Fachhochschule Gelsenkirchen

Lage der IT-Sicherheit

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

- **Motivation**
- **Herausforderungen in der IT**
- **Moderne IT-Sicherheitslösungsansätze**
- **Ausblick**

Inhalt

- **Motivation**
  - Herausforderungen in der IT
  - Moderne IT-Sicherheitslösungsansätze
  - Ausblick

Lage der IT Sicherheit
→ Motivation

- **Veränderung, Fortschritt, Zukunft**
  - Entwicklung zur **vernetzten Informations- und Wissensgesellschaft**.

- **IT-Sicherheit ist eine sich verändernde Herausforderung**
  - Das Internet geht über alle Grenzen und Kulturen hinaus
  - Zeit und Raum werden überwunden!
  - Die zu schützenden Werte steigen ständig
  - Die Werte, die wir schützen müssen, ändern sich mit der Zeit!
  - Die Angriffsmodelle innovieren und Angreifer werden professioneller
  - IT-Sicherheitsmechanismen werden komplexer, intelligenter und verteilter
  - **Mit der Zeit werden die Sicherheitsprobleme immer größer!**

Lage der IT Sicherheit
→ ~ 1985: Kommunikationssicherheit

- **IT-Trend:**
  - Mit dem PC kam eine Individualisierung und Dezentralisierung der IT.
  - Der Wunsch, diese dezentralen IT-Systeme über Leitungen oder Daten-Netze, wie X.25-Netz zu verbinden.

- **IT-Sicherheitstrend:**
  - Mit ***Leitungsverschlüsselung*** (Modem, 2 MBit/s, …) und ***X.25-Verschlüsselungsgeräten*** die neuen Sicherheitsprobleme lösen.

- **Unsere Einstellung:**
  - Wir müssen uns beeilen, sonst sind alle IT-Sicherheitsprobleme gelöst.

Lage der IT Sicherheit
→ ~ 1995: Perimeter Sicherheit

- **IT-Trend:**
  - Unternehmen haben sich ans Internet angeschlossen, um am **E-Mail-** und **Web-System** teilhaben zu können.
  - Zusätzlich wurden Niederlassungen über das Verbundnetz Internet einfach angebunden.

- **IT-Sicherheitstrend:**
  - Abwehrmodell: Firewall- und VPN-Systeme
  - Digitale Signatur, E-Mail-Sicherheit, PKI

- **Unsere Einstellung:**
  - Wir haben die IT-Sicherheitsprobleme im Griff!

Lage der IT Sicherheit
→ ~ 2005: Malware / Software-Updates

- **IT-Trend:**
  - Immer mehr PCs, Notebooks, SmartPhones zunehmend über GSM, UMTS, … (an der zentralen Firewall vorbei) ins Internet
  - Die Anzahl der Schwachstellen durch **Softwarefehler** wird immer größer (die Marktführer im SW-Bereich erkennen, dass es einen SW-Entwicklungsprozess gibt :-))

- **IT-Sicherheitstrend:**
  - **Verteilte Softwareangriffe** mit Hilfe von Trojanischen Pferden
  - Anti-Malware, Software-Upgrades und Personal Firewalls
  - Generierung der Sicherheitslage

- **Unsere Einstellung:**
  - Die IT-Sicherheitsprobleme wachsen uns über den Kopf!

Inhalt

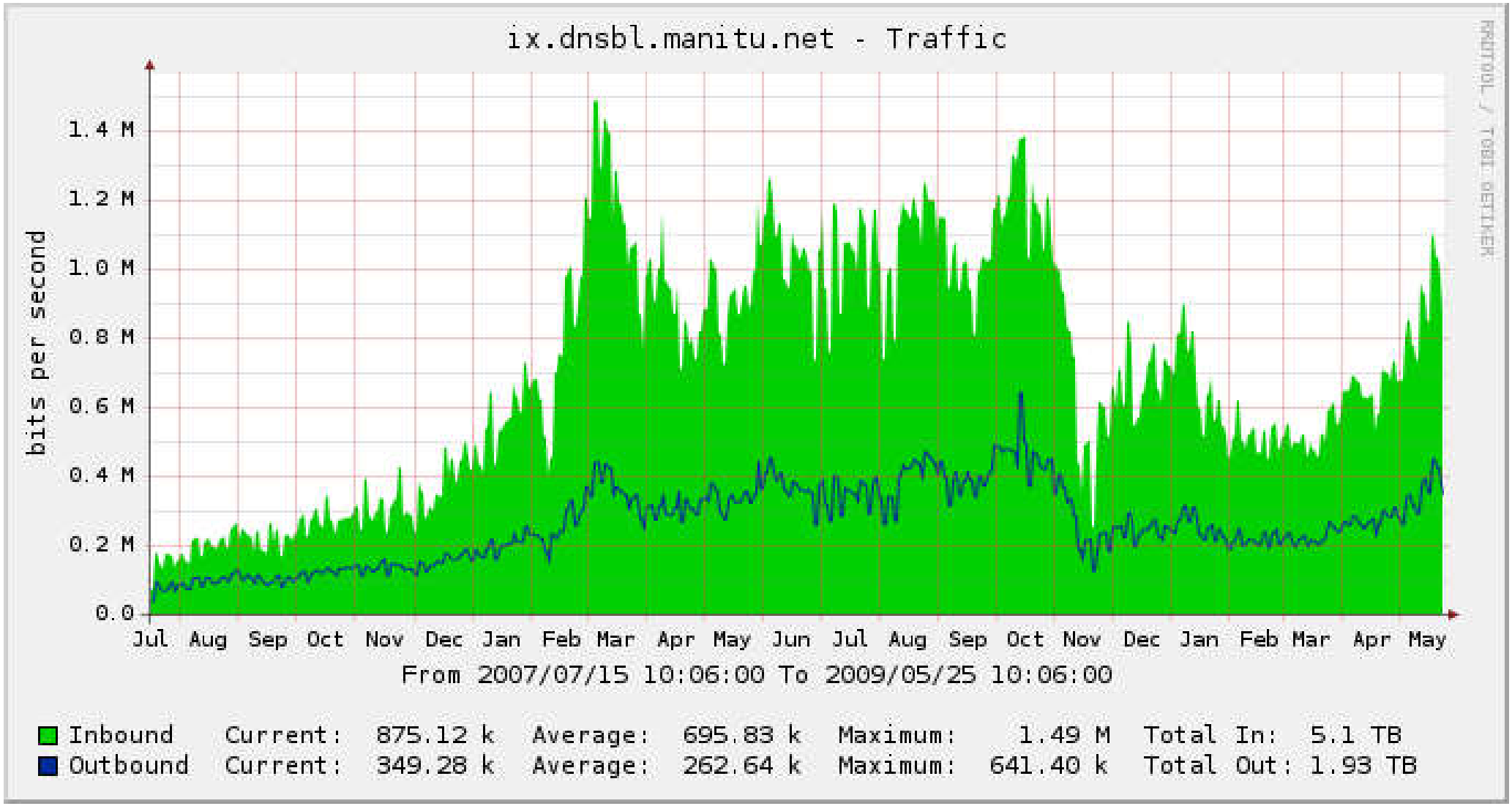
- Motivation
- **Herausforderungen in der IT**
- Moderne IT-Sicherheitslösungsansätze
- Ausblick

