Einführung in die Informationstechnik

VI – Sicherheit im Internet

Aussagen zum Thema Bedrohung

(etwas älter)

- Mit einer Wahrscheinlichkeit von rund 50 Prozent wird ein Windows-PC ohne Virenschutz und aktuelle Sicherheits-Patches innerhalb von nur 12 Minuten durch einen Internet-Wurm infiziert.
  - http://www.sophos.de/pressoffice/news/articles/2005/07/pr_20050701midyearroundup.html
- Test von BBC News: ein mit dem Internet verbundener PC mit einem Windows-Betriebssystem wird durchschnittlich alle 12 bis 15 Minuten angegriffen oder nach Sicherheitslücken abgesucht.
- Umfrage Großbritannien (2006): 21 Prozent der Befragten sagten, sie hätten Angst vor Internetkriminalität, nur 16 Prozent fürchteten sich vor einem Einbruch.
- http://www.naiin.org/de/content/phishing/v13.php
- „Chinesische Hacker dringen ins Netz des Weißen Hauses ein“, Spiegel-Meldung vom 07.11.2008, http://www.spiegel.de/netzwelt/web/0,1518,589048,00.html

Meldungen zum Thema Bedrohung

- Riesen-Botnetz identifiziert: Kriminelle kontrollieren 1,9 Millionen Zombies (22.04.2009)
  http://www.trojaner-info.de/news2/botnetz-ukraine-finjan.shtml
- Internetkriminalität gilt als lohnendes Geschäftsfeld für Betrüger … Die PC-Zeitschrift "Chip" ging auf die Suche - und fand Gauner mit 800.000 Euro Einkommen. (06.05.2010)
  http://www.spiegel.de/netzwelt/web/0,1518,692888,00.html
- Zwei Entwickler haben die Technik zum Durchstöbern der Browser-History so weit verfeinert, dass Webseiten sogar zuletzt gelesene Artikel auf Newsseiten, die genaue Postleitzahl eines Besuchers und auf Suchmaschinen eingegebene Begriffe herausfinden können. (21.05.2010)
  http://www.heise.de/newsticker/meldung/History-Stealing-2-0-Ich-weiss-wo-du-wohnst-1005016.html

Aktuelle Bedrohungsmeldungen

- 01.03.2011: Attacke auf US-Großbank - Cyber-Gangster hackten Morgan Stanleys Netzwerk
- http://www.spiegel.de/wirtschaft/unternehmen/0,1518,748277,00.html
- 20.04.2010: Zeitungsbericht - China-Hacker sollen Googles Passwort-System gestohlen haben
- http://www.spiegel.de/netzwelt/web/0,1518,690005,00.html
- 03.05.2011: Sicherheitsrisiko - Hacker konnten Daten von 100 Millionen Sony-Kunden kopieren
- http://www.spiegel.de/netzwelt/games/0,1518,759830,00.html
- 28.5.2011: Cyber-Attacke gegen Lockheed Martin - Datendiebe greifen US-Rüstungskonzern an
- http://www.spiegel.de/netzwelt/web/0,1518,765422,00.html

Übersicht

- Vergangene Wochen: Internet, Grundlagen und Dienste
- Heute:
  - Gefährdungen
    - Viren, Würmer & Co.
    - Aktive Inhalte
    - Phishing
    - Spam
    - Scareware
    - DoS, Bot-Netze
    - Dialer & Co.
  - Absicherung;
    - (Personal) Firewall, Anti-Viren Programme, Intrusion Detection
  - Schutz der Privatsphäre
  - Jugendschutz
- Orientierung am BSI-Grundschutz

Viren

- Original Definition von Fred Cohen (1984): A "computer virus" is a program that can "infect" other programs by modifying them to include a possibly evolved version of itself.
- Definition: Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)
- Viren schleusen sich in andere Programme ein und verbreiten sich dadurch

https://www.bsi-fuer-buerger.de/cln_174/BSIFB/DE/ITSicherheit/VirenUndAndereTiere/Virenchronik/virenchronik_node.html

Arten von Viren, Verbreitungswege

- Boot-Viren:
  - Booten → laden des Betriebssystems
  - Virus schreibt sich in den Bootsektor eines Datenträgers
  - Ausführung beim Starten des Rechners
- Datei-Viren:
  - Infizieren Programme, werden Teil des Programms
  - Beim Starten des Programms wird Virus ausgeführt
- Makro-Viren:
  - Makros: Skripte, die Programmschritte automatisiert ausführen
  - Beispielsweise in Word, Excel
  - Makroviren bevölkern die erzeugten Dokumente
- Skript-Viren:
  - Ähnlich Makroviren, meist auf Webseiten

