Privacy, Security, Internet – ein unlösbarer Zielkonflikt ?

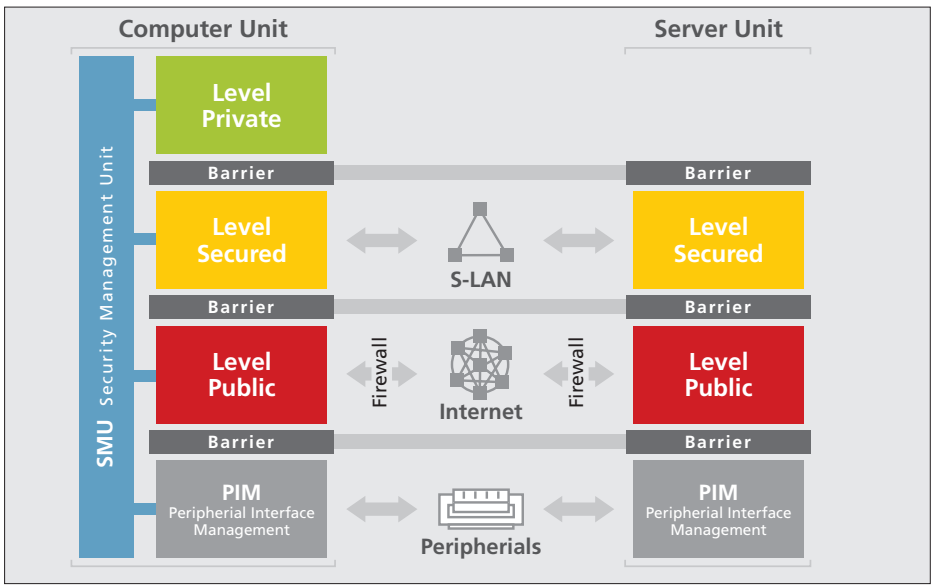
Die technologische Entwicklung in der ICT-Branche weist gegenüber den früheren industriellen Entwicklungen wie beispielsweise der Elektrizität oder dem Automobil einen deutlich höheren Gradienten der Verbreitung über die Zeit aus. Zudem steigt die Leistung der drei wesentlichen Komponenten – Prozessoren, Speicherdichte, Datentransfer – permanent. Mit der steigenden Anzahl der Nutzer und deren Kommunikation explodiert das Volumen der global akkumulierten Daten förmlich.

VON ADOLF FLÜELI

Die Dynamik der ICT-Branche ist durch die permanente Leistungssteigerung der drei wesentlichen Komponenten der Rechner und deren Einbindungen in die Kommunikation gegeben. Die Leistung der Prozessoren verdoppelt sich in jeweils 18 Monaten entsprechend dem Moore'schen Gesetz. Die Speicherdichte der Speichermedien verdoppelt sich jeweils innert zwölf Monaten. Die Kommunikationsraten der Netze verdoppeln sich in ähnlichen Dimensionen. Zudem entwickelt sich die Zunahme der Datenverbreitung exponentiell zu der Anzahl der vernetzten Teilnehmer. Dadurch explodiert das Volumen der global akkumulierten Daten förmlich. Auf der Rechnerseite werden diese Trends zu grösseren Datenmengen durch die zunehmend komplexeren und voluminöseren Betriebssysteme und die Vielzahl speicherfüllender Anwenderprogramme noch verstärkt. Im Gegensatz zu der Hardware zeichnet sich die Software weder mit einem stetigen Preiszerfall – noch mit permanenten drastischen Leistungssteigerungen aus.

