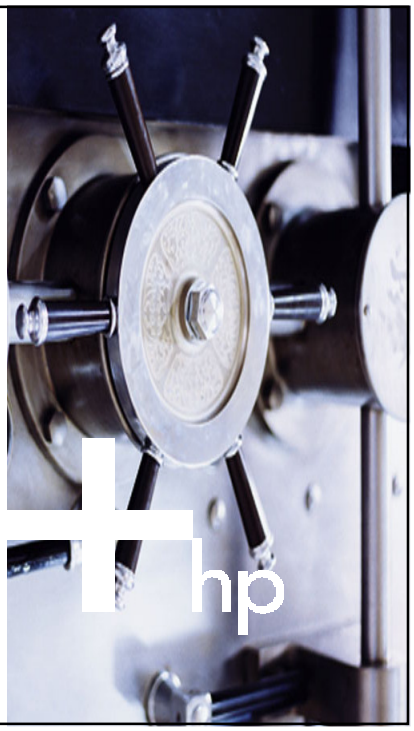
DECUS 2007
HP NonStop Security

Vortrag 3H10



Gerhard Schwartz
HP NonStop Enterprise Division

Agenda

IT Security und deren Auswirkung auf die Kosten

- Das Internet hat alles verändert
- Wie bekommt man sichere Systeme ?
- Das Security-Konzept der HP NonStop Server
- Was kostet IT Security ?
- HP Atalla Security Products

April 18, 2007 2

Das Internet hat alles verändert

- Früher war IT Security ein nettes Spezialgebiet für einige Experten ...
- in den meisten Anwendungsbereichen nicht allzu kritisch, mit relativ wenig Bezug zur Außenwelt („Gute alte Zeit“, der Elfenbeinturm läßt grüßen ...)

April 18, 2007 3

Sicherheit im Internet

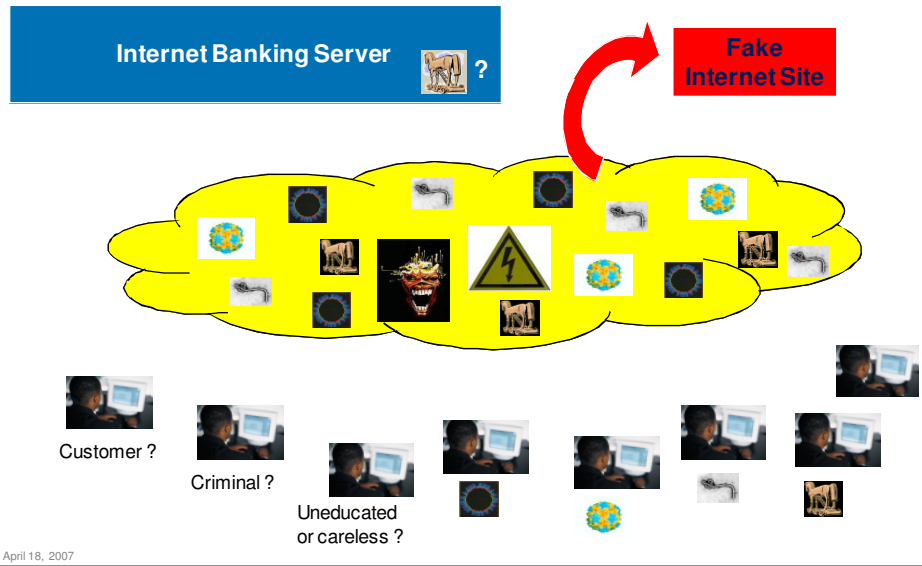
- Heute - ein extrem kritisches Thema !
- World wide ocean

- Tons of data

- Das Internet ist sicherheitstechnisch gesehen ein absolutes Notstandsgebiet – und ein riesiger Markt für Firewalls, Virenscanner und ähnliche Produkte …

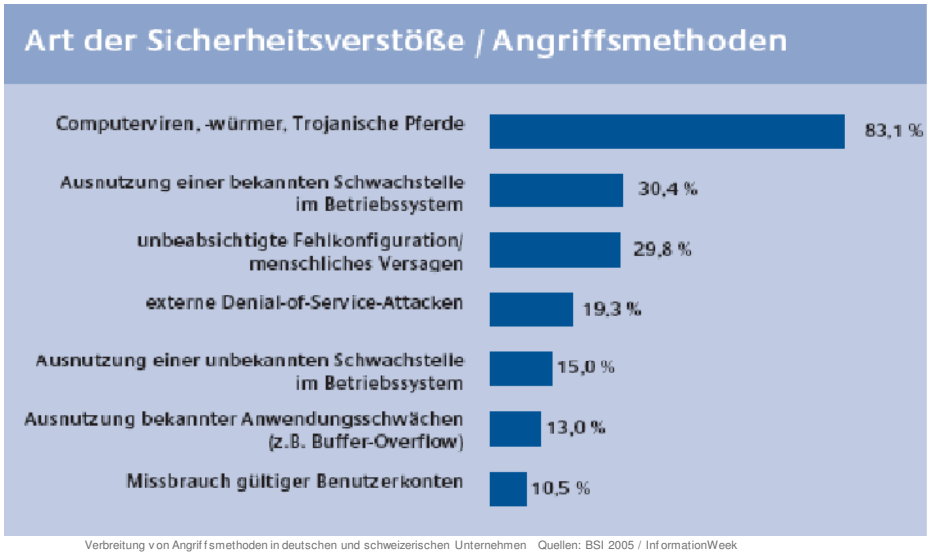
April 18, 2007 4

The Internet is a dangerous place



April 18, 2007 5

Verbreitung von Angriffsmethoden



Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen Quellen: BSI 2005 / InformationWeek

