Informatik

Sicherheit

Irene Rothe

Zi. B 241
irene.rothe@h-brs.de
Instagram: irenerothedesign

Umfrage

Hatten Sie schon einmal irgendwie mit Informationssicherheit zu tun?

Sicherheit…

…Freiheit von unvertretbaren Risiken

Beispiele

• 2022: Universität Essen (Daten veschlüsselt, Zugriff auf digitale Unterrichtsmaterialien und die An- und Abmeldefunktion zu Prüfungen lahmgelegt, Daten in Darknet aufgetaucht)

•2020: Universität Gießen: Emotet (interessiert an Forschungsergebnissen + Erpressung mit Geld, Weiterentwicklung eines Online-Banking-Trojaners, Verbreitung über echtaussehende Spam-emails mit Anhängen wie .pdf.exe., Man-in-the-Browser-Angriff)

• seit 2011 bis heute: Stuxnet (Wurm via Stick): Störung von Urananreicherungsanlagen

• 2009: Anti-Virus (Verschlüsselungstrojaner): verschlüsselte Windows-Dateien

• 2004: SASSER (Wurm): schaltete Rechner ab

• 2000: I LOVE YOU (Wurm)

• 1999: Melissa (Virus)

• Bundestrojaner

• 1994: „Hackerjagd im Internet“: Jagd nach dem Eindringling Mitnick

• 1986: „Kuckucksei“ Clifford Stoll

Sicherheit im Internet

- Was sind Besonderheiten am Internet bzgl. Angriffen?
- Welche Entschlüsselungsangriffsarten gibt es?
- Was sind Viren, Würmer und Trojaner im Zusammenhang mit dem Internet?
- Warum kann in Computern eingebrochen werden, trotz all der sicheren Verfahren wie RSA?
- Was ist das menschliche Problem bzgl. Sicherheit im Internet?

Bemerkung: Gegen Stromausfall, Erdbeben … helfen nur Backups, Backups,…

Das Internet

Das Internet ist ein sehr komplexes System

- mit Millionen von Computern,
- mit zahlreichen Softwareprogrammen pro Computer,
- wo jede Menge Programme übers Netz agieren und
- Eingaben von Millionen Benutzern zur gleichen Zeit entgegen genommen werden.

Eigenschaften von Systemen:

- sie interagieren miteinander und dann entstehen noch größere Systeme.
- sie besitzen emergente Merkmale (es passieren Dinge, die man nicht erwartet, aber positiv sind)
- es entstehen unerwünschte Beigaben.

Motive

Angreifer	Motive
Internetbenutzer	hat Spaß, emails anderer Leute zu lesen
Hacker	will Sicherheitssystem auf die Probe stellen, Daten stehlen
Geschäftsmann	Interesse an Konzepten der Konkurrenz
Mitarbeiter	rächt sich an ehemaligem Arbeitgeber durch ein „Abschiedsgeschenk“
Buchhalter	will Geld für sich abzweigen
Betrüger	klaut Kreditkartennummern aus Online-Geschäften, verkauft kopierte CDs und DVDs
Spion	interessiert sich für die militärische Stärke
Terrorist	Systemzerstörung

Das große Problem

Sicherheitstheorie
Kryptografie
Firewalls
Einbruchserkennung

Sicherheitspraxis

In der Theorie besteht kein Unterschied zwischen Theorie und Praxis, in der Praxis besteht wohl einer. (Yogi Berra)

Besonderheiten bei Angriffen im Internet

- ein Pfennig von jedem Sparkonto abheben (ohne Computer undenkbar)
- automatisches Passwort knacken mit Softwareprogramm
- Computerdaten können einfach durchsucht werden, um Liebhabereien von Menschen herauszubekommen: Verkauf dieser Daten für Geld (das Neue ist nicht, dass solche Daten vorhanden sind, sondern dass sie so einfach zu erhalten sind), versenden von Spams
- Angreifer müssen sich ihrem Opfer physikalisch nicht nähern (Mitnick benutzte Adresse aus Israel)
- erfolgreiche Hackertechniken sind total einfach verbreitbar (nur der aller erste Hacker muss Ahnung haben)
- es gibt Sites, wo beschrieben wird, wie man Computerviren bauen kann
- Übeltäter brauchen wenig Sachkenntnisse, um Erfolg zu haben

