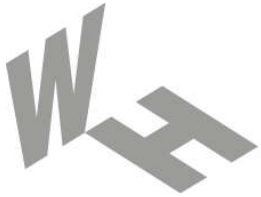


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyberkriminalität
→ Wie kann ich mich schützen?

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

Inhalt

- **IT-Sicherheit**
  (Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**
  (Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Selbstschutz**
  (Basisschutz, richtiges Verhalten, …)
- **Innovationen im Bereich IT-Sicherheit**
  (spotuation, Xign, Quvert, …)

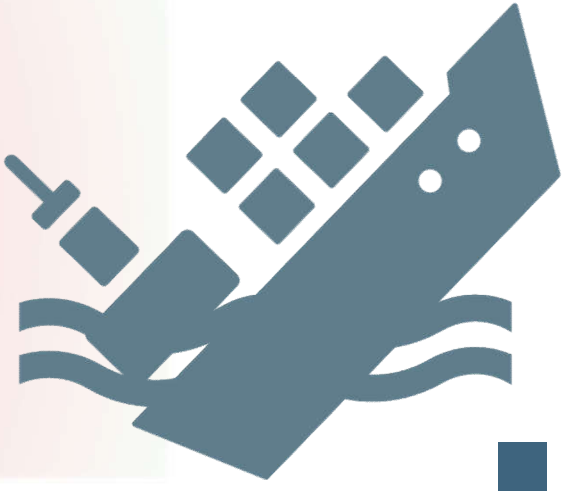
Inhalt

- **IT-Sicherheit**
  (Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**
  (Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Selbstschutz**
  (Basisschutz, richtiges Verhalten, …)
- **Innovationen im Bereich IT-Sicherheit**
  (spotuation, Xign, Quvert, …)

IT und IT-Sicherheit
→ Situation

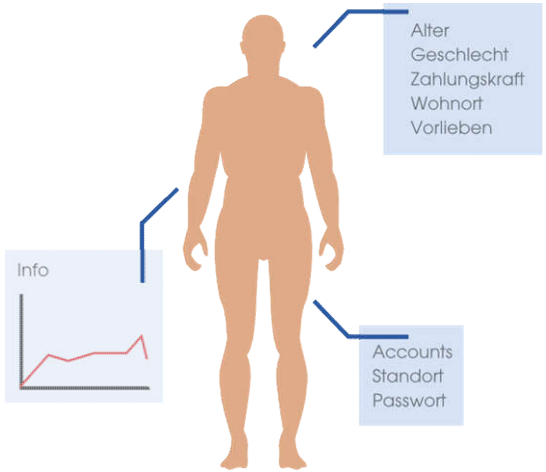
- IT ist **„der Motor“** und **die Basis** für das **Wohlergehen** unserer modernen und globalen **Gesellschaft.**
- Der **Digitalisierungsprozess** wird **immer schneller** und damit auch die **Veränderungen** in unseren **Lebensräumen.**
- Unsere Arbeit, unsere Firmen, unsere Hochschulen, unsere Freizeit, unser ganzes **Leben wird sich wandeln**.

- Die IT und IT-Sicherheitstechnologien sind nicht sicher und vertrauenswürdig genug *(**Widerstandsfähigkeit**)*!
- Professionelle **Hacker greifen** alles **erfolgreich an!**
- Das **Risiko wird immer größer**, die Schäden auch!

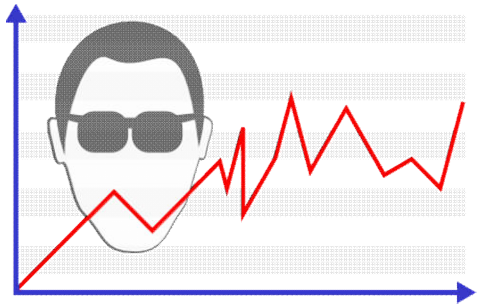


Immer noch nicht sicher?
→ Problemfelder

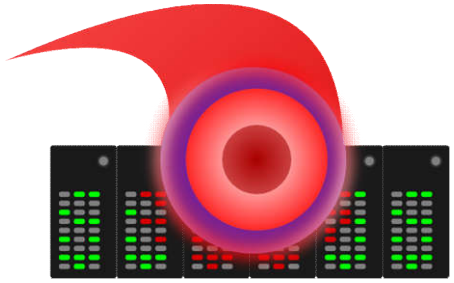
- **Privatheit und Autonomie**
  - → Kulturelle Unterschiede
  - → Geschäftsmodelle „Bezahlen mit persönlichen Daten“
  - → Staat (NSA, BND, …):
    Identifizieren von terroristischen Aktivitäten
  - → Nutzer: Autonomie im Sinne der Selbstbestimmung



