

IT Sicherheit im Wandel



Von der sicheren Insel zum Netz der
Möglichkeiten

IT-Sicherheit im Wandel



Matthias Nagel

SNS Connect GmbH

Geschäftsfelder: IT-Sicherheit
 IT-Netzwerke
 IT-Service

Sitz in Hanau

www.snsconnect.de

Phasen der IT-Sicherheit



- Historie
- Gegenwart
- Ausblick
- Fazit

Historie



- Die Anfänge
 - Computer waren unverbundene Inseln
 - Datenaustausch über Transportmedien
 - nur Spezialanwendungen



Historie



- Beginn der Vernetzung
 - In den 70er Jahren kam das Internet
 - Kaum Bewusstsein für Sicherheit im Netz
 - Netze waren noch unabhängig voneinander



Geschichte



- Das Internet ist bis heute rasant gewachsen
 - Durchbruch kam mit dem WWW ab den 90er Jahren
 - Mail ist heute wichtigstes Kommunikationsmedium
- Die Netze wachsen zusammen

Bestandsaufnahme IT-Sicherheit heute



- Das Bewusstsein ist vorhanden
- Betriebssystemhersteller haben „Hausaufgaben“ gemacht

aber:

- Anwendungsprogramme teilweise noch katastrophal
- Je kleiner das Unternehmen, desto weniger wird für die IT-Sicherheit getan

Bestandsaufnahme IT-Sicherheit



- klassische Bedrohungsszenarien sind weitestgehend eingedämmt
- Mobile Computing und Cloud Computing stellt neue Anforderungen an die IT-Sicherheit, bietet aber auch neue Lösungen

Beispiele für Angriffe über das Internet



- „Erpresser verlangt zehn Millionen Dollar für ein Passwort“ (Spiegel Online 05.05.2009)
- Cyberattacke auf Estland am 27.04.2007 (Englische Wikipedia, Cyberattacks on Estonia)
- Defacement von Webseiten (www.zone-h.org)

Defacement Beispiel



Mirror saved on: 2004-08-07 13:06:48

Notified by: 404
System: Linux

Domain: <http://www.nicanordavid.com>
Web server: Apache

IP address: 69.72.218.26
[Notifier stats](#)

404 Not Found

The requested URL was not found on this server.

Additionally, a you have been **owned** by **404** !!

Apache/1.3.31 Server at www.blscs.com Port 80

Sicherheit neben der IT-Sicherheit

- „Festplatten bei Luftwaffe gestohlen“
(Focus Online, 25.05.2009)
- „Serverklau in Bad Hersfeld“
(c't magazin, 12.3.2011)
- „Patientenakten im Müll“
(Der Westen, 04.04.2011)
- „Festplatten mit Kontodaten auf eBay“
(heise online, 26.08.2008)



Wie geht man mit der Bedrohung um?



- Klassischer Schutz heute vorhanden
 - Firewalls heute fast überall vorhanden
 - Patche werden regelmäßig installiert
- Szenarien in der Gegenwart
 - Dezentrale Datenhaltung, starke Vernetzung untereinander
 - Mobile Mitarbeiter

Wie geht man mit der Bedrohung um?



- Durch permanente Verfügbarkeit der Daten und Verbundenheit mit dem Netz sind Angriffe immer und überall möglich
- Neue Strukturen teilweise sehr komplex

Neuer Ansatz



- Ergänzung der klassischen IT-Sicherheit
- Jetzt Prozesssicherheit und Funktionssicherheit
- Sicherheit ist nicht mehr ein Zusatz, sondern wird im Prozess integriert
- Jeder einzelne Schritt muss sicher werden

Neue Möglichkeiten nutzen

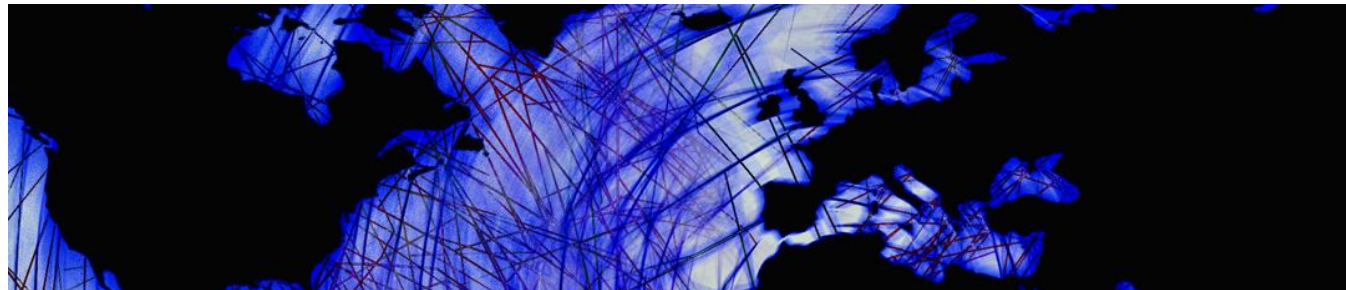


- Daten und Dienste sicher auslagern
 - Backup
 - Mail und Groupware Server
 - Virens Scanner

Ausblick



- Vernetzungsgrad nimmt zu
- Verschlüsselung wird immer wichtiger
- Nachweis der Identität wird immer wichtiger



Schwachstelle Mensch



- Der Mensch ist die größte Gefahr für die Daten
- Die Abwehrtechnik wird immer besser
- Social Engineering verspricht den größten Erfolg für Angreifer

Zusammenfassung



- IT-Sicherheit ist und bleibt wichtig
- Bedrohungsszenarien ändern sich
- Kriminalität wird zum Geschäftsmodell
- Den Bereich „neben“ der Technik im Blick behalten

Zusammenfassung



- Probleme
 - Zu viel Sicherheit wird als störend empfunden
 - Sicherheit fällt nicht positiv auf, wenn sie funktioniert, nur negativ, wenn sie nicht funktioniert

Zusammenfassung



- Lösungen
 - Sensibilisierung der Anwender
 - Sicherheit muss Teil des Ganzen werden
 - Integriert in alle Prozesse
 - Sicherheit selbst wird zum Prozess

Fragen?