Bundesamt
für Sicherheit in der
Informationstechnik

Sicherer als sicher

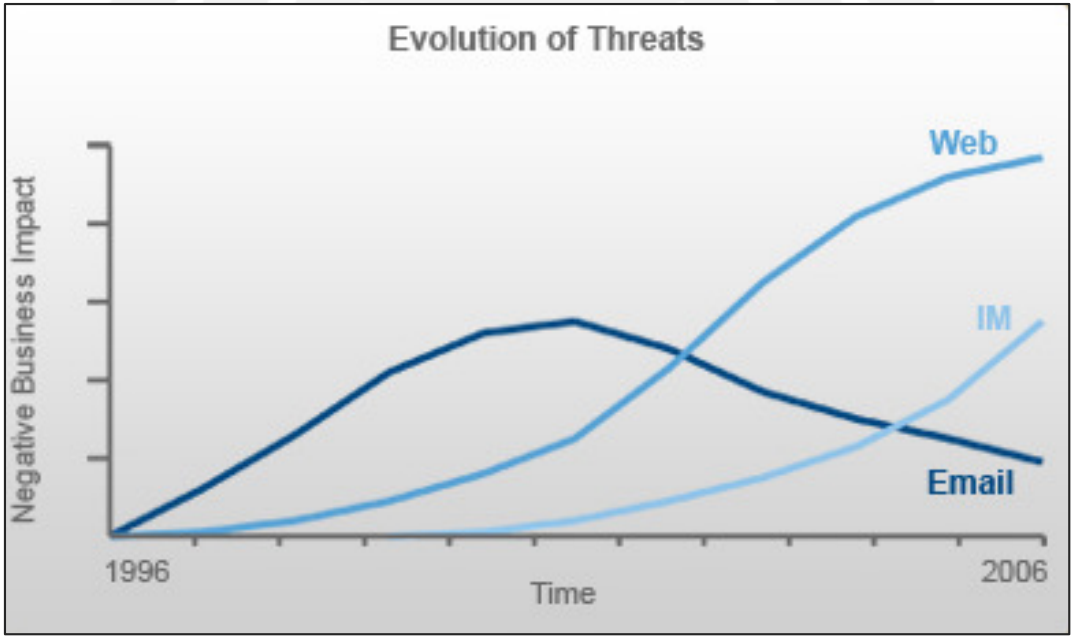
Sicherheit in IT und Internet – Handlungsmöglichkeiten

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.

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

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 .

ONLINE FOCUS

MILLIONEN PCS INFIZIERT

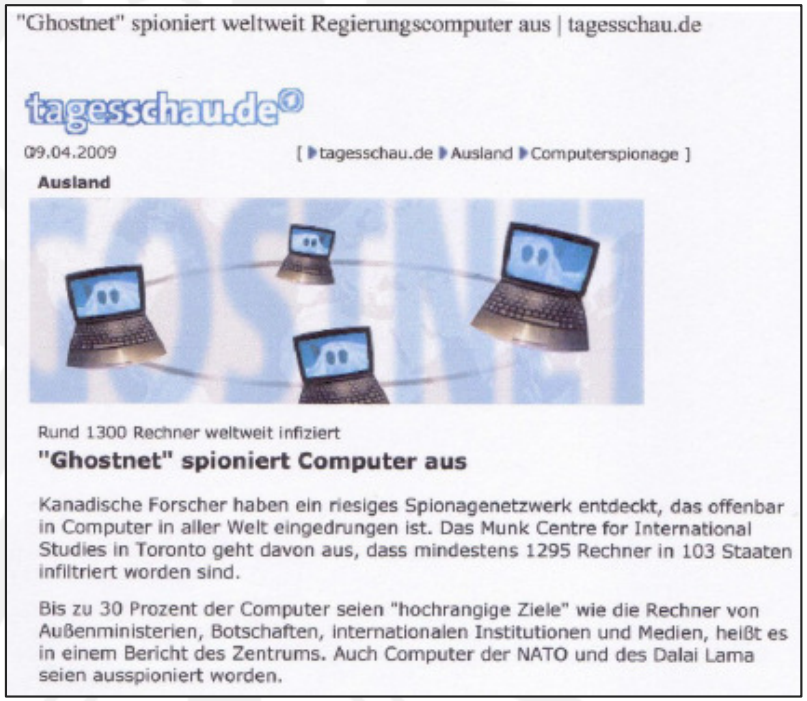
Abzocke mit gefälschtem Virenschutz

von Alfred Krüger

Virenscanner 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

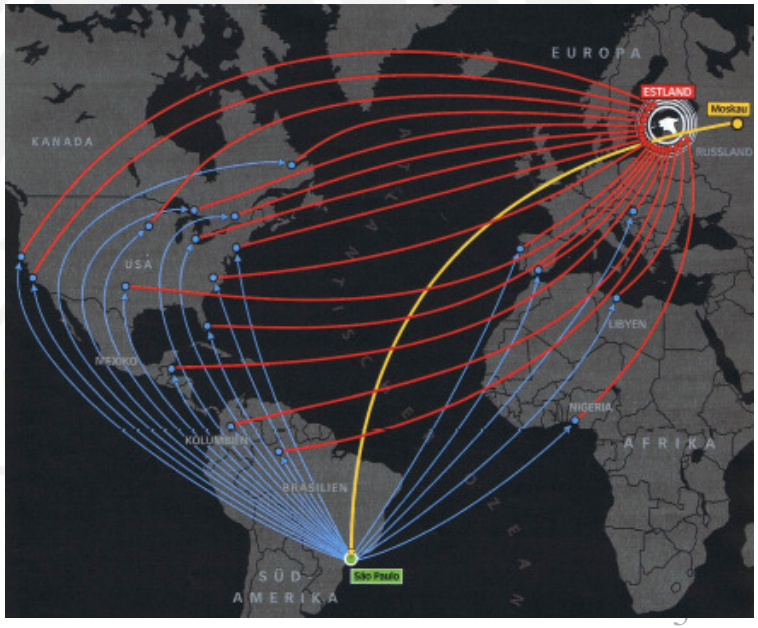
"Ghostnet" spioniert Computer aus

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.