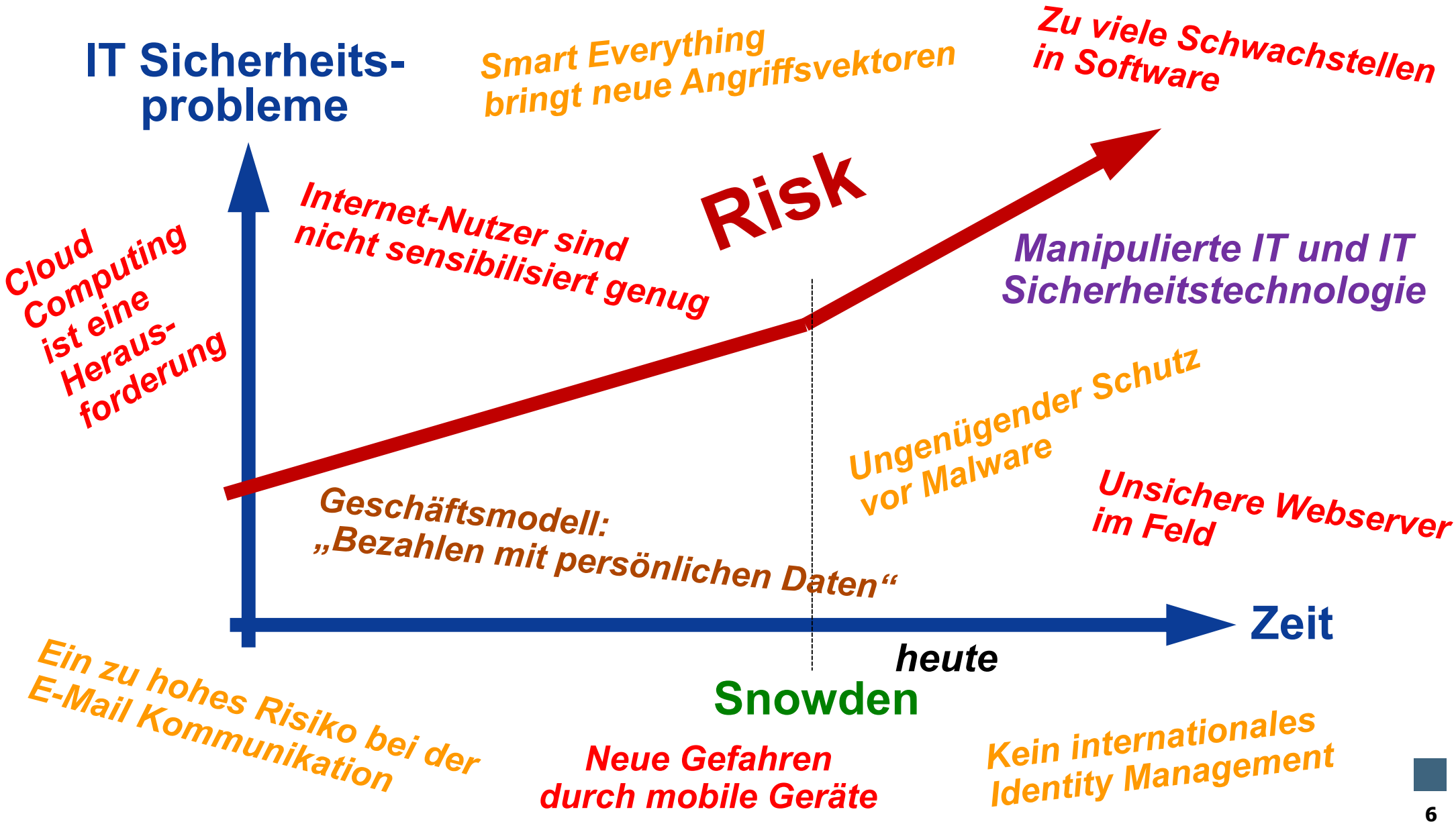
- **Wirtschaftsspionage**
  - → 51 Milliarden Euro Schaden im Jahr
  - → Internet-Kriminalität; ca. 100 Mio. im Jahr
    (Online Banking, DDoS, …)



- **Cyber War**
  - → Umsetzung von politischen Zielen
    („einfach“ und „preiswert“)
  - → Angriffe auf Kritische Infrastrukturen
    (z.B. Stromversorgung, Wasserversorgung, …)