Entschlüsselungsangriff: Schlüsselrekonstruktion aus Klartextkopie und Chiffretext

- z.B. haben MS emails bekannte Kopfteile (Headers), daraus ist dann Rekonstruktion möglich

- z.B beginnen alle MS Worddateien mit den gleichen Bytes

- auch Enigma wurde so geknackt (Wetterbericht stand immer am Anfang)

- Chosen-Plaintext-Attacke: man schleust gefakte Nachricht ein und hofft, den Chiffretext zu bekommen

Entschlüsselungsangriff:

Brute-Force Attacke

• Geheimtext knacken durch Ausprobieren **aller** möglicher Schlüssel (Computer arbeiten ja immer brav), auch Wörterbuchangriff genannt (hilft bei 80% aller Passwörter)

• funktioniert für **jeden** Algorithmus

• 1999 Deep Crack Project: 250 Milliarden Schlüssel pro Sekunde
• hier muß man Schlüssel also groß genug wählen, wenn Schlüssel ein Bit länger ist, wird Entschlüsselung gleich doppelt so schwierig

• Maschinen, die eine Milliarde mal schneller sind als Deep Crack, brauchen für 128 Bit Schlüssel eine Million Jahre, um alle Schlüssel auszuprobieren

Über Passwörter: https://www.youtube.com/watch?v=jtFc6B5lmIM

Entschlüsselungsangriff: Ausnutzung von Unterschied zwischen Theorie und Praxis

- Kryptografie ist nur die Theorie
- Einbrecher benutzt nicht Schlüsselbund, sondern benutzt Bohrer oder Hammer
- Passwörter haben in der Regel eine niedrige Entropie (Unordnung)
- Problem der Zufallszahlenerzeugung (beruhen oft auf Passwörtern)
- private Schlüssel werden durch Passwörter geschützt
- Qualität der Algorithmen schwer nachprüfbar (dauert sehr lange und ist sehr kompliziert)
- es besteht immer die Gefahr, dass jemand eine neue Berechnungsart findet, die den Verschlüsselungsalgorithmus zunichte macht

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Alice gibt Bob Papiere und Autoschlüssel
2. Bob gibt Alice Scheck
3. Alice löst Scheck ein

Wo kann hier betrogen werden?

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Alice gibt Bob Papiere und Autoschlüssel
2. Bob gibt Alice Scheck
3. Alice löst Scheck ein

Wo kann hier betrogen werden?

SCHECK NICHT GEDECKT!!!

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Bob stellt Scheck aus und gibt ihn der Bank
2. Bank zertifiziert Scheck, dass er gedeckt ist
3. Alice gibt Bob Autopapiere und Autoschlüssel
4. Bob gibt Alice zertifizierten Scheck
5. Alice löst Scheck ein

Wo kann hier betrogen werden?

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Bob stellt Scheck aus und gibt ihn der Bank
2. Bank zertifiziert Scheck, dass er gedeckt ist
3. Alice gibt Bob Autopapiere und Autoschlüssel
4. Bob gibt Alice zertifizierten Scheck
5. Alice löst Scheck ein

Wo kann hier betrogen werden?

Autopapiere nicht echt!!!

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Alice gibt Papier an Anwalt
2. Bob gibt Scheck dem Anwalt
3. Anwalt zeigt Scheck der Bank
4. Anwalt überprüft Papiere
5. Anwalt gibt Alice den Scheck und Bob die Papiere

Schutz mit Protokollen

Beispiel ohne Computer: Alice verkauft Bob ein Auto:

1. Alice gibt Papier an Anwalt
2. Bob gibt Scheck dem Anwalt
3. Anwalt zeigt Scheck der Bank
4. Anwalt überprüft Papiere
5. Anwalt gibt Alice den Scheck und Bob die Papiere

ANWALT IST EIN BETRÜGER!!!