Herausforderungen in der IT
→ E-Mail Sicherheit

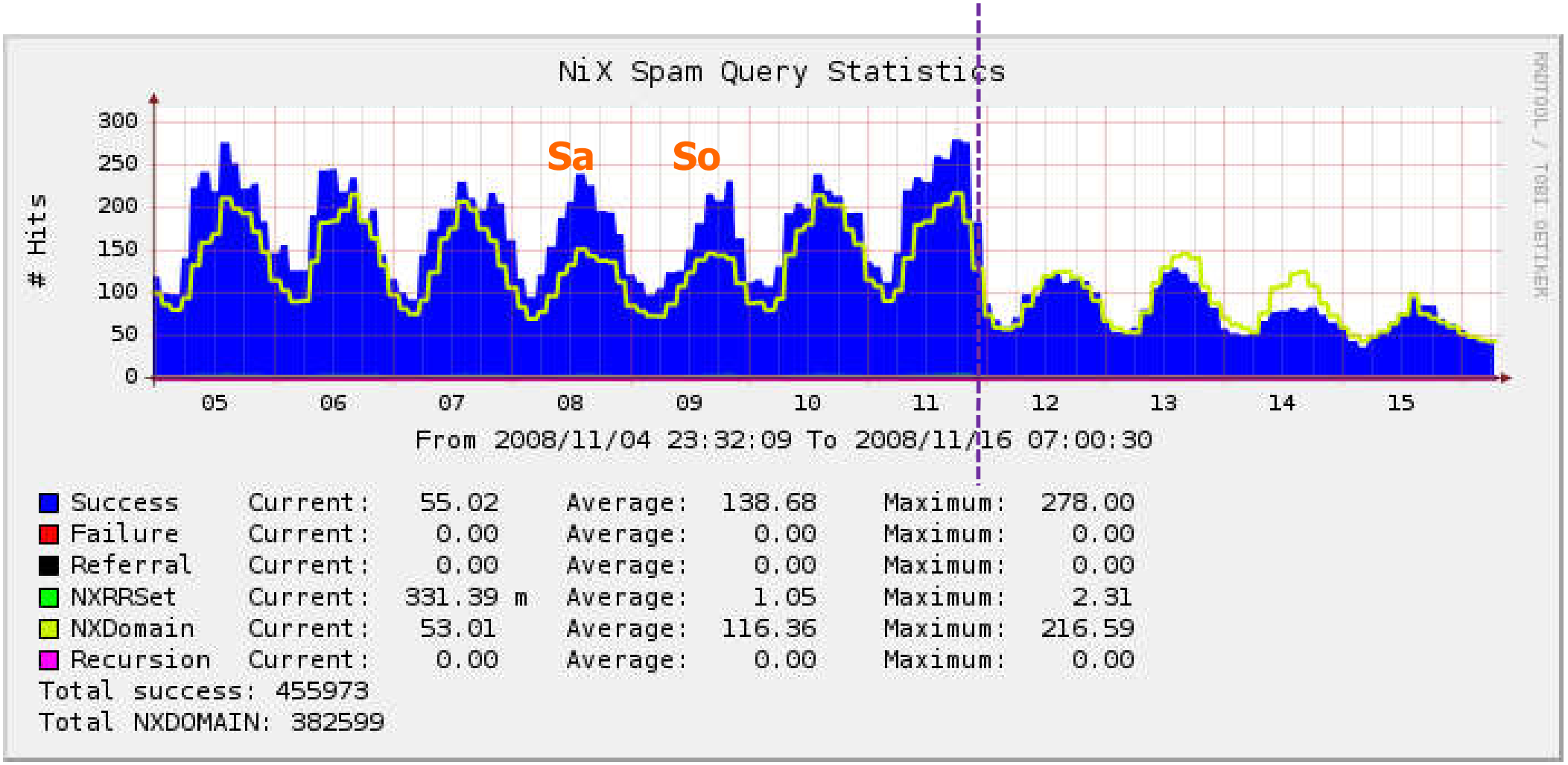
- Verschlüsselte E-Mails weniger als 4 %
  (S/MIME, PGP, Passphrase-gestützt, …)
- Signaturen unter E-Mails weniger als 6 %
  (Finanzbereich deutlich mehr)
- Spam-Anteil größer als 95 % (in der Infrastruktur)