Immer noch nicht sicher?
→ Die größten Herausforderungen



IT-Sicherheit
→ Evaluierung der Situation

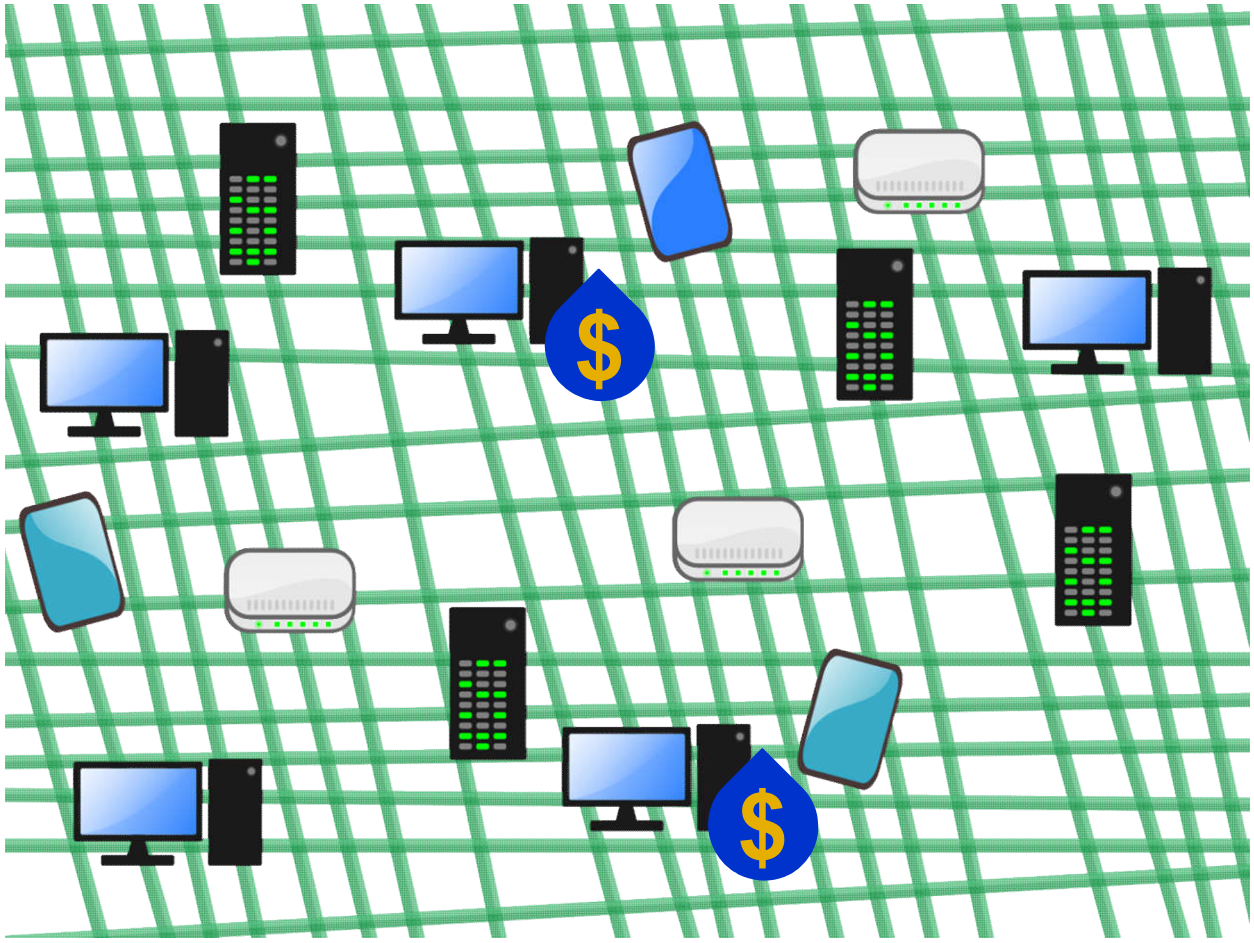
- **Wir kennen die IT-Sicherheitsprobleme**, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen **reduzieren das IT-Sicherheitsrisiko nicht** ausreichend**!**
- Es handelt sich um ein globales Problem
- Die zukünftigen Angriffe werden die heutigen **Schäden** noch deutlich **überschreiten**
- **Wir brauchen innovative Ansätze** im Bereich der Internet-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren

Inhalt

- **IT-Sicherheit**
  (Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**
  (Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Selbstschutz**
  (Basisschutz, richtiges Verhalten, …)
- **Innovationen im Bereich IT-Sicherheit**
  (spotuation, Xign, Quvert, …)

Prinzipielle IT Sicherheitsstrategien
→ Fokussierung

- Im Schnitt sind nur ca. **5 %** aller **vorhandenen Daten** in Unternehmen **besonders schützenswert.**



- Aber **welche Daten** sind besonders schützenswert und wie können diese **angemessen geschützt** werden?

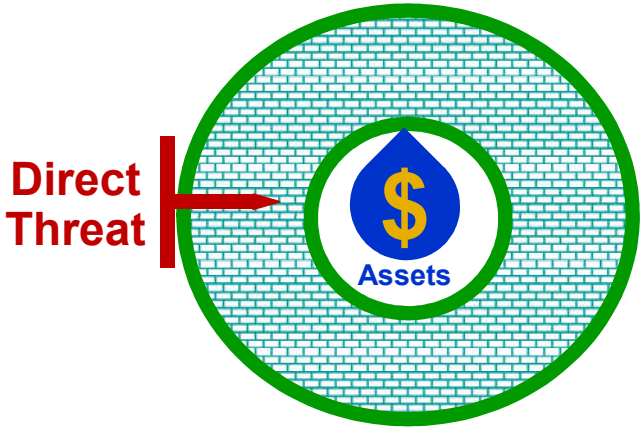
Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (1)

- **Generell gilt: Das Prinzip der digitalen Sparsamkeit.**
  → So wenig Daten generieren wie möglich, so viele wie nötig.
- **Keine Technologie und Produkte mit Schwachstellen verwenden**
  (z.B. Browser, Betriebssysteme, Internet-Dienste, …)

- **Bewertung der Vermeidung**
  - **Vermeidung von Angriffen ist die beste IT-Sicherheitsstrategie!**
  - **Ist nur begrenzt umsetzbar,**
    wenn wir IT mit allen Vorteilen nutzen wollen!