Internetprotokolle

- **SSL**: Secure Socket Layer sichert WWW-Verbindungen (verschlüsselte Informationen an Websites verschicken)
- **PGP**: Pretty Good Privacy sichert e-mails (durch zufällige Primzahlen wird mit RSA verschlüsselt)
- **SET**: Secure Electronic Transaktion - Sichert Internet-Kreditkartentransaktionen

Ist nun alles sicher?

- Vertraue ich der Bank?
  → Fähigkeit der Bank ordentliche Sicherheitssoftware zu besitzen

- Vertraue ich dem Algorithmus (RSA)?
  → ausreichende Schlüssellänge ist wichtig (1024Bit und mehr)
  → es gibt bis jetzt keinen Grund, RSA nicht zu trauen

- Vertraue ich meinem Computer?
  → Viren- und Wurmsuche, Suche nach Trojanern

- Vertraue ich mir selbst?
  → Aufmerksamkeit bzgl. Instruktionen, nicht zu leichtsinnig OK klicken, iTans/Handy sicher aufbewahren

Problem der Protokolle

- Wie überprüft man den Algorithmus von Protokollen?
- man kann nur aus fehlgeschlagenen Versuchen lernen
- Überprüfung von Experten (ABER: Welcher Arzt ist wirklich gut?)
- Beispiel: PPTP von MS mit eigenen Authentifikationsalgorithmus und eigener Schlüsselerzeugung ist schwach
- alles Neue ist erst einmal verdächtig (möchte ich beim Arzt das Meerschweinchen sein?)
- neue Kryptografie = Quacksalberei?

Identifizierung und Authentifizierung

- Kontakt mit Computern: gewährt dem einen Zugang und hält andere ab - beides zusammen ist nicht ganz so einfach (Tür ist offen oder zu)
- wird geregelt über Passwörter + login und PINs + login (ähnlich wie Kontonummer und Kartenbesitz)
- System ist so sicher, wie das schlechteste Passwort
- Widerspruch bei Passwörtern: es soll leicht merkbar sein, dann ist es nicht wirklich zufällig ODER es ist sehr zufällig, dann klebt man es an seinen Bildschirm

Angriffe auf vernetzte Computer

- **Viren**: passiv, benötigen Wirt
- **Würmer**: aktiv, vermehren sich selbstständig
- **Trojaner**: geben sich als harmlose Datei aus

Angriffe auf vernetzte Computer: Viren

- winzig kleiner Krankheitserreger, vermehren sich nur in geeigneter Wirtszelle
- Computervirus: Kette von Code, der sich an ein Programm ranhängt, Wirtszelle wird vom Virus dann so verändert, dass sie Kopien an andere Programme ranhängt
- Verhalten sich ***passiv***, das heißt jemand muss etwas tun, damit sie Schaden auslösen
- 1983 Fred Coven: 1. Virus zum Demonstrieren des Konzepts, weil niemand ihm glaubte
- **Ziel**: Verbreitung, nach Computerneustart weiter arbeitsfähig, nerven durch Netzauslastung, Datenzerstörung, Festplattenformatierung, Dokumente ins Internet versenden (SPAM), Dateisystemverschlüsselung
- **Virenbeispiele**: Tschernobyl-Virus (1986), Melissa (1999) via Outlook, XM/Compat-Virus (1998)

