

## Kurzreferat zur Eröffnungs-Pressekonferenz zur TeleNetCom 2000

**Rolph Haefelfinger, Präsident der Fachgruppe Security der Schweizer Informatiker Gesellschaft (SI) Tel. 079 419 49 09 E-Mail: har@infosec.ch**

Meine sehr verehrten Damen und Herren

Die Denial of Service Attacken im Februar dieses Jahres und die Untaten des sich seit kurzem explosionsartig verbreitenden „I love you“-Virus haben es wieder gezeigt: Sicherheit in der Telekommunikation und insbesondere im Internet ist ernst zu nehmen. Dies ist auch zunehmend der Fall. Doch bleibt noch einiges zu tun.

- Sicherheit hat nach wie vor einen noch allzu negativen Stellenwert. Sicherheitsmassnahmen sind oft lästig, kosten etwas, sind schwierig durchzusetzen und bieten nie hundertprozentigen Schutz. Es kommt noch hinzu, dass ein gutes Sicherheitsmanagement ganz klare Regeln der Verantwortung voraussetzt, welche in dieser schnelllebigen, von Wechseln geprägten Zeiten schwierig zu definieren, wie auch umzusetzen sind. Die Frage, wer wofür bei den Telekommunikationssystemen - welche heute in allen Lebensbereichen omnipräsent sind - zuständig ist, lässt sich oft nur ungenügend beantworten; oder man macht es sich einfach und überlässt die Verantwortung dem – meist ahnungslosen – Endbenutzer.
- Sicherheitsanforderungen werden bei der Entwicklung von Systemen wohl erfasst, erhalten jedoch in zu vielen Fällen eine zu niedrige Priorität bei der Realisierung. Funktionalität kommt eben vor Sicherheit. (Paradebeispiel: Microsoft Windows!) Die Sicherheit kommt erst später zum Zug, nachdem die ersten nicht trivialen Probleme aufgetreten sind. Nebst unmittelbaren finanziellen Verlusten, die man sich damit einhandelt, ist dieses Vorgehen erwiesenermassen wesentlich teurer. *Sicherheit kostet, keine Sicherheit kostet mehr!*
- Warum wird die Weitergabe von ad personam vergebenen Passwörtern an Dritte – obwohl in entsprechenden firmeninternen Weisungen ausdrücklich verboten - immer noch zu oft ohne irgendwelche Konsequenzen toleriert? Sicherheitsweisungen im Informatikbereich werden in den Firmen noch zu wenig deutlich durchgesetzt und selten geahndet.
- An Hochschulen werden Sicherheitsfragen erfreulicherweise zunehmend thematisiert. Hervorzuheben sind die seit einigen Jahren verfügbaren Nachdiplomkurse und –studien in Informatiksicherheit des Institutes für Wirtschaftsinformatik der Hochschule für Wirtschaft Luzern, welche sich grosser Beliebtheit erfreuen ([www.hsw.fhz.ch/fr\\_weitb.htm](http://www.hsw.fhz.ch/fr_weitb.htm)). Wie kommt es aber, dass es noch Informatiklehrgänge gibt, in denen Sicherheitsaspekte kaum gestreift werden?
- Der Bundesrat und die Wirtschaft haben erkannt, dass die Schlüsselinfrastrukturen wie Energieversorgung, Gesundheits-, Transport- und Finanzwesen, Industrie und Gewerbe, sowie die Verwaltungen der Schweiz durch ihre totale Durchdringung und Vernetzung ganz erheblich von einer intakten Informations- und Telekommunikationsinfrastruktur abhängen. Aus dieser Erkenntnis heraus hat die Wirtschaft Ende letzten Jahres die Stiftung „Infosurance“ gegründet, welche zum Ziel hat: *„Wirkungsvoll und langfristig dazu beitragen, dass die organisatorischen und infrastruktureitigen Voraussetzungen geschaffen werden, um die Nutzung der Informationstechnologien durch Gesellschaft, Wirtschaft, Staat und Wissenschaft jederzeit sicherzustellen.“* Gerne verweise ich Sie auf die Home-

page der Stiftung, aus der Sie weitere Informationen über ihre Ziele und Tätigkeiten [www.infosurance.ch](http://www.infosurance.ch) entnehmen können.

