

GO OUT

T-SECURITY

IT-Sicherheit

Andreas Wisler
Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, IT-SIBE BSI, MCITP

GO OUT

T-SECURITY

Agenda

- Aktuelle Situation
- Phishing, Identitätsdiebstahl
- Internet – Schwachstellen
 - ScareWare, SQL-Injection, XSS
- Demo

GO OUT

T-SECURITY

Aktuelle Situation

- BSI Lagebericht – 4. Quartal 2010
 - Hacker nutzen RTF-Dateien für Angriffe

The diagram illustrates the process of using RTF files for attacks. It shows a flow from a user (Hacker) to a document (RTF file) which is then used to attack a system (Web browser). The diagram includes labels for 'RTF-Anwendung', 'Web browser', and 'Web-Tour-Portal (BSP)'. The flow is: Hacker (RTF-Anwendung) -> RTF-Datei -> Web browser -> Web-Tour-Portal (BSP). There are also labels for 'Web browser (Schwachstelle)' and 'Web browser (Schwachstelle)'.

Aktuelle Situation

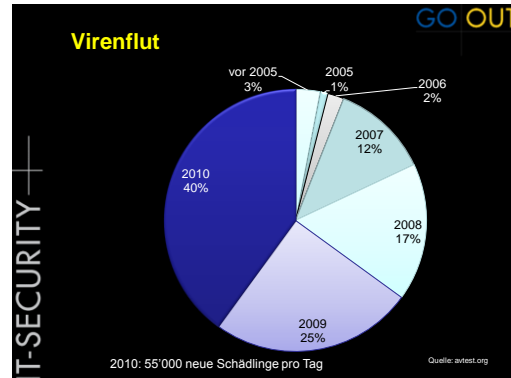
- BSI Lagebericht – 4. Quartal 2010
- Carberp: Online Banking Troj. Pferd

Aktuelle Situation

- BSI Lagebericht – 4. Quartal 2010
- Zugangsdaten

In einer Stichprobe des BSI im Dezember 2010 wurden 373.973 infizierte Systeme entdeckt, die länderübergreifend verteilt waren. Davon lieferten 86.507 Computer Zugangsdaten von Webseiten mit der Top Level-Domain DE.

| Domain | Anzahl |
|------------------------|--------|
| login.web.de | 16.020 |
| login.ebay.de | 13.932 |
| www.amazon.de | 13.269 |
| mailrecht.web.de | 12.944 |
| cgi.ebay.de | 11.781 |
| mailrecht.gmx.de | 9.849 |
| secure.web-kant-wen.de | 7.771 |
| mp.ebay.de | 6.671 |
| www.web-kant-wen.de | 5.614 |
| image.google.de | 5.339 |
| offer.ebay.de | 5.254 |
| fm.rtl.de | 4.913 |
| gallery.athrebay.de | 4.873 |
| www.kapflingfilm.de | 4.849 |
| www.zippy.de | 4.611 |
| reisenscout.bahn.de | 4.560 |
| cgi.ebay.de | 4.248 |
| www.rhlp.de | 3.988 |
| contact.ebay.de | 3.849 |
| payment.ebay.de | 3.655 |
| www.autoscout24.de | 3.469 |
| de.gemoo.de | 3.390 |
| www.myvideo.de | 3.123 |
| www.sweetz.de | 3.028 |
| banking.postbank.de | 3.013 |



GO OUT

Aktuelle Situation

T-SECURITY

- 15.06.11
Paypal.com enthält XSS-Schwachstelle
- 09.06.11
Citigroup verliert bei Angriff Daten von 210.000 Kunden (URL Manipulation)
- 03.06.11
Skype-Protokoll als Open Source veröffentlicht
- 30.05.11
Hacker brechen in Server von US-Rüstungskonzernen ein
- 26.05.11
Noch ein Einbruch bei einem Comodo-Partner (SSL-Problematik!!)
- 23.05.11
Gefährliche Sicherheitslücke in Business-Netzwerk LinkedIn entdeckt

Weitere News: www.go-security.ch/news

GO OUT

Aktuelle Situation

T-SECURITY

- Pharma Hack, 10. Juni 2011
In der Schweiz sind anscheinend hunderte Seiten mit dem so genannten Pharma-Hack verseucht worden. Der Pharma-Hack scheint sich vor allem auf Wordpress und Typo3 spezialisiert zu haben. Vermutlich wird er durch unsichere Plugins ins System eingeschleust. Es befinden sich grosse Anbieter wie die Livit oder das Institut für Informatik der Universität Zürich darunter. Auch Seiten der Uni Basel wurden gehackt, ebenso wie die Seite des FC Thun oder dem Schweizer Volleyballverband. Daneben hunderte von weiteren Schweizer Domains, wie Gemeinden, Verbänden, Blogs und Kleinbetrieben.