Virenschutz

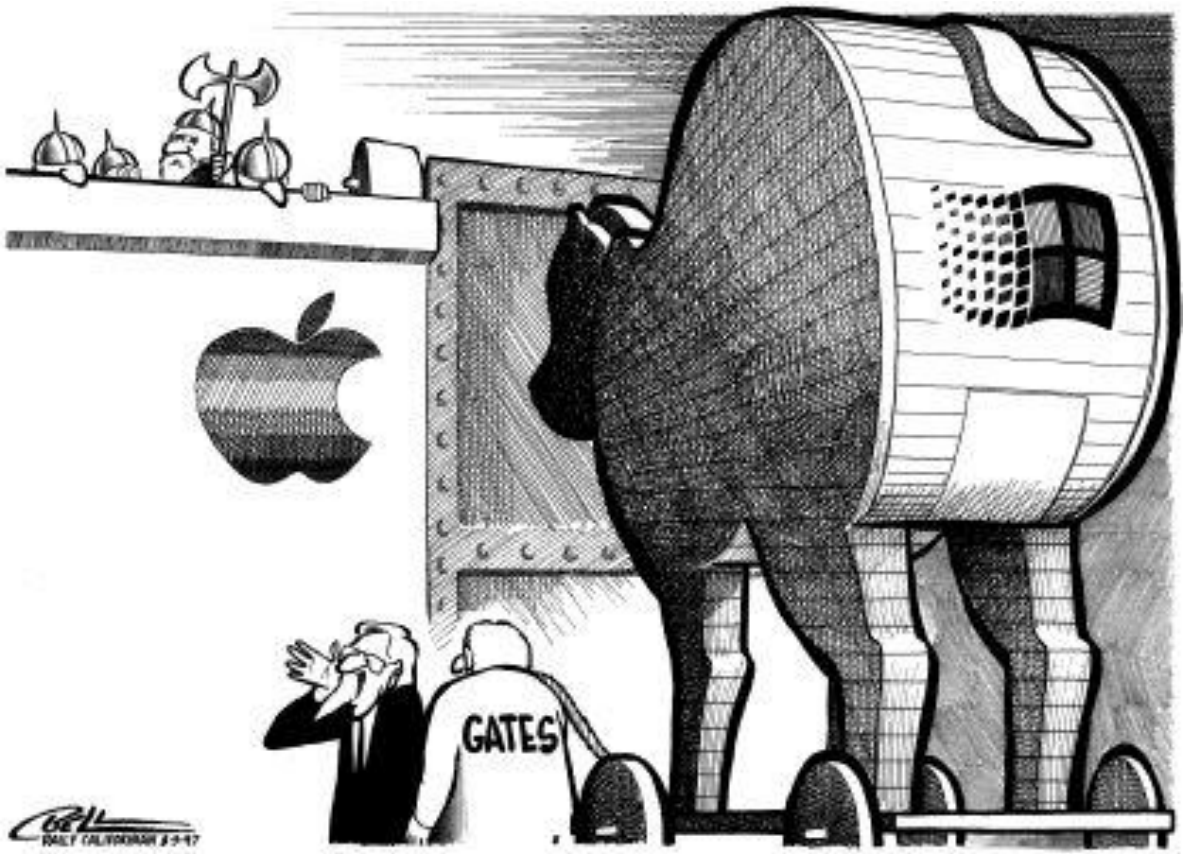
- Antivirenprogramme: scannen aller Dateien, verwalten Datenbank mit Viren-Footprints, desinfizieren Dateien, hängen aber immer hinterher

- Sicherer Kern bei Betriebssystemen (großes Forschungsthema): umso kleiner, desto weniger Fehler (UNIX), heute oft Kernelaufblähung (sinnlose Funktionalität mit root-Berechtigung, z.B. Windows NT - Druckertreiber)

Angriffe auf vernetzte Computer: Würmer

- selbstreplizierendes Programm
- versteckt sich nicht in anderen Programmen
- wandert durch Computernetze, verhält sich also ***aktiv***
- 1988 Morris kreierte einen Internet-Wurm, der 6000 Computer zum Absturz brachte ("Kuckucksei" von Clifford Stoll)
- Wurm startet auf einem Rechner und versucht dann mit allen möglichen Techniken übers Netz in andere Computer reinzukommen, wenn der Wurm Glück damit hatte, schickt er eine Kopie von sich selbst dorthin
- erzeugt nicht direkt Schaden, sondern überfordert das Netz
- Beispiel: ILOVEYOU (2000)-Makrovirus: ILOVEYOU.txt.vbs,
- SASSER (2004)
- Würmer sind heute „moderner“ als Viren

Trojanische Pferde



"He says he comes bearing gifts!"

