Hacking & Konkurrenzspionage

Oliver Münchow

oliver@muenchow.ch

IT - Security Forum #7

Aufbau & Zielsetzung

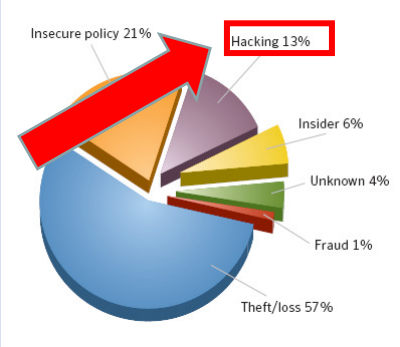
- Allg. Bedrohungssituation & Risiken
- Konkurrenzspionage – Beispiele
- Gezieltes Ausspionieren mit „Malware made in Switzerland“
- Was nun?

MELANIE SCHWEIZ

http://www.melani.admin.ch

„Wirtschaftsspionage: Erstmals **gezielte Angriffe** auf Schweizer Unternehmen. MELANI hat erstmals gezielte Spionageangriffe über das Internet auf Schweizer Betreiber kritischer Infrastrukturen beobachtet. Die benutzte **individualisierte Malware** wird von Antivirensoftware meist nicht erkannt und gefährdet generell Firmen in Form von Diebstahl von Geschäftsgeheimnissen.„

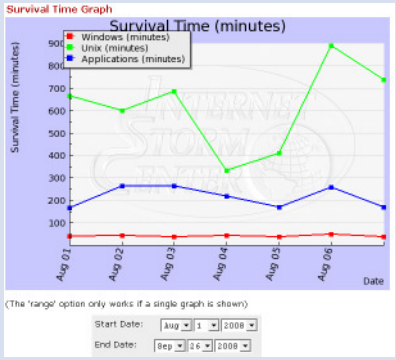
SYMANTEC 2008 THREATS



IT - Security Forum #7

Das Geschäft mit der Angst

SURVIVAL TIME



www.dshield.org

Wieso aber gibt es die dann noch?..

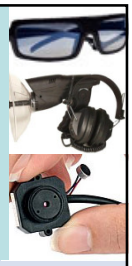
Demo - Webseite A

Demo - Webseite B

Demo - Webseite C

…und viele mehr …..

Konkurrenzspionage



… mehr als nur „Hacking“

- Wanzen / Hardware-Keylogger / Miniatur Kameras (Mobiltelefon als Wanze) / Laser Monitoring / Richtmikrophon etc.
- Tempest (Van-Eck-Phreaking): Die elektromagnetische Abstrahlung
- Abhören von drahtlosen Datennetzen / Telefon (VoIP) etc.
- **Individualisierte Malware**
- Mitarbeiter (Einschleusen von Praktikanten)
- **Social Engineering (Telefon / Besuch etc.)**
- Sichere Abfallentsorgung
- etc.

Angriffspunkt „Mensch“

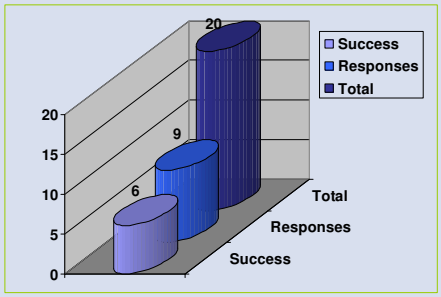
- Telefon
- Besuch
- Malware via USB / Mail

BSP: Das Telefon

BSP: Durchschnittsergebnis von letzten 5 Social-Engineering Attacken von NetProtect AG:

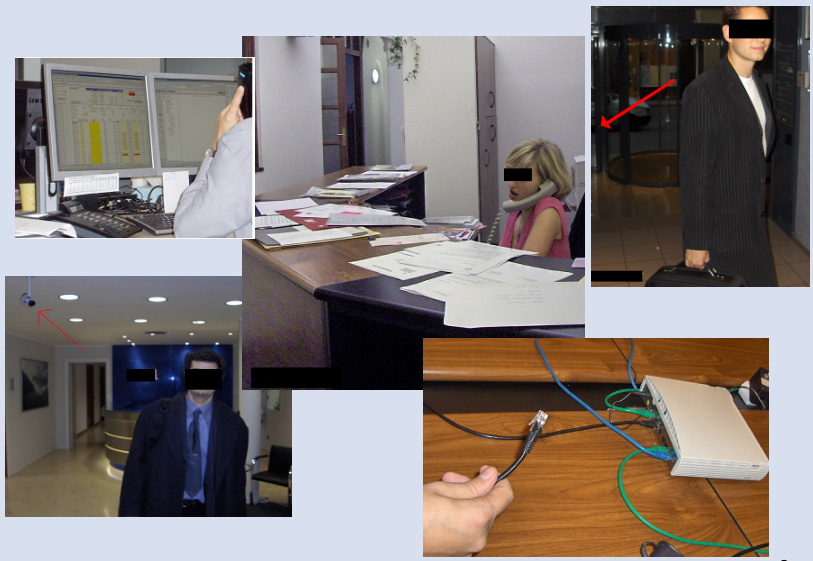
Grafik: „6 von 9 Personen geben am Telefon Auskunft über Username/Passwort“

Social Engineering:
Beim Social Engineering wird versucht, eine Person zu beeinflussen und sie dazu zu bringen, sensible Informationen preiszugeben.



IT - Security Forum #7

BSP: Der Besuch

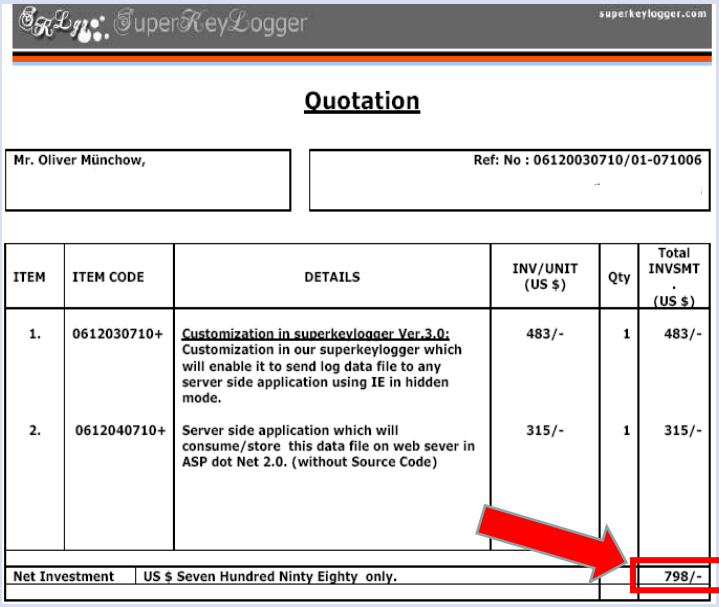


IT - Security Forum #7

BSP: Individualisierte Malware

Wieviel muss ich als Firma für die Entwicklung eines elektronischen Spionagetools budgetieren, um meinen Konkurrenten auszuspionieren?

Made in Israel: günstig



SuperKeyLogger superkeylogger.com

Quotation

Mr. Oliver Münchow,

Ref: No : 06120030710/01-071006

ITEM	ITEM CODE	DETAILS	INV/UNIT (US $)	Qty	Total INVSMT. (US $)
1.	0612030710+	Customization in superkeylogger Ver.3.0: Customization in our superkeylogger which will enable it to send log data file to any server side application using IE in hidden mode.	483/-	1	483/-
2.	0612040710+	Server side application which will consume/store this data file on web sever in ASP dot Net 2.0. (without Source Code)	315/-	1	315/-
Net Investment		US $ Seven Hundred Ninty Eighty only.			798/-

Our little swiss made Backdoor

Was würden wir gerne von unseren Konkurrenten haben?

- Word & Excel Dokumente
- Mails aus dem Outlook .PST File

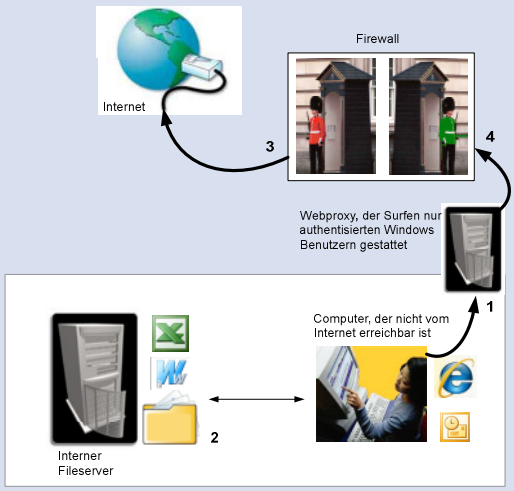
GO OUT IT-SECURITY HOSTING
insinova
digilan
phion
NETPROTECT AG
IT - Security Forum #7
IT-SECURITY
Blickpunkt KMU
InfoWeek.ch

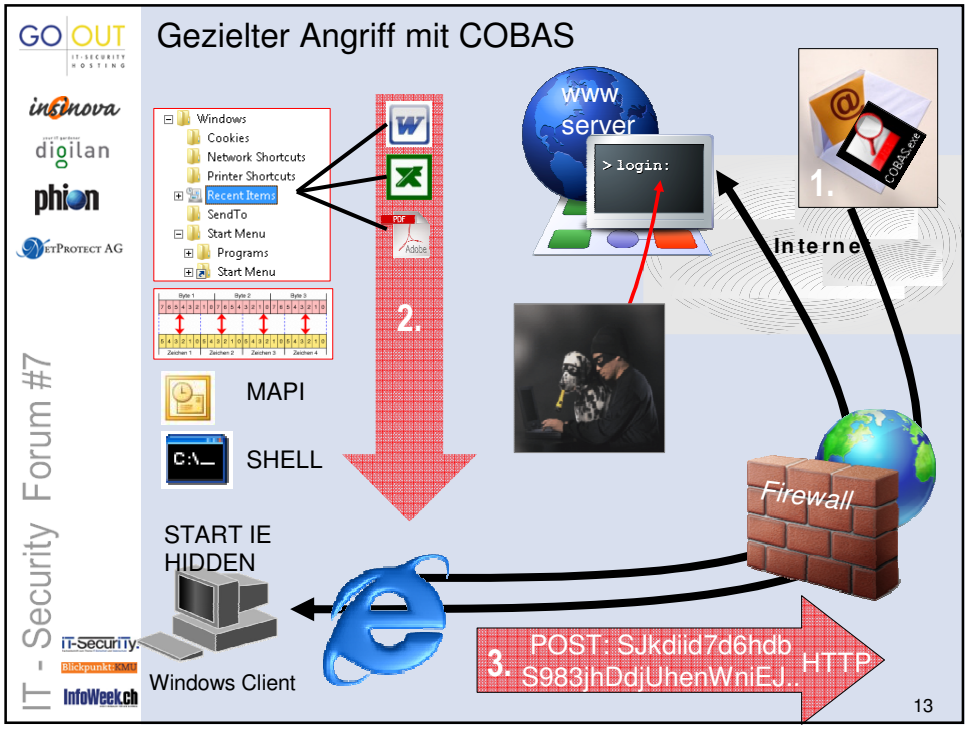
Ausgangslage Netzwerk

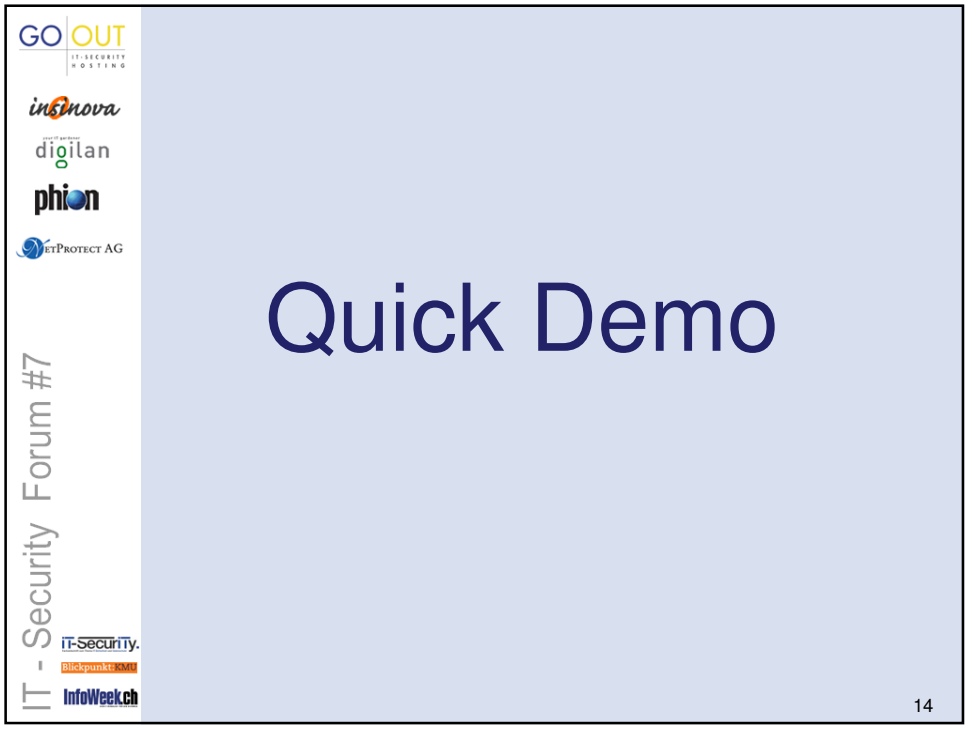
Der Standardschutz

Die Firewall erlaubt **KEINE eingehenden Verbindungen** (3) aus dem Internet. Ein interner Computer darf aber im Internet surfen und Mails abrufen (4). Zum Surfen muss sich der Windowsbenutzer beim **Webproxy** authentisieren (1).

Der Benutzer hat Word & Excel Dateien auf dem Fileserver auf seinem freigegebenen Laufwerk abgelegt (2) auf das nur er mit seinem Windows Account Zugriff hat.




Gezielter Angriff mit COBAS
Windows
Cookies
Network Shortcuts
Printer Shortcuts
Recent Items
SendTo
Start Menu
Programs
Start Menu
MAPI
SHELL
START IE HIDDEN
Windows Client
www server
> login:
1.
COBASexe
Internet
2.
Firewall
3. POST: SJkdiid7d6hdb S983jhDdjUhenWniEJ.. HTTP
GO OUT
insinova
digilan
phion
NETPROTECT AG