Die Ansprüche des Individuums auf Privacy

Die Aspekte der Privacy umfassen sowohl die Wahrung der individuellen Geheimsphäre und Privatsphäre als auch der Wahrung von entsprechenden kollektiven Interessen. Die Grenzen dieser Sphären werden beim täglichen Einsatz von einfachsten ICT-Geräten wie einem Mobiltelefon bereits latent in Frage gestellt, vielfach ohne dass der Anwender sich dessen bewusst ist. Dies betrifft sowohl den Zugriff auf den Inhalt der Kommunikation als auch die Offenlegung eines Beziehungsnetzes durch die jeweils aufgebauten Verbindungen zu den Kommunikationspartnern sowie das Bewegungsprofil des Teilnehmers durch die permanenten lokalen Netzeinbindungen bei eingeschaltetem Gerät. Beim alltäglichen Einsatz eines Laptops während einer Zugfahrt konnte schon auf eindrückliche Weise beobachtet werden, wie sich dieses Gerät versuchte, mit demjenigen des Passagiers vis-à-vis eine Verbindung über die IR-Schnittstelle aufzubauen. Über eine derartige Schnittstelle kann grundsätzlich auf die Daten des Gerätes zugegriffen werden, zudem lassen sich über diese Schnittstellen auch Trojaner auf äusserste elegante Art und Weise installieren. Nachdem die Betriebssysteme der Geräte im Hintergrund meistens per default auf den Betrieb aller Funktionen eingestellt sind, ist dem unbedarften User ein latent offenes und für Dritte indirekt zugängliches Gerät überlassen. Durch die Komplexität der Betriebssysteme und der installierten Software kann in der Regel davon ausgegangen werden, dass entweder eine sichere Konfiguration des Gerätes und aller installierten Programme durch einen Spezialisten erfolgt und durch diesen zudem dauernd gepflegt wird oder aber dass die Geräte in latent unsicheren Konfigurationen betrieben werden.



Das Schema zeigt die Architektur der physischen Datentrennung in den Geräten sowie in deren Verbund.

Die Ansprüche des Individuums auf Security

Die Aspekte der Security umfassen sowohl die Wahrung des individuellen Zugriffes auf Daten, die Sicherstellung der Verfügbarkeit, der Integrität und der Unverletzlichkeit der Daten sowie die sichere Übermittlung von Daten. Die Sicherstellung der Verfügbarkeit kann durch Backupsysteme und Disziplin für das Individuum relativ einfach bewerk-

Adolf Flüeli

Dipl.- Ing. HTL / Wirtschaftsing. FH führt als Innovationsberater die Firma ADF Innovation Consulting. In dieser Funktion begleitet er Projekte von der Idee bis zur Realisation.

stelligt werden. Die Sicherstellung der Integrität, der Unverletzlichkeit und einer sicheren Übermittlung der Daten ist wesentlich komplexer und wird primär durch die Einbindung der Geräte in die moderne Kommunikation gefährdet. Von zentraler Bedeutung erweist sich dabei die Tatsache, dass bei diesen Netzeinbindungen in der Regel das gesamte Gerät diesen Risiken mehr oder weniger ausgesetzt werden und dabei meist sämtliche Daten auf dem entsprechenden Gerät vollumfänglich exponiert werden. Hierbei sind die Grenzen der Gefährdung vorwiegend durch die Professionalität der Schutzmassnahmen und des Anwenders gegeben.

Die Ansprüche des Individuums auf Connectivity

Die Aspekte der Connectivity umfassen sowohl die Wahl des Individuums auf Kommunikationsaufnahme als auch die Sicherstellung der stetigen Erreichbarkeit. Hierbei sollen diese Aspekte jederzeit und unabhängig vom Standort der jeweiligen Kommunikationspartner erfüllt werden. Die Kommunikation umfasst dabei sämtliche Verfahren von der Sprachkommunikation bis zum Datenaustausch in beliebigen Dateien und Formaten, wobei dieser Datenaustausch vorwiegend über Internet erfolgt. Die Einbindung in Netzwerke erfolgt zunehmend auch mobil und permanent aktiv (always on) über lokale Funknetze, WLAN.

Die Bildung von partiellen Idealitäten

«Die bedeutenden Probleme, mit denen wir konfrontiert werden, können nicht auf dem gedanklichen Niveau gelöst werden, auf dem wir waren, als wir sie schufen. (A. Einstein)

Die Bildung von partiellen Idealitäten von Systemen zur Lösung von Zielkonflikten ist in der Technik seit langem grundsätzlich bekannt. Durch die partielle Variation eines als Ganzes ursprünglich nicht idealen Gesamtsystems lassen sich für verschiedene Betriebszustände spezifische Idealitäten bilden, wodurch sich die Idealität des Gesamtsystems über das gesamte Einsatzspektrum steigern lässt. Damit ein Verbrennungsmotor zum Antrieb von Fahrzeugen einigermassen sinnvoll eingesetzt werden kann, werden sequenziell eine Kupplung und vorzugsweise ein Schaltgetriebe eingesetzt. Dadurch lassen sich für verschiedene Betriebszustände sequenziell verschiedene Idealitäten herstellen, beispielsweise die Bewegungsrichtung des Fahrzeuges wechseln, ohne dass hierzu das ganze Fahrzeug umkonfiguriert werden muss. Bekannt ist beispielsweise das Einziehfahrwerk bei Flugzeugen, welches für gewisse Betriebszustände wie Start und Landung vorzugsweise ausgefahren und für den Reiseflug eingefahren wird.

Physische Datentrennung als partielle Idealität

Die physische Datentrennung definiert physisch separierte Datenräume beliebiger Dimensionen als partielle Idealitäten. Diese Datenräume sind entweder Bestandteil einer IT-Infrastruktur oder Bestandteil einer beliebigen IT-Plattform, beispielsweise eines Computers. Die Datenräume sind als funktionale Levels ausgebildet und werden dementsprechend bezeichnet.

Der Lösungsansatz von «Multilevel IT Security»

Der Lösungsansatz von «Multilevel IT Security» basiert auf unseren zentraleuropäischen Wertvorstellungen bezüglich der Qualität von Informatiklösungen und der nachhaltigen Sicherheit von physisch getrennten IT-Architekturen. Durch die physische Datentrennung können die Idealitäten von Privacy, Security und Connectivity sowohl in ICT-Infrastrukturen (Netzwerken) als auch in beliebigen ICT-Plattformen realisiert werden. Zugleich wird damit eine weitere Idealität bezüglich Economy durch die Multifunktionalität der ICT-Plattform und dessen sequenzielle Nutzung auf jeweils einem der Levels erreicht.

Ausführungsformen von IT-Infrastrukturen und IT-Plattformen

Die konventionellen IT-Infrastrukturen werden durch mit in sich geschlossenen und von externen Netzwerken vollständig physisch getrennten autarken Netzwerken partiell ergänzt (S-LAN). Die IT-Plattformen sind als einfache multifunktionale Einheiten in der Form von Geräten wie PC, Laptop oder Handheld modular aufgebaut. Die IT-Plattformen können entsprechend den Zielfunktionen der Anwendergruppen hardwaremässig spezifiziert und konfiguriert werden. Dies umfasst nebst der Zuweisung der Funktion der Levels auch gleichzeitig die Konfiguration der auf den jeweiligen Levels aktivierbaren Schnittstellen über das Peripherial Interface Management PIM, sodass beispielsweise die IR-Schnittstelle auf einem sensitiven Level per Definition ausser Betrieb ist. Die Kompatibilität ist durch die Verwendung von zeitgemässen Hardware- Standardbauteilen vollumfänglich gegeben.

Funktionalitäten entsprechender IT-Plattformen

Die nachhaltige Sicherheit wird durch die vollständige physische Datentrennung unmittelbar in den Geräten erreicht. Das Gerät ist derart ausgeführt, dass es sequenziell auf jeweils nur einem der verschiedenen Levels betrieben werden kann. Dadurch wird eine ungewollte Durchmischung von Daten auf dem Gerät verhindert. Somit können diese multifunktionalen Geräte einerseits auf dem Level «Public» mit externen Netzwerken wie dem Internet verbunden werden, ohne dass dabei die Levels «Private» und «Secured» über externe Netzwerke geortet und erkannt und diese somit auch weder gescannt, eingesehen, gestört, manipuliert, attackiert oder gar zerstört werden können.

Die physische Datentrennung unmittelbar in den Geräten ermöglicht jedem Anwender eine sehr einfache multifunktionale Nutzung derselben. Die Komplexität dieser Anwendung entspricht in etwa derjenigen eines üblichen Tintenstrahl-Drucker-Kombigerätes, welches sequenziell auch zum Scannen oder Kopieren eingesetzt werden kann.

Durch die sequenzielle Nutzung des Gerätes lässt sich die gleiche Sicherheit wie bei der Installation von drei verschie-

Die Idealitäten von ICT- Systemen

Die Ansprüche von Privacy, Security, Connectivity und Economy für den Einsatz von ICT-Infrastrukturen und ICT- Plattformen lassen sich für das Individuum wie folgt idealisieren

Privacy	**Security**
System von der Aussenwelt nicht ortbar, dedektierbar, angreifbar	System von der Aussenwelt nicht ortbar, dedektierbar, angreifbar
Zugriff ausschliesslich persönlich auf das eine spezifische Gerät	Zugriff ausschliesslich für einen engen definierten Kreis auf die entsprechenden Geräte
Keine Einsicht für Administratoren	Keine Einsicht für Administratoren ausserhalb des definierten Kreises (keine hierarchischen Privilegien)
Economy & (Sustainability)	**Connectivity**
Modulare Systeme und Netzwerke	System mit der Aussenwelt verbunden
HW- und SW-Kompatibilität	Beliebige Kommunikationsarten und Kanäle
System aufrüstbar, ausbaubar und anwenderspezifisch konfigurierbar	Beliebige flankierende Sicherheitsmassnahmen wie Virenscanner, Firewalls, Verschlüsselungen, Sandboxes usw. einsetzbar
Ressourcen schonender sequenzieller Einsatz, ökologisch, kompakt, leicht	
Wirtschaftlichkeit, TCO, LCC	
Nachhaltige in sich beständige Lösung	

denen und entsprechend separierten Geräten zu diesem Zweck erzielen. Die neue integrale Lösung ist jedoch bezüglich Investitionen bedeutend wirtschaftlicher und in Bezug auf Platzbedarf, Energieverbrauch und Abwärmeentwicklung wesentlich ökologischer.

Bedienung von «Multilevel IT Security»

Die Bedienung von Multilevel IT Security ist so einfach wie das Einschalten des Gerätes selbst. Die Wahl des entsprechenden Levels erfolgt direkt manuell am Gerät, durch die Betätigung eines Wahlschalters oder von Drucktasten am Security Interface Controller SIC. Die Eingaben des SIC werden über die Security Management Unit SMU im Gerät durch entsprechende hardwaremässige Beschaltungen umgesetzt. Gleichzeitig wird der gewählte operative Level über eine entsprechende Anzeige auf dem Gerät visualisiert. Dies entspricht der einfachsten Form zur Wahl eines Levels auf einer multifunktionalen Plattform. Diese Multifunktionalität der Plattform eröffnet dem Benutzer einen weiteren Freiheitsgrad im Computereinsatz. Somit ergibt sich gemäss nachfolgender Analogie eine 3. Generation der Computerbedienung, welche eine vollkommen neue Nutzung des Gesamtsystems «Personal Computer» erlaubt:

1. Generation der Bedienung:
Tastatur ➜ DOS-Befehle auf Bildschirm
2. Generation der Bedienung:
Maus ➜ Ikons auf Bildschirm (sind über Tastatur schwierig bedienbar)
3. Generation der Bedienung:
SIC ➜ Hardwarebasierte Sicherheitskonfiguration des Computers (ist mit den derzeitigen Peripheriegeräten ebenfalls schwierig bedienbar).