GO OUT

iPhone Passwörter

Auswertung aus 200'000 Passwörtern (15.06.11)

| Code | Frequency |
|------|-----------|
| 1234 | 8,884 |
| 0000 | 5,246 |
| 2580 | 4,753 |
| 1111 | 3,282 |
| 5555 | 1,774 |
| 5683 | 1,425 |
| 0852 | 1,221 |
| 2222 | 1,139 |
| 1212 | 944 |
| 1998 | 822 |

T-SECURITY

GO OUT

**Einschub:
Soziale Netzwerke ermöglichen ...**

- sich zu präsentieren
- mit Freunden in Kontakt zu bleiben
- Daten auszutauschen (Bilder, Filme, ...)
- schnell neue Kontakte zu knüpfen
- Ideen auszutauschen und zu diskutieren

Mehr als 2,2 Millionen Facebook-Benutzer in der Schweiz, was einem Anteil von knapp 30 % entspricht.

T-SECURITY

GO OUT

Beispiele sozialer Netzwerke

T-SECURITY

GO OUT

Facebook-Statistik


- Mehr als 500 Millionen aktive Benutzer weltweit
- 50 % der Benutzer melden sich mindestens einmal täglich an
- Ein Benutzer hat durchschnittlich 130 Freunde
- Die Weltbevölkerung verbringt pro Monat über 700 Milliarden Minuten auf Facebook
- Pro Monat werden über 30 Milliarden Inhalte (Links, News, Fotos, ...) hochgeladen

T-SECURITY

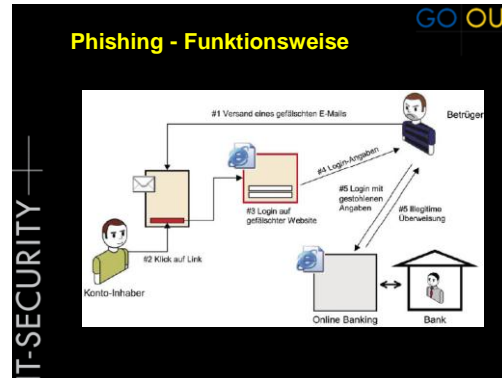
GO OUT

Phishing

- Phishing ist die Bezeichnung für einen interaktiven Informationsdiebstahl (password harvesting fishing, das Passwort fischen)
- Nutzt meist eine geschickte Tarnung
 - E-Mail mit einem "plausiblen" Inhalt
 - Eingebettete Skripte auf Webseiten oder in E-Mails (html)
 - Komplett nachgemachte Seiten



T-SECURITY



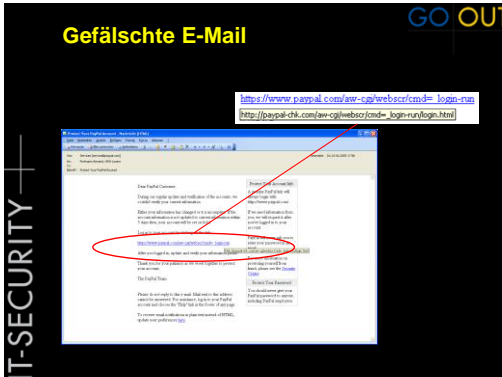
GO OUT

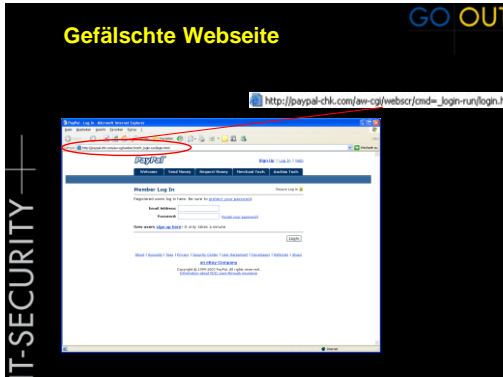
Informationssuche

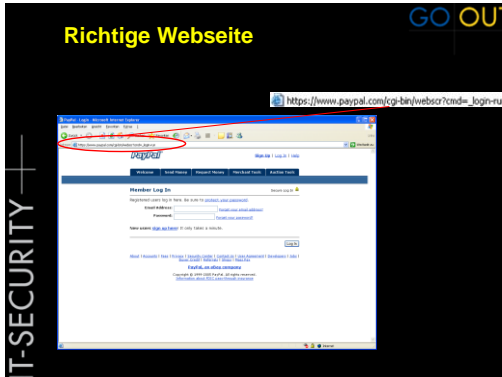
Yasni, Facebook, Xing und Co...