- **Was kommt in der Zukunft?**
  - DE-Mail (ab ~2010?) → Bürgerportal Gesetz?
    - SSL-Verschlüsselung zwischen den Gateways
    - Zustell-Garantie
    - Verpflichtende Authentifizierung
    - Sichere Dokumentenablage

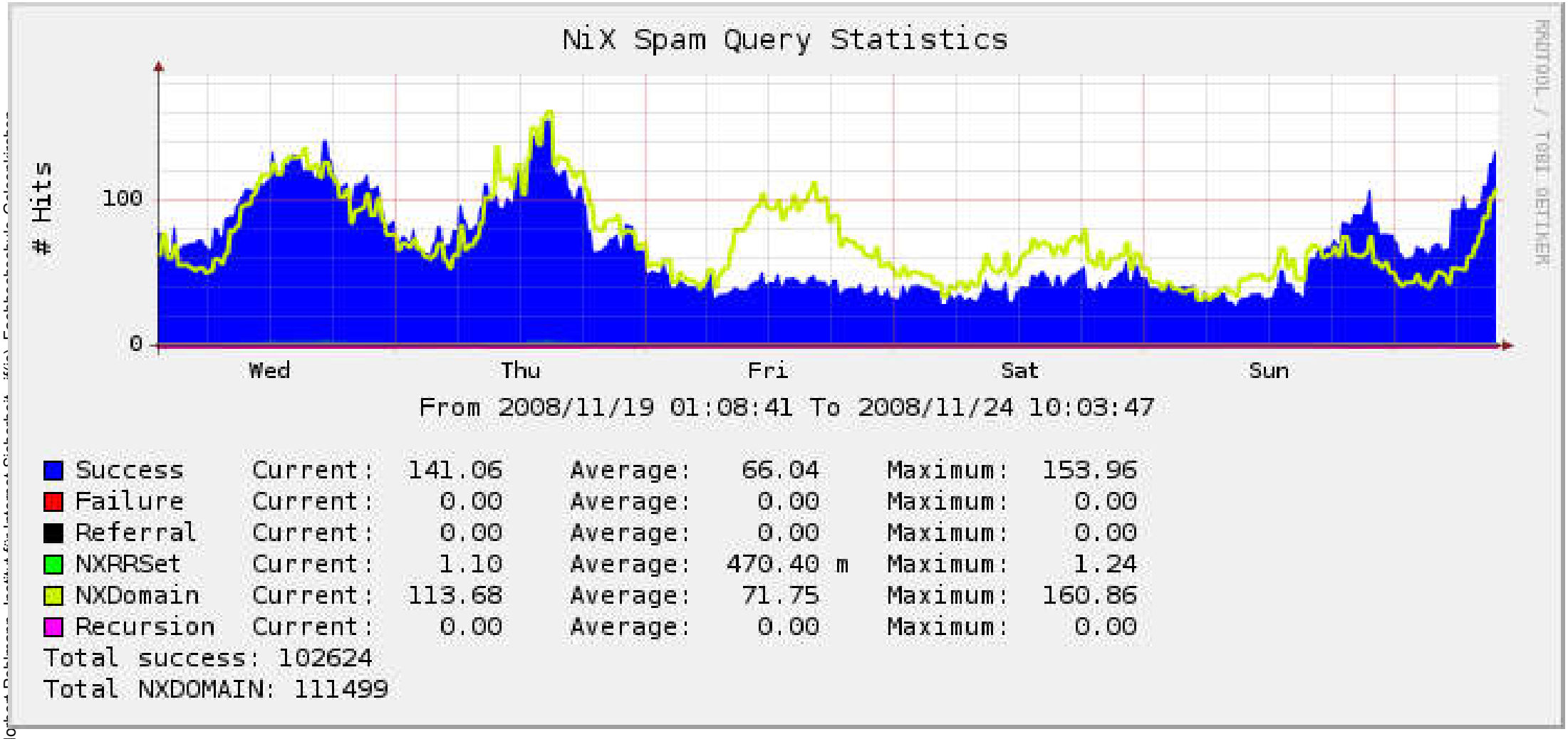
Spam
→ Das Problem



McColo (US ISP) taken offline → 11/11/2008



DDoS on InternetX (Schlund NS) → 21/11/2008



Herausforderungen in der IT
→ Identity Management

- **Passworte**, **Passworte**, **Passworte**, … sind das Mittel für eine Authentikation im Internet!
- Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld, nicht international!
- Föderationen sind noch nicht verbreitet genug!