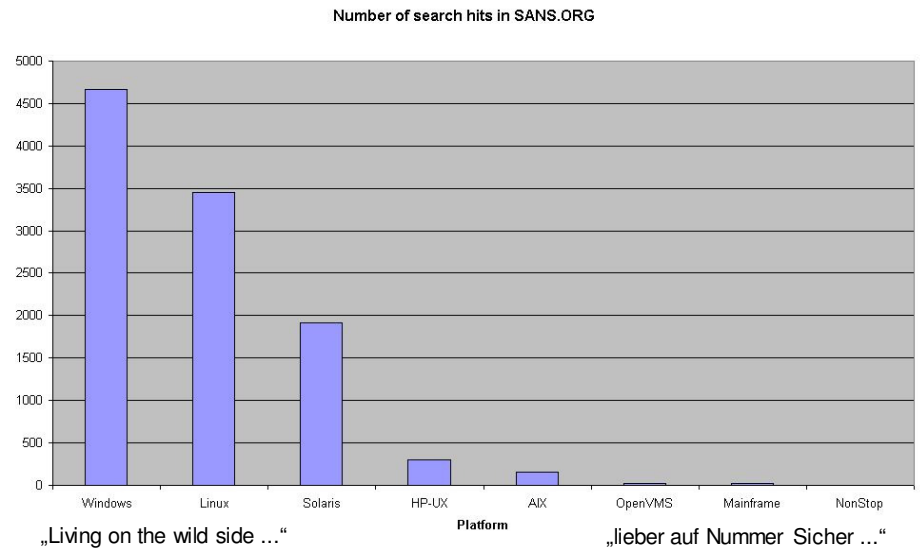
April 18, 2007 6

Sichere Systeme kann man nicht kaufen ...

- ... sondern man muß sie bauen !
- **Absolute** Sicherheit gibt es nicht ...
- Aber es gibt sehr wohl erhebliche Unterschiede zwischen verschiedenen Systemen
- *„It's extremely hard to build a secure system based on a vulnerable platform"*
- Daher: Wer eine möglichst sichere Plattform wählt, hat es wesentlich leichter ein sicheres System zu vernünftigen Kosten zu bauen und zu betreiben ...

April 18, 2007 8

Vulnerabilities ...



„Living on the wild side ...“ „lieber auf Nummer Sicher ...“

April 18, 2007 9

Top 10 Vulnerabilities to Windows Systems

- W1 Web Servers & Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

April 18, 2007 10

Top 10 Vulnerabilities to UNIX Systems

- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

April 18, 2007 11

Die Plattform HP NonStop

- Ein weitestgehend selbstverwaltendes System
- Selbstheilendes System, automatische Rekonfiguration bei Hard- und Softwarefehlern
- Extreme Verfügbarkeit: 99,999 %, eine Größenordnung besser als Mainframecluster („Parallel Sysplex“)
- State of the art: Open System (POSIX compliant), powered by Intel Itanium
- Integrierter HW/SW - Stack, kein „mix-and-match“, sehr geringe Kosten für Systemadministration
- Massive Skalierbarkeit (MPP - Architektur) – lineares Leistungswachstum bis über 4000 CPUs

April 18, 2007 13

Die Plattform HP NonStop (2)

- Keine bekannten Vulnerabilities, daher kein Security Patching erforderlich
- Für Hacker wäre der Zugang zu NonStop Hardware, Software und speziellem Knowhow äußerst schwierig
- –> sehr begrenztes Bedrohungspotential
- Kurz – das System ist extrem sicher
- Seit langem in der Finanzwirtschaft bestens etabliert (ATM/POS – Netzwerke, Zahlungsverkehrssysteme, Börsensysteme ...
- „designed and built for security“ – auch in Bezug auf interne Bedrohungen

April 18, 2007 14

Why the Integrity NonStop server is more secure

Modularity isolates OS

- Modular NonStop operating system
  - HP NonStop OS functionality is handled by specialized system processes
    - memory manager,
    - communications manager,
    - network manager,
    - and disk access manager
  - No calls, communicate through interprocess messages

April 18, 2007 15

Why the Integrity NonStop server is more secure

No Memory Abuse

- Processes that run in their own virtual address space
  - non privileged process cannot view memory, or negatively impact, any other process running on the system
  - Processes send messages to each other; therefore, they cannot overwrite each other's memory
- Separation of code and data

April 18, 2007 16

Why the Integrity NonStop server is more secure

Minimum privilege

- Virus & Trojan have no chance to enter the system in the first place
- Virus & Trojan have no chance to execute non certified Code
  - application processes get limited administrator or root privileges
  - starts application under different user IDs, creating multiple security domains

