

Die 5 Zeitalter der IT-Sicherheit

Dr. Hannes P. Lubich
Head of E*MEA Business Continuity, Security and Governance Practice
British Telecom Global Professional Services

Die Informationssicherheit als eine noch vergleichbar junge Disziplin der Informatik hat innert weniger Jahrzehnte bereits mehrere grosse Entwicklungsschritte durchlaufen. Jeder dieser Schritte ist definiert durch eine jeweilig unterschiedliche Bedrohungslage und die für die Gefahrenabwehr zur Verfügung stehenden Kenntnisse und Hilfsmittel. Im Folgenden werden die bisherigen Entwicklungsschritte und Lektionen aus deren Umsetzung vorgestellt. Basierend auf diesen Erkenntnissen wird eine Prognose für den nächsten Entwicklungsschritt gestellt.

Die **Vor- und Frühgeschichte** der IT Sicherheit war gekennzeichnet durch Mainframes und vergleichsweise „dumme“ Terminals in zentralen Rechenzentren sowie durch Benutzer ohne direkten Zugriff auf konfigurierbare IT-Mittel. Dementsprechend war das Bedrohungspotential beschränkt auf „Insider“, auf die sich auch die internen Abwehrmechanismen konzentrierten. Obgleich sich nur wenige IT-Betreiber oder Anwender diese Zeiten zurückwünschen, war dies das „goldene Zeitalter“ der IT Sicherheit – manche modernen IT-Infrastrukturen wie Terminal Server für Web-basierte Anwendungen basieren ihre Sicherheit unter anderem auf der Separierung der Benutzer von der verwendeten Infrastruktur.

Die **klassische Antike** der IT Sicherheit umfasste die ersten Generationen von PCs und vergleichbaren „standalone“ Geräten, welche entweder nicht oder nur über vergleichsweise langsame Modem-Leitungen mit funktional eingeschränkten Protokollen verbunden waren. Bedrohungen in dieser Zeit umfassten erste einfache Viren und lokale Trojaner (oft übertragen durch Disketten), sowie den physischen Diebstahl der vergleichsweise teuren und attraktiven Hardware. Ohne einen einheitlichen, strukturierten Ansatz für IT Sicherheit waren die Besitzer dieser Systeme für ihren eigenen Schutz vollständig verantwortlich – jedoch waren die entsprechenden Mittel und Kenntnisse begrenzt. Eine interessante Erkenntnis aus dieser Zeit betrifft jedoch die Eigenverantwortung der Benutzer, welche heute noch immer ein „heisses“ Thema ist.

Das **Mittelalter** der IT Sicherheit war gekennzeichnet durch einfache PC-LAN's mit zentralen Servern, jedoch mit herstellerepezifischen Netzwerk-Protokollen, keiner einheitlichen Konnektivität und sehr einfachen Netzwerk-basierten Filtern. In dieser Periode bestand das Bedrohungspotential im Wesentlichen aus Viren (im LAN), Hackern (ebenfalls meist lokal, selten über Wählleitungen) und einem eher schwachen lokalen System-Schutz. Die Administratoren dieser Netzwerk-Umgebungen waren zudem oft keine eigentlichen Fachkräfte und hatten keine adäquaten Mittel für den Schutz „ihrer“ Systeme und Nutzer zur Verfügung. Jedoch lässt sich als eine Lehre aus dieser Periode schliessen, dass gezielte Protokollbrüche aus Sicht der IT-Sicherheit durchaus interessante Schutzelemente bilden können, dass aber andererseits das "Ritterburg-Modell" oder auch „harte Schale, weicher Kern“ nicht geeignet ist, Schutz gegen interne Angriffe zu bieten.

Das Zeitalter der **industriellen Revolution** war die „Sturm und Drang“ Zeit der IT und damit wohl eine der schwierigsten Phasen der IT Sicherheit. Das Internet formte den Basis-Standard für WAN- und LAN-Kopplung, alle IP-basierten Endsysteme und Server „sprachen die gleiche Sprache“, waren damit aber auch global erreichbar und angreifbar – die neu gewonnene und rasch wachsende Konnektivität drängte allfällige Sicherheitsbedenken in den Hintergrund. Als

Abwehrmechanismen standen jedoch nur einfache IP-Filter zur Verfügung, während die angeschlossenen Endsysteme weiterhin nur schwach geschützt waren und substantielle Schwachstellen aufwiesen, die von den Herstellern zunächst nur zögerlich geschlossen wurden. Der erste Internet Wurm von 1988 und das weltweite Scannen nach Schwachstellen in vernetzten Systemen beendete diese Phase der „Unschuld“ des Internet und zeigte auf, dass Grundschutz-Modelle immer alle Komponenten einer IT-Umgebung umfassen müssen und dass starkes Wachstum immer auch entsprechende Opportunitätsrisiken mit sich bringt.

Die **Neuzeit** der IT Sicherheit ist gekennzeichnet durch praktisch überall verfügbare drahtlose oder drahtgebundene Internet-Konnektivität mit E-Mail, Web-basierten Applikationen und einer wachsenden Zahl von „peer to peer“ Anwendungen für die private und kommerzielle Nutzung. Die IT Sicherheit ist „der Not gehorchend“ ein Thema von allgemeinem Interesse geworden und nicht spezifisch IT-geschulte Endanwender müssen sich mit Verschlüsselung ihrer WLANs, „personal firewalls“ und regelmässigen Security Updates der verschiedenen Software-Hersteller auseinandersetzen. Auch das Risikopotential gegenüber den schützenswerten vernetzten Gütern und Eigenschaften und die „Breite“ der Angreifer, d.h. ihrer Motivationen, Hilfsmittel usw. hat entsprechend zugenommen.

Fünf Zeitalter der IT Sicherheit sind nun also bereits in weniger als einem Menschenalter vergangen und damit wird der Blick voraus ein Blick ins Ungewisse – die **Zukunft** der IT Sicherheit ist voraussichtlich gekennzeichnet durch noch komplexere Systeme und Abhängigkeiten sowie durch die vollständige Mobilität und ggf. spontane Vernetzung von technischen Systemen. Sowohl „Angreifer“ als auch „Verteidiger“ sind sich dabei ihrer jeweiligen Chancen und Risiken durchaus bewusst und betreiben ein eigentliches Wettrüsten, welches, auch angesichts eines zunehmenden Rechts- und Regulationsdrucks, immense Kostenfolgen hat – nicht umsonst zählt die IT Sicherheit zu den signifikanten Wachstumsmärkten in der IT Branche. Dieser Kostenexplosion sind jedoch in der Zukunft ökonomische Grenzen gesetzt – wenn die Kosten für das Sicherheitsdispositiv und die Rückstellungen für allfällige Restrisiken den Gesamtwert der schützenswerten Güter mittelfristig übersteigen, ist eine Grenze erreicht, die weitere Investitionen als fragwürdig erscheinen lässt. Die IT Sicherheit der Zukunft basiert demzufolge auf einer ganzheitlichen und balancierten Betrachtung der IT-Risiken vom Design bis zum Betrieb über die gesamte Prozesskette hinweg – die IT Sicherheit wird damit zu einer von mehreren Teildisziplinen des unternehmerischen Risiko-Managements und der Corporate Governance. Dabei wird es durchaus möglich und notwendig sein, Teile der IT Sicherheit nicht mehr in eigener Kompetenz zu entwerfen und zu betreiben, sondern diese Teildienstleistungen von spezialisierten Anbietern ausführen zu lassen. Auch hierin liegen Chancen und Risiken, die die Informatik zu nutzen bzw. zu bewältigen hat.