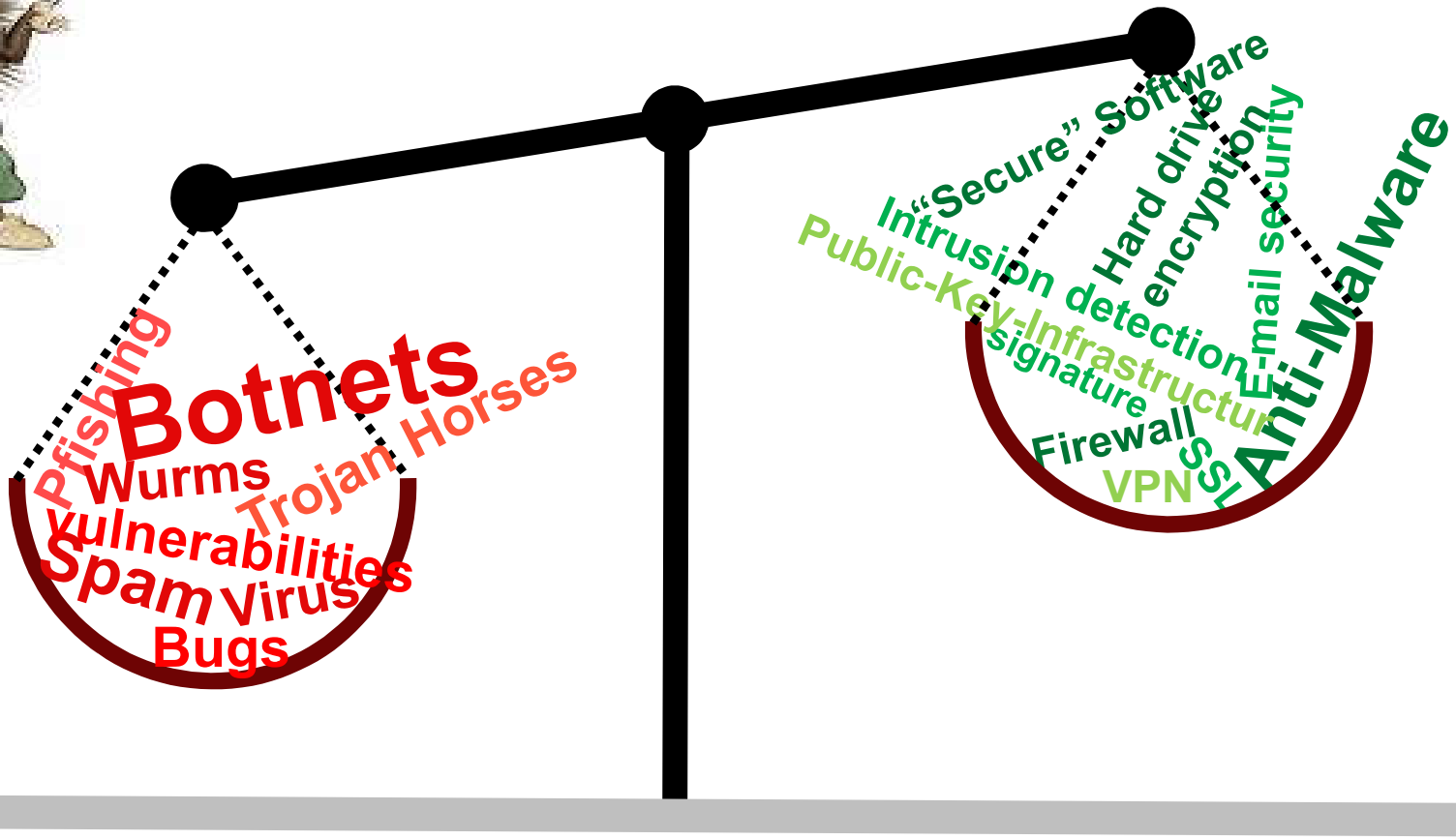
- **Was kommt in D?**
  - **ePA** (elektronischer Personalausweis mit Authentikationsfunktion)

Herausforderungen in der IT
→ Webserver Sicherheit

- **Schlechte Sicherheit auf den Webservern / Webseiten**
  - Heute wird Malware hauptsächlich über Webseiten verteilt
  - Viele Webseiten sind nicht sicher aufgebaut
  - Patches werden nicht oder sehr spät eingespielt (siehe Analyse if(is))
  - SSL nicht richtig verwendet

- **Gründe**
  - Firmen geben kein Geld für IT-Sicherheit aus!
  - Mitarbeiter haben keine Zeit (Geld)
  - Verantwortliche kennen das Problem nicht!

IT Sicherheit und Vertrauenswürdigkeit → Unser Problem (1/2)