Angriffe auf vernetzte Computer: Trojanische Pferde

- Programme mit ***versteckter*** (in der Regel bösartiger) Funktion
- ***tarnen*** sich als harmloses Programm (Animation, Bild) und tun so, als ob sie gut wären (BSP: Backdoor des Programmierers)
- werden oft von einem Wurm im Anhang transportiert
- sie transportieren und verbreiten sich nicht selbst
- nutzen ***Sicherheitslücken*** installierter Software aus
- können die Tastatur überwachen, um Passwörter oder Kreditkartennummern zu bekommen und diese dann weiter zu senden, Computeröffnen für Fernzugriff (Möglichkeit des Verschickens von SPAM)
- Regierungen benutzen trojanische Pferde zur Überwachung (Bundestrojaner 2006)

Beispiele von Würmern aus jüngster Zeit

- **SQL-Slammer (2003):** infiziert binnen einer halben Stunde 75000 Rechner auf denen Microsoft SQL läuft, verstopfte Internetleitungen, erzeugt von Einzelperson
- **Storm Worm (2007):** kommt in emails mit netten Betreffzeilen, macht Rechner zu Bots (Marionette) für SPAM-Mail-Sendungen, organisierte Kriminalität
- **Stuxnet (2010):** sabotiert Industrieanlagen, z.B. Kraftwerke, kommt via USB-Stick, Urheber vermutlich Geheimdienste

Andere Angriffsmöglichkeiten

- Versuch URLs umzuleiten durch Beeinflussung von Ergebnissen von Suchmaschinen (z.B. eBay „Dieser billige Pulli (nicht Prada, nicht Armani) ist rot.“)
- Typo-Piraten: Websitesnamen sehr ähnlich zu viel genutzter Seite, wie Google, und dann Erhalt einer Pornoseite (BSP: 2007 Dresdner Bank)
- Hausbesetzer: Registrierung von Domainnamen, um sie später teuer zu verkaufen (Frage: Haben Sie schon die Domain auf Ihren Namen gekauft?)
- Hack auf Router: Hacker C teilt Router mit, dass kürzester Weg von A und B immer über C geht, danach Durchschnüffeln aller Pakete

Abwehrmaßnahmen

- **Firewalls**: Computer am Eingang eines internen Netzwerkes: halten Eindringlinge fern und erlauben autorisierten Benutzern den Zugang, sind nutzlos gegen einen bewaffneten Angriff von innen (70 % aller Angriffe kommen von innen)
- **Einbruchserkennungssystem**: Überwacher, der nach verdächtigen Verhalten Ausschau hält: so überprüfen auch Kreditkarten-Firmen alle Transaktionen, sollten während des Angriffs warnen, eine Diagnose stellen und Vorschlag zu Hilfemaßnahmen nennen, Problem: falsche Alarme
- **Netzwerküberprüfung** nach Schwachstellen, Scanner simulieren Angriffe
- **Kopierschutz**: Code, der kopieren verhindern soll, dies ist unmöglich umsetzbar, Hacker können alles außer Kraft setzen, Hersteller kann die Arbeit eines Hackers nur erschweren - was aber der Hacker liebt)

Alles besteht aus Software und alle Software ist fehlerhaft! (1996 Ariane 5 Absturz, 1999 Marssonde weg)

Das menschliche Problem

- Art wie Menschen Risiken wahrnehmen (oft ignorieren Menschen Fehlermeldungen: „Ach, die rote Lampe leuchtet doch immer“)
- Umgang der Menschen mit Situationen, die sehr selten vorkommen
- Problem mit Benutzern, die Computern vertrauen
- Mühe, Menschen zu intelligenten Sicherheitsentscheidungen zu bewegen (Guckt man sich die Fenster bei Geldüberweisungen denn genau an? Man klickt immer ganz schnell OK!)
- böswillige Insider (wer ein Sicherheitsprogramm schreibt, kann sich selbst immer eine Hintertür (back door) lassen)
- Social Engineering: hilfsbereite Menschen (Hacker gehen aufs schwächste Glied) Frage: Wie verleitet man Menschen, einen Anhang zu öffnen?