Prinzipielle IT Sicherheitsstrategien
→ Entgegenwirken von Angriffen – (2)

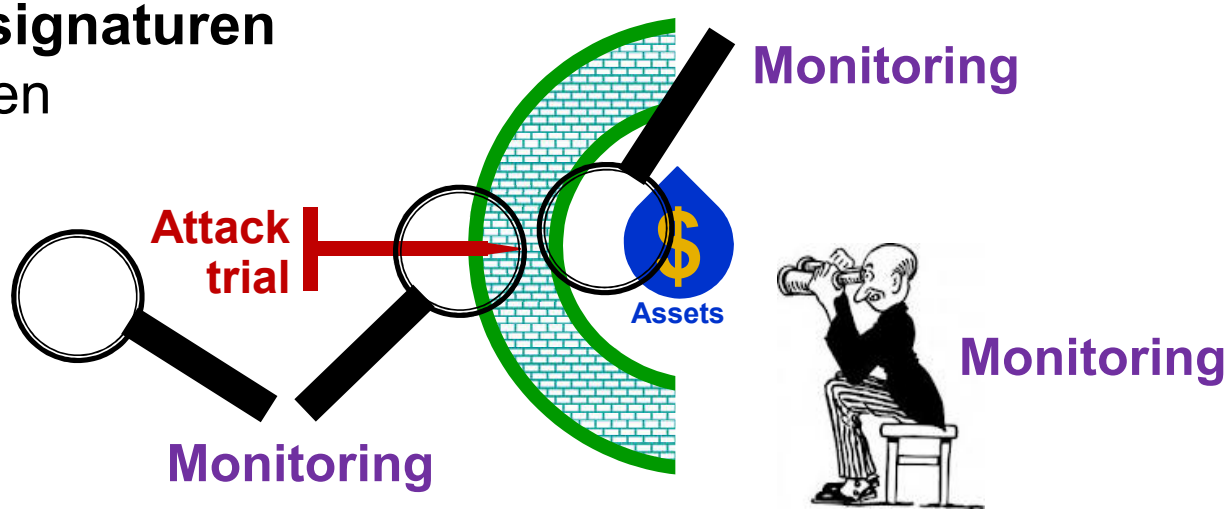
- Meist verwendete IT-Sicherheitsstrategie
- Beispiele, bei denen ein hoher Nachholbedarf besteht:
  - **Verschlüsselungssicherheitssysteme**
    (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, ...)
  - **Authentikationsverfahren**
    (Challenge-Response, globale Identität, Föderation, …)
  - **Vertrauenswürdige IT-Systeme**
    (Security Kernel, Isolierung u. Separierung, ..)
  - …



- **Bewertung des Entgegenwirkens**
  - Eine naheliegende IT-Sicherheitsstrategie
  - **Leider stehen zurzeit nicht genug *wirkungsvolle* und *vertrauenswürdige* IT-Sicherheitstechnologien, -lösungen und -produkte zur Verfügung oder sind nicht im Einsatz**

Prinzipielle Sicherheitsstrategien
→ Erkennen von Angriffen – (3)

- **Erkennen** von Angriffen, denen nicht entgegengewirkt werden kann
- Angriffe erkennen und versuchen, den Schaden so schnell wie möglich zu minimieren (APT)
- Generell IT-Sicherheitssysteme, die Warnungen erzeugen, wenn Angriffe mit Hilfe von **Angriffssignaturen** oder **Anomalien** erkannt werden



- **Bewertung des Erkennens**
  - Die IT-Sicherheitsstrategie, Erkennen von Angriffen, ist sehr hilfreich, hat aber definierte Grenzen

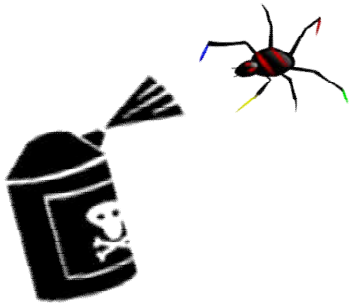
Inhalt

- **IT-Sicherheit**
  (Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**
  (Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Selbstschutz**
  (Basisschutz, richtiges Verhalten, …)
- **Innovationen im Bereich IT-Sicherheit**
  (spotuation, Xign, Quvert, …)

Selbstschutz
→ Basisschutz für den Computer (1/2)

- **Sicherheit durch Einschränkung – Benutzerrechte**
  - Eingeschränkte Benutzerkonten schützen das Gesamtsystem!
  - Potentiell gefährliche Aktivitäten (auch unabsichtliche) werden im Vorhinein blockiert!