Schäden durch Viren in der Vergangenheit

- Harmlose Schäden:
  - Der Microsoft Word-Makro-Virus WAZZU fügt bei den befallenen Dokumenten an zufälligen Stellen das Wort "Wazzu" ein.
  - MIX-1 Virus stört das Ausdrucken von Texten und Grafiken auf einem Drucker
    - Aus "Sehr geehrte Damen und Herren" wird auf dem Ausdruck dann "Rahr gaahrta Deman ond Harran„
      (Quelle: BSI, http://www.bsi-fuer-buerger.de/viren/04_0205.htm)
- Datenlöschung/-zerstörung:
  - Der Boot-Virus Michelangelo überschreibt an jedem 6. März die ersten Spuren der Festplatte mit stochastischem Inhalt und macht sie dadurch unbrauchbar (1992).
  - Der Virus Onehalf verschlüsselt maximal die Hälfte des Inhalts der Festplatte. Wird der Virus entfernt, sind die verschlüsselten Daten nicht mehr verfügbar.
  - XM/Compat-Virus: Makro-Virus, der Microsoft-Excel-Dateien befällt.
    - Durchforstet ein zufälliges Dokument aus der Bearbeitungs-History nach ungeschützten Zellen mit numerischen Werten. In diesen Zellen ändert er die Werte mit einer einprozentigen Wahrscheinlichkeit zufällig in einem Rahmen von +5 bis −5 % ab.
- Hardwarezerstörung:
  - Übertaktung von Hardwarekomponenten
  - Zerstörung von Festplatten
  - Heute eher unüblich/schwierig, auf Grund der Heterogenität der Hardware

Trojaner

- Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen.
- Arbeiten im Hintergrund
- Ermöglichen beispielsweise Zugriff von außen
- Verbreiten sich nicht selbstständig
- Verbreitungswege:
  - ICQ, Email, Tauschbörsen, Download
- Ziel: Ausspionieren vertraulicher Daten
- Beispiel:
  - Bildschirmschoner, der Passwörter weiterleitet
  - veränderte Login-Programme

Würmer

- Ähnlich Viren, Verbreitung autark, ohne Wirtsprogramm
  - Benötigt aber Hilfsprogramm wie Email oder Netzwerkdienst
  - Nutzt bestehende Infrastrukturen
- Virus: Weitergabe durch infizierte Datei
- Im strengen Sinn sind Würmer sich selbst verbreitende Programme
  - Bringen oft eigene Email-Routine mit
- Verbreitung durch:
  - Email - oft als Anhängsel
  - peer to peer, Tauschbörsen
  - Instant Messaging
- Erster Wurm: Robert T. Morris (1988)
- verschleiern Ihre Existenz ähnlich den Trojanischen Pferden
- Nutzen oft gezielt Programmierfehler zur Ausführung

Rootkit

- Root=Admin ⟶ Rootkit=Admin-Baukasten
- Ziel: (vollständige) Kontrolle über das befallene System
- Softwarewerkzeuge zum Verschleiern von Einbrüchen, ersetzen wichtiger Systemprogramme
- Klinkt sich in laufende Prozesse ein
  - Gelangt so an „interessante“ Daten
- Drei wesentliche Varianten
  - RKs die sich in den Betriebssystemkern einschleusen ⟶ Kernel Rootkits
  - RKs die sich in laufende Prozesse einhaken und deren Aufrufe auf die eigenen Programmteile umlenken ⟶ Userland Rootkits
  - Auch möglich Speicher-Rootkits
- Ziel: Kontrolle des Systems, Öffnen von Hintertüren

MailBombing, Archivbombe

- Mailbombe: Versenden von großen Dateien als Emailanhang → nur wirksam bei begrenztem Emailspeicherplatz
  - Oft auch mehrere Emails notwendig
- Archivbombe: gepackte Datei, die beim Entpacken sehr viel Speicherplatz benötigt
  - Problem für Antivirenprogramme
  - Bekanntestes Beispiel: 42.zip

Hoax

- Scherz oder Falschmeldung, Ente
- Kettenbriefe, Aufrufe zum Löschen von Dateien
- Irreführende Nachricht, die gelöscht werden kann und sollte
- Laut BSI enthalten die meisten „Hoaxes“ folgende Elemente:
  - Einen Aufhänger, der Seriosität vermitteln soll (etwa einen Bezug zu einem bedeutenden Unternehmen)
  - Eine angebliche Sachinformationen über ein Ereignis von besonderer Bedeutung (etwa das Auftauchen eines Computerschädlings) oder sensationelle Einkunftsmöglichkeiten (etwa angebliche Provisionen durch große Softwarekonzerne für die Weiterleitung von Mails), Hinweise auf Katastrophen (z. B. Tsunami) oder Verschwörungstheorien
  - Keine Daten, dafür aber Aktualität signalisierende Bezüge wie "gestern" oder "soeben"
  - Die dringende Bitte, die Information oder Warnung möglichst allen Bekannten zukommen zu lassen.
- Liste aktueller Email-Enten: http://www2.tu-berlin.de/www/software/hoaxlist.shtml
  - Aufrufe zum Tank-Boykott als Protest gegen die Preispolitik der Mineralölkonzerne