Verwundbarkeitslandschaft

- Mit was rechnet man?
- Wie weit gehen Angreifer?
- Flugzeugüberwacher hätten nie an die Möglichkeit eines 11.9.2001 gedacht (Angreifer wird sich ja wohl nicht sich selbst zum Absturz bringen)
- Hacker bieten Hack-Tools auf Websites an, aber oft ist in diesen ein Zugang für sie selber noch vorhanden: Poetische Gerechtigkeit (Aristoteles)

Sicherheit mit **systemischen** Ansätzen

Menschen wollen und können keine Algorithmen ausführen, deshalb sind Sicherheits*anleitungen* für Menschen sinnlos. Algorithmen sind für Maschinen.
Es gibt technische Mängel, menschliches Fehlverhalten, organisatorische Mängel.

→ Deshalb…Systemtheorie: mit Menschen agil diskutieren, wie es besser werden könnte und sinnvoll ist und alle Bock drauf haben

Besonderheiten:

- Wirklichkeitskonstruktion (Keine Eindeutigkeit von Beobachtungen, da subjektiv/ Keine Eindeutigkeit von Erklärungen und damit Unsicherheit über Entscheidungen, Beobachter(in) wählt für ihn relevantes Merkmal der Unterscheidung und konstruiert daraus eine für SIE oder IHN plausible Erklärung)
- Lebende Systeme (kreisförmige und rekursive Kausalität, bei der Systeme ihre eigenen Grenzen und Strukturen durch interne Prozesse aufrechterhalten/ Keine direkte Anweisung möglich/ nicht vorhersehbar, da lebende Systeme adaptive und dynamische Prozesse haben/ Sehr hohe Komplexität/ Paradoxien/ Hohe Selbstreferenz)

Übung

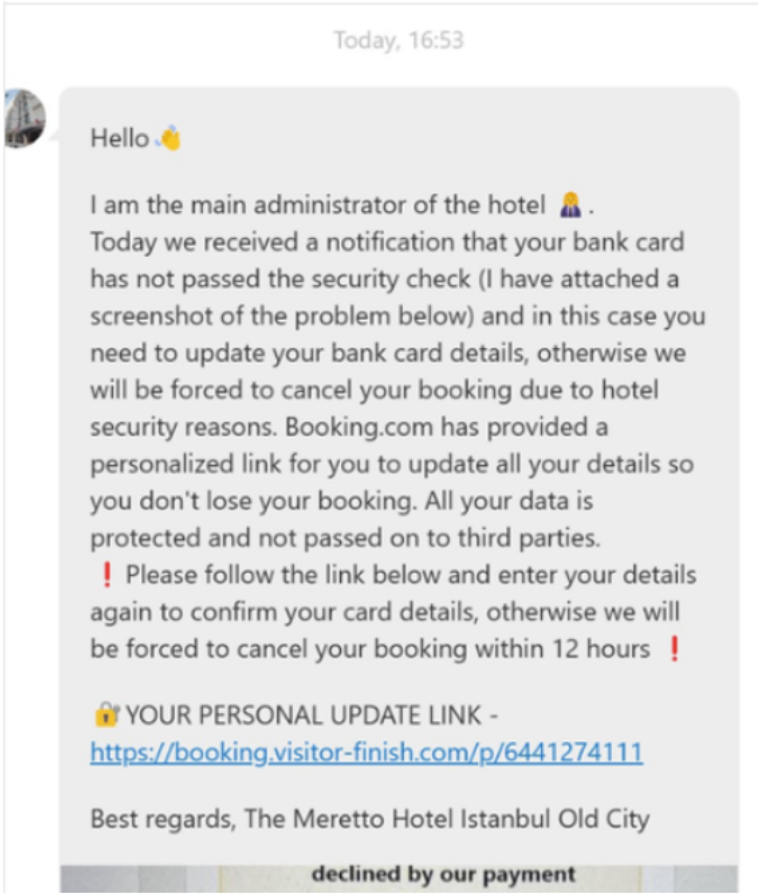
- Wer ist schuld beim Öffnen einer schlimmen email?

- Haben Sie weitere Beispiele für die unterschiedliche Ursachenzuschreibung eines IT-Schadens?

Übung

(Beobachtung) = Aufmerksamkeit: Social Engineering

Was ist hier falsch?



Eventuell: Quiz Petra Einführung

Sicherheitsmanagement - Zusammenfassung

- Informationen sind Daten mit ‚Kontext'.
- Sicherheit als „Abwesenheit von Risiko"
- Informationssicherheit strebt nach „Vertraulichkeit, Integrität und Verfügbarkeit"
- Informationssicherheitsmanagementsystem kann nicht wie Maschine gesteuert werden! Es ist ein lebendes System.
- verschiedene Wirklichkeitskonstruktionen (Beobachten, erklären und bewerten) aus verschiedenen Perspektiven

Umsetzung

- schrittweise
- kontinuierliche Erprobung einzelner Veränderungen
- mit anschließender Nutzenbewertung
- mit kollegial-selbstorgansierten Führungs- und Organisationsprinzipien

Der einzig sichere PC

… liegt 100 Meter unter der Erde ohne Strom und Zugangsmöglichkeiten durch Menschen begraben.

Bester Schutz für den Heimgebrauch

- Backups
- alternative Betriebssysteme zu Windows (z.B. alle Bankgeschäfte auf Linux)
- Alternative Webbrowser (Firefox, Opera)
- nie emails öffnen, die von unbekannten Absendern kommen (manche Viren sind schon gefährlich bei der Outlookvorschau), schon gar nicht Anhänge öffnen
- auf alle Fenster achten und gucken, auf was man OK klickt
- gesunde Skepsis gegenüber Unbekannten haben

Kurze Bemerkung zu Bankautomaten und KK

- **Bankautomat**: keine Verschlüsselung der Daten nötig, nur Authentifikation (PIN und Magnetstreifen), Karte muss physisch vorhanden sein, Limit 500 Euro

- **Kreditkarte**: physisch aufwendig, wenn gestohlen, gleich auf schwarzer Liste, Programme laufen ständig, die nach verdächtigen Transaktionen rund um die Uhr suchen, ab 5000 Euro sowieso gesperrt

Übung: Safe and Secure Systems

Googlen nach einem Unfall/Unglück, der durch Software verursacht wurde:

- Was ist passiert?
- Was war der Fehler?
- Warum wurde der Fehler vorher nicht gefunden?

Sicherheit - Zusammenfassung

- **Angriffsbesonderheiten**: Unsichtbarkeit, Angriffsautomatisierung
- **Entschlüsselungsangriffe**: Chosen-Plaintext-Attacke, Brute-Force Attacke, Ausnutzung von Unterschied zwischen Theorie und Praxis
- **Angriffsschutz**: durch Protokolle (SSL, PGP, SET)
- **Viren**: Kette von Code, der sich an ein Programm ranhängt
- **Würmer**: selbstreplizierendes Programm, das durch Computernetze wandert
- **Trojaner**: eingebettete Programme, die so tun, als ob sie gut wären
- **Schutz**: Firewalls, Einbruchserkennungssystem, Kopierschutz
- **Das menschliche Problem**: falsche Risikowahrnehmung, zu großes Vertrauen in Computer, hilfsbereite Menschen, Faulheit
- Sicherheit an Menschen anpassen als Prozess mit ihnen zusammen (Mensch mag keine Algorithmen ausführen, dafür hat er Maschinen)

Literatur:

- Clifford Stoll: „Kuckucksei“
- „Hackerjagd im Internet“
- J. Gallenbacher: „Abenteuer Informatik“, Spektrum