- **Virenschutzprogramme / Anti-Malware Programme**
  - Überwachen fortlaufend die Aktivitäten des Computers
  - Muss zur zuverlässigen Arbeit aktuell sein
    → **Automatische Updates aktivieren**

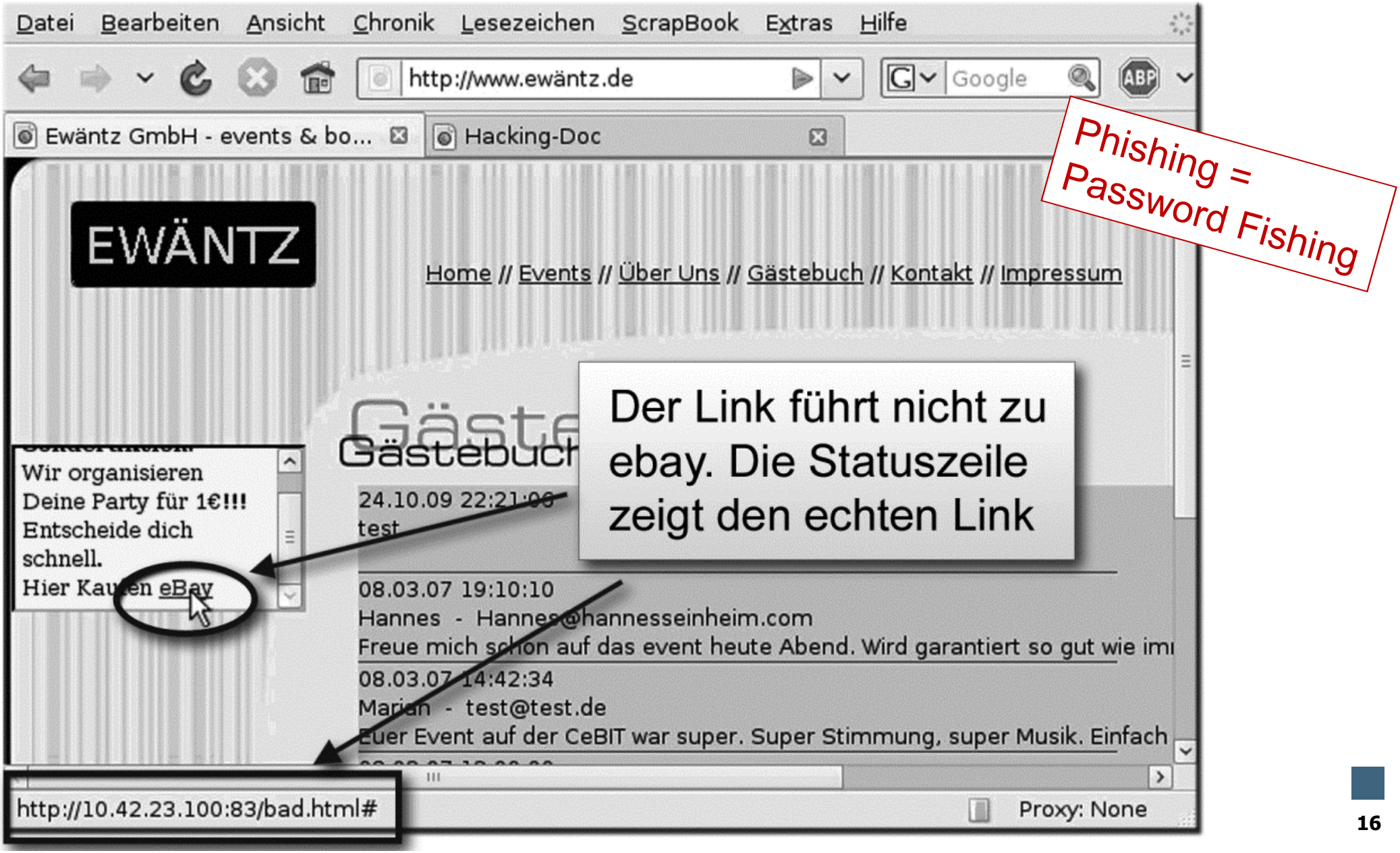


- **Personal Firewall**
  - Wie ein Pförtner: Regelt den Netzwerkverkehr
  - Zugriff nur erlauben, wenn der Grund dafür ersichtlich ist