ONLINE FOCUS DIGITAL

« Home

POLITIK | FINANZEN | WISSEN | GESUNDHEIT | KULTUR | PANORAMA | SPOR

Comput

06.10.2009, 14:10 | ★★★★☆ | 1 Kommentar Artikel merken

Angriff auf Hotmail-Konten: Die Tricks der Phishing-Betrüger

Die Daten von 10 000 Kunden des Microsoft-E-Mail-Dienstes Hotmail sind im Internet aufgetaucht. Doch wie sind die Betrüger darangekommen?

Von FOCUS-Online-Autorin Claudia Frickel

Windows Live™
Hotmail
Neu | Löschen
nordreport@live.de
Posteingang (3)
Junk-E-Mail
Entwürfe
Sortieren nach
dpa

Tausende Hotmail-Kunden in ganz Europa können derzeit nicht auf ihre E-Mail-Postfächer zugreifen: Nachdem ihre Zugangsdaten mitsamt Passwörtern im Internet aufgetaucht sind, sperrte Microsoft die betroffenen Konten. Um wieder Zugriff zu bekommen, müssen die Kunden ein Sicherheitsformular auf einer Microsoft-Seite ausfüllen. Abgefragt werden unter anderem Datum und Uhrzeit der letzten erfolgreichen Anmeldung bei Hotmail und persönliche Daten. Wer unsicher ist, ob sein Konto betroffen sein könnte, kann die Seite ebenfalls zur Überprüfung nutzen.

Lagebericht IT-Sicherheit

Bedrohungen steigen an: quantitativ und qualitativ

- Professionalisierung der Internet-kriminalität 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

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheit muss praktikabel sein!

Unterstützung für Privatanwender:

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

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

Elektronischer Personalausweis

- stärkere Bindung von Dokument und Inhaber durch Biometrie auch beim Personalausweis
- elektronischer Personalausweis
- neue Technologien erfordern eine sichere elektronische Identifizierung, z.B. für Online-Geschäfte, Finanztransaktionen oder E-Government-Anwendungen

Gegenseitiger Identitätsnachweis erhöht die Sicherheit

Bürgerinnen und Bürger:

Ist das Unternehmen vertrauenswürdig?

Diensteanbieter weist sich mit Berechtigungszertifikat aus

Sowohl Bürger als auch Diensteanbieter können sich bei der Nutzung des ePA auf die Identität des Gegenüber verlassen!

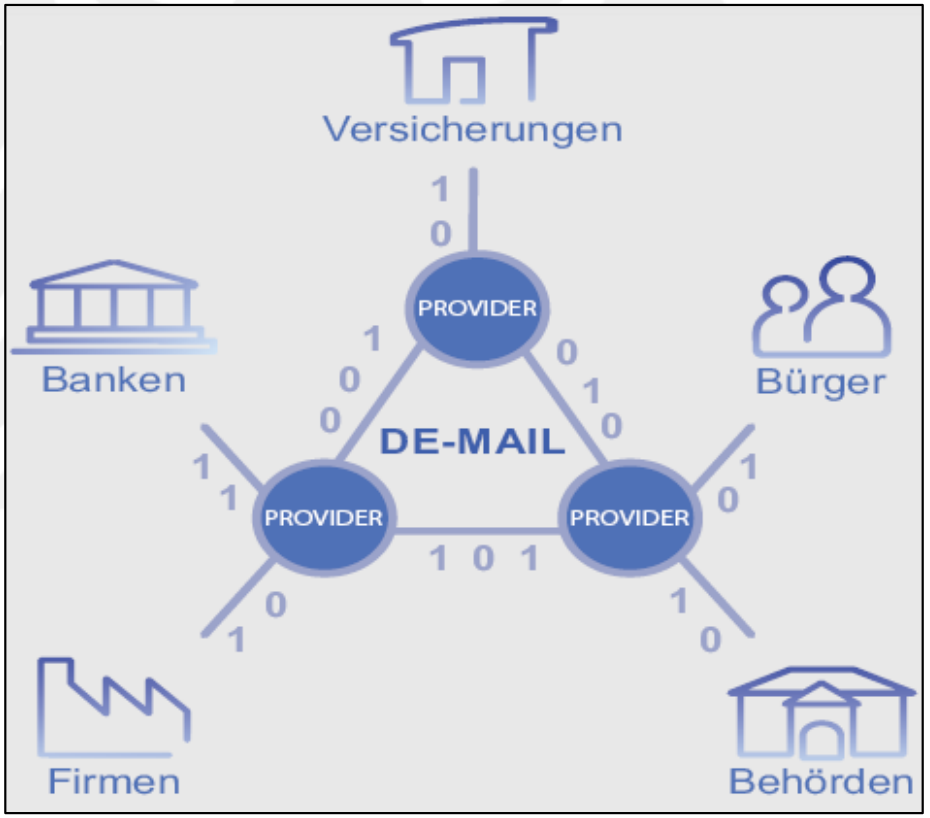
Bürger weist sich mit ePA aus

Diensteanbieter:

Gibt es die anfragende Person wirklich?

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