T-SECURITY







Farbcodierung IE

- Extended Validation Zertifikat, korrekte SSL-Verbindung
- Normales Zertifikat, korrekte SSL-Verbindung
- Fehlerhafte SSL-Verbindung

T-SECURITY


Farbcodierung Firefox

- Extended Validation Zertifikat, korrekte SSL-Verbindung
- Normales Zertifikat, korrekte SSL-Verbindung
- Fehlerhafte SSL-Verbindung

T-SECURITY

Internet - Schwachstellen

- ScareWare
- SQL-Injection
- XSS



T-SECURITY

GO OUT

ScareWare

T-SECURITY

- Praktisch täglich tauchen neue Variationen desselben Schemas auf:
 - Internet-Nutzer werden mit vorgetäuschten Schädlingbefunden zur Installation vorgeblicher Schutzprogramme genötigt.
- Die Google-Forscher haben etwa 240 Millionen Web-Seiten untersucht und dabei mehr als 11.000 Domains entdeckt, die Scareware verbreiten

GO OUT

ScareWare

T-SECURITY

News-Meldung vom 01.04.2011 16:00

Hunderttausende gehackter Webseiten sollten Scareware verbreiten

Kommerzielle haben über eine automatisierte SQL-Injection-Attacke hunderttausende von Webseiten manipuliert und dabei Links zu Containern mit Scareware eingebettet. Besucher einer infizierten Webseite bekamen durch Umstände eine weitere Seite zu Gesicht, in der ein vorgegeblicher Viren-Scanner eine Infektion des Systems vorgeschaltete.

News-Meldung vom 21.01.2011 15:26

Scareware-Welle schwappte durch Twitter

Am gestrigen Donnerstag verbreiteten sich über Twitter in offenbar großer Zahl Links die zu Scareware-Seiten führten. Die Links zu den Seiten waren über Short-URLs wie goo.gl verschleiert und wurden in verschiedenen Tweets von unterschiedlichen Nutzern etwa mit "Cool", "Very Nice" oder "Google's search page has done it again" angeschlossen.

GO OUT

ScareWare

T-SECURITY

WARNING!

WARNING! IN CONSENT!

Angriffspunkte

The diagram illustrates the flow of data from a user (Benutzer) through a Firewall to a Web-Server, then to an Application-Server, and finally to a Datenbank. A Browser window shows the URL `http://foo.de/shop/buy.php?product=0815`. A red flame icon is positioned at the Firewall, indicating a point of attack.

Fehlerhafte Datenübergabe

- Formulare zur Datenübergabe
- Informationen werden in Hidden-Felder übermittelt
- Gefahr: Tools zum Manipulieren der Daten

Web Developer

The screenshot shows the Web Developer toolbar in Firefox, with the 'View CSS' option selected. Below the toolbar, the URL `https://addons.mozilla.org/de/firefox/addon/60` is displayed.

SQL Injection

| user | Pwd | email |
|------|------------|---------------|
| Pete | perObiNa | peter@pan.org |
| John | hogeldogel | john@wayne.us |

Benutzerverwaltung:
Tabelle **Users**

Username: Pete
Password: [redacted]
Submit

```
SELECT * FROM Users
WHERE user=' ' AND pwd=' '
```

Skript `login.php` erhält die eingegebenen Zugangsdaten und verwendet diese in einer SQL Query

Benutzername/Passwort existiert: Query gibt eine Zeile zurück
→ der Benutzer ist **identifiziert** und erhält Zugang

GO OUT

SQL Injection

Ziel des Angreifers: Zugang zum System ohne Kenntnis von Benutzername/Passwort

Bei Logins funktioniert dies häufig mit ' or '='

```
SELECT * FROM Users
WHERE user=' ' or '=' AND pwd=' ' or '='
```

immer TRUE

T-SECURITY

GO OUT

Cross-Site Scripting (XSS)

Javascript: In Webseiten eingefügter Code, der im Browser ausgeführt werden

Oft enthalten **dynamisch generierte Webseiten** die von einem Benutzer eingegebenen Daten
 Produktresultatseiten, Google etc. zeigen den eingegebenen Suchstring an

Bei **XSS** nutzt ein Angreifer dieses Feature aus:

T-SECURITY


GO OUT

Testen auf XSS

Eingabe eines **einfachen Javascripts** in verschiedenen Feldern von Web-Formularen:

```
<script>alert("Testing XSS vulnerability");</script>
```

Bei Erfolg öffnet sich ein **Popup-Fenster**



T-SECURITY

GO OUT

Beispiel: XSS

- Achtung: Der Link kann in verschiedenen Dokumenten hinterlegt sein:
 - Email
 - Diskussions-Forum / Chat
 - Instant Messaging
 - PDF, Excel, Powerpoint, Word, etc.
 - Hochgeladene Datei
- Welchen Quellen trauen Sie?

