



Skript für das Eröffnungsreferat an der 3. Berner Tagung für Informationssicherheit 2000 von Peter Trachsel, ISB.

Sehr geehrte Damen und Herren

Im Namen der Fachgruppe Security der Schweizer Informatiker Gesellschaft

und des Informatikstrategieorgans Bund

darf ich Sie an dieser 3. Berner Tagung für Informatiksicherheit ganz herzlich begrüßen.

Es freut uns, dass Sie so zahlreich erschienen sind!

Unser Dank geht natürlich auch an die Sponsoren dieser Tagung,
nämlich an die Firmen ARTHUR ANDERSON, DIGICOMP und IBM.

Die 1. Tagung 1998 widmete sich dem sicheren „Outsourcing“ von Informatikdiensten,
also eher sicherheitspolitischen und juristischen Aspekten.

Die 2. Tagung vom letzten Jahr ging mit „Schützenswerte Daten in offenen Netzen“
vermehrt auf technische Fragen ein.

Dieses Jahr befassen wir uns nun mit dem „Menschen als Sicherheitsfaktor“,
also den Chancen und Risiken, welche der Mensch als Knoten
eines modernen computergestützten Informationsflusses einnimmt.

Mit dem Menschen einerseits und dem Computer andererseits
treffen zwei äusserst komplexe und zeitvariante Systeme aufeinander,
deren erwünschtes Zusammenspiel
nur beschränkt gesteuert oder kontrolliert werden kann.

Hier der Mensch, welcher zwar meist im Rahmen eines erwarteten Handlungsmusters operiert,
aber mitunter auch emotional, irrational oder bösartig agiert.

Ihm gegenüber der Computer, welcher sich kaum vor menschlicher Willkür schützen kann,
da er selber ein Produkt des Menschen ist.

Es gibt zur Zeit weder prozedurale, technische, organisatorische noch juristische Methoden,
mit denen man vollständig erkennen oder gar ausschliessen könnte,
dass sich der Mensch als Entwickler, Betreiber, Benutzer oder Risikoanalytiker
falsch resp. gefährdend verhält.

Mit dieser Tatsache muss man zur Zeit einfach leben.

Sie wird aber leider oft auch aus Bequemlichkeit oder Mittelknappheit missbraucht
um angemessenen Sicherheitsmassnahmen aus dem Wege zu gehen.

Wir oft musste wir uns schon anhören,

dass Virenschutz, Kryptosysteme, Bildschirmschoner etc. nutzlos seien,

weil sie der Mensch ja eh umgehe,

und zudem finde man klassifizierte oder datenschutzrelevante Informationen

in den Papierkörben.

Solche Argumentation ist falsch und unfair!

Denn es gilt auch hier die Regel,

dass man mit relativ bescheidenen Aufwänden
einen sehr grossen Teil des Risikos reduzieren kann.

Die zu treffenden Massnahmen hängen allerdings sehr stark davon ab
ob man es mit menschlicher Nachlässigkeit, Unwissenheit oder Vorsatz zu tun hat,
ob man Vertraulichkeit, Verfügbarkeit, Integrität und/oder Nachweisbarkeit schützen muss
und ob man proaktiv vorbeugen oder reaktiv korrigieren und beheben will.

Die Informatik-Sicherheitspezialisten müssen zugestehen,
dass sie diesen menschlichen Schwächen
zumindest bis heute meist mit zu technischen Massnahmen begegnet sind.

Auch mittelfristig zumindest scheint sich das kaum zu ändern:
Surft man etwas im Internet und der Literatur herum, wird klar,
dass sich zwar viele Universitäten und auch die Industrie vermehrt mit
der Mensch-Computer-Schnittstelle befassen.

Ehrgeizige Ansätze sind z.B.
die Verbesserung der kognitiven Akzeptanz durch neuartige multimediale Benutzeroberflächen,
der Einsatz KI-basierender Mustererkennung von Computermanipulationen,
die Bestätigung sicherheitsrelevanter Systemaktionen durch eine digitale Signatur,
oder Verfahren eines vom Computer erzwungenen 4- oder Mehraugenprinzips.

Aber wie bereits gesagt,
auch hier handelt es sich fast ausschliesslich um technische Massnahmen.

Meine persönliche Erfahrung der letzten 8 Jahre IT-Sicherheit hat gezeigt,

dass es meist Unwissenheit, Ignoranz oder Stress waren,
welche zu menschlichen Problemen am Computer geführt haben.

Nur in sehr wenig Fällen hatten wir es nachweisbar mit vorsätzlichem Verhalten zu tun.

Und wenn, dann war es in den meisten Fällen der Spieltrieb von
gelangweilten und mehr oder weniger unprofessionellen Hackern, Crackern und Knackern.

Nur ganz selten ging es um Vorsätzlichkeit, bedingt durch Frust oder Gewinnsucht.

Dies allerdings wird sich relativ schnell ändern.

Mit dem Internet steigt das Bedrohungspotential durch

auffallend jugendliche Amateurhacker resp.

deren hohe Vernetztheit und immer mächtiger und zahlreicher werdende

Share- und Freeware-Angriffs-Werkzeuge.

Ich bin überzeugt, dass wir unsere Sicherheits-Tagung

auch einmal schwergewichtig mit Jugendlichen, Kindern, „Kids“

veranstalten könnten.

Sie sprechen in diesen Dingen eine sehr faszinierende Sprache...!

Das Risiko steigt natürlich auch

mit der Verlagerung der ehemals militärischen Bedrohungen

in den Bereich des generellen, also auch zivilen Information-Warfare.

Hier liegt das Gefahrenpotential weniger in der Masse der Angreifer

als in deren Professionalität.

Der Mensch ist also nicht nur Chance,

für seine notabene von ihm selber erstellten Computer,

sondern bleibt ein wachsendes und ernstzunehmendes Risiko.

Dort wo heute technische Massnahmen nicht mehr greifen,
beginnt meist der heikle Umgang mit dem Vertrauen,
das Trust-Management.

Trust-Management muss in Zukunft
vermehrt zentralster Bestandteil eines integralen Sicherheitsprozesses sein.
Dies wiederum bedingt, dass man sich etwas weniger mit Informatiktechnik
und etwas mehr mit psychologischen Aspekten und damit verbunden
mit Massnahmen im Sinne von Sensibilisierung, Motivation, Belohnung etc. beschäftigt.

Wir haben auch dieses Jahr
eine kompetente Referentin und Referenten gewinnen können,
welche in Referaten und dann auch im Podium
auf diese Thematik eingehen werden.

Ich wünsche Ihnen einen spannenden Nachmittag!