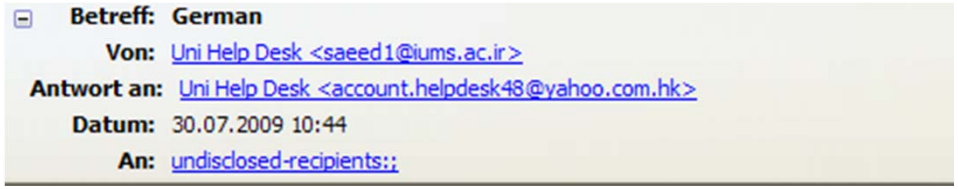
Social Engineering

- Nutzen des Sozialen Umfeldes um an persönliche Daten zu gelangen
  - Ausspionieren des persönlichen Umfeldes
  - Ausnutzen von Verhaltensweisen
- Identity Theft: Nutzung persönlicher Daten durch Dritte.
  - Eigentlich Identitätsmissbrauch
- Social Hacking: nutzen von Social Engineering um ein ein fremdes Computersystem einzudringen
- Phishing
  - Allgemein
  - Spear Phishing
  - Dumpster Diving

Phishing

- Kunstwort aus password und fishing
  - „nach Passwörtern fischen“
- Ermittlung von Passwörtern und Zugangsdaten über gefälschte Emails und Webseiten
  - beeinhalten oft Link auf gefälschte Webseite
  - Falsche, versteckte Absenderadresse

Phishing Email



Wir haben Ihnen am 29. Juni 2009 beraten, dass Sie die Passwort auf Ihrem Konto, um zu verhindern, dass Unbefugte Konto Zugang im Anschluss an die Netzwerk-Anweisung wir zuvor kommuniziert werden.
Alle E-Mail-Hub-Systeme wird sich regelmäßig geplante Wartung. Zugriff auf Ihre E-Mail über das Webmail-Client wird für einige Zeit nicht verfügbar
Während dieser Gewährleistungsfrist. Wir sind derzeit die Modernisierung unserer Datenbank und
E-Mail-Konto-Center i.e Startseite.

Wir werden das Löschen alter E-Mail-Konten, die nicht mehr aktiv zur Schaffung von mehr Platz für neue Benutzer-Konten. Wir haben auch untersucht, ein Security-Audit-weit zu verbessern und unsere aktuellen Sicherheitseinstellungen.

Im Hinblick auf die Fortsetzung der Nutzung unserer Dienste werden Sie benötigen zur Aktualisierung und wieder bestätigt, Ihre E-Mail-Konto, wie unten. Um Ihr Konto wieder bestätigen, müssen Sie eine Antwort auf diese E-Mail sofort und geben Sie Ihre Kontodaten wie unten.

Benutzername: (*********)
Passwort: (*********)
Geburtsdatum:
Zukunft Passwort: (*******)(Option)

Sollte dies nicht sofort machen wird Ihr Konto deaktiviert aus unserer Datenbank und den Service nicht unterbrochen werden, wie wichtig Nachrichten können auch verloren gehen durch Ihre rückläufig wieder comfirmed Sie uns Ihre Kontonummer Details. Wir entschuldigen uns für die Unannehmlichkeiten, dass dies dazu führen, dass Sie während dieser Zeit, sondern vertrauen, dass wir sind hier, um Sie besser bedienen zu können und mehr Technologie, die dreht sich um Sichere E-Mail.

Es ist auch relevant, Sie verstehen, dass unser primäres Anliegen ist die Sicherheit für unsere Kunden, und für die Sicherheit ihrer Daten und Dateien. Bestätigungs-Code: / 93-1A388-480 Technische Support-Team Grüße UNI Help Desk Support / Maintainance Team TSRa

Erkennen von Phishing-Emails

- gefälschte Absenderadressen – im Header nachsehen
- unpersönliche Anrede („lieber Kunde der ...-Bank“)
- dringender Handlungsbedarf signalisiert (sonst Datenverlust)
- es wird gedroht ("Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren…")
- Vertrauliche Daten (z. B. PINs und TANs) werden abgefragt
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt bzw. geöffnet werden sollen
- manchmal in schlechtem Deutsch verfasst
- E-Mails enthalten kyrillische Buchstaben oder falsch dargestellte bzw. fehlende Umlaute

