Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 9

Artikel: Beherrschte Risiken bieten Chancen

Autor: Haefelfinger, Rolph

DOI: https://doi.org/10.5169/seals-876480

Beherrschte Risiken bieten Chancen

Die Denial-of-Service-Attacken im Februar dieses Jahres und die Untaten des sich explosionsartig verbreitenden «I-love-you»-Virus haben es wieder gezeigt: Sicherheit in der Telekommunikation und insbesondere im Internet ist ernst zu nehmen.

ROLPH HAEFELFINGER

Sicherheit hat in unserer Gesellschaft nach wie vor einen allzu negativen Stellenwert. Sicherheitsmassnahmen sind oft lästig, kosten Geld und Zeit, 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 Zeit, schwierig zu definieren wie auch umzusetzen sind. Die Frage, wer wofür bei den Telekommunikationssystemen 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 in der Regel erfasst, erhalten jedoch in vielen Fällen eine zu niedrige Priorität bei der Realisierung. Funktionalität kommt oft vor Sicherheit. Die Sicherheit kommt erst später zum Zuge, 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 immer noch zu oft ohne irgendwelche Konsequenzen toleriert, obwohl dies in entsprechenden firmeninternen Weisungen ausdrücklich verboten wird? 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).
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 umfassende 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 infrastrukturseitigen Voraussetzungen geschaffen werden, um die Nutzung der Informationstechnologien durch Gesellschaft, Wirtschaft, Staat und Wissenschaft jederzeit sicherzustellen» (Homepage www.infosurance.ch).

Der Wille zu schützen ist wichtiger als der Schutz selbst

Trotz aller raffinierter Technik bleibt der Mensch auch im Umgang mit der Informationstechnologie deren Hauptelement und -risiko.
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, das heisst 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 das Thema «Der Mensch als Sicherheitsrisiko» stellen (Programm: www.fgsec.ch).
Sicherheitsprobleme in der Informatik und in der Telekommunikation sind grundsätzlich in ihrer Art nicht neu. Die beiden 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, das heisst, 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. 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. Sicherheitsrisiken wirklich im Griff haben, bedeutet, die unermesslichen Chancen, welche in der Informatik und in der Telekommunikation vorhanden sind, besser nutzen zu können. [13]

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

Quelle
Kurzreferat anlässlich der Pressekonferenz zur TeleNetCom 2000.