Sicherheitsfaktor Mensch

Fraunhofer Institut Sichere Informations-Technologie

Sicherheitsfaktor Mensch

Ist der Benutzer eine vertrauenswürdige Komponente?

Sven Türpe
Fraunhofer SIT

Rheinstraße 75
64295 Darmstadt

tuerpe@sit.fraunhofer.de
+49 (0)6 15 1/8 69 - 42 38

Fraunhofer Institut Sichere Informations-Technologie

x0%kL^By-Wo3n

ssh-keygen(1): „Good passphrases are 10-30 characters long, are not simple sentences or otherwise easily guessable (...), and contain a mix of upper and lowercase letters, numbers, and non-alphanumeric characters.“

„There is no way to recover a lost passphrase.“

Fraunhofer SIT Institut Sichere Informations-Technologie

CA-2000-04 Love Letter Worm

„Exercise caution with attachments in email. (...) Users should never open attachments from an untrusted origin, or that appear suspicious in any way.“

(CERT Advisory CA-2000-04)

Akzeptanz der digitalen Signatur

„Durch das Festschreiben bürokratischer, komplizierter Verfahren und überzogener technischer Anforderungen, (...) dazu beigetragen, dass die digitale Signatur für viele Bürger und Unter-nehmen in Deutschland schlicht unattraktiv ist. Der Gebrauch ist so umständlich und teuer, dass kaum ein Bürger oder Unternehmen in Deutschland die digitale Signatur haben will."

(CDU/CSU-Fraktion im Bundestag)

Akzeptanz der digitalen Signatur (Forts.)

„For some time, C&E has been encouraging electronic VAT returns (...), but until recently required the use of an X509 client certificate to submit.

Presumably this has proved unpopular, since they are now permitting good old username/ password to be used.“

(Risks Digest Vol. 23, Issue 56)

Fraunhofer SIT Institut Sichere Informations-Technologie

Phishing

Quelle:
www.antiphishing.org

Dear PayPal valued member,

Due to concerns, for the safety and integrity of the PayPal community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account deletation. This notification expires on April 16th 2004.

Once you have updated your account records your PayPal will not be interrupted and will continue as normal.
Please note that you are prohibited to send or receive money until you confirm that you are the trueholder of this account.

Please follow the link below
and renew your account information.
https://www.paypal.com/cgi-bin/webscr?cmd=login-run

PayPal

PayPal Service Department

Was nun?

Sichtweisen

Usability Engineering:

Sicherheitstechnik ist zu kompliziert

Security Engineering:

Benutzer sind zu blöd

Ein unlösbarer Widerspruch?

Usability Engineering

- Aufgaben und Ziele des Benutzers
- Einfacher/schneller als ohne Computer
- Benutzer kennt sich im Gegenstandsbereich aus
- zum Beispiel:
  - Aufgabenangemessenheit
  - Erlernbarkeit, Selbstbeschreibung
  - Effizienz
  - Keine katastrophalen Fehler

Sicherheit aus Sicht der Mensch-Maschine-Interaktion

Sicherheitstechnik hat besondere Eigenschaften (Whitten & Tygar, 1999):

- Sicherheit ist Sekundärziel
- Sicherheit ist kompliziert
- Wenig und schlechtes Feedback
- Kein „Undo“
- Angreifer muss nur *eine* Lücke finden

Security Engineering

- Bedrohung: intelligenter Angreifer
- System
- Komponenten
- Interaktion
- Vertrauensbeziehungen
- Sicherheitsmechanismen
  - Stärke, z.B. bei Kryptographie

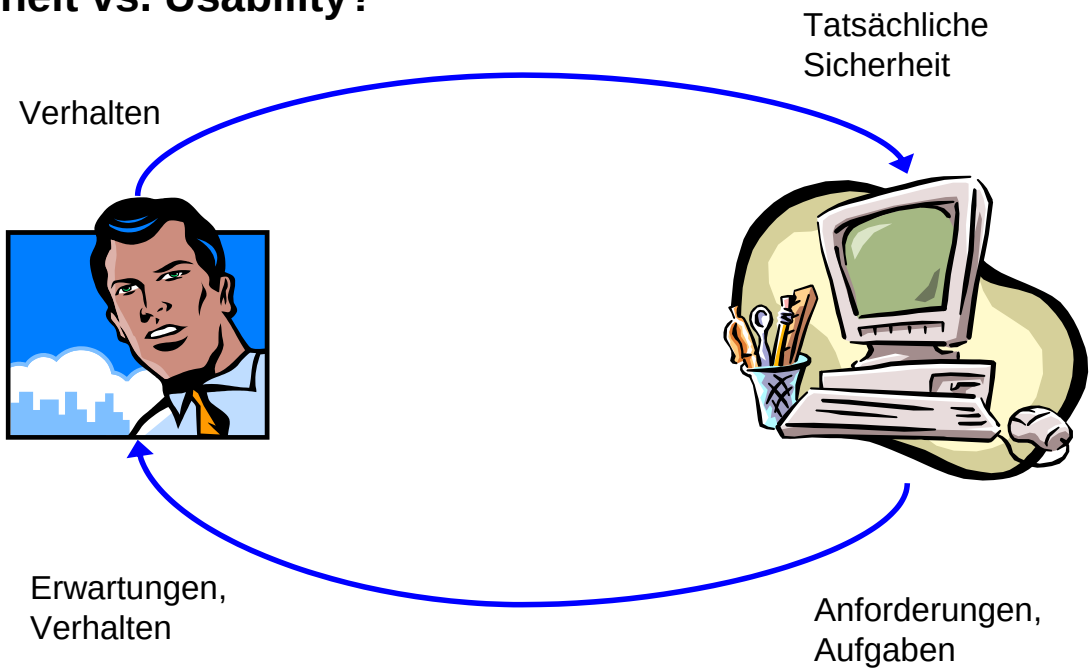
Fraunhofer SIT Institut Sichere Informations-Technologie

