Physische Datentrennung – die Antwort auf pervasive Computing

Die zunehmende Verletzlichkeit der Informationsgesellschaft beruht auf der zunehmenden Vernetzung der Systeme sowie insbesondere auf den bisher monolithisch ausgebildeten Hardwarearchitekturen.

Die integrale physische Datentrennung unmittelbar in der Anwenderplattform ermöglicht sowohl multifunktionale Nutzungen als auch zusätzliche Redundanzen. Die zielführende Hardware- Konfiguration ermöglicht die sequentielle Erschliessung des gesamten Spektrums von der "totalen Isolation" bis zur "maximalen Kommunikation".

Sie ermöglicht dem Anwender die proaktive Verwirklichung der "informationellen Selbstbestimmung", indem die zunehmende digitale Versklavung durch Fremdmanipulations- und Spionagepotentiale gezielt und dauerhaft unterbunden wird.

VON ADOLF FLÜELI

Die Verletzlichkeit der Informationsgesellschaft

Mit der Einführung des Internetbrowsers sowie dessen Implementierung auf den damals nicht für diesen Zweck konzipierten Betriebsystemen auf den historisch gewachsenen monolithisch ausgebildeten Rechnerarchitekturen wurde 1993 die Basis für die enorme Verletzlichkeit der heutigen Informationsgesellschaft gelegt.

Die Interneteinbindung eines monolithischen Rechners ins Internet stellt eine offene Flanke für den Zugriff sämtlicher auf diesem Rechner vorhandenen Daten sowie gleichzeitig auch *ein Einfallstor auf sämtliche weiteren* mit diesem Rechner verbundenen Rechnern und Geräten dar.

Die Kombination von folgenden Risikofaktoren führt zu einer gigantischen Risikoeskalation:

- die permanente Steigerung der Rechnerleistungen
- die zunehmende Voluminösität und Komplexität der Betriebsysteme
- die permanente Steigerung der Datenübertragungsraten (xDSL, Fernsehkabelnetz)
- die zunehmende Einbindungszeit der Rechner in die Netze (vielfach bereits permanet)
- die zunehmenden Möglichkeiten von automatischen Einbindungen in diffuse Netze (W-LAN)
- die permanente Steigerung der Vernetzungsdichte (Anzahl Internetgeräte und Anwender)
- die zunehmende Aggressivität, Agilität und "Intelligenz" von Malware (Viren, Würmer, Trojaner etc.)

Die Risikoentwicklung verläuft durch die Multiplikation der vorgenannten Risikotreiber mit *einem exponentiellen Gradienten,* währendem die Entwicklung der Schutzmassnahmen bestenfalls stetig erfolgt, und deren Anwendung zudem meist den Ereignissen *reaktiv* hintennachhinkt (Patches). Dies manifestiert sich u. A. in den immer rasanteren globalen Störungsausbreitungsgeschwindigkeit von Viren, Würmern etc.

Somit hat sich im Laufe des vergangenen Internetjahrzehntes die Verletzlichkeit und Anfälligkeit der Informationsgesellschaft drastisch erhöht. Da deren wirtschaftliche Bedeutung ebenfalls enorm zugenommen hat, steigt zugleich die wirtschaftliche

Abhängigkeit der gesamten Gesellschaft bezüglich der Verfügbarkeit der gesamten Information and Communication Technologies, ICT.

Zu den bereits geschilderten Bedrohungen ergeben sich für sämtliche Nutzer zudem eine Fülle individueller und teilweise sehr heimtückischen Informations- und Datenschutzrisiken, von der meist unbemerkbaren Erhebung von individueller Nutzerprofilen über die Rekonstruktion von Dokumenteninhalten (Entwürfe, Kopien) sowie Passwortspionageprogramme welche die Tastaturanschläge aufzeichen, bis hin zur Erhebung von geographischen Bewegungsprofilen des Opfers.

Die 2 wunden Punkte der gesamten ICT

1. Der Zerfall der Sicherheit und insbesondere des Informations- und Datenschutzes basiert im wesentlichen auf der unglücklichen Kombination von Betriebsystem und Browser auf monolithisch aufgebauten Rechnern sowie der zunehmenden Vernetzungen der Systeme.
2. Gleichzeitig steigt die Komplexität des Datenhandlings und Informationsmanagementes mit der stetig anschwellenden Datenflut.

