



Informationssicherheit im Next Generation Network

Von Günter Calaminus

ES WAR EINMAL im Jahre 1984, als im Land der Dichter und Denker, mitten in der Hochphase der atomaren Bedrohung die erste E-Mail auf einem Computerbildschirm aufblinkte und die Kommunikationskultur der westlich modernisierten Welt revolutionierte. Das Internet war geboren. Heute gehören für den Geburtsjahrgang 84 Breitband- und UMTS-Technologie sowie unbegrenzter Informationszugang zur Normalität. SMS und MMS, You-Tube und Twitter vereinfachen den Zugang zum globalen Dorf. Sprach man zu jener Zeit noch von Bites und Bytes, werden heute täglich Terra-Bytes über das „Netz“ verschickt. Jegliche Information wird im globalen Kollektiv der Internetgemeinde gespeichert, ohne dass eine „wirkliche“ Kontrolle ausgeübt werden kann. – Einmal im Netz, immer im Netz!

Hier kommt es unweigerlich zu sicherheitsrelevanten Fragen. Grundsätzlich lauten diese, wer, wann und wie lange Zugang zu Informationen hat, um was damit zu tun. Beispielhaft für die strategische Bedeutung des Zugangs zu Informationen kann das erste amerikanische Engagement unter Bush dem Älteren im Golf-Krieg herangezogen werden. Der Einsatz jedweder Information zur Umsetzung außen- und innenpolitischer sowie militärischer Ziele der U.S.-Administration unterstrich deutlich, wer über die Fähigkeit verfügt, als erster Zugriff auf Informationen zu haben, kann diese zu seinen (strategischen) Zielen nutzen. – First in, first out!

Der Kampf um die Informationshoheit zum Wettbewerbsvorteil wird auch im Next Generation Network (NGN) die zentrale Herausforderung bilden. Künftig wird die Internetnutzung auch zum Versand strategischer und somit sicherheitsrelevanter Unternehmensdaten deutlich zunehmen. Daher liegt der Schutz dieser Daten im vitalen Interesse jeder Organisation. – In Deutschland wird der Verlust geistigen Eigentums von Unternehmen auch durch Ausspähungen und Angriffe über das Internet mit einer zweistelligen Milliardensumme angegeben.

Dennoch bietet das „Netz“ für seine Teilnehmer enorme Vorteile. Es vereinfacht Kommunikation sowie Informationszugänge und ermöglicht weltweite Echtzeitaktionen. Organisationen und Unternehmen profitieren von der Fähigkeit, vernetzte Operationen durchzuführen und sich dabei Vorteile für die eigene Position durch rechtzeitigen Zugang zu vitalen Informationen verschaffen zu können. Gleichzeitig werden sie angreifbar. – „Die Geister, die ich rief!“

Die allgemeine Risikoposition sowie der singuläre und klassische Anspruch physischer Sicherheit haben sich demnach verschoben. Sie entwickelten sich zu einem Bündel interdependenter Risikopositionen. Deren gegenseitige Abhängigkeit und Beeinflussung bedingen in jedem

GÜNTER CALAMINUS begann 1996 seine Laufbahn bei SECURITAS als Kaufmännischer Leiter und Betriebsleiter der SECURITAS GmbH Sicherheitsdienste in Frankfurt.

2000 wechselte der studierte Diplom-Ökonom als Prokurist und Leiter für Marketing und Unternehmensentwicklung in die SECURITAS Sicherheitsdienste Deutschland Holding GmbH & Co. KG. Seit 2003 ist er Geschäftsführer der heutigen Niscayah Holding GmbH.

25 Standorte | 300 Techniker | 24/7 im Einsatz

Niscayah – Partner für Sicherheit. Niscayah ist Partner für Unternehmen mit anspruchsvollen Sicherheitsbedürfnissen. Mit dem Ziel, das Sicherheitsrisiko für ihre Kunden zu minimieren, entwickelt und managt Niscayah individuelle, technische Sicherheitslösungen – kundenorientiert, erfahren, zuverlässig.

www.niscayah.de

Fall den Austausch entscheidungsrelevanter Informationen. Daher ist es für die Qualität der Informationssicherheit heute wichtiger denn je, eine qualitativ hochwertige und isolierte Betrachtung der Einzelrisiken durchführen zu können; in einer vernetzten Welt ist die Informationshoheit schon lange zum essentiellen Produktionsfaktor geworden. Kein Sicherheitsentscheider sollte sich der Hoffnung hingeben, dass die Entwicklung des NGN ins Stocken geraten wird. Vielmehr ist zu erwarten, dass Stabilität und steigende Datenübertragungsgeschwindigkeiten die Weitergabe komplexerer Informationen und größerer Datenvolumina in kürzerer Zeit ermöglichen werden.

Zusammenfassend werden auf diese Weise die künftigen Herausforderungen für das Management der Weitergabe sicherheitsrelevanter Informationen immer komplexer. Eine Fähigkeit, die jeden Entscheider vor die Frage stellen wird, eigene Ressourcen für den Kompetenzaufbau abseits des eigenen Kerngeschäftes zu binden oder sich einen Partner zu suchen, dessen Kerngeschäft vollumfängliche Informationssicherheit ist. ●