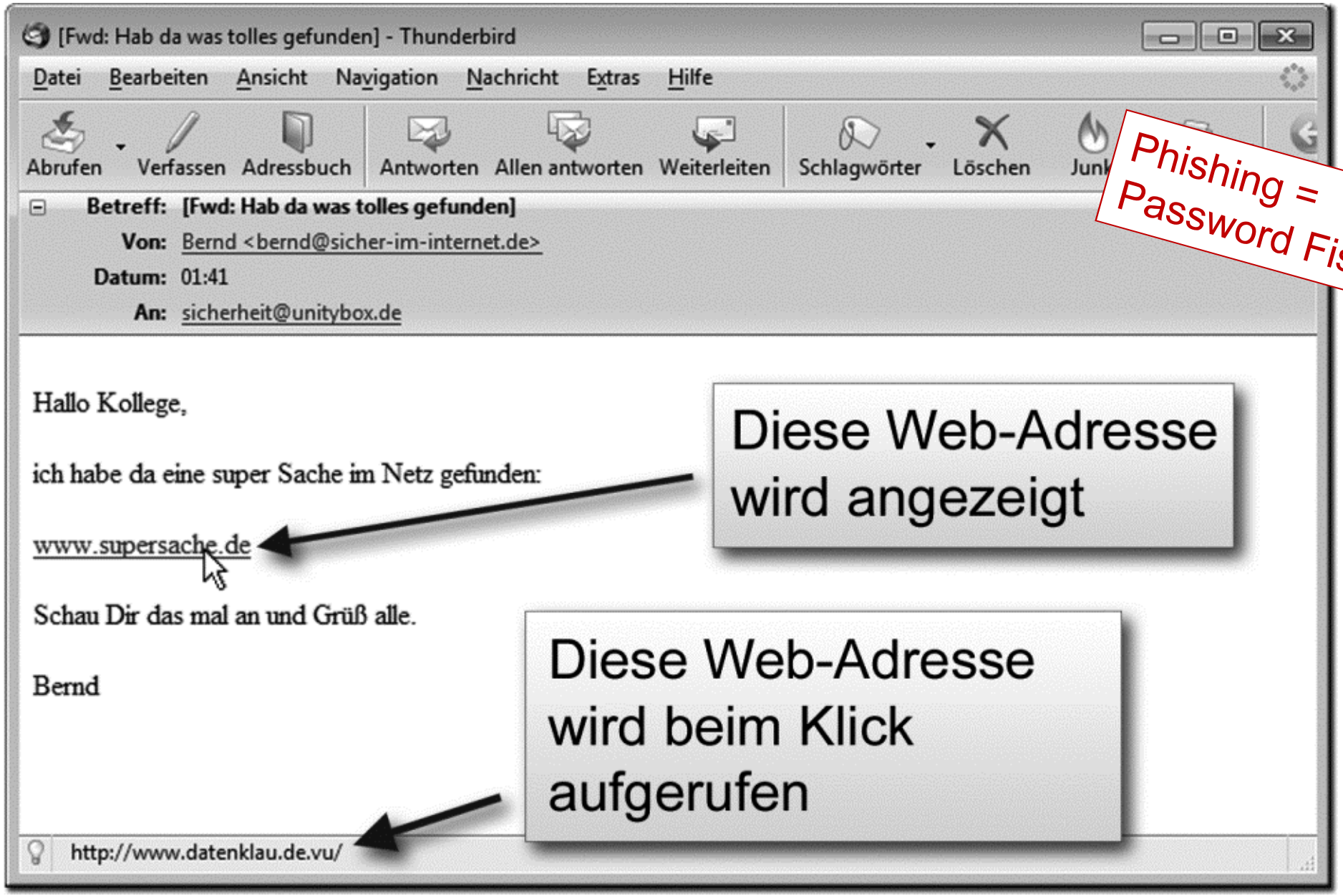
Selbstschutz
→ Basisschutz für den Computer (2/2)

- **Ist Ihr PC up-to-date?**
  - Sicherheitslücken untergraben Anti-Malware-Programme
    - Angriffe zielen auf Fehler in Computerprogrammen ab
    - Malware verbreitet sich über Schwachstellen
  - Softwarehersteller bieten Updates an
    - regelmäßig
    - nach Bekanntwerden einer Sicherheitslücke!