- Gefahren / Angriffe - **- Sicherheitsmechanismen -**

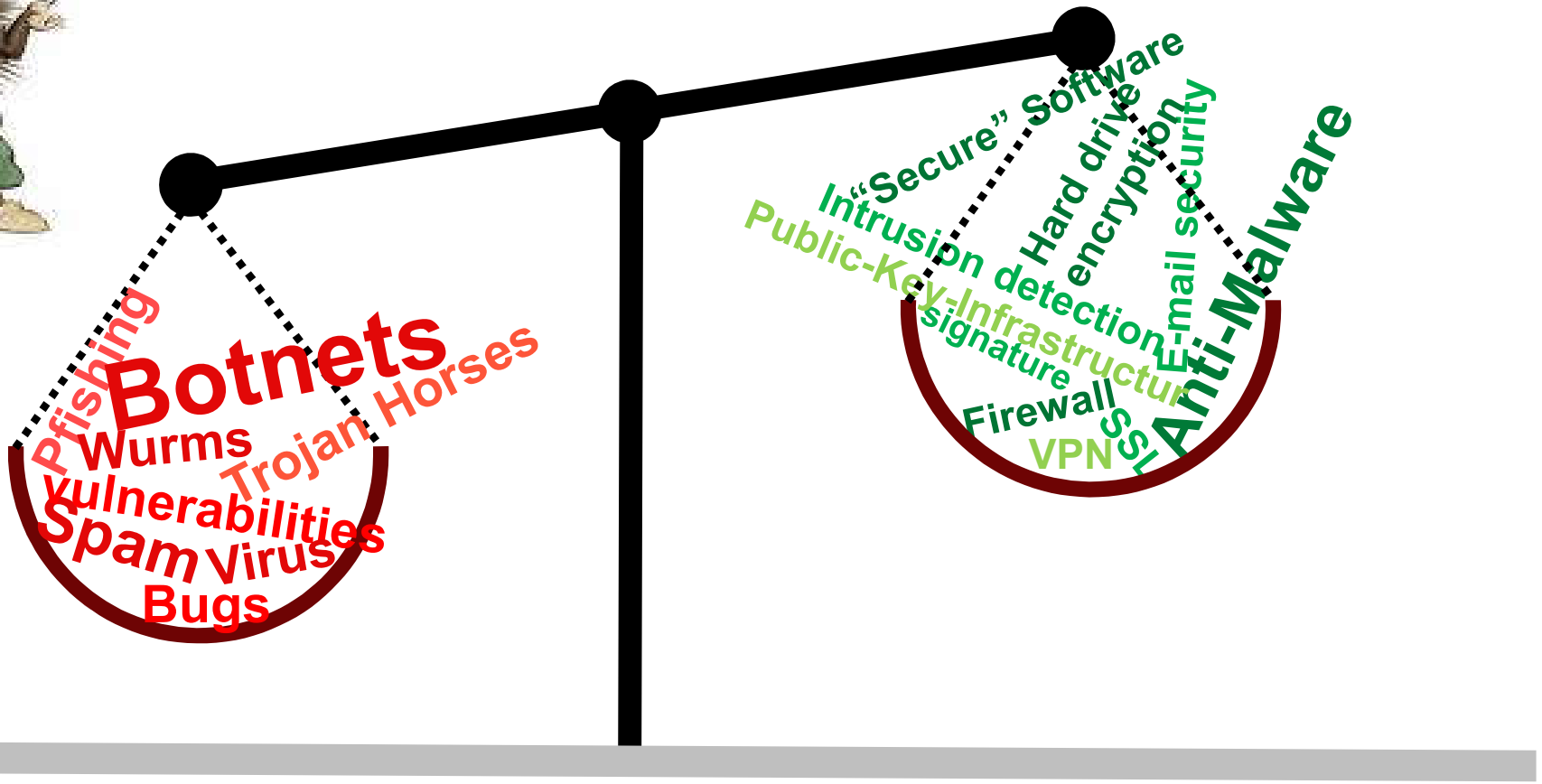
IT Sicherheit und Vertrauenswürdigkeit → Unser Problem (2/2)

- Wir rennen den IT-Angriffen hinterher!

- Anti-Malwareprodukte reichen nicht mehr aus!
  - Millionen Rechner sind mit „Trojanischen Pferden“ verseucht!
  - Sehr große Botnetze kontrollieren unsere IT-Systeme (PCs, Notebook, …)
  - Unsere IT-Systeme werden fremd-gesteuert und …
    - spammen
    - werden für Pfishing Angriffe genutzt!
    - sammeln Passworte
    - werden als DDoS-Hilfsmittel verwendet
    - …