Die resultierenden Schadenspotentiale

Die gefährlichen Potentiale von Informationsmissbrauch liegt nicht primär bei der allfälligen Zerstörung von Daten z.B. durch Viren und den dadurch verursachten lästigen Arbeitsausfällen und Komplikationen. Ein allfälliger aktiver Datenmissbrauch ist nicht auf meist kurzfristigen Kreditkartennummern- Missbrauch beschränkt, sondern ist auf die "Gewinnung" von sensitiven Informationen ausgelegt, und kann im worst-case zum langfristigen Verlust von Aufträgen und Kunden führen. Somit belaufen sich derartige Verluste in kaum bezifferbare Dimensionen von geleisteten CRM- Aufbauarbeit und Investitionen in Forschung und Entwicklung über Jahre, und münden zugleich in den Verlust von Vertrauen, Know-How und den darauf basierenden Wettbewerbsvorteilen.

Derartige Daten- und Informationsverluste können bei den heutigen Vernetzungsdichten durch eine einmalige kurzfristig Unachtsamkeit entstehen, sind irreversibel und stellen zudem meist nicht versicherbare langfristige Risiken dar.

Die Lösung des Zielkonfliktes von Privacy, Security und Connectivity

"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)

Der grösste Vorteil der Software, deren beliebige Kopier- und Manipulierbarkeit sowie deren unkontrolierbaren "Flüchtigkeit und Unsichtbarkeit", stellt gleichzeitig auch deren grössten Nachteil bezüglich Sicherheit und Zuverlässigkeit dar. Somit empfiehlt sich für die Gewährung einer langfristig stabilen Sicherheit ein rein physischer, in sich beständiger "unveränderlicher" Ansatz.

Die Lösung besteht darin, die Hardwarearchitektur physisch mehrdimensional zu strukturieren und dadurch dem Anwender völlig neue Dimensionen und Freiräume zur nachhaltigen Lösung der Zielkonflikte von "Privacy", "Security" und "Connectivity" zu eröffnen. Somit wird dem Anwender ein selbstbestimmbares *proaktives* "Handling" analog zum Papier, "Private" = Safe, "Secured" = Kasten, "Pubic" = Plakat ermöglicht.

Die Umsetzung bedingt einen Paradigmenwechsel und führt konsequenterweise zu einer völlig neue Auslegung sowohl der stationären ICT- Infrastrukturen und ICT- Geräten (Bild 1) als auch eine dementsprechend kongruente Auslegung der mobilen ICT- Geräten (Bild 3).

Integrale Lösung

Die neue integrale Lösung der physischen Datentrennung unmittelbar im Computer ergibt einen "mehrdimensionalen" multifunktionalen Rechner.

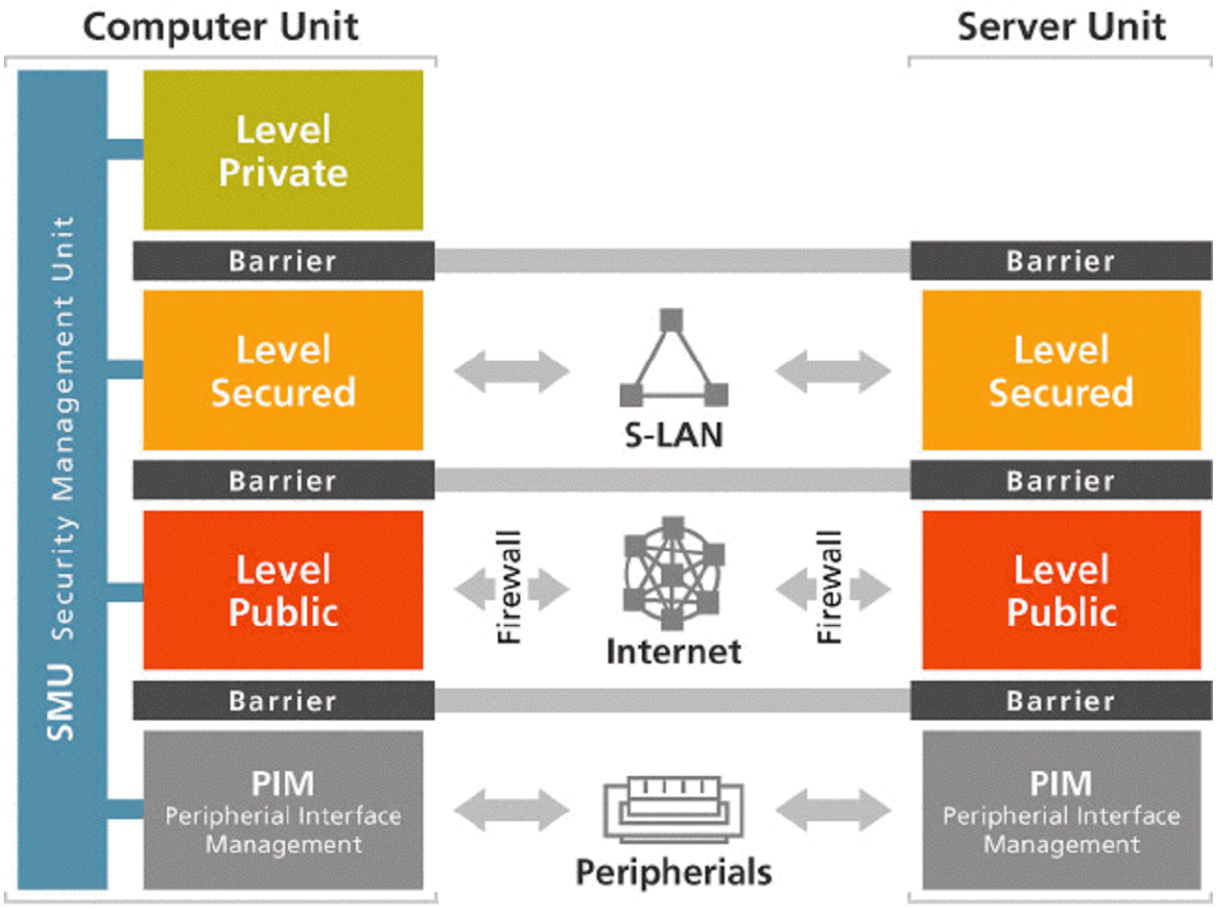


Bild 1: Schema der physischen Datentrennung im Computer

Hierbei wird jeweils einer der physisch getrennten "Levels" (Bild 1) über eine vom Rechner unabhängige Steuerung SMU, Security Management Unit, sequentiell zum Einsatz gebracht. Zugleich werden über die SMU verschiedene Schnittstellen wie beispielsweise IR, Bluetooth etc. entsprechend der zielführenden Konfiguration des Levels mit beschaltet.

Die verschiedenen Levels realisieren folgende zielführende Funktionen in einem einzigen Gerät:

Level Private:	vollständig isolierter Computer	lässt sich von aussen nicht dedektieren *beschränkt Zugriffe auf ein einziges Individuum*
Level Secured	vollständig isoliertes internes Netz	lässt sich von aussen nicht dedektieren (S-LAN) *beschränkt Zugriffe auf ein definiertes Kollektiv*
Level Public:	offener Computer	extensive Kommunikationseinbindung (W-LAN) *permanente globale Exposition*

Bedienung

Die Einleitung der Umschaltung erfolgt durch Selektion des gewünschten Levels und Bestätigung über Tastendruck "activate" (Bild 2), der anschliessende Ablauf der Umschaltung wird über die SMU automatisch gesteuert.

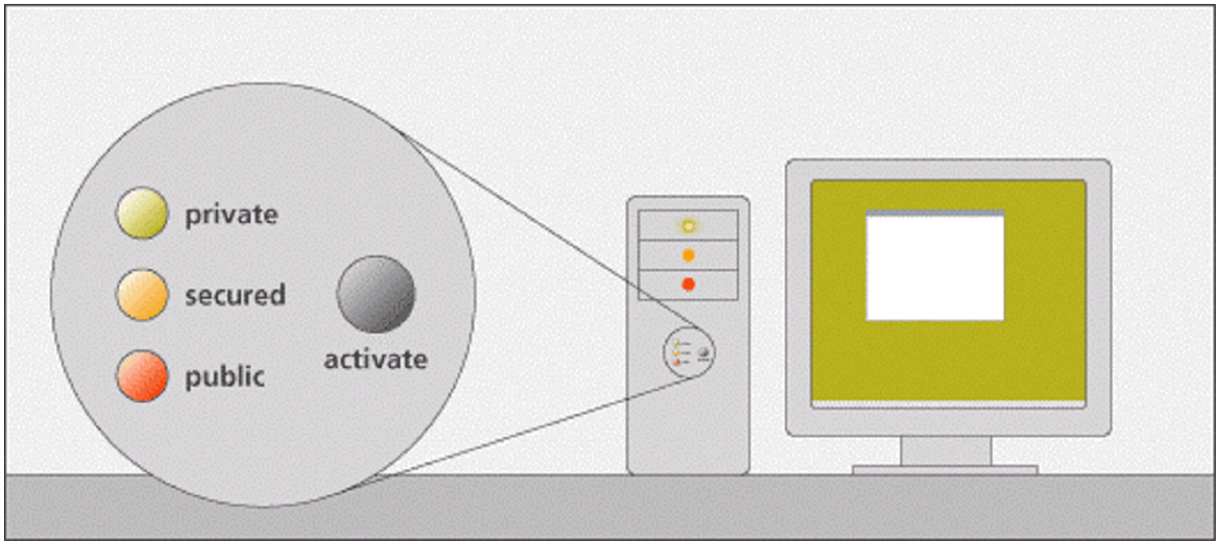


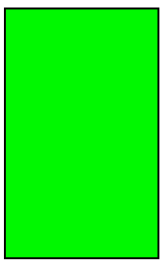
Bild 2: Bedienung des multifunktionalen Computers

Die integrale Ausführung unmittelbar in der Anwenderplattform stellt jeweils eine sinngemässe Beschaltung der Schnittstellen zusammen mit den verschiedenen Sicherheitsstufen (Levels "Private","Secured", "Public") automatisch sicher, was Zuordungsfehler praktisch ausschliesst.

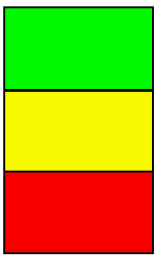
Die Bedienung dieser multifunktionalen Anwenderplattformen entspricht in Analogie der einfachen Bedienung bekannter und ebenfalls sequentiell nutzbarer Kombigeräte, wie beispielsweise eines multifunktionalen "Drucker- Scanner- Kopierers".

Multifunktionalität

Im Gegensatz zu der bisherigen "monolithischen" Architektur weist die neue "mehrdimensionale" Architektur mit verschiedenen autarken Levels entsprechende Redundanzen auf. Somit führt eine Störung oder ein Ausfall auf einem Level in der Regel nicht zu einem vollständigen "Groundig" des ganzen Gerätes sondern ermöglicht dessen weitere Nutzung auf den restlichen verfügbaren Levels.



monolithisch



multifunktional

Zudem verfügen diese multifunktionalen Geräte entsprechend der Anzahl der installierten Levels gleichzeitig über entsprechend höhere installierten Speicherkapazitäten (HDD`s). Somit lässt sich nebst dem beschriebenen Risikosplitting gleichzeitig auch die anfallende Datenflut nach neuen Kriterien bewirtschaften, beispielsweise nach dem Kriterium des Zeitwertes der Daten resp. der Halbwertszeit der Daten.

Zusammenfassung

Im Zuge des "Pervasive Computing" stellt die integrale physische Datentrennung eine einfache, kostengünstige und wirksame Methode (zur Wiedererlangung) der Kontrolle des Anwenders über seine Daten und Informationen dar. Sie ermöglicht dem Owner der Daten und Informationen die unmittelbare und selbstbestimmbare Regelung des Zugriffes auf seine immateriellen Güter (Intellectual Property) direkt an deren Quelle.

Im Gegensatz zu sämtlichen reaktiven Abwehrmassnahmen zum Schutze von "monolithischer" Hardware ermöglichen mehrdimensionale Hardwarearchitekturen ein proaktives anwenderbestimmtes Informations- und Knowledge- Controlling.

Bild 3: aktuelle Laptopentwicklung mit integraler physischer Datentrennung

Weitere Informationen

Das vorgestellt Konzept wird durch Multilevel IT Security als neue hardwarebasierte integrale Informations- und Datenschutzlösung zur individuellen Gewährung höchster Sicherheitsstandards postuliert und realisiert. www.multilevel-it-security.com

Adolf Flüeli
Dipl.- Ing. HTL / Wirtschaftsing. FH hat das Konzept der integralen physischen Datentrennung entwickelt und leitet die Firma Multilevel IT Security in Winterthur. (info@multilevel-it-security.com)