Anwendungen entsprechender IT-Plattformen

Für die stationären Anwendungen stehen vor allem die kostengünstigen und ökologischen Anwendungen der physischen Trennung der Daten in kleineren sensitiven Umfeldern wie bei Anwälten, Treuhändern, Ärzten, Gemeinden und lokalen Behörden usw. im Vordergrund. Daneben sind SOHO-Anwendungen für shared Computers auch für private Anwendungen attraktiv, beispielsweise kann der eine Level den Kindern zur Verfügung gestellt (und beispielsweise auch mit Internetfilter ausgerüstet) werden, ohne dass dadurch bei irgendwelchen Störfällen das ganze Gerät gefährdet wird. Ebenfalls lässt sich ein Level ausschliesslich für Geschäftsanwendungen konfigurieren, welcher eine gesicherte Kommunikation von zu Hause mit der Firma ausschliesslich über VPN ermöglicht. Es lässt sich beispielsweise auch ein Level ausschliesslich für e-banking einsetzen, wodurch die Zeit der Exposition dieser Dateien und der Schlüsselinformationen auf dem entsprechenden Level des Gerätes auf die wenigen Minuten des effektiven Einsatzes beschränkt werden können. Bei den mobilen Anwendungen stehen die Business-Anwendungen beispielsweise für Konzerne im Vordergrund, für welche erstmals eine Lösung mit sauberer Datentrennung Business/Private auf ein und demselben Gerät ermöglicht wird. Hierbei kann der eine Level Secured ausschliesslich intern sowie für die Kommunikation über VPN eingesetzt werden.

Integration entsprechender IT-Plattformen

Die Einbindung der multifunktionalen Geräte in bestehende IT-Infrastrukturen lässt sich dank dem modularen Aufbau und der Kompatibilität der Geräte zu konventionellen Personal Computern sehr einfach und kostengünstig realisieren. Insbesondere können sichere interne Netzwerke, S-LANs, sehr einfach und kostengünstig modular aufgebaut ergänzend zu den bisherigen IT-Infrastrukturen lokal betrieben werden. Durch den modularen Aufbau der IT-Plattformen und IT-Architekturen sind sämtliche weiterführenden Möglichkeiten für den Einsatz aller sicherheitsspezifischen Softwarelösungen gegeben. Dieses Spektrum reicht vom Virenscanner über VPN bis hin zu speziellen Verschlüsselungen sowohl für die Datenübermittlung als auch für die Datenspeicherung.

Ausblick

Die physische Datentrennung gewährleistet den vollständig autonomen Betrieb von Hardware und Software auf verschiedenen Levels in einem einzigen multifunktionalen Gerät. Dadurch wird eine neue Dimension von Sicherheit bezüglich der Dedektierbarkeit und der Verletzlichkeit von IT-Systemen und Daten sowie eine neue Qualität der Privacy und des Datenschutzes ermöglicht. Im Gegensatz zu den hierarchischen Zugriffsverwaltungen über Berechtigungen kann der Zugriff auf Daten zusätzlich physisch begrenzt und dadurch auch für die Administratoren partiell ausgeschlossen werden. Die physische Datentrennung ermöglicht zudem eine neue Qualität bezüglich der Datenhygiene, indem ungewollte Durchmischungen von verschiedenen Anwendungsgebieten wie der Berufs- und Privatsphäre direkt auf der Plattform verhindert werden. Diese Lösung zeichnet sich insbesondere durch deren hardwaremässig gegebene Beständigkeit und deren Einfachheit in der Handhabung aus. Zudem ermöglicht die physische Datentrennung eine Datenablage und Datenbewirtschaftung nach neuen zukunftsgerichteten Kriterien, beispielsweise nach der Halbwertszeit der Daten. Dadurch resultiert eine erste Komplexitätsreduktion der Daten, welche dem Anwender die Bewältigung der Datenflut erleichtert. ■