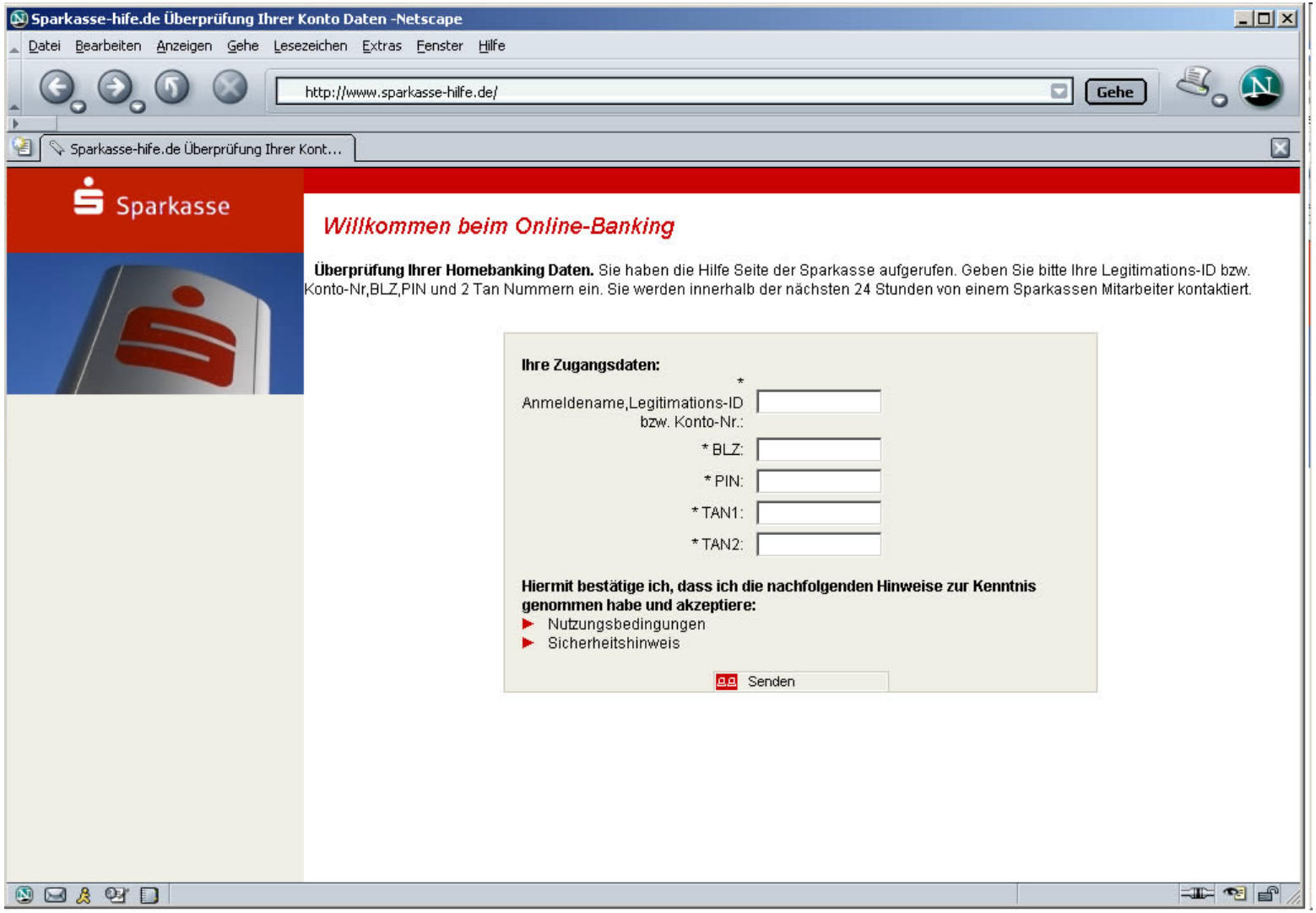
http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

Erkennen von Phishing-Webseiten

- oft fehlt Sicherheitshinweis im Browser (http**s**://), kann aber auch gefälscht werden
- Domainnamen enthalten unübliche Zusätze, sehen den tatsächlichen aber ähnlich
  - www.x-bank.servicestelle.de
- Sicherheitszertifikat fehlt, erkennbar durch das Schlosssymbol
  - in Statusleiste
  - in Eingabezeile