April 18, 2007 17

Why the Integrity NonStop server is more secure

Less space for Human Errors

- Marginal complexity
- Simple system management
  - System Management
  - Security Management
  - Application Management
  - Database Management
- Very little chance for human err

April 18, 2007 18

Why the Integrity NonStop server is more secure

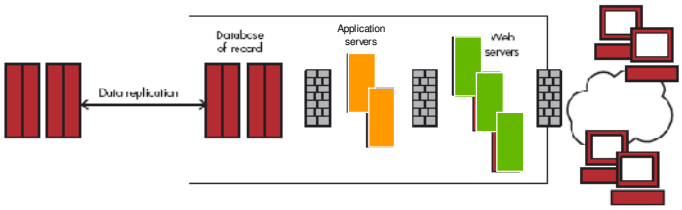
System access strictly controlled

- System management access restricted
  - Authentication, Authorization,
  - Auditing, Availability and manageability
  - Different roles and privileges for system manager and security manager
- Security management
  - application program interfaces (APIs)
  - Similar to IBM's RACF Resource Access Control Facility

April 18, 2007 19

Top Vulnerability to NonStop Servers

- N1 Insecure systems attached to the same network



Ein Trojaner im vorgeschalteten Webserver kann recht schädlich sein ...

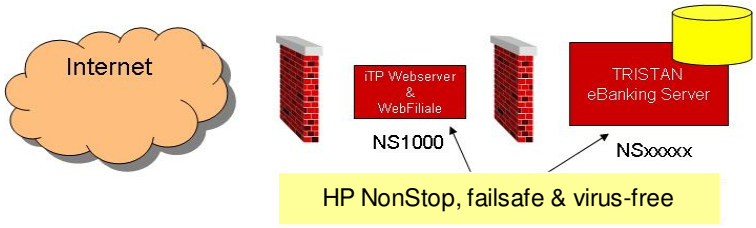
April 18, 2007 20

Bei hohen Sicherheitsanforderungen ...

... HP NonStop auch als Zugangsserver verwenden (iTP Webserver)
... Keine Fremdsysteme am gleichen Netzwerksegment

Beispiel Internet Banking (Lösung der Fa. XCOM):

2nd Generation eBanking:



April 18, 2007 21

Kosten der Sicherheit ?

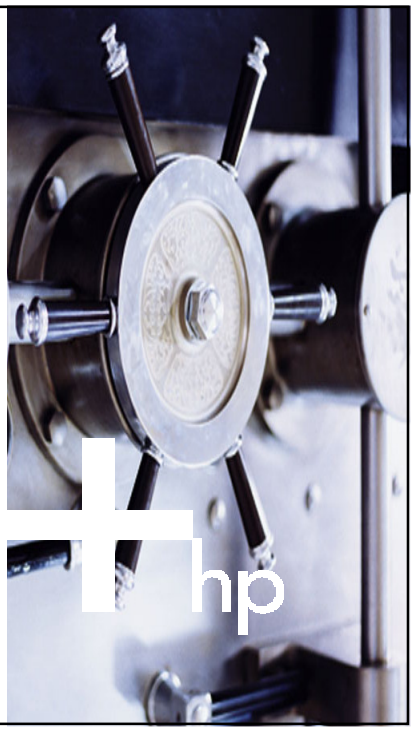
- **Wieviel geben Sie für Security Patching aus ?**
- **Keine bekannten Vulnerabilities, daher kein Security Patching bei HP NonStop**
- **(Auch) dadurch Betrieb mit geringerem Personalbedarf und höherer Verfügbarkeit**
- **Typischerweise werden bei HP NonStop im Vergleich zu Standardsystemen nur etwa 30 bis 50 % des Personals benötigt**
- **Besser und zugleich billiger ...**
- **Weitestgehende Eliminierung der Sicherheitsrisiken und der daraus resultierenden Missbrauchsverluste**
- **Sicherheitsprobleme können ein Unternehmen schnell in die Pleite treiben (Beispiel CardSystems ...)**

April 18, 2007 22

Atalla™

Security Products Group

Raising the bar
on security processing



Holger Villringer
Technology Consultant
HP NonStop Enterprise Division

Atalla Security Products Group (SPG)

- **Teil der NonStop Enterprise Division**
- **Spezialisiert auf die Hochleistungs – Kryptographie**
- **Marktführer in PIN - Verschlüsselung per Hardware**
  - **Für Geldautomaten, POS-Terminals und Zahlungsverkehrsnetze**
  - **Unterstützt die führenden Anwendungen im Bereich des Zahlungsverkehrs**

Atalla™ NSP series
Simple and secure manageability

- *Atalla* NSP remains secure even during management operations
- Tamper-resistant service audit log
- Secure key initialization is assisted by a portable graphical user interface
- Easy release upgrades via CD-ROM

April 18, 2007 25

Market and technology leadership

- **80% of North America market**
- **Over 1,350 financial institution customers worldwide**
- **Up to $9 trillion US $ secured by Atalla security engines every day**

Ihre Fragen ?