T-SECURITY

GO OUT

Man in the Middle Angriffe

Dienst / Webseite

T-SECURITY

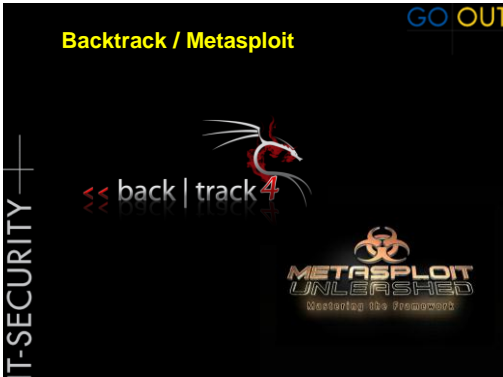
GO OUT

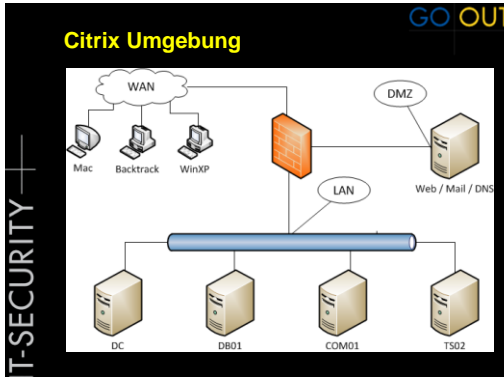
Man in the Middle Angriffe

- Cain & Abel

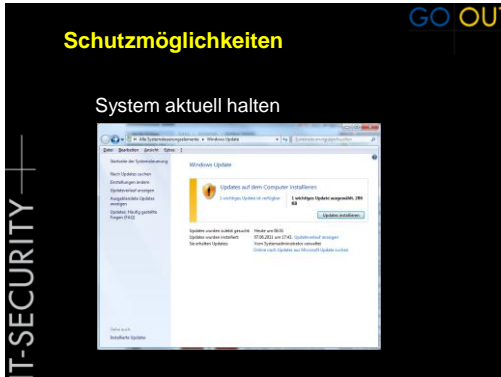
T-SECURITY

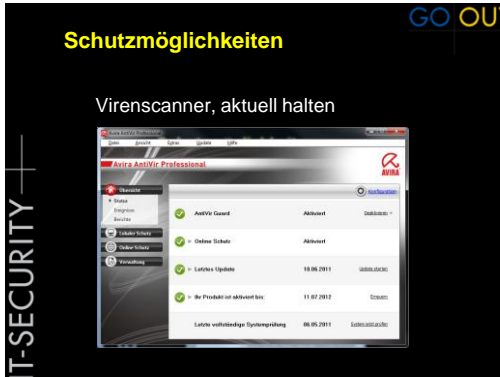










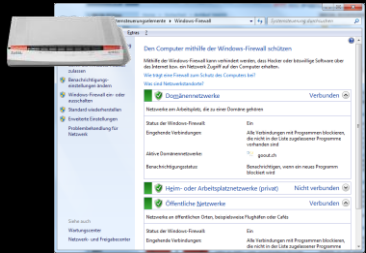


GO OUT

Schutzmöglichkeiten

Firewall, aktuell halten

T-SECURITY




GO OUT

Schutzmöglichkeiten

Gesunder Menschenverstand

T-SECURITY



GO OUT

Animationsfilm Infosurance

- Illustriert die „5 Schritte für Ihre Computer-Sicherheit“
- Wurde für den SwissSecurityDay 2009 von der Hochschule Luzern – Design & Kunst erstellt
 - http://www.youtube.com/watch?v=K_bs-BX2l_E
- Im gleichen Kontext wurden die 5 Schritte auch von Peach Weber in Form eines Filmes interpretiert und dargestellt
 - <http://www.youtube.com/watch?v=9gEfj-cvxrk>

GO OUT

Informieren Sie sich!

- <http://www.infosurance.ch>
- <http://www.melani.admin.ch>
 - Infoseite zu den Gefahren im Internet
- <http://www.ebankingabersicher.ch>
 - Infoseite für sicheres e-Banking
- <http://www.geschichtenausdeminternet.ch>
 - Infoseite zu den Gefahren im Internet
- <http://www.security4kids.ch>
 - Infoseite für Jugend- und Kinderschutz im Internet

T-SECURITY

GO OUT

GO OUT Production GmbH

Wissen Sie, wie es um Ihre IT-Sicherheit steht?

GO OUT Production GmbH
 Security Audits, -analysen und -beratungen
 Schulstrasse 11
 8542 Wiesendangen
 052 320 91 20
<http://www.goSecurity.ch>



T-SECURITY