Selbstschutz
→Die Statuszeile (Browser) - Kompetenz

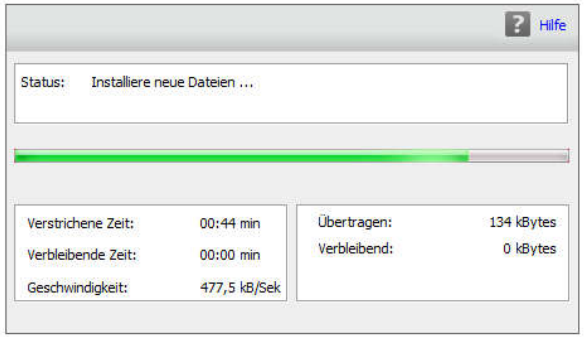


Selbstschutz
→ Die Statuszeile (E-Mail) - Kompetenz



Selbstschutz
→ Richtiges Verhalten

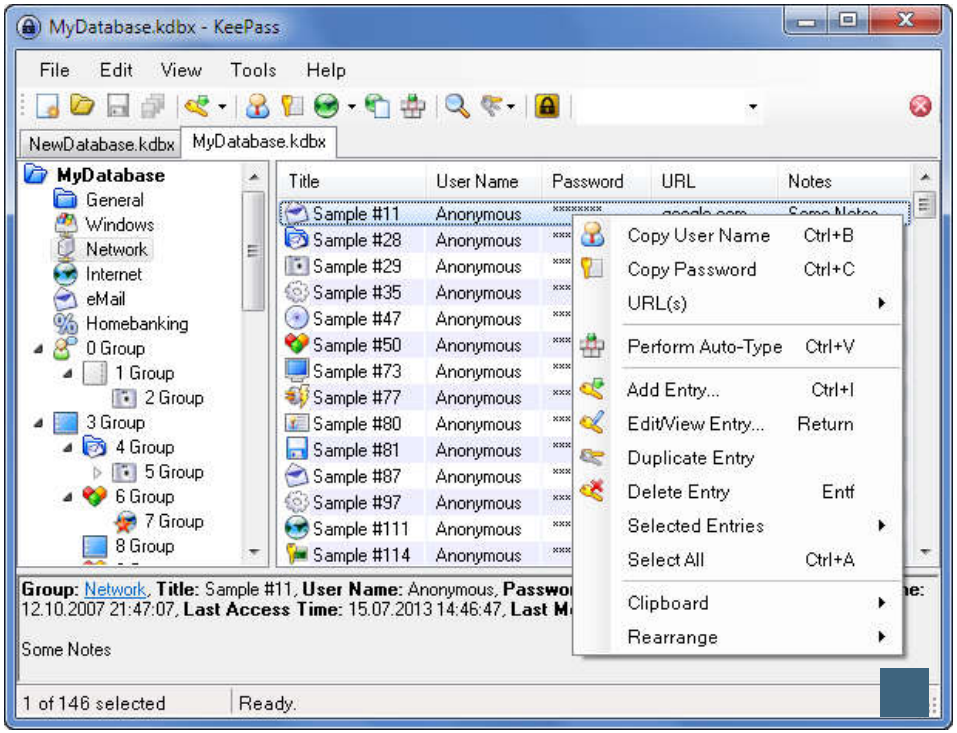
- **Ins Internet?**
  - **Erst Sicherheitsupdates installieren**
    (für Betriebssystem **und** Anwendungsprogramme)
  - Malwaresignaturen erneuern
  - **Erst dann:** E-Mails abrufen, Surfen… Onlinebanking usw.



- **E-Mail-Kommunikation**
  - Dateianhänge nur mit Bedacht öffnen, auch bei seriöser Quelle
    Absender fälschen ist einfach – elektronische Postkarten
  - Bei Unsicherheiten telefonisch Rückfrage halten!
  - Niemals unbekannte, seltsame oder verlockende Anhänge öffnen!
    z.B. → Anwälte versenden keine Abmahnungen/Rechnungen per E-Mail!

Selbstschutz
→ Starke Passwörter

- Absicherung vor unerwünschter Nutzung durch andere
  - Starke Passwörter enthalten mind. **10 Zeichen** (besser **mehr**), **Groß-** und **Kleinbuchstaben**, **Zahlen** und **Sonderzeichen**
  - Problem: Sie müssen sie sich gut merken können!
  - Merkbar durch eine Eselsbrücke und Buchstaben durch Zahlen oder Sonderzeichen ersetzen. Ein Beispiel:
    - WeaeiGgr,f5eh!
      Wer **a**nderen **ei**ne **G**rube **gr**äbt,
      fällt **sel**bst **h**inein**!**
  - Passwörter nicht weitergeben, nicht aufschreiben
  - Regelmäßig neue und andere Passwörter vergeben
  - Keinen Universalschlüssel vergeben
    → falsche Webseiten