IT - Security Forum #7
IT-SECURITY
Blickpunkt KMU
InfoWeek.ch
13


Quick Demo
GO OUT
insinova
digilan
phion
NETPROTECT AG
IT - Security Forum #7
IT-SECURITY
Blickpunkt KMU
InfoWeek.ch
14

Was kann man tun?

Eintrittspunkte sichern (Class-1 auf GW filtern & USB Schutz)

User Awarness

Clientschutz (z.B. GPO Software Restriction Policies)

IE Zugang: zusätzliche Authentisierung

Firewall: POST & GET Request Grösse einschränken

Netzwerkdesign: Internetzugang via Citrix oder TS in separater Zone

Windows: Zusatzsoftware à la Defender

Systemsettings: beim Logoff Recent Docs löschen

Zusammenfassung

Wichtig für die Geschäftsleitung

- Sicherheitsinvestitionen im Verhältnis zu den Bedrohungen abwägen & die Frage beantworten: gibt es wertvolle Infos & wie wertvoll wären diese für die Konkurrenz?

Wichtig für die IT - Abteilung

- Mut zur Lücke – aber sich nicht auf Marketingversprechen von Produkten verlassen. Und: nur weil sich die meisten ähnlich (schlecht) schützen kann man dennoch eigene Wege gehen.

Wichtig für den Benutzer

- Please don‘t fu… click on that!!!!!!!