Trotz aller smarterer Technik bleibt der Mensch auch im Umgang mit der Informationstechnologie deren Hauptelement und -risiko. Schon Tacitus soll gesagt haben: „*Der Wille zu schützen ist wichtiger als der Schutz selbst*“.

- Die Entscheidungsträger sind gefordert, die Risiken zu verstehen und diese zu gewichten. Sie sollen auch das Verständnis besitzen die adäquaten Massnahmen zu wählen und Voraussetzungen zu schaffen, damit dieselben effektiv und effizient implementiert und unterhalten werden können.
- Die Endbenutzer der Systeme, d.h. wir alle, müssen die Verhaltensregeln kennen und verstehen und zur Einhaltung angehalten werden.
- Die Informatiker und Telematiker sollen sensibilisiert werden, ihr Bestes zu geben, um mit dem notwendigen und stets à jour gebrachten Wissen das gewünschte Mass an Sicherheit mit optimalen Mitteln zu erreichen.

Fokussiert auf das Management wird die *Fachgruppe Security* am 14. November dieses Jahres ihre dritte „*Berner-Tagung für Informationssicherheit*“ unter dem Thema „*Der Mensch als Sicherheitsrisiko*“ stellen. Ich würde mich freuen, Sie auch dort begrüßen zu können. Zu gegebener Zeit werden Sie das Programm auf unserer Webseite: [www.fgsec.ch](http://www.fgsec.ch) vorfinden.

Die Fachtagungen der nächsten Tage sind hingegen besonders an die Informatiker und Telekommunikationsfachleute gerichtet.

An fünf Halbtagen werden eine Reihe von Fachvorträgen, welche jeweils auf ein bestimmtes Thema eingehen, geboten. Es wurde sehr darauf geachtet, dass die bestens ausgewiesenen Referenten praxisorientiertes Wissen aus verschiedenen Blickwinkeln vermitteln. Es ist uns gelungen, Referenten aus den Lehranstalten, aus der Wirtschaft und von Beratungsfirmen zu verpflichten. Wir haben folgende Themenkreise der Kommunikationssicherheit gewählt:

- *Management von Sicherheitsrisiken*: Die aktuellen Risiken und ihre Trends werden vorgestellt. Es werden rechtliche Aspekte der Kommunikationssicherheit behandelt. Ferner geht es darum, Erfolgsfaktoren und Hemmnisse in der Abwicklung von Sicherheitsprojekten zu kennen.
- *Tools und Lösungsmöglichkeiten*: Es wird auf die Möglichkeiten und Grenzen von Virtual Private Networks wie auf den Betrieb und die Überwachung von Intranets und Firewallsysteme eingegangen. Hier werden auch Hinweise für den praktischen Einsatz von Smartcards gegeben. Ein Referat befasst sich mit den viel gepriesenen jedoch noch wenig realisierten Public Key Infrastrukturen (PKI), und schliesslich kommen noch verschiedenste Aspekte der Digitalen Zertifikate zur Sprache.
- *E-Commerce*: Hier steht die Bedeutung des gegenseitigen Vertrauens zwischen Geschäftspartnern und der sichere Zahlungsverkehr im Internet im Vordergrund. Ferner wird auf Access Management Systeme für ein sicheres E-Business eingegangen.

Spätestens mit dem Aufkommen des E-Commerce musste das einfache Modell der Informationssicherheit, welches bisher nur aus den drei Komponenten Vertraulichkeit, Integrität und Verfügbarkeit (engl. Confidentiality, Integrity and Availability: CIA!) bestand, revidiert werden. Zusätzliche Komponenten wie z.B. die Forderung der Nichtabstreitbarkeit von elektronischen Geschäftstransaktionen und die Authentisierung von Geschäftspartnern müssen neu bei der Verwendung der Informatik und der Telekommunikation entscheidend mitberücksichtigt werden. An dieser Stelle verweise ich auf die dringend fälligen schweizerischen Bestimmungen über die digitalen Signaturen. Diese sind dringend erforderlich, um uns den Wettbewerbsvorteil gegenüber dem Ausland zu wahren.

- *Sicherheit in der Telekommunikation*: Vorgehen und Trends im Risk Management werden angesprochen. Es wird der Frage nachgegangen, ob wir es bei den Hackern mit Verbrechern oder modernen Helden zu tun haben. Dann kommen Anforderungen an Schutzkonzepte gegen die Virenplage zur Sprache. Virtual Private Networks werden als Alternative

zu Stand- und Wahlleitungen vorgestellt. Schliesslich geht es darum, auch effektive „Einbrüche“ in Netzwerke laufend zu erkennen und entsprechende Massnahmen zu treffen (Intrusion Detection).

- *Sicherheit im Internet – Intranet*: Es geht hier um die sichere Einbindung von Internet-Applikationen in die Geschäftsprozesse und um diejenige von Web-Servern. Der Beitrag der Virtual Private Networks zur Sicherheit, wie auch die Sicherstellung der Aktualität und des Management von Web-Sites werden erläutert.

Beachten Sie bitte, dass auch hier ein – an und für sich trivialer Begriff – Einzug in Sicherheitsüberlegungen hält: der Begriff der Aktualität. Als Presseleute ist Ihnen natürlich geläufig, dass es nicht ausreicht, dass Informationen nur zuverlässig, verfügbar und integer sein müssen, sondern mit Recht wird auch gefordert, dass sie dem neuesten Stand der verfügbaren Tatsachen und des Wissens entsprechen.

Der Fachkongress ist als eine „value added“-Leistung zur Messe zu verstehen. Im Wissen darum, dass die Tagungsteilnehmer mehrheitlich nicht alle fünf Tagungen besuchen können, haben wir Themenüberschneidungen eingeplant oder bewusst in Kauf genommen.

Sicherheitsprobleme in der Informatik und in Telekommunikation sind grundsätzlich in ihrer Art nicht neu. Die beiden eingangs erwähnten Zwischenfälle haben ihre Analogien in der übrigen Welt: Denial of Service Attacks kann man mit Sitzstreiks, Viren mit eingespritztem Gift in Lebensmitteln vergleichen. Neu ist allerdings, dass bei Angriffen auf die Informatik mittels Informatik und Telekommunikation:

- Distanzen keine Rolle mehr spielen, d.h. man braucht nicht persönlich dorthin zu gehen, wo etwas erreicht werden soll.
- Vorbereitungen lassen sich völlig unbeobachtet treffen und die Aktionen können zeitgleich an verschiedenen Orten zu einer beliebigen Zeit ausgelöst werden.
- Ein elektronischer Sitzstreik durch einen Einzelnen durchgeführt werden kann. Sind Mitläufer notwendig, so lassen sich dieselben leicht übers Internet mobilisieren.
- Die Kosten sind vernachlässigbar.

Diese Aussagen stimmen nicht gerade optimistisch; wir sollen jedoch bedenken, dass

- Sicherheitszwischenfälle durch unsachgemässe Handlungen und Fehler viel häufiger und kostspieliger sind als solche, welche durch bösartige Energie ausgelöst werden;
- Investitionen in die Sicherheit sich nicht nur auszahlen, indem man u.a. besser schlafen kann, weniger Betriebsunterbrüche, Verluste und Schaden am Image in Kauf nehmen muss. Sicherheitsrisiken wirklich im Griff haben, bedeutet auch die unermesslichen Chancen, die in der Informatik und in der Telekommunikation vorhanden sind, besser nutzen zu können. *Denn beherrschte Risiken bieten Chancen!*

Diese Fachtagungen bieten einen Beitrag, diese Risiken besser zu verstehen und zu managen und damit Chancen wahrnehmen zu können. Zusätzlich zur Wissensvermittlung bietet die Tagung Möglichkeiten Erfahrungen auszutauschen, was insbesondere auch in unserer Fachgruppe Security (FGSec) stets weiter gepflegt werden kann.

Ich habe mich über Ihre Aufmerksamkeit gefreut! Besten Dank!