Selbstschutz
→ Für Handys und Smartphones/Tablets

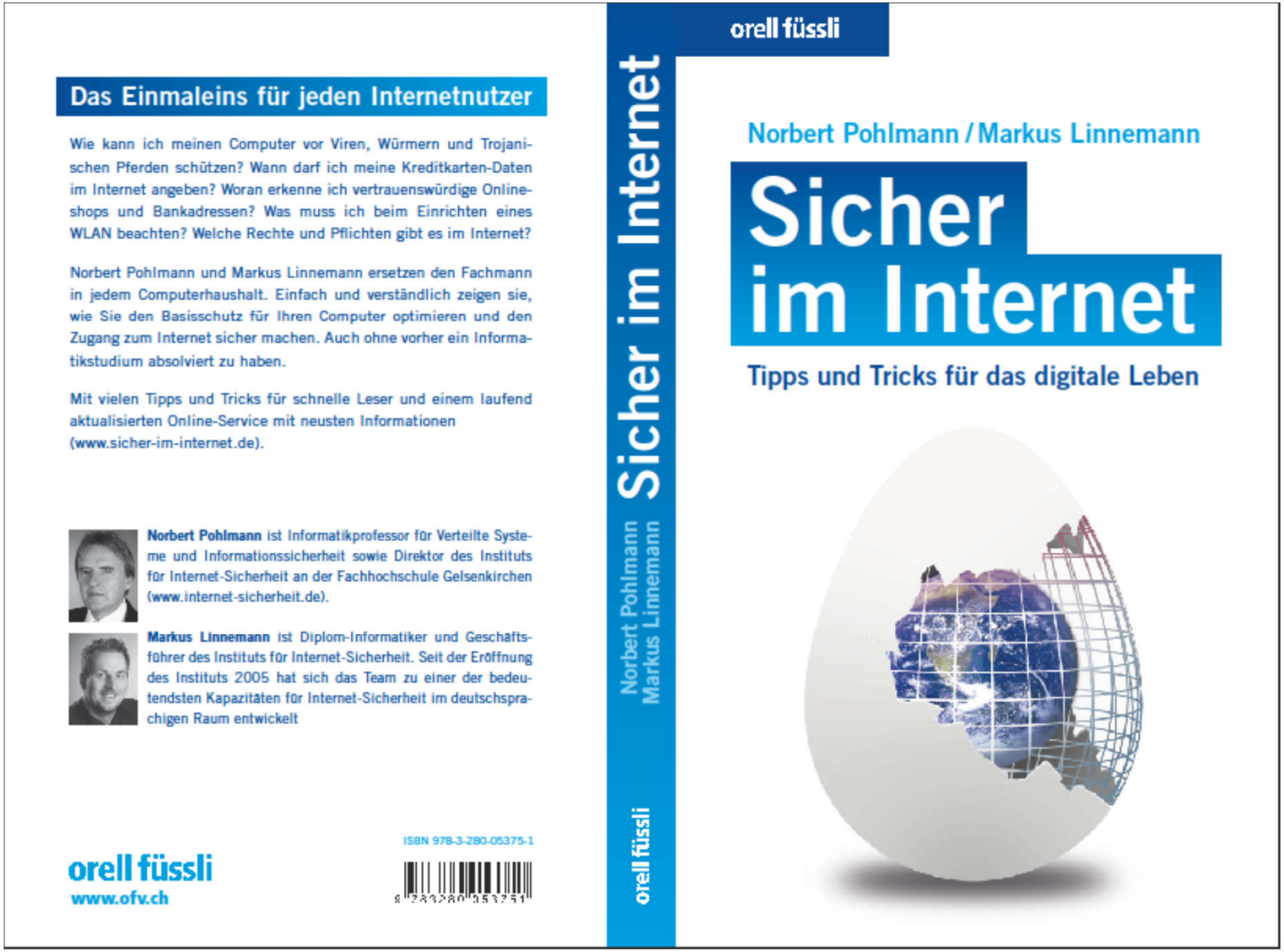
- Vergeben Sie eine PIN für die SIM-Karte!
- Richten Sie eine passwortgeschützte Display-Sperre ein! (Screen-Lock)

- **Speziell für Smartphones, Tablets und Notebooks**
  - Verwenden Sie einen Basisschutz und aktivieren Sie automatische Updates!
  - Schalten Sie nicht benötigte Dienste aus (z.B. WLAN, Bluetooth, GPS)!
  - Verschlüsseln Sie sensible Daten!
  - **Surfen Sie nicht in offenen WLANs!**
    (automatisches Einloggen ist ein großes Risiko)
  - Informieren Sie sich umfassend über eine App (Malware), bevor Sie sie installieren (Geschäftsmodell: „Bezahlen mit persönlichen Daten“)
  - **Verlieren der mobilen Geräte**
  - Bewegungsprofilbildung
  - **Öffentliche Einsicht**
  - …

Schutzmaßnahmen
→ Was man noch selbst tun kann

- Sehr wichtig: **Sich** selbst **informieren** oder jemanden fragen
  - Autofahrer sind ebenfalls stets verpflichtet, sich über Änderungen von Regeln im Straßenverkehr zu informieren
- **Internet-Kompetenz** ist in einer digitalen Welt nicht nur sehr hilfreich, sondern heute notwendig
- **Sicherheitskataloge** bieten viele Informationen rund um die Sicherheit im Netz: www.bsi-fuer-buerger.de
- **Der eigene Verstand ist der wirksamste Schutz**
- Sicherheitssoftware kann (und soll auch nicht) den Benutzer vor sich selbst schützen

Das Einmaleins für jeden Internetnutzer
→ Tipps und Tricks für das digitale Leben



www.sicher-im-internet.de

Inhalt

- **IT-Sicherheit**
  (Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**
  (Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Selbstschutz**
  (Basisschutz, richtiges Verhalten, …)
- **Innovationen im Bereich IT-Sicherheit**
  (spotuation, Xign, Quvert, …)

Landkarte für das Netzwerk
→ spotuation Security Intelligence

spotuation
Sicherheit im Blick.

Mehr Informationen finden Sie unter

www.finally-safe.com/spotuation

Die persönliche Landkarte Ihres Netzwerks

- Die gesamte Netzwerk-**Sicherheitslage** im Überblick
- Reporting und **Alarmierungen**
- Zugang zu **Experten-Know-how**
- Passive **Netzwerk-Monitoring**-Lösung

Ziele der Technