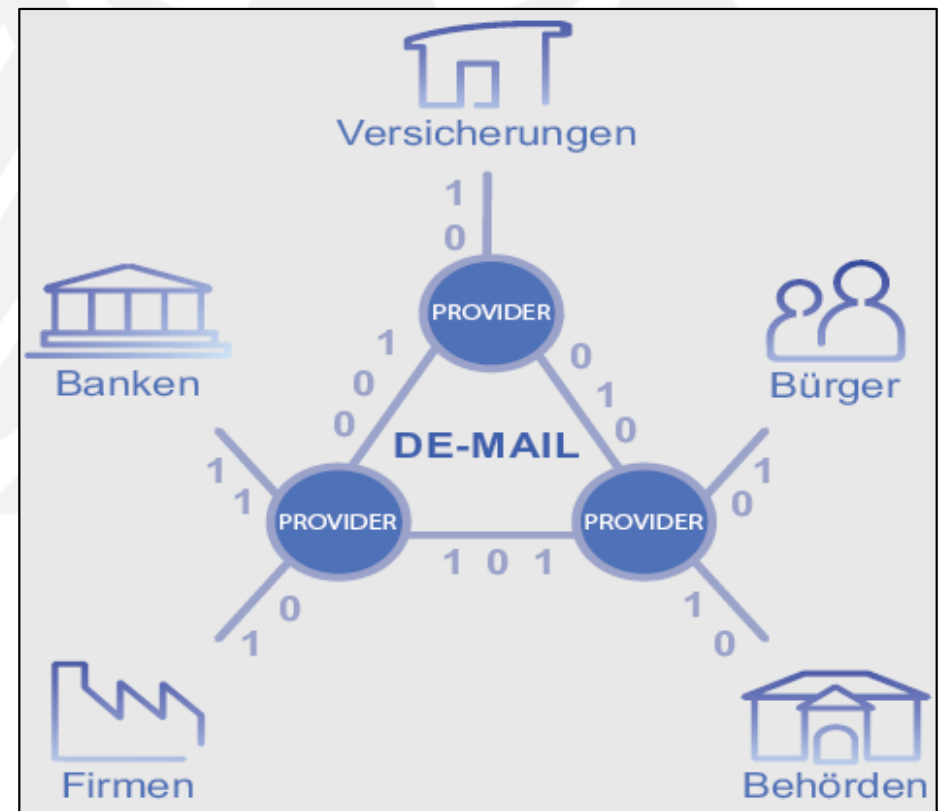
Gegenseitiger Identitätsnachweis erhöht die Sicherheit





DE-Mail

- ➔ sicherer Austausch rechtsgültiger elektronischer Dokumente über das Internet („elektronisches Einschreiben“).
- ➔ vom Bund gemeinsam mit privaten Partnern entwickelt
- ➔ BSI akkreditiert die Anbieter
- ➔ Pilotprojekt in Friedrichshafen (16. Okt. 2009)





Kontakt

Horst Flätgen

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

horst.flaetgen@bsi.bund.de
www.bsi.bund.de