

Sicherheitsbedrohungen heute und mögliche Lösungen

Dirk.Schadt@CA.com

6.Mai 2004



Computer Associates®

ca.com

Charakteristik von IT Security

Funktionalität

Störung

Nutzen

- betrifft Organisation, Prozesse und Technik
- Störungen bestehen aus:
 - bewusstem und unbewusstem Missbrauch
 - Soft- und Hardware Fehlern
 - Design Mängeln
- Bedrohungsmodell \neq Geschäftsmodell
- ROI ist schwer nachweisbar
- der Schaden kommt durch die kleinste Lücke



Risiko ≠ Spielen

„A risk is a chance you take;
if it fails, you can recover.
A gamble is a chance taken;
if it fails, recovery is impossible.“

Field Marshall Erwin Rommel



Was ist ein “Risiko”?

- Das bewusste oder unbewusste Inkaufnehmen eines Verlusts in einer bestimmter Höhe im Verhältnis zu einer Wahrscheinlichkeit des Eintretens.
 - Mögliche Behandlung durch:
 - Abwehr
 - Abwälzung
 - Verminderung
 - Akzeptanz
 - Ignoranz
- je nach Typ des Risikos



Vorbeugende Maßnahmen I

Die informelle Vorsorge besteht aus

- der Definition und Umsetzung der **Sicherheitspolicy** und Richtlinien - (Geschäftsführung)
- der Schaffung ausreichenden **Sicherheitsbewusstseins** - (Awarenesskampagnen und Schulungen)
- der **Definition** und **Dokumentation** von **Verantwortlichkeiten** mit Vertretern für alle Sicherheitsbereiche
- der regelmäßigen **Kontrolle** der Maßnahmen zu den festgelegten **Sicherheitsrichtlinien** - (Datenschutz, Betriebsrat, Gesetze)
- der Beschaffung von Informationen zu aktuellen Systemschwächen - (Mcert & eTrust Vulnerability Manager)
- einer **Verwundbarkeitsanalyse**, **Risikoeinstufung** und „Best Practises“ - (Revisionsbericht, Auditierung & externe Beratung)
- der Erstellung von **Ersatzverfahren**, **Notfallplänen** und Erweiterung von Betriebshandbüchern - (DRP, BCP & Prozessmanagement)

Vorbeugende Maßnahmen II

Die technische Vorsorge besteht aus

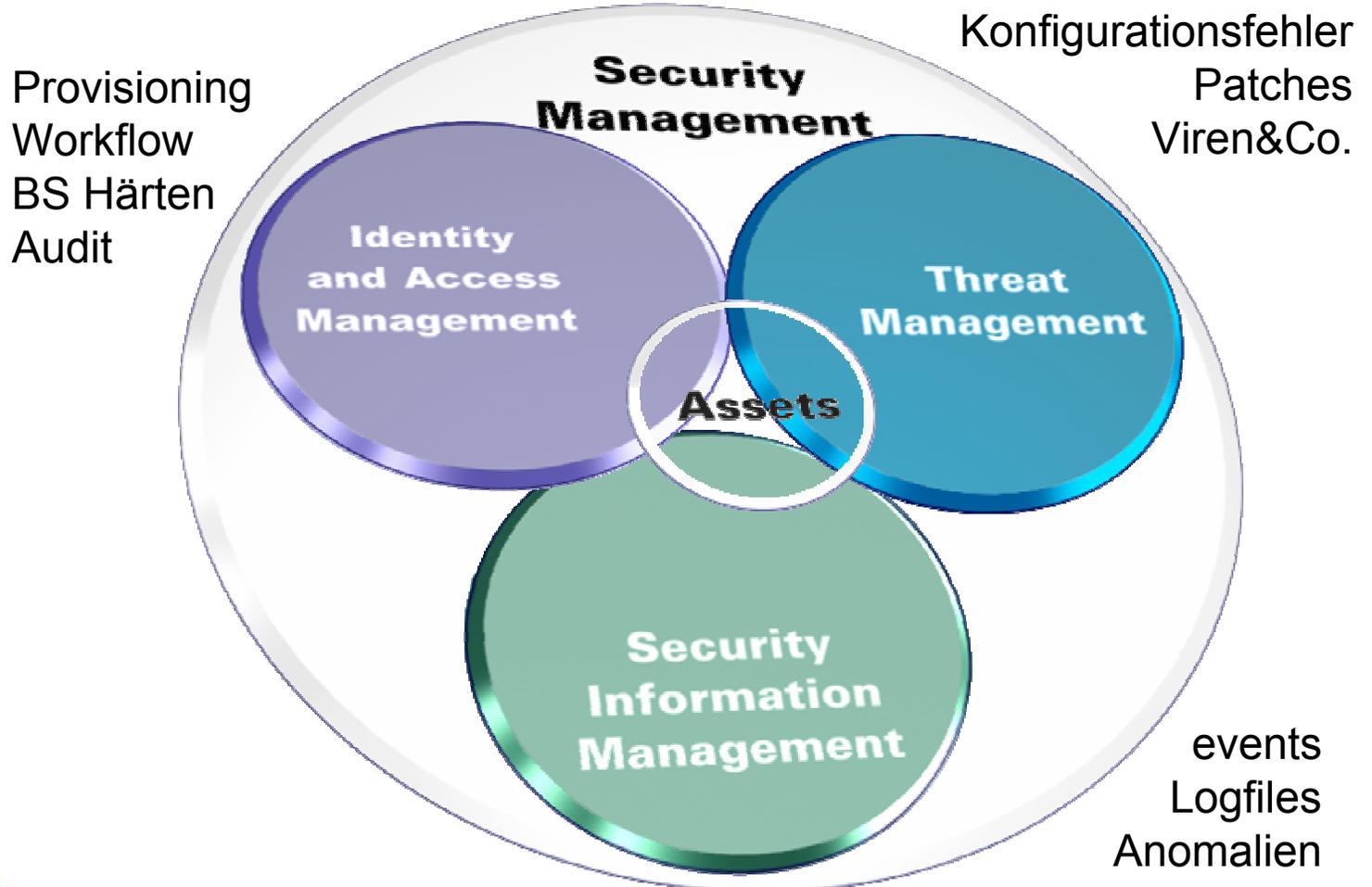
- der fortlaufenden **Feststellung von Existenz und Ausstattung** aller Endgeräte im Netzwerk einer IT-Landschaft
 - (Unicenter Asset Management)
- der **Kontrolle** von Klienten-Konformität zu den festgelegten **Sicherheitsrichtlinien** - (eTrust Policy Compliance)
- der Beschaffung von Informationen zu aktuellen Systemschwächen
 - (Mcert & eTrust Vulnerability Manager)
- einer **Verwundbarkeitsanalyse**, **Risikoeinstufung** und „Best Practise“ Empfehlungen - (Patch Management & eTrust Vulnerability Manager)
- zentraler **Softwareverteilung** zum Einspielen von Patches, Updates und neuen Software Releases die einem höheren Sicherheitsstandard entsprechen - (Patch Management & Unicenter Software Delivery)
- dem Themenbereich **Virenschutz vom Gateway bis zum PDA**
 - (eTrust Antivirus & Secure Content Manager)
- einer **zentralen Überwachung** aller Sicherheitsbereiche und eingesetzten Tools mittels einer zentralen portalbasierenden Management Konsole
 - (eTrust Security Command Center)
- dem **Präventivschutz** mittels **Disaster Recovery-Funktionen** für Server
 - (BrightStor Enterprise Backup inkl. Disaster Recovery Option)