Benutzer aus Sicht der Sicherheitstechnik

- Trusted Component ...
  - Ich bin `root`, ich darf das.
- ... aber nicht vertrauenswürdig, sondern
  - Fehleranfällig
  - Ahnungslos
  - Subversiv
- Schutz des *Systems* im Vordergrund
  - Angriffe auf Benutzer?
- Ist Sicherheit einfach zu kompliziert? Können wir User erziehen und schulen?

Fraunhofer SIT Institut Sichere Informations-Technologie

Sicherheit vs. Usability?



Fraunhofer SIT Institut Sichere Informations-Technologie

Human Factors

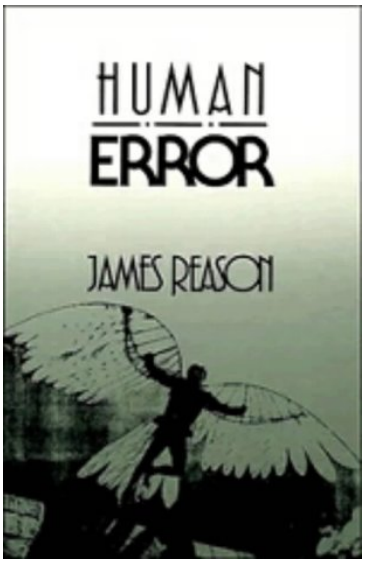
Missverständnis: Sicherheit einfacher machen.

- Fähigkeiten
- Wissen
- Verhalten
- Stress
- Wahrnehmung

→ Übereinstimmung zwischen Anforderungen an die User und ihrem tatsächlichen Verhalten.

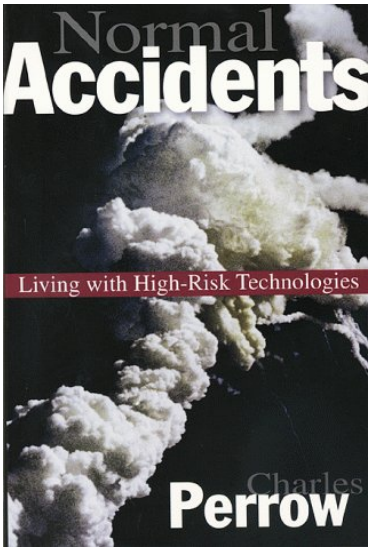
Fraunhofer SIT Institut Sichere Informations-Technologie

James Reason: „Human Error“



- Rasmussen: Skill – Rule – Knowledge
- Generic Error Modeling System (GEMS)
  - Fehlerklassen analog Verhaltensebenen
  - Unterschiede z.B. in
    - Vorhersagbarkeit
    - Fokus der Aufmerksamkeit
    - Einfluss der Randbedingungen
    - Erkennungsmöglichkeit

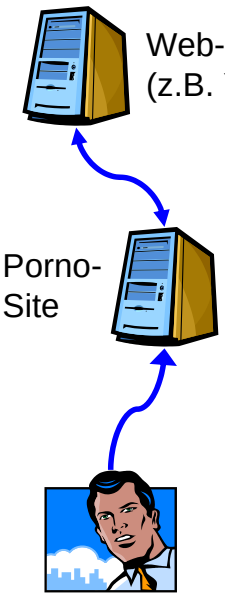
Charles Perrow: „Normal Accidents“



- Unfälle in technischen Systemen
  - z.B. Kernkraftwerk Harrisburg
- Was geht warum schief?
- „System Accident“
  - Komplexe Interaktion
  - Enge Kopplung
  - Mehrfachfehler
- Nur Sicherheit == Safety betrachtet

Stand der Technik:

Mein Lieblingshack

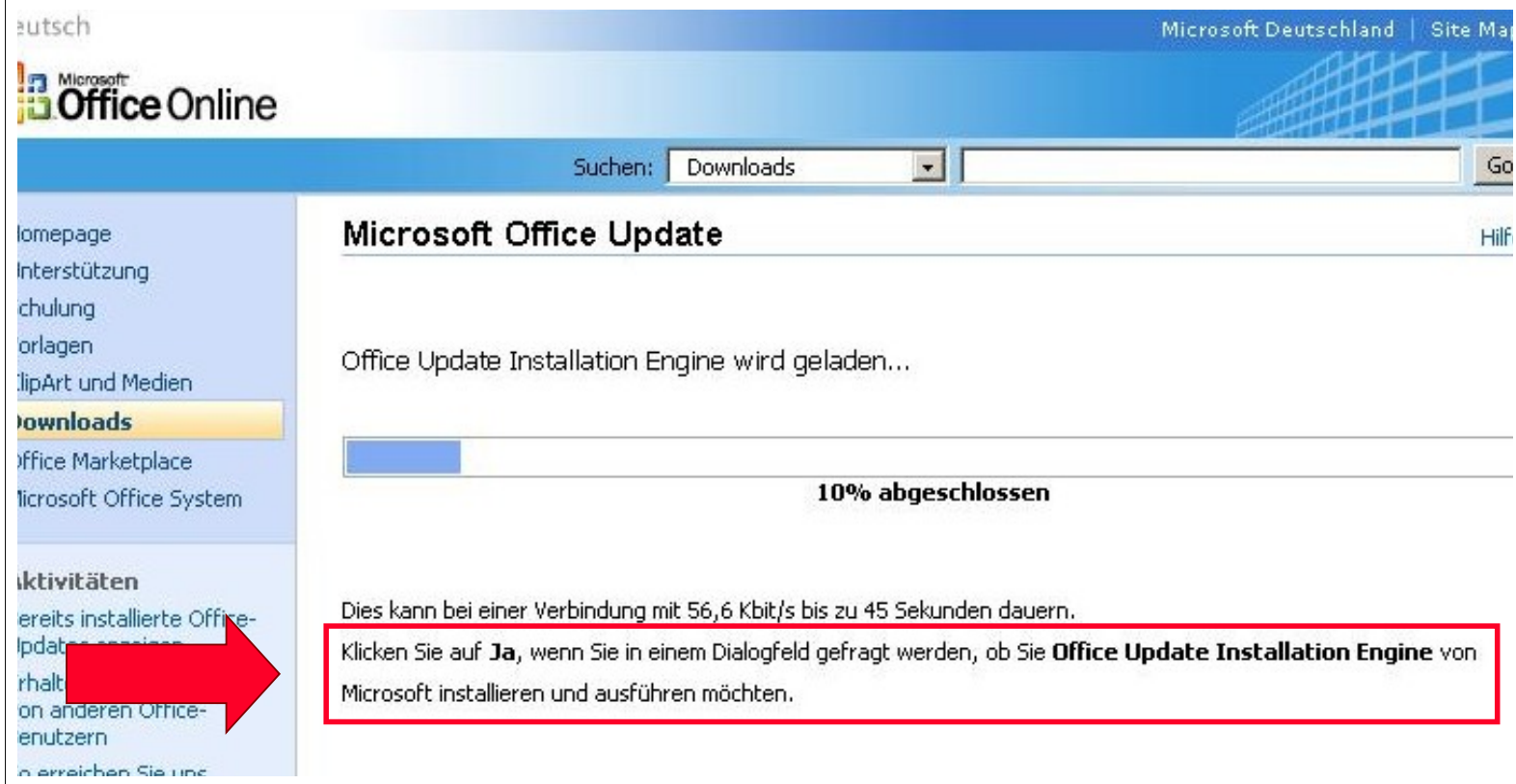


CAPTCHA:

Completely **A**utomatic **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

Fraunhofer SIT Institut Sichere Informations-Technologie

Ungewollte Lerneffekte



Ungewollte Lerneffekte

Was lernt uns das?

„Subversives“ Verhalten

Wissen Sie das Passwort noch?

x0%kL^By-Wo3n

Benutzerreaktionen:

- Aufschreiben
- Variation eines Standardpassworts
- ...

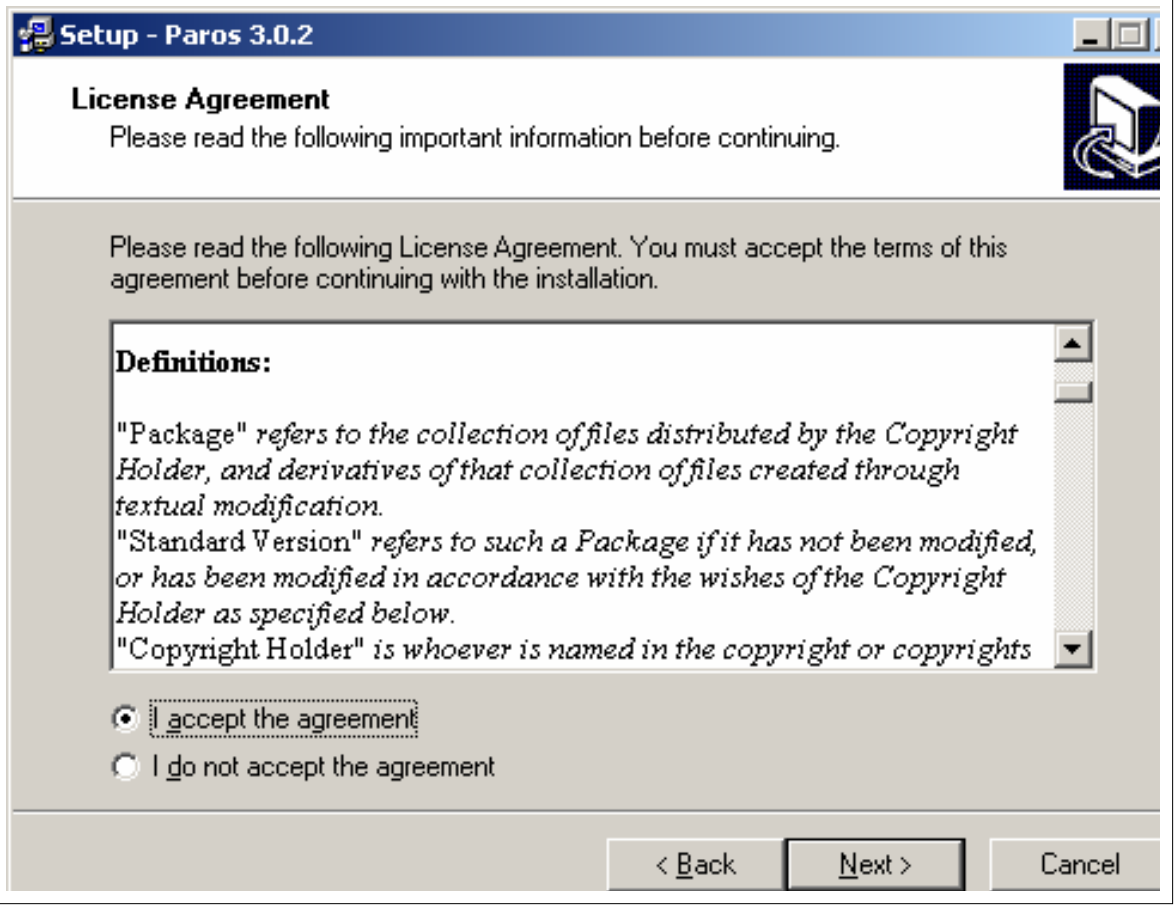
Adams & Sasse: Users are not the enemy

„Subversives“ Verhalten

- Problem: Laptop borgen. Deadline: in 2 Stunden.
- Gastzugang?
  - Wie geht das?
  - Account “Gast” gesperrt
  - Wo steckt der Admin?
- Ergebnis: Gastzugang mit schlechtem Passwort
  - Problem gelöst
- Es hätte schlimmer kommen können

Fraunhofer SIT Institut Sichere Informations-Technologie

Informierte Entscheidung



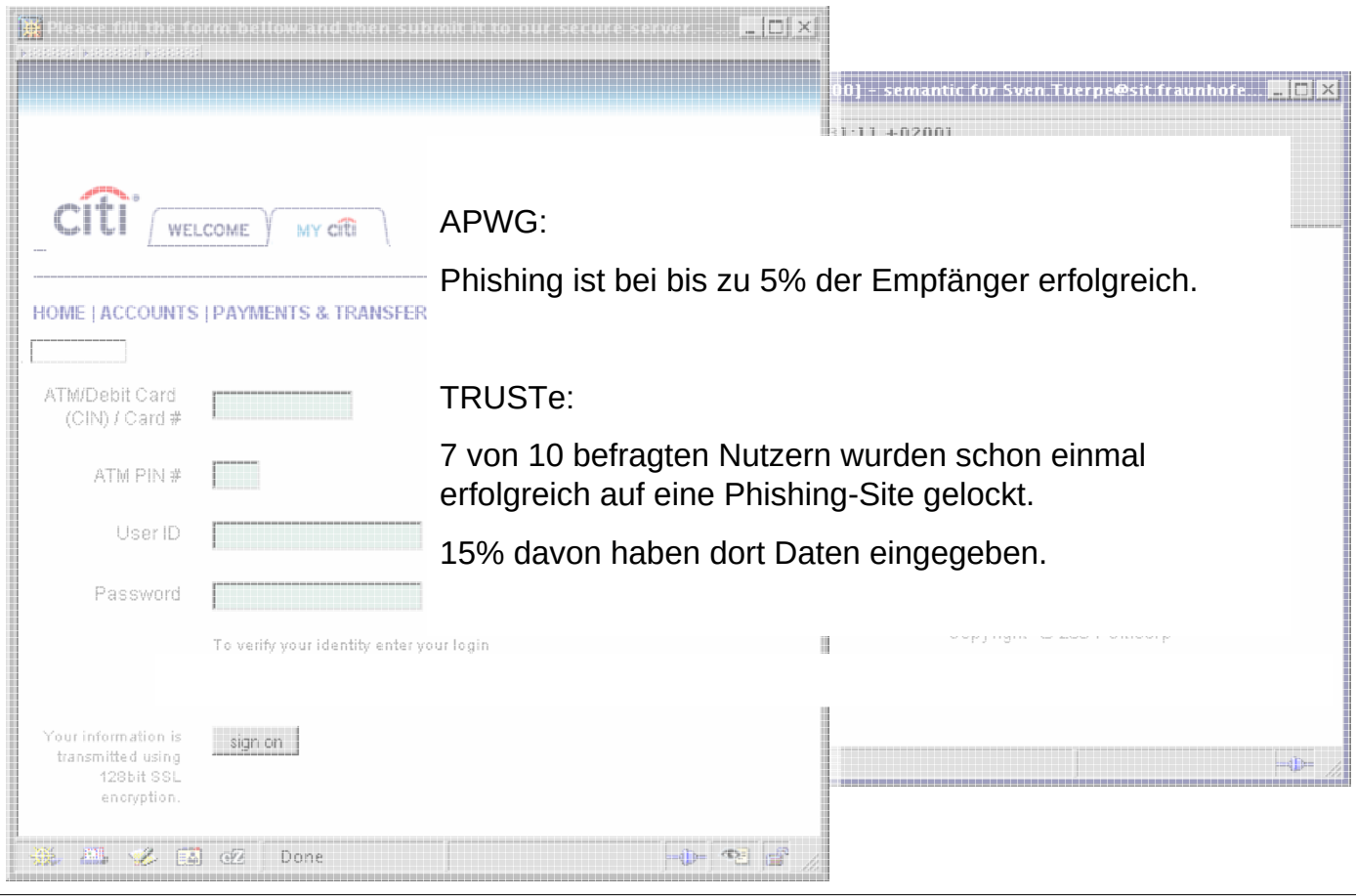
Informierte Entscheidung

Friedman, Howe & Felten:
Informed Consent in the Mozilla-Browser

- Cookie-Verwaltung als Sidebar im Browser
  - Farbcodierung für Herkunft
  - Unmittelbare Eingriffsmöglichkeit
- Vorgänge werden sichtbar und verständlich gemacht
- Kein Zwang, keine Störung

