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

Band: 74 (1996)

Heft: 12

Vorwort: Sicherheit, Vertraulichkeit und Integrität

Autor: Gysling, Hannes

SICHERHEIT, VERTRAULICHKEIT UND INTEGRITÄT

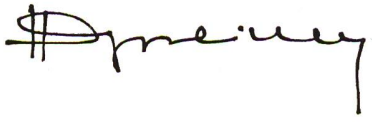
Die Sicherheit im Telekommunikationsbereich ist ein bedeutender Teilaspekt eines weit gespannten Schutzes der Telekommunikation geworden. Dabei umfassen diese Sicherheitsbedürfnisse nicht nur die Abwehr von Missbrauch, Störungen, bis hin zur Zerstörung oder von unerlaubten Zugriffen, sondern auch die Sicherstellung von Telekommunikationsdienstleistungen in Krisensituationen. Der Begriff «Sicherheit» ist unmittelbar mit den Begriffen «Bedrohung» und «schutzwürdige Belange» verknüpft. Sicherheit in der Telekommunikation kann sich daher nach heutigem Verständnis nicht bloss auf den Schutz des Fernmeldegeheimnisses beschränken. Vielmehr ist unter den Oberbegriffen «Vertraulichkeit», «Integrität» und «Verfügbarkeit» auch der Schutz personenbezogener Daten, der Schutz vor unerlaubtem Zugriff Dritter auf programmgesteuerte Telekommunikations- und Datenverarbeitungsanlagen, der Schutz vor Störungen von Telekommunikationsnetzen und der Schutz von Telekommunikations- und Datenverarbeitungssystemen vor Angriffen und Einwirkungen in Katastrophenfällen zu verstehen. Wie dies bewerkstelligt wird, zeigen einige Beiträge in dieser Ausgabe.

Auch der Bürger, der sich keine Verschlüsselungseinrichtung leisten will oder kann, hat Anspruch auf ein gewisses Mass an Schutz seiner Nachrichteninhalte und seiner persönlichen Daten gegenüber Netzbetreibern, Diensteanbietern oder Aussenstehenden. Der Schutz der Telekommunikation ist keine absolute Grösse, die man mit einem definierten Aufwand erreichen kann. Ökonomische, technische und soziologische Aspekte spielen bei der Bewertung der Schutzmassnahmen eine Rolle. Dass es nicht genügt, Betriebsräume abzuschliessen oder Zugangskontrollsysteme zu installieren, beweisen die zahlreichen Drittaufschaltungen an verschiedenen Stellen innerhalb der Netzinfrastruktur und die Missbrauchsfälle durch unternehmenseigenes Personal.

Der Wettbewerb entfaltet im Bereich der Sicherheit nur eine begrenzte Wirkung. Zwar ist unstrittig, dass Wettbewerb im allgemeinen die besten Marktergebnisse für Verbraucher und Wirtschaft erbringt. Wettbewerb versagt, wenn es darum geht, technische Eigenschaften, Dienstemerkmale oder Versorgungsanforderungen, die am Markt nicht oder nicht im erwünschten Umfang nachgefragt werden, durchzusetzen. Die Sicherheit in der Telekommunikation ist heute nur für einen sehr kleinen Teil der Marktteilnehmer ein Kriterium bei der Kaufentscheidung. Der Markt ist somit als Regulativ weitgehend ungeeignet.

Missbrauch in der Telekommunikation zum Zweck ungesetzlicher Aktivitäten ist mittlerweile zu einem sehr einträglichen Geschäft geworden. Der jährliche Verlust, der dadurch verursacht wird, ist, als Prozentsatz vom Gesamtumsatz betrachtet, sicherlich noch klein, beläuft sich aber mit Sicherheit auf mehrere Milliarden Franken. Kein Betrieb kann sich davor absolut sicher schützen. Sogenannte Hacker sind weltweit ständig dabei, zum Teil aus missverstandenem Sportgeist, meistens aber mit krimineller Absicht, mittels ausgeklügelter Methoden das Telekommunikationssystem auf Schwachstellen hin zu untersuchen, um auf diese Weise Zugang zu fremden Datennetzen und Datenverarbeitungssystemen zu erhalten. InfoSecurity News in den USA schätzt, dass zurzeit rund 35 000 Hacker allein in den USA ihr Unwesen treiben. Und je intelligenter die Netze und die Schutzmassnahmen werden, um so raffinierter gehen die Hacker vor. Raymond Cheng, Inhaber des Internet-Providers Asia Connect, beispielsweise, installierte in Malaysia ein Sicherheitssystem, das er nach langen Tests als unüberwindbar einschätzte. Demjenigen, der das System knacken würde, versprach er eine Belohnung von 20 000 Dollar. Bereits wenige Minuten nach Bekanntgabe dieses Angebots brachen zwei Hacker in das System ein und kassierten die Belohnung . . .

Vor diesem Hintergrund, vor allem aber wegen der gegenwärtigen weltweiten Liberalisierung des Telekommunikationsbereichs, wird die Sicherheitsfrage das heisse Thema der nächsten zehn Jahre.



Hannes Gysling