Maßnahmen im Schadensfall

Lösungen für den Schadensfall umfassen die Themen

- **Feststellung** von unzureichendem Versionsstand, bzw. **Patch-Level** auf den betroffenen Zielsystemen - (Unicenter Asset Management, eTrust Policy Compliance & eTrust Vulnerability Manager & Patch Management)
- **Ausrollen** von Updates und Patches zur **Eliminierung von Sicherheitslücken** - (Unicenter Software Delivery)
- **Virenschutz Signaturen-Updates** der eingesetzten Antivirus Produkte - (eTrust Antivirus Pattern Update – eTrust Antivirus & Secure Content Mgr.)
- **Eröffnung** eines **Trouble-Tickets** im Service Desk - (Unicenter Service Desk)
- **Meldung** des Vorfalls unter Berücksichtigung seiner Auswirkung auf die **Geschäftsprozesse** des Unternehmens - (eTrust Security Command Center)
- **Forensische Analyse** von Quelle und Ursache der Bedrohung(en) und Unregelmäßigkeiten - (eTrust Network Forensics)
- **Systemwiederherstellung** - (BrightStor Enterprise Backup Disaster Recovery)

eTrust™ = Security Management



Computer Associates®

ca.com

eTrust™ Identity and Access Management

- Die Hauptkomponenten des Identity and Access Management Portfolio, mit gemeinsamer GUI sind:
 - eTrust Admin
 - eTrust Access Control
 - eTrust CA-ACF2
 - eTrust CA Top Secret
 - eTrust Clean-up
 - eTrust Directory
 - eTrust Single Sign On
 - eTrust Web Access control



Computer Associates®

ca.com

eTrust Security Command Center

- Eine zentrale Konsole
- Rollen-basierte Visualisierung und Administration
- Unterstützung einer Vielzahl von 3rd-Party Produkten
- Prozessoptimierung: Erkennen, Analysieren, Handeln
- “Drill Down” bei Bedarf — Ursachenforschung
- Erstellen von Zustandsmodellen
- Remote Control Möglichkeiten



Computer Associates®

ca.com

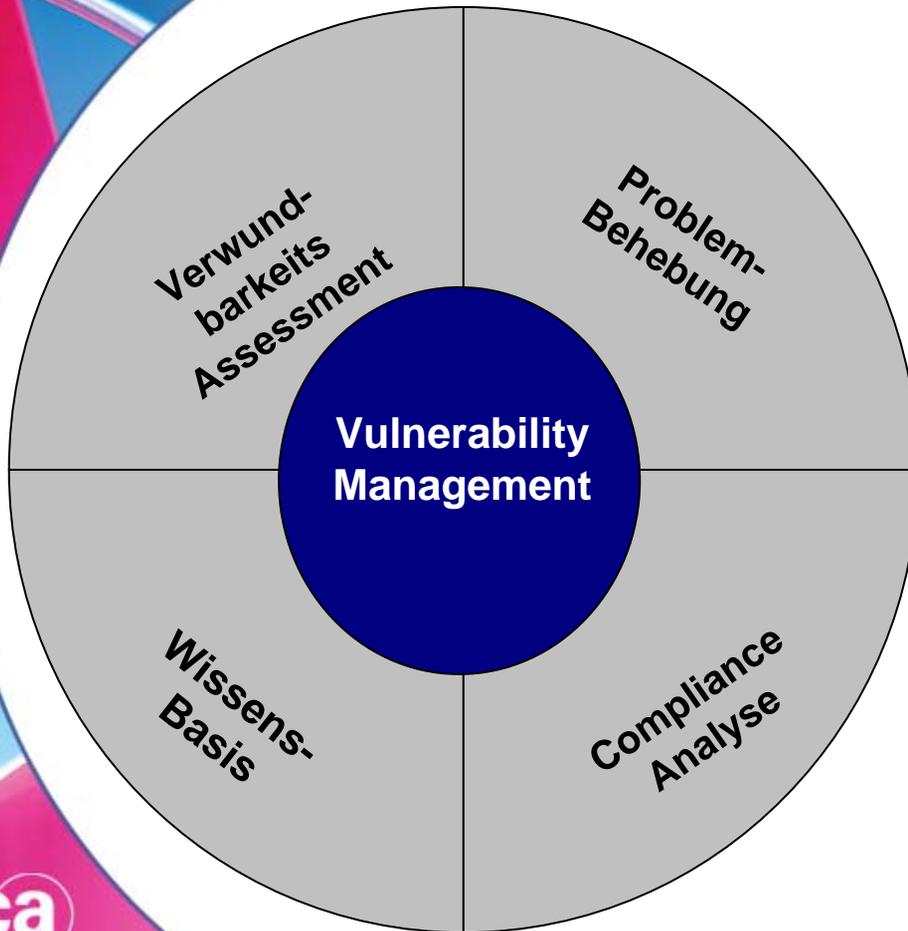
Atos-Origin: Olympiade Athen 2004

The image displays a Microsoft Internet Explorer browser window showing the eTrust Security Command Center interface. The browser title bar reads "eTrust Security Command Center - Microsoft Internet Explorer provided by Computer Associates Intl.". The interface includes a navigation menu with "WORKPLACES" and "KNOWLEDGE" tabs, and a search bar. The main content area is divided into two panes:

- Left Pane:** Titled "OIH - Olympic Indoor", it shows a network diagram with various nodes and connections. Nodes include "IDS Sensor 4210", "MGMT & IDS VLANs", "Catalyst 2950G-48G-E", and "VENU".
- Right Pane:** Titled "Test Olympic Map", it displays a 3D topographical map of the Olympic venue area. Numerous sports venues are marked with small images and labels, including: "Cycling (Mountain Bike)", "Marathon Start", "Canoe/Kayak (Sprint)", "Olympic Village", "Wrestling Judo", "Table Tennis Rhythmic", "Boxing", "Weightlifting", "Cycling (Road Race)", "Modern Pentathlon Bedminton", "Archery Marathon Finish", "Volleyball", "Taekwondo Handball", "Basketball Handball", "Fencing", "Baseball Softball", "Hockey Canoe/Kayak (Slalom)", "Equestrian", "Shooting", "Triathlon Cycling (Time Trial)", "Marathon Race", "Marathon Finish", "Athletics Tennis Basketball Water Polo Swimming Synchronised Swimming Diving Gymnastics Artistic Gymnastics Trampoline Cycling (Track)", and "Beach Volleyball".

The Windows taskbar at the bottom shows the "start" button, several open applications including "Inbox - Micros...", "eTrus...", and "Windows Media Pl...", and the system clock indicating "9:29 AM". A Computer Associates logo and "ca.com" are visible in the bottom left corner.

Treat Management



- **Vorsorge**
 - Virenschutz und Content Management
- **Verwundbarkeits Prüfung**
 - Identifizierung und Priorisierung der Verwundbarkeiten von Assets
- **Problembehebung**
 - Verwundbarkeits-basiertes Patch Management
 - Policy-basierte Konfigurations-Anpassung
- **Wissensbasis**
 - 24X7 Globales Research Team
- **Compliance Analyse**
 - Verifizierung der System Konfiguration in Anlehnung an ihre internen / externen Anforderungen

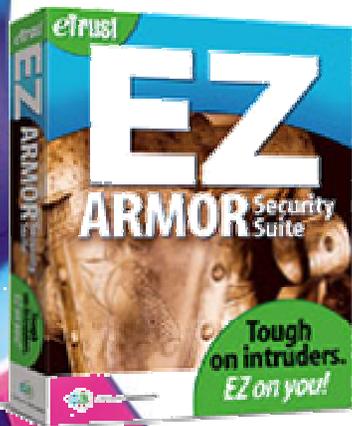


Computer Associates®

ca.com

FREE
Antivirus and
Firewall Software.
A \$49.95 value!

- Computer Associates (CA) unterstützt die „Protect Your PC“ Kampagne von Microsoft
- CA und Microsoft bieten ein kostenloses Sicherheitspaket für Privatanwender mit eTrust EZ Armor:
 - Antivirus und
 - Personal Firewall
- Gebührenfrei für 1 Jahr



<http://www.microsoft.com/security/protect>

<http://www.my-etrust.com/microsoft>



- Technik hilft nur bedingt, kann aber gut unterstützen
- ‚virtuelle‘ Risiken sind schwer einzuschätzen
- reaktive Kosten sind lästig, proaktive Ausgaben können zum Wettbewerbsvorteil führen
- Betreiben Sie Sicherheit so professionell wie den Rest Ihres Geschäfts

Fragen?



Welcome to the
eTrust Security Command Center

Please login:

User Name

Password

OK

 Computer Associates®

Dirk.Schadt@CA.com

www.ca.com/eTrust