Fraunhofer SIT Institut Sichere Informations-Technologie

Phishing: Betrug mit gefälschten E-Mails und Webseiten



APWG:

Phishing ist bei bis zu 5% der Empfänger erfolgreich.

TRUSTe:

7 von 10 befragten Nutzern wurden schon einmal erfolgreich auf eine Phishing-Site gelockt.

15% davon haben dort Daten eingegeben.

Problem: Tatsächliches vs. formal korrektes Nutzerverhalten

- Formal korrekt:
  - Sicherheitszertifikat prüfen
- Tatsächlich:
  - Aussehen
  - Gewohnheit
  - Erwartungen
  - Nur Abweichungen fallen auf

Fraunhofer SIT Institut Sichere Informations-Technologie

Es gibt kaum technische Gegenmittel

„Die erste grundlegende Sicherungsinstanz ist der bloße Anschein. Sofern Sie große Abweichungen zu den erwarteten Informationen sehen, könnte hier eine Manipulation im Hintergrund stehen“

http://www.1822direkt.com/onlinebanking/sicherheit_pintan.html

→ Was tun Anbieter, um ihre Kunden bei der Erkennung zu unterstützen?

Fraunhofer SIT Institut Sichere Informations-Technologie

Studie: Was tun Banken, um ihre Online-Banking-Kunden bei der Phishing-Abwehr zu unterstützen?

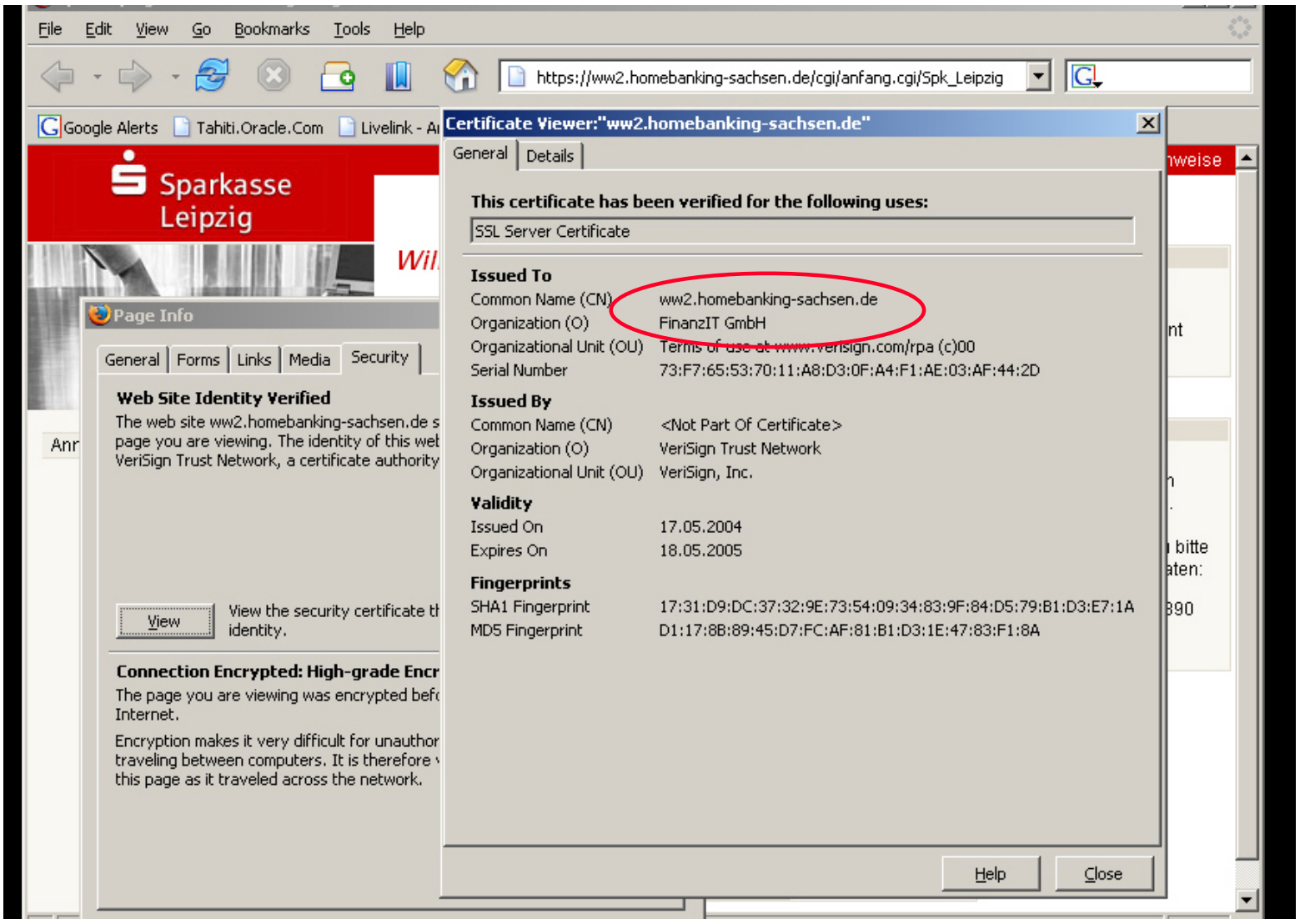
- Vergleichstest: Websites von 12 Banken
  - Allgemein zugängliche Informationen
- Heuristische Bewertung:
  - Technik
  - Homebanking-Software
  - Kundeninformation
- Annahme: idealer Nutzer
- Punkte für erfüllte Kriterien