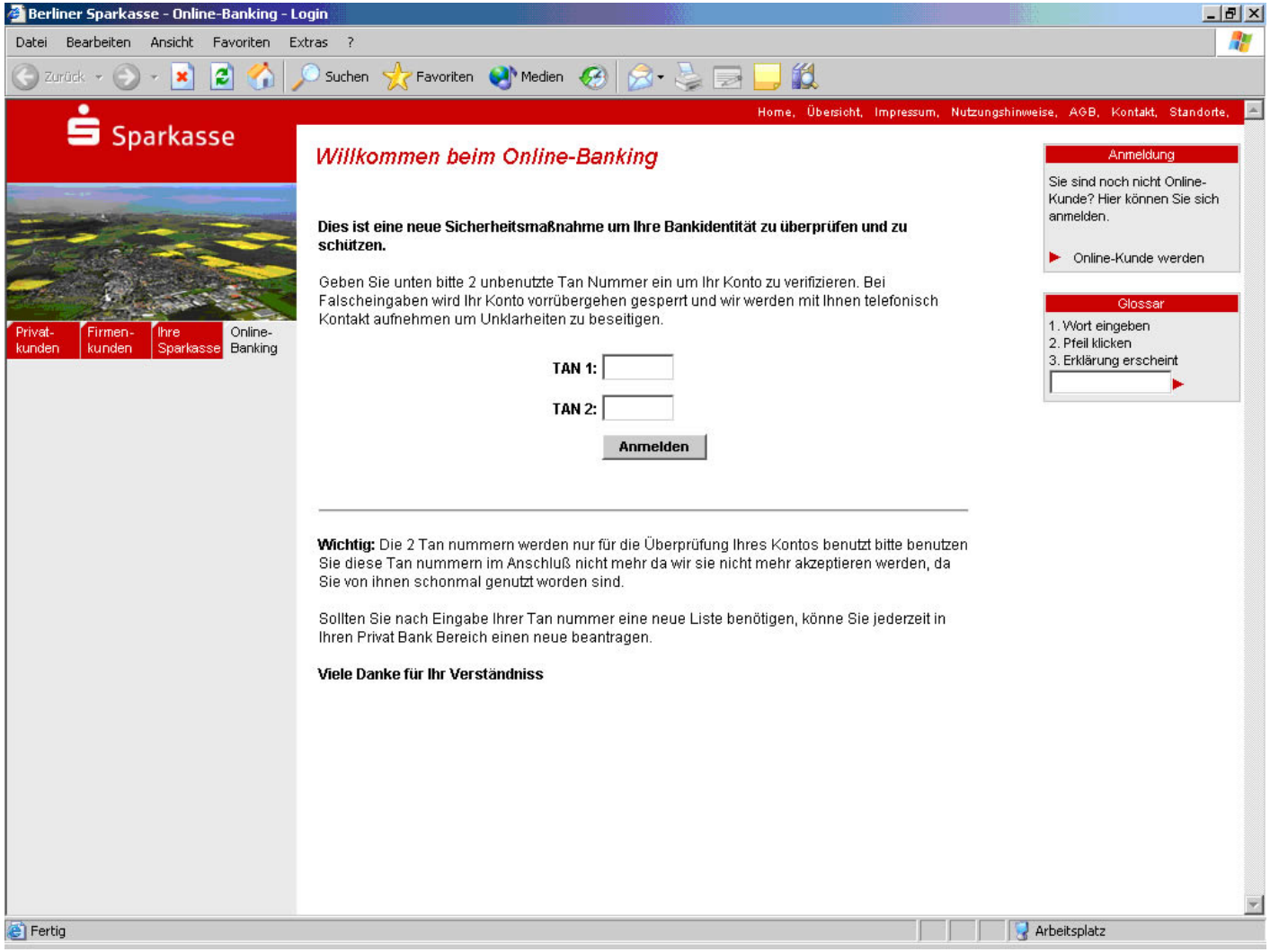
http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