- **Der Level an Vertrauenswürdigkeit unserer IT-Systeme ist ungenügend!**

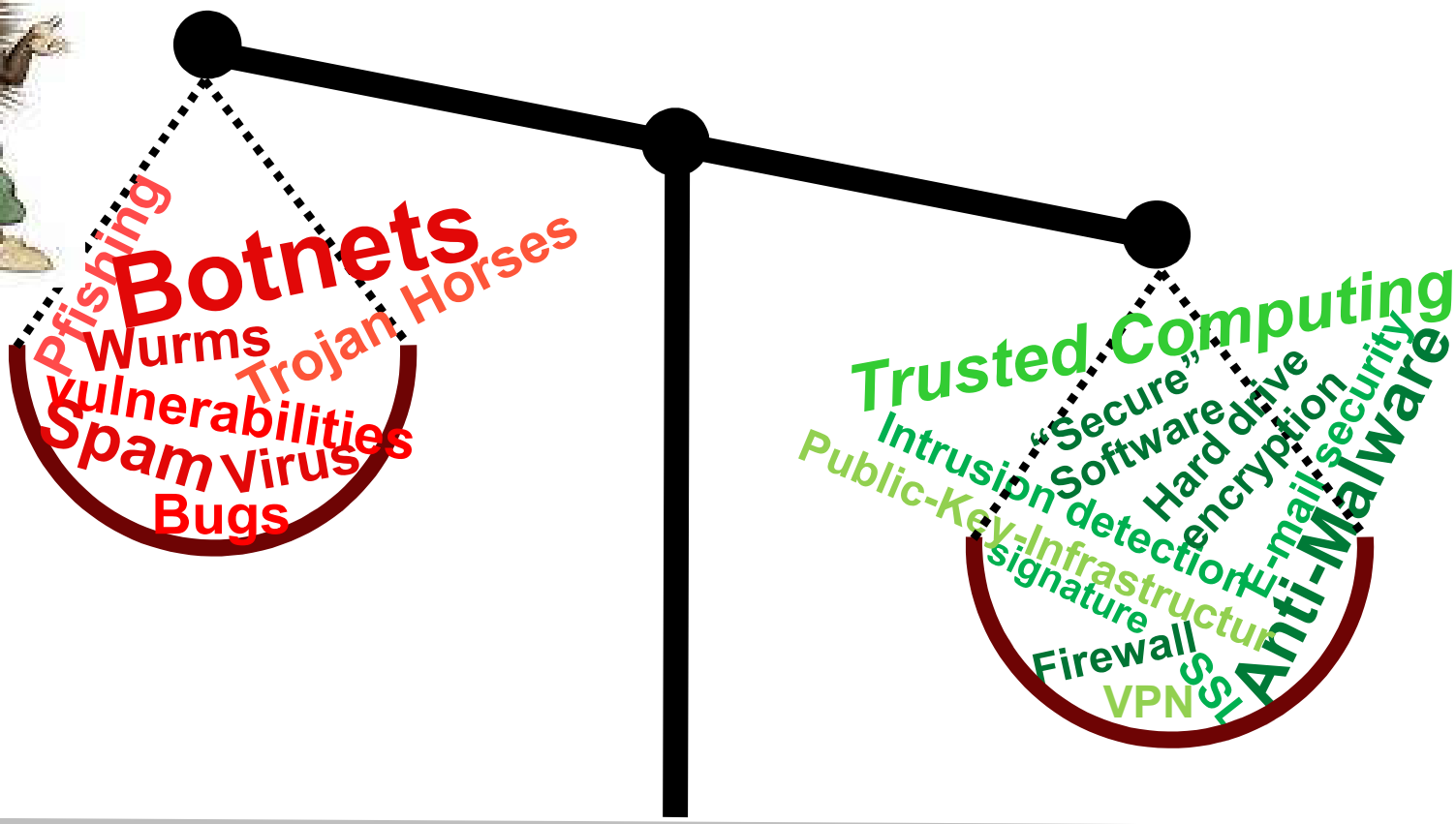
IT Sicherheit und Vertrauenswürdigkeit → Unser Ziel (1/2)



- Gefahren / Angriffe - **- Sicherheitsmechanismen -**

IT Sicherheit und Vertrauenswürdigkeit → Unser Ziel (2/2)

angemessenes Sicherheitsniveau



- Gefahren / Angriffe - **- Sicherheitsmechanismen -**

Inhalt

- Motivation
- Herausforderungen in der IT
- **Moderne IT-Sicherheitslösungsansätze**
- Ausblick

Sicherheitsplattform/Trusted Computing → Motivation

Wir brauchen eine vertrauenswürdige IT,
realisierbar durch eine Sicherheitsplattform,

- die **Sicherheitsprobleme** existierender Rechnersysteme löst, bzw. die schädlichen Auswirkungen von z.B. Viren, Würmern, Trojanern, Phishing, Exploits, SW-Updates, …, stark einschränkt.
- die eine vertrauenswürdige Verarbeitung von Informationen auf dem **eigenen** und auf **fremden** Rechnersystemen garantiert.
- die die Verwendung existierender Betriebssysteme unterstützt.
- die transparente Sicherheit (Vertrauenswürdigkeit) bietet.

Trusted Computing
→ Idee

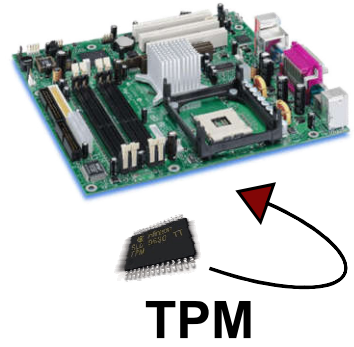
- ***Trusted Computing Group (TCG):***
  Industriekonsortium bestehend aus den führenden 126 IT-Firmen
  (Hewlett-Packard, IBM, Intel, AMD, Microsoft, Sony, Sun, Infineon, ...)

- ***Grundmotivation***
  - Entwicklung **offener Spezifikationen** für **vertrauenswürdige IT-Systeme** (Server, PC, eingebettet, usw.)
  - Sicherheit verteilter Anwendungen mit wirtschaftlich vertretbarem Aufwand verbessern
  - Keine massive Veränderung existierender Hard- bzw. Software

- ***Hauptidee***
  - Manipulationssichere Komponente in Hardware (sicherer als Software)
    → Stärkung gegen Software-basierte Angriffe
  - Sicherheit des Systems reduziert auf die Sicherheit eines Moduls
  - Integrität und Authentizität eines IT Systems zuverlässig überprüfbar, auch aus der Distanz

Trusted Computing
→ Funktionen (1/2)

- ***Trusted Platform Modules (TPM)***
  - Sicherer Zufallsgenerator (sichere kryptographische Schlüssel)
  - Kryptographische Funktionen: Signatur (RSA), Hash (SHA-1)
  - Erzeugung verschiedener kryptographischer Schlüssel
  - **Platform Configuration Register (PCR) → Zur Speicherung der Systemkonfiguration**



- ***Sicherer Speicher***
  - Erzeugung sicherer kryptographischer Schlüssel und
  - Speicherung Schlüssel im Hardwaremodul

- ***Sealing (versiegeln)***
  - Kryptographische Schlüssel können an das IT-System und/oder eine bestimmte Softwarekonfiguration gebunden werden
    - → Schutz vor Manipulationen des Betriebssystems

Trusted Computing Group
→ Funktionen (2/2)

- ***(Remote) Attestation***
  - Aktuelle Systemkonfiguration des IT-Systems wird dargestellt
  - Erkennung manipulierter IT-Systeme (Verteilte Systeme, Web-S.)
  - Kommunikation nur mit vertrauenswürdigen IT-Systemen
- ***Access Control***
  - Durchsetzung von Zugriffsregeln in einem Netzwerk mit unbekannten IT-Systemen (TNC)
- ***Überprüfbares Booten***
  - Systemkonfiguration kann überprüft werden, z.B. mittels eines persönlichen Gerätes (Smarcard, USB-Stick, Handy, …)
- ***Verbreitung von TPMs***
  - 60 Millionen bis Ende 2007
  - 130 Millionen bis Ende 2008
  - 200 Millionen bis Ende 2009

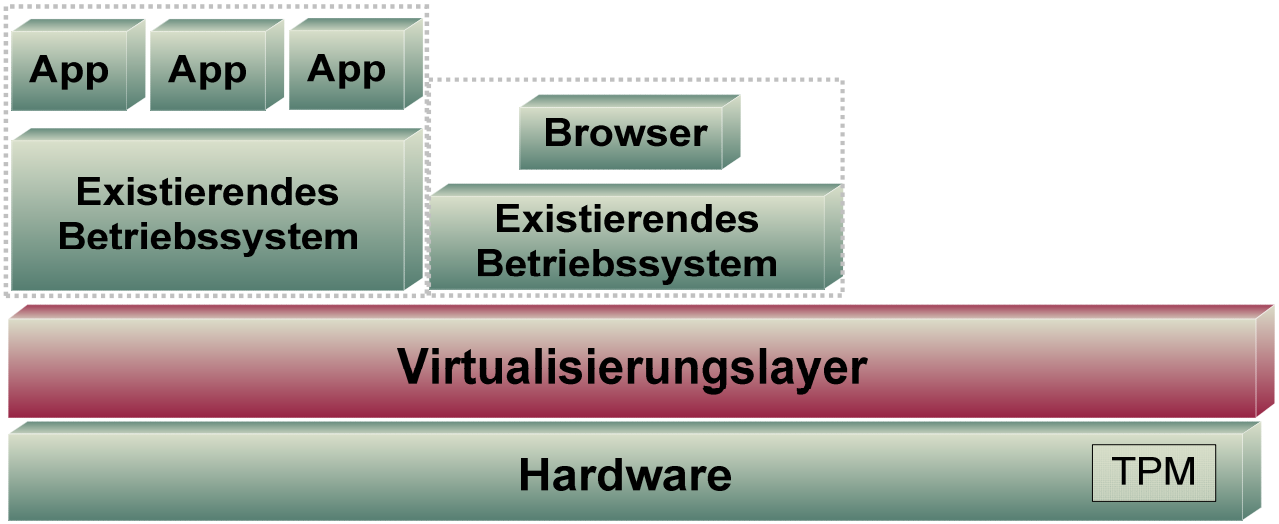
TPM

Sicherheitsplattform Turaya
→ Architektur und Technologie 1/3

- ***Herkömmliche Hardware***
  - CPU / Hardware Devices
- ***TPM***
  - Höchster Schutz durch hardwarebasierte Sicherheit
- ***Vorteile der Trusted-Computing-Technologie nutzen***

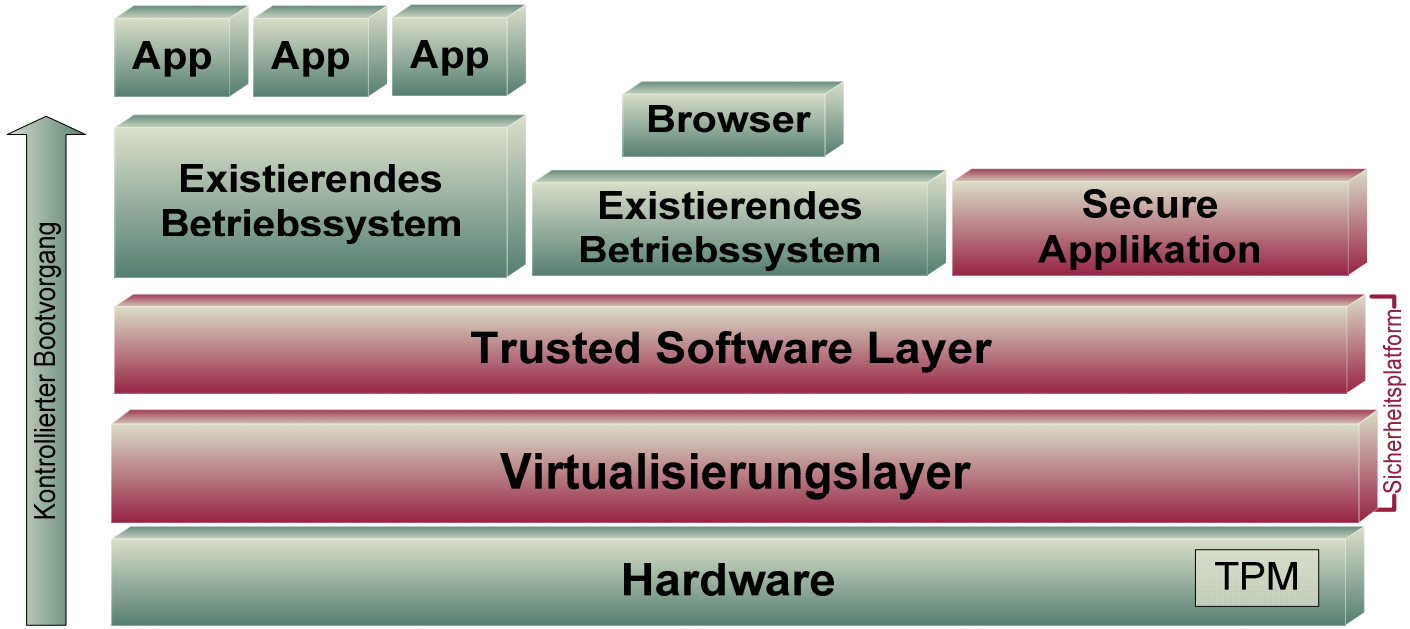
Sicherheitsplattform Turaya
→ Architektur und Technologie 2/3

- ***Virtualisierungslayer zur Isolation ...***
  - Schutz der Applikationen
  - Schutz der Anwenderdaten
  - Schutz vor Manipulationen einer Applikation (bspw.: Browser)
- ***... mittels moderner Virtualisierungstechniken***
  - Mikrokern-Architektur
  - Verwendbarkeit existierender Komponenten in Compartments



Sicherheitsplattform Turaya
→ Architektur und Technologie 3/3

- ***Sicherheitsplattform (Trusted Software Layer)***
  - **Authentifikation** einzelner Compartments
  - **Binden von Daten** an einzelne Compartments
  - **Trusted Path**
    - Zwischen Anwender & Applikation / Applikation & Smartcard
  - **Sicheres Policy Enforcement**



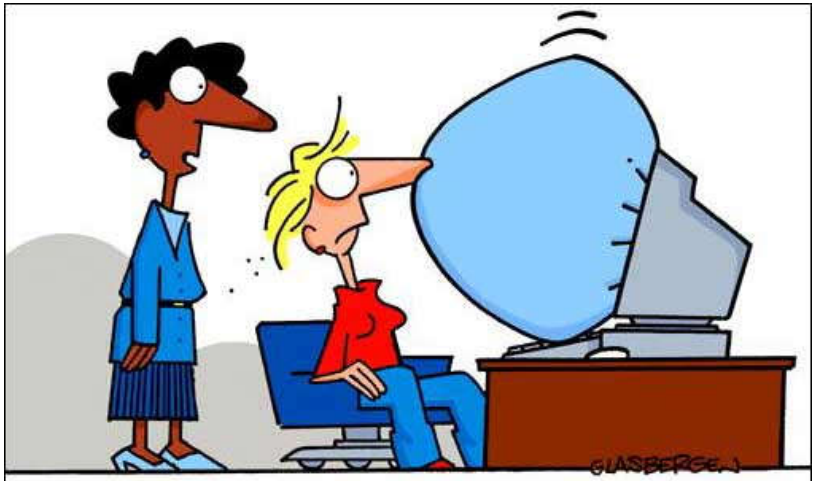
Sicherheitsplattform / TPM
→ Ein Quantensprung in der IT-Sicherheit

- Mit Hilfe von Sicherheitsplattformen können wir das **Risiko minimieren**!
  - Minimale SW-Basis für die Kontrolle der Ressourcen
  - Kombiniert mit Sicherheitsanwendungen

- Mit der Kombination von **TPM**s und einer **Sicherheitsplattform**, z.B. **Turaya** können wir unsere IT-Systeme auf einem hohen Sicherheitslevel auf Integrität hin überprüfen und damit **SW-Angriffe** verhindern!

- Damit erreichen wir einen **Quantensprung in der IT-Sicherheit** und **Vertrauenswürdigkeit** für unsere IT-Systeme!

- **Der Airbag für unsere IT-Systeme!**



"It's the latest innovation in office safety.
When your computer crashes, an air bag is activated
so you won't bang your head in frustration."

Inhalt

- Motivation
- Herausforderungen in der IT
- Moderne IT-Sicherheitslösungsansätze
- **Ausblick**

Lage der IT Sicherheit
→ Ausblick

- **Schnellere Verbreitung von Informationen und Wissen**
  - Schnellere Innovationen
  - Wie schützen wir Wissen?
    (Trend zum freien Mitarbeiter)

- **Mehr Prozessoren, mehr Kommunikation**
  - Von überall auf alles Zugriff
  - Neue IT-Sicherheitsarchitekturen sind notwendig
    (Sicherer Mikrokern, Trusted Computing, …)

- **Sehr viel mehr Leistungen**
  - Erzeugt mehr nutzbare künstliche Intelligenz
  - Jeder bekommt SW-Assistenten und kann optimierter arbeiten

- **Sehr viel mehr Intelligenz steht zur Verfügung**
  - Neuer Wert (Intelligenz + Wissen), der geschützt werden muss

Ausblick
→ Zusammenfassung

- Wir müssen etwas tun,
  um unsere Zukunft **sicherer** und **vertrauenswürdiger** zu gestalten.

- Dazu brauchen wir einen **Quantensprung**
  - in der **Sicherheitstechnologie**,
  - in der **Vorgehensweise** und
  - in der **Zusammenarbeit** mit anderen.

- Die Zukunft beginnt jetzt, also lassen Sie uns anfangen!

Fachhochschule Gelsenkirchen

Lage der IT-Sicherheit

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.