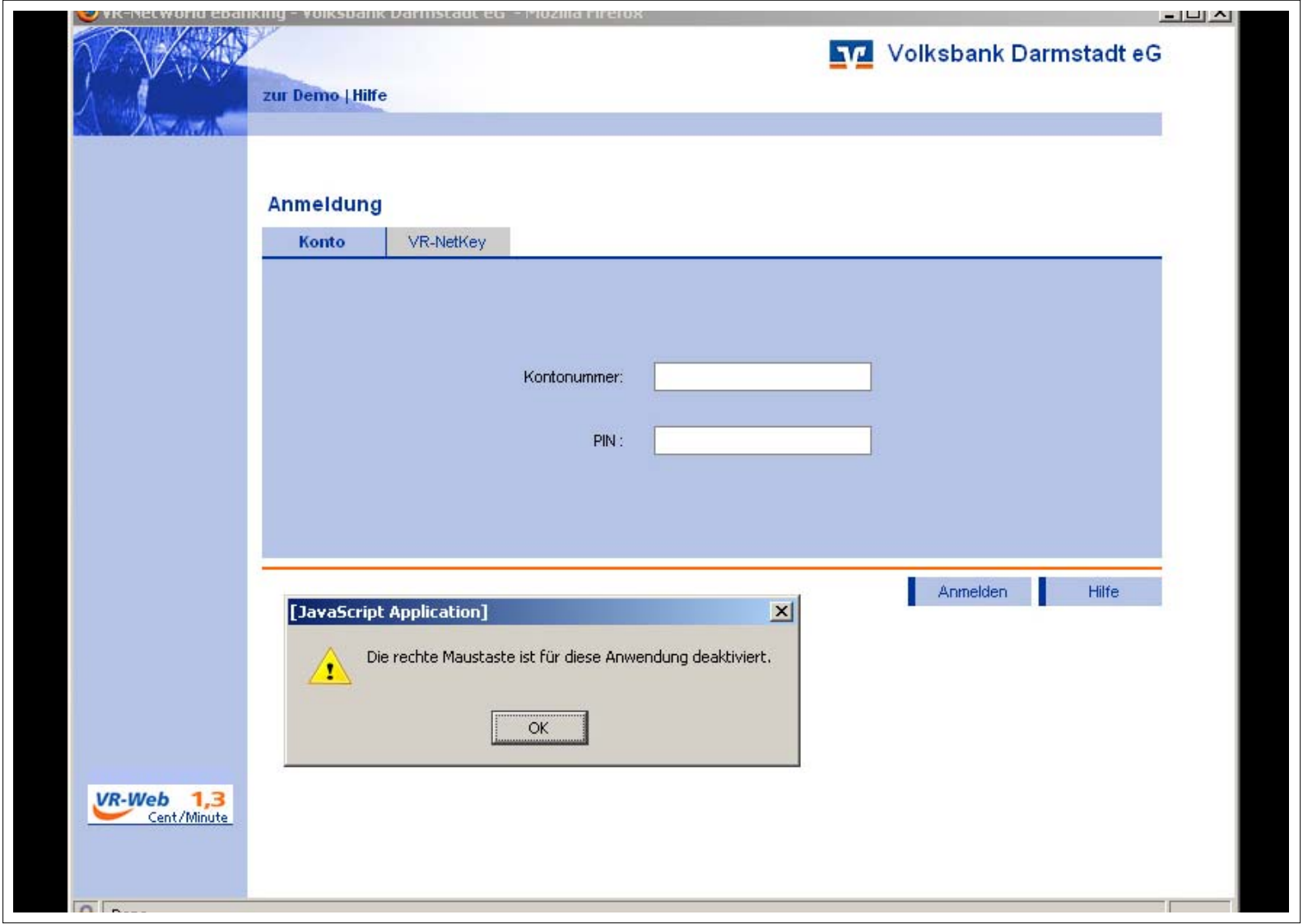
Fraunhofer SIT Institut Sichere Informations-Technologie

Kategorie Technik

- Konsistenz der URLs
- URL sichtbar?
- SSL vor dem Login?
- Zertifikat auf die Bank ausgestellt?
- Doppelt gewichtet: maximal 8 Punkte