Phishing Webseiten - Beispiel



http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

Phishing Webseiten - Beispiel



http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

Identitätsmissbrauch

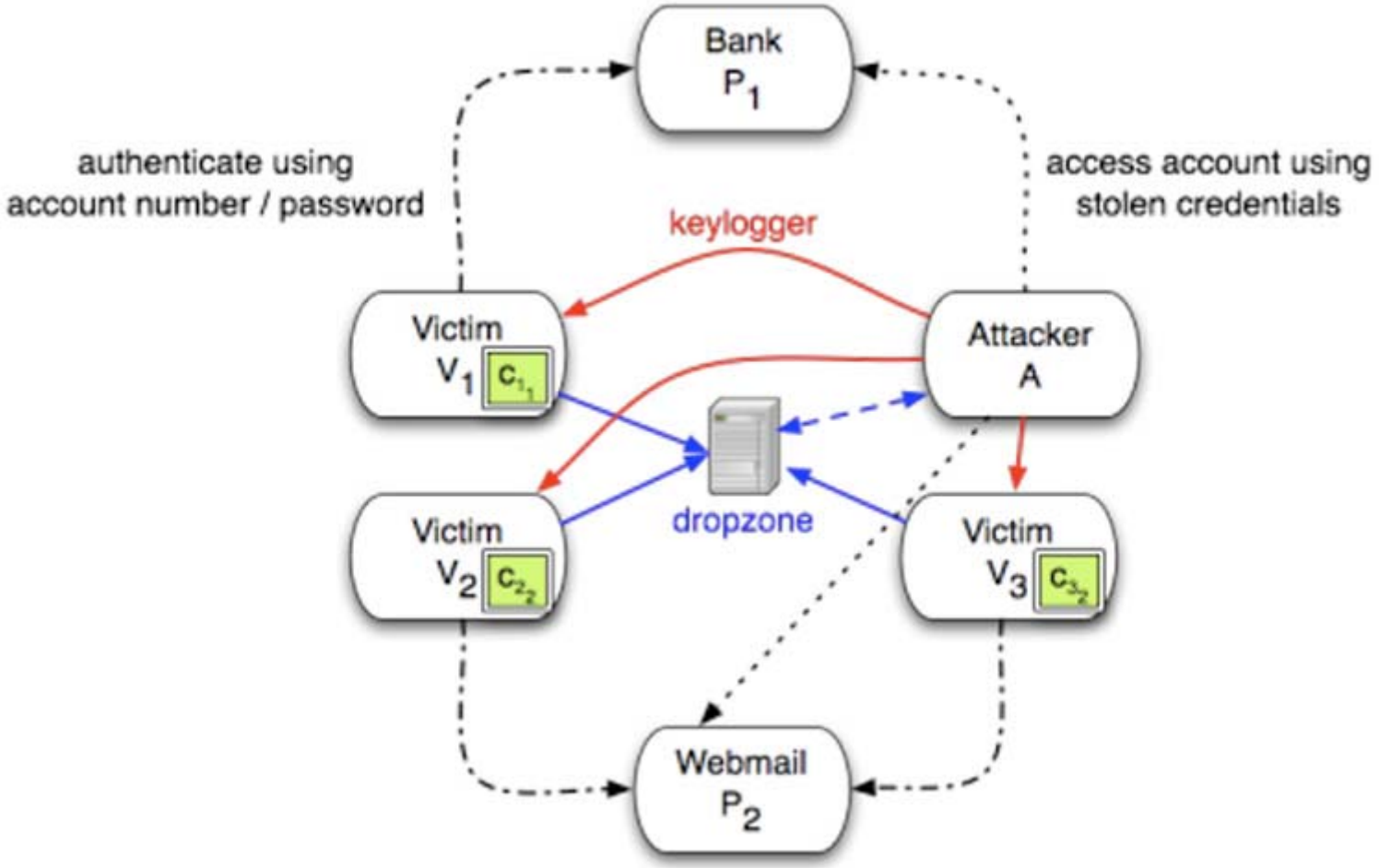
- Vorgeben falscher Identität für verschiedene Zwecke
  - Einen Betrug durchzuführen: Bestellungen bei Versandhäusern
  - Um in Rechnersysteme einzubrechen
  - Dienstleistungen kostenlos zu nutzen
  - Weitere Daten zu erhalten
- Nicknapping: Benutzen fremder Nicknames
- Anlegen von Accounts unter fremdem Namen
  - Kann genutzt werden, um Person zu schaden
  - Kann dazu führen, dass betroffene Person keinen Account mehr anlegen kann -> echter Identitätsdiebstahl

Netzbasierte Manipulationen

- Pharming, Spoofing: Manipulation der DNS-Abfragen
- Ziel:
  - Umleitung von Nutzern auf alternative Webseiten
    - Obwohl die richtige URL eingegeben wurde
  - Verschleierung der eigenen Identität
- Angriffsziele: DNS-Server, hosts Dateien

Spyware

- Software, die das Verhalten von Nutzern ausspioniert
- ähnlich Phishing, allerdings passiv
- kann auf Rechner gelangen über:
  - Aktive Inhalte auf Webseiten
  - Freeware oder Shareware
- gefährlich: keylogger, können auch Passwörter ermitteln



