DEUTSCHER PRÄVENTIONSTAG

Prävention durch Informationssicherheit

von

Ansgar Heuser

Dokument aus der

Internetdokumentation Deutscher Präventionstag www.praeventionstag.de

Hrsg. von

Hans-Jürgen Kerner und Erich Marks

im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe
(DVS)

Zur Zitation:
Heuser, A. (2003): Prävention durch Informationssicherheit. **In:** Kerner, H.-J.; Marks, E. (Hrsg.): Internetdokumentation Deutscher Präventionstag. Hannover. http://www.praeventionstag.de/content/5_praev/doku/heuser/index_5_heuser.html

Prävention durch Informationssicherheit

Ansgar Heuser

Elektronische Daten sind für die Dauer ihrer Speicherung in Rechnersystemen oder während ihrer Übertragung durch Kommunikationssysteme durch kriminelle Handlungen bedroht, deren Ziel ihre *unbefugte Kenntnisnahme*, *Veränderung*, *Vernichtung* oder schlicht die *Verhinderung des Zugriffs* auf sie sein kann. Die neue Qualität gegenüber der Gefährdung der vertrauten papiergetragenen Information durch derartige Delikte besteht zum einen in der *Spurenlosigkeit*, mit der etwa betrügerische Manipulationen an Daten vorgenommen werden können, zum anderen im *großen Umfang*, mit dem dies durch Einsatz von Datenverarbeitung möglich ist.

Dabei reicht unbefugte Kenntnisnahme von der *Ausspähung von Firmengeheimnissen* bis hin zum *Landesverrat*; *Veränderung in betrügerischer Absicht* kann sich auf den Inhalt selbst beziehen oder den Autor einer Information (dies im mehrfachen Sinne: ungerechtfertigte Behauptung oder – im Gegenteil – Bestreiten der eigenen Autorenschaft, Vortäuschung einer fremden Autorenschaft); Zerstörung von Daten oder die Störung der Funktionsfähigkeit von Rechner- oder Kommunikationstechnik sind Beispiele von *Computersabotage*.

Andererseits kann gerade Elektronischer Handel (neudeutsch: E-Commerce), d.h. die Abwicklung von Geschäftsprozessen durch Austausch elektronischer Dokumente mit Rechtsfolgen (wie Angebote, Bestellungen, Quittungen, Mahnungen usf.), auf Dauer nur funktionieren, wenn diesen Informationen das mindestens gleiche Maß an Verbindlichkeit zukommt, wie es der klassische Geschäftsbrief für sich in Anspruch nehmen konnte. Neben der Vertraulichkeit und schieren Verfügbarkeit von Daten kommt also in diesem Falle ihrer Fälschungssicherheit (wie gesagt: des Inhalts wie des Autors) besondere Bedeutung zu.

Kriminalitätsvorbeugend wirkt damit der Einsatz *informationssichernder Techniken*, von Techniken also, die den genannten Bedrohungen elektronischer Information wie Bruch der Vertraulichkeit, Fälschung oder Vernichtung wehren können:

Verschlüsselung gespeicherter oder übertragener Daten ist das Mittel der Wahl zur Wahrung ihrer Vertraulichkeit; derartige Technik steht heute für jedwede Art digitaler Informationen wie Texte, Sprache, Computerdaten usf. zur Verfügung (übrigens auch für Fernsehsignale – beim Pay-TV dient die Chiffrierung nicht der Geheimhaltung, sondern vielmehr der Verhinderung des *Gebührenbetrugs*). Diese Technik ist zudem in der Lage, Informationsinhalte vor Manipulationen in betrügerischer Absicht zu schützen.

Digitale Signierung (deren Rahmenbedingungen in der Bundesrepublik durch ein diesbezügliches Gesetz geregelt sind) blockiert durch unauflösliche Verbindung von Inhalt und Autor eines elektronisches Dokuments dessen inhaltliche Veränderung in Verfälschungsabsicht,

ebenso aber auch den Versuch, dieses einem Dritten zu unterschieben oder die eigene Urheberschaft zu leugnen. (Genauer gesagt: eine digitale Signatur verhindert dies nicht direkt, sondern erlaubt im Streitfalle einem Unabhängigen, also etwa dem Richter, eine nachträgliche Echtheitsprüfung von Inhalt und Autor.)

Ein *digitales Wasserzeichen* gewährt einem Dokument (Text, Graphik, Musikstück, Videosequenz oder was immer) Schutz des Copyrights und erlaubt so die Durchsetzung des Urheberrechts. Dabei fügt der Autor seinem Dokument versteckte Zusatzinformationen bei, die er – und nur er – im Falle einer rechtlichen Auseinandersetzung wieder den streitigen Daten entnehmen kann.

Durch die Techniken der *Netzabsicherung* (dazu zählen Zugangskontrollmechanismen, Virenschutzprogramme, Firewallrechner, sog. Intrusion Detection - Systeme) kann der *Computersabotage* (im engeren Sinne, also begangen durch logische Angriffe, nicht mittels physischer Gewalt) begegnet werden. Vor allem geht es hier um die Absicherung von Rechnern und Lokalen Netzen, die mit dem Internet verbunden sind, das als solches keinerlei Sicherheitsmechanismen bietet, sondern vielmehr als permanente Gefahrenquelle betrachtet werden muss.

Zunehmende Bedeutung als *Zugangskontrollinstrument* (im wörtlichen wie übertragenen Sinne) werden Biometrische Verfahren gewinnen, die große Vorteile gegenüber den heute gebräuchlichen Passwort- oder PIN-Verfahren bieten.

Informationssicherheit in diesem umfassenden Sinne, also die Herbeiführung eines Zustands, in dem innerhalb eines Systems die Daten, Prozesse und auch die Rechner selbst gegen die genannten Bedrohungen durch kriminelle Aktivitäten mittels adäquater Technik abgesichert sind, greift jedoch noch weiter: ihr konsequenter Einsatz vereitelt nicht nur Betrugsdelikte, Geheimnisverrat oder digitalen Vandalismus, sondern würde darüber hinaus *„Kritische Infrastrukturen“*, also die für eine moderne Gesellschaft lebenswichtigen informationsverarbeitenden Systeme – man denke an Energieversorgung, Verkehrswesen, Medizintechnik, Kreditwirtschaft, Telekommunikation – auch vor terroristischen High-Tech-Anschlägen schützen.
Es ist überflüssig zu erwähnen, dass wir heute von einem solchen gesicherten Zustand in den genannten Bereichen weit entfernt sind.