Fraunhofer SIT Institut Sichere Informations-Technologie


File Edit View Go Bookmarks Tools Help
https://ww2.homebanking-sachsen.de/cgi/anfang.cgi/Spk_Leipzig
Google Alerts
Tahiti.Oracle.Com
Sparkasse Leipzig
Page Info
General Forms Links Media Security
Web Site Identity Verified
The web site ww2.homebanking-sachsen.de s
page you are viewing. The identity of this wet
VeriSign Trust Network, a certificate authority
View
View the security certificate th
identity.
Connection Encrypted: High-grade Encr
The page you are viewing was encrypted befo
Internet.
Encryption makes it very difficult for unauthor
traveling between computers. It is therefore
this page as it traveled across the network.
Certificate Viewer:"ww2.homebanking-sachsen.de"
General Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) ww2.homebanking-sachsen.de
Organization (O) FinanzIT GmbH
Organizational Unit (OU) Terms of use at www.verisign.com/rpa (c)00
Serial Number 73:F7:65:53:70:11:A8:D3:0F:A4:F1:AE:03:AF:44:2D
Issued By
Common Name (CN) <Not Part Of Certificate>
Organization (O) VeriSign Trust Network
Organizational Unit (OU) VeriSign, Inc.
Validity
Issued On 17.05.2004
Expires On 18.05.2005
Fingerprints
SHA1 Fingerprint 17:31:D9:DC:37:32:9E:73:54:09:34:83:9F:84:D5:79:B1:D3:E7:1A
MD5 Fingerprint D1:17:8B:89:45:D7:FC:AF:81:B1:D3:1E:47:83:F1:8A
Help
Close


Volksbank Darmstadt eG
zur Demo | Hilfe
Anmeldung
Konto
VR-NetKey
Kontonummer:
PIN :
Anmelden
Hilfe
[JavaScript Application]
Die rechte Maustaste ist für diese Anwendung deaktiviert.
OK
VR-Web 1,3 Cent/Minute

Kategorie Homebanking-Software

- Alternative zum Web
- Wird HBCI unterstützt?
- PIN/TAN?
- Informationen zu Software, Konfiguration etc.?
- 3 Punkte

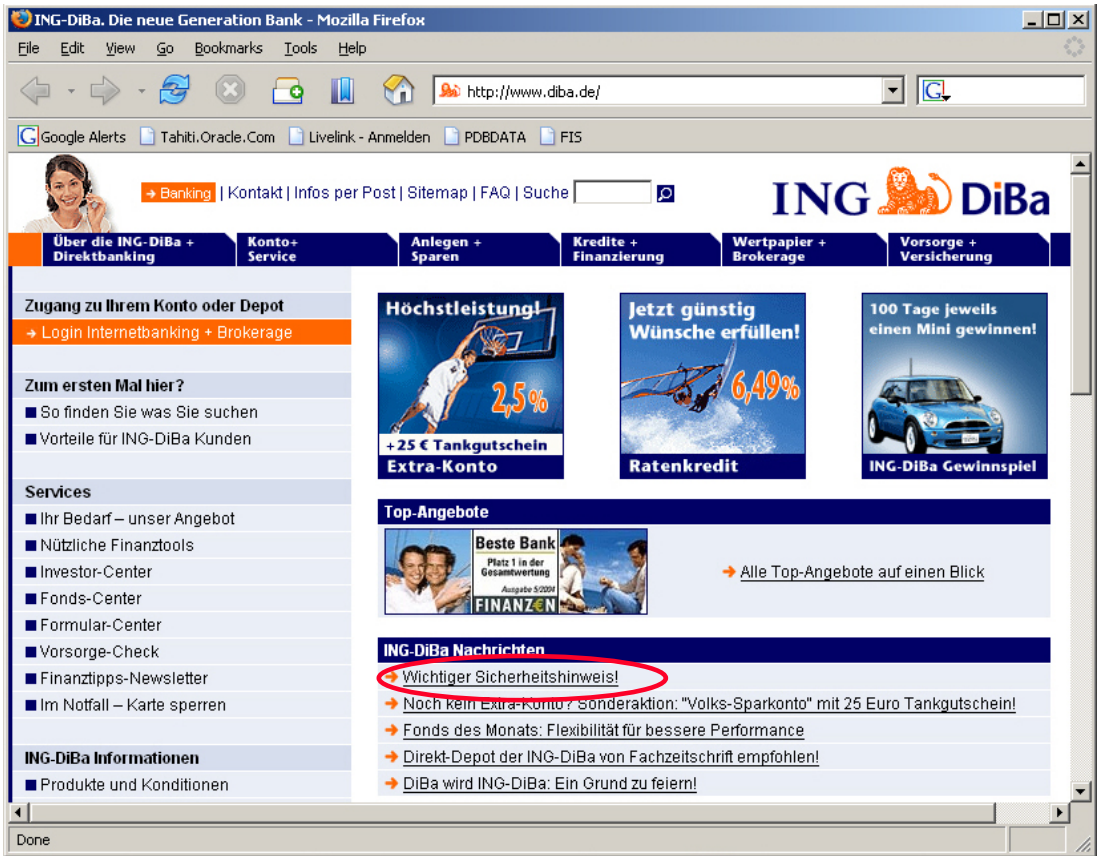
Fraunhofer SIT Institut Sichere Informations-Technologie