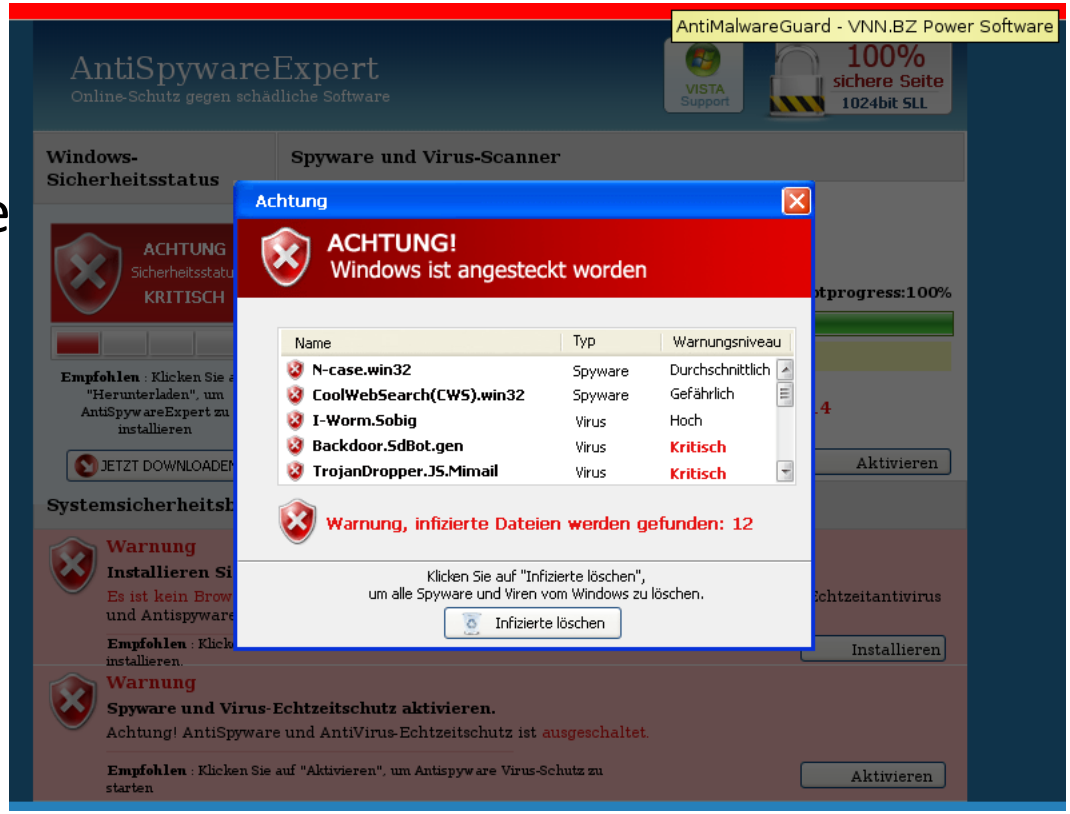
Spiegel-Artikel: Cyber-Verbrecher gehen IT-Forschern in die Falle, http://www.spiegel.de/netzwelt/tech/0,1518,600971,00.html

Spam

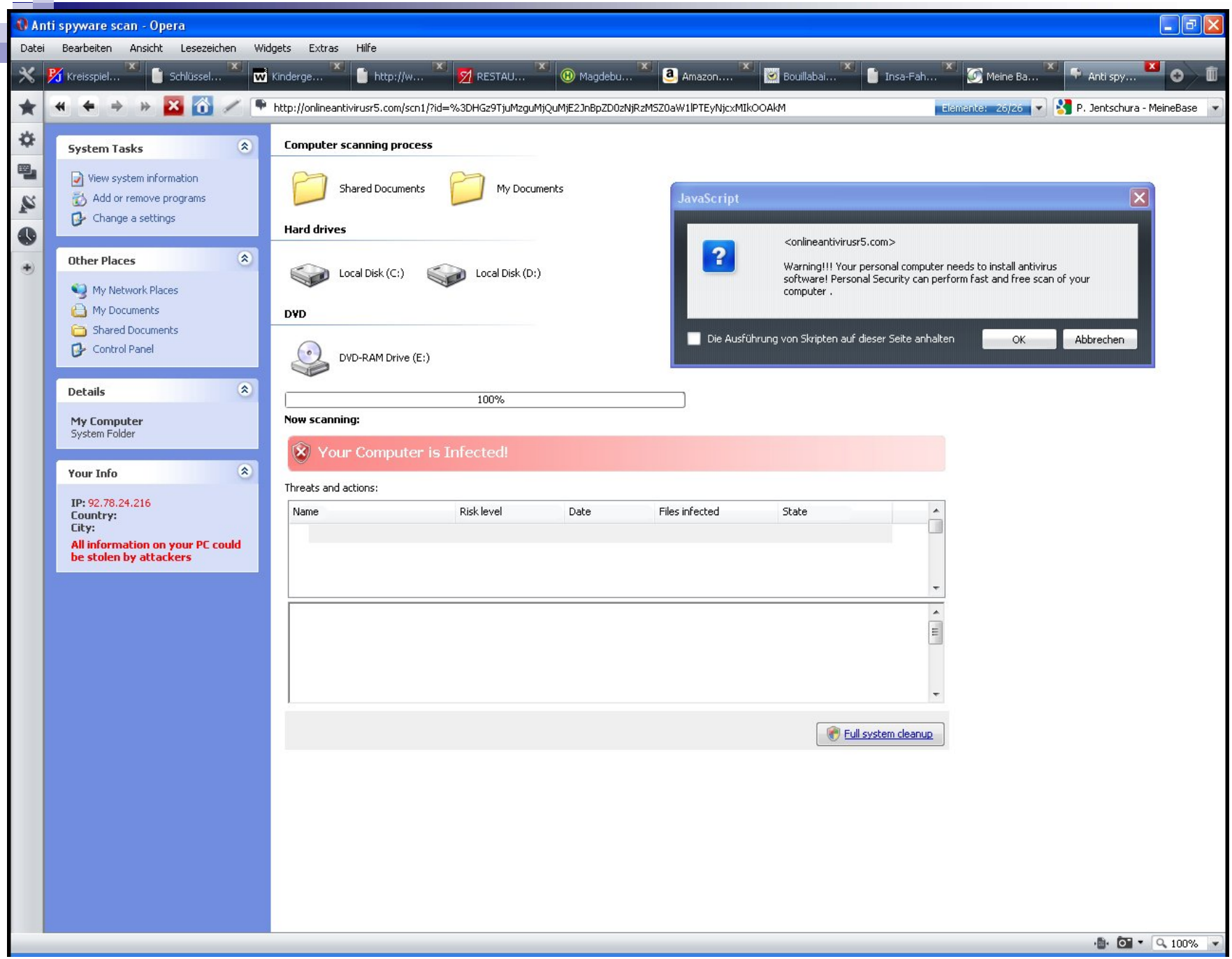
- Spam ist dem Dosenfleisch SPAM (Spiced Porc and Ham) entliehen (deutsch: Frühstücksfleisch)
- Als Spam, Spamming oder Junk Mail (Müllpost) bezeichnet man:
  - Massenversand nichtangeforderter Werbe-EMails
  - Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben.
  - Kettenbriefe
- Vorraussetzung: Email-Adressen

Scareware

- Werbung, die die Angst von BenutzerInnen ausnutzt → Trickbetrug
- gezielte Platzierung von Werbung für nutzlose oder gefährliche Software
- auch Vorgaukeln einer Schadsoftwarediagnose
- Betroffen u.a.: New York Times, Microsoft



http://www.heise.de/security/artikel/Zweifelhafte-Antiviren-Produkte-270094.html


Anti spyware scan - Opera
Datei Bearbeiten Ansicht Lesezeichen Widgets Extras Hilfe
http://onlineantivirusr5.com/scn1/?id=%3DHGz9TjuMzguMjQuMjE2JnBpZD0zNjRzMSZ0aW1lPTEyNjcxMIkOOAkM
P. Jentschura - MeineBase
System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
Your Info
IP: 92.78.24.216
Country:
City:
All information on your PC could be stolen by attackers
Computer scanning process
Shared Documents
My Documents
Hard drives
Local Disk (C:)
Local Disk (D:)
DVD
DVD-RAM Drive (E:)
JavaScript
<onlineantivirusr5.com>
Warning!!! Your personal computer needs to install antivirus software! Personal Security can perform fast and free scan of your computer .
Die Ausführung von Skripten auf dieser Seite anhalten
OK
Abbrechen
100%
Now scanning:
Your Computer is Infected!
Threats and actions:
Name
Risk level
Date
Files infected
State
Full system cleanup
100%

Aktive Inhalte auf Webseiten

- Browser können kleine Programme innerhalb der Webseite ausführen
  - Java-Applets, JavaScript, ActiveX, VBScript
- benötigt, um Inhalte dynamisch zu aktualisieren
- Gefahrenpotential, da Programme auf Rechner ausgeführt werden
  - Ausführung sollte vom Browser kontrolliert werden
  - Schwachstelle bei:
    - fehlerhafter Programmierung
    - gezieltem Angriff

DoS – Deny of Service

- Außer Betrieb setzen von technischen Einrichtungen
- bombardieren von Servern mit Anfragen → Überlastung
- oft verteilte Angriffe – distributed DoS
  - Verbreitung der Angriffsprogramme vorher als Wurm
  - Nutzung von Bot-Netzen

Bots

- Ro(bot-Net), ferngesteuertes Netz von gekaperten Rechnern
  - Zombie-PCs
- Jeder Rechner kann einzeln ferngesteuert werden oder
- Im Verbund arbeiten
  - genutzt für Spam, DoS