Kategorie Kundeninformation

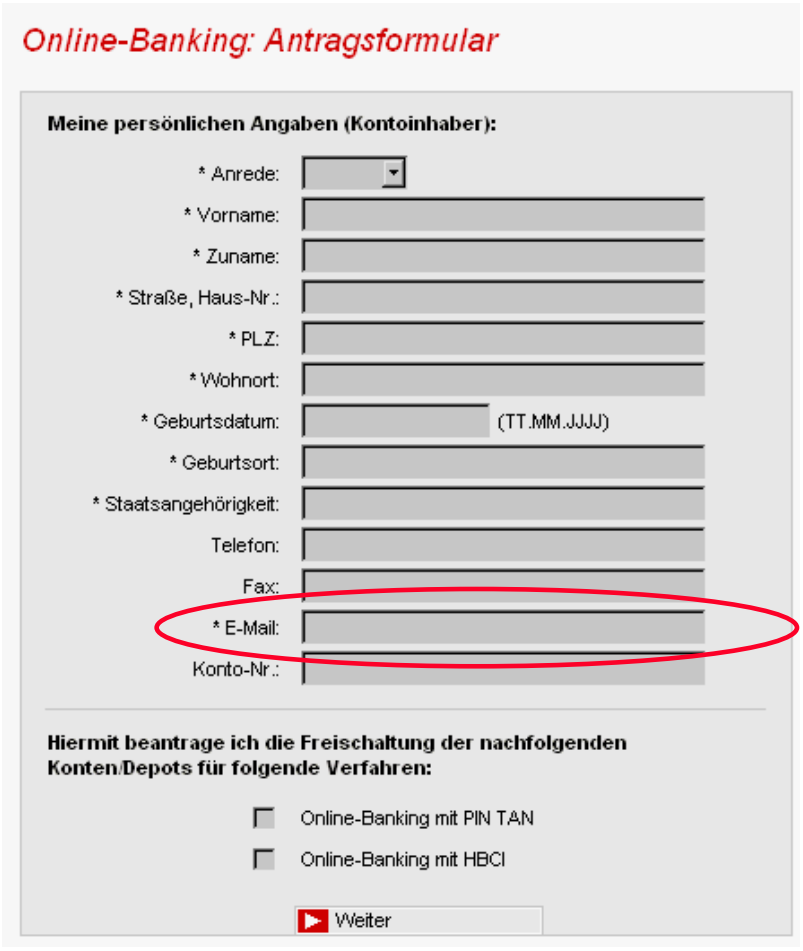
- Informationen über Phishing?
- Kontaktmöglichkeit für Sicherheitsfragen?
- Konkrete Parameter für die Zertifikatsprüfung?
- Formulare: Frage nach E-Mail-Adresse?
- 4 Punkte

Fraunhofer SIT Institut Sichere Informations-Technologie

Wichtiger Sicherheitshinweis!



Neugierig



Phishing-Studie: Ergebnisse

1 x „sehr gut“

0 x „gut“

5 x „befriedigend“

5 x „ausreichend“

1 x „mangelhaft“

Technische Mängel bei 6 Banken (50%)

http://www.sit.fraunhofer.de/german/hps1/phishing.pdf

Fraunhofer SIT Institut Sichere Informations-Technologie

Nicht nur User

OWASP Top Ten:

- Unvalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

Fraunhofer SIT Institut Sichere Informations-Technologie

Sicherheit und Barrierenfreiheit

- Zugang für Nutzer mit Einschränkungen
  - z.B. Blinde
  - z.B. Alte
- Für eGovernment vorgeschrieben
- Behörden *lieben* die digitale Signatur
- Funktioniert das zusammen?

Fraunhofer SIT Institut Sichere Informations-Technologie

Sicherheit und Barrierenfreiheit

- Hürden bei Beantragung und Zertifikatsabfragen
- Medienbrüche bei Erstauthentisierung
- Kartenleser für Blinde schwer zu nutzen
  - Hilfsmittel funktionieren nur für Standard-UI (Tastatur, Bildschirm)
- Accessibility-APIs nicht unterstützt
- Biometrie?
  - Erleichterung vs. vorgegebene Merkmale
- Fraunhofer SIT: Prototyp barrierenfreie Signatur

Fraunhofer SIT Institut Sichere Informations-Technologie

Barrierenfrei?

CAPTCHA:

Completely **A**utomatic **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

Fraunhofer SIT Institut Sichere Informations-Technologie

Fazit

- Benutzer funktionieren nicht
- Technik muss damit zurechtkommen
  - Nur das verlangen, was Benutzer leisten können
  - Restrisiko
- Fahrlässigkeit, Schuld, Haftung?
- Sicherheit nicht auf Verhinderung beschränken
  - Reaktion auf Vorfälle
  - Regelungen für den Schadensfall

Fraunhofer SIT Institut Sichere Informations-Technologie

Pläne

- Schwieriges Thema
- Forschung:
  - Erste Ansätze
  - Kleine Community
- Im Alltag: Viele Probleme, kaum Lösungen
- NoE im 6. Forschungsrahmenprogramm?

Fraunhofer SIT
Institut Sichere Informations-Technologie

Kontakt

Fraunhofer Institut für Sichere Informationstechnologie

Sichere Prozesse und Infrastrukturen

Sven Türpe

Rheinstraße 75
D-64295 Darmstadt

Telefon: +49-6151-869-4238
Telefax: +49-6151-869-224

mail: tuerpe@sit.fraunhofer.de
www: http://www.sit.fraunhofer.de

Fraunhofer SIT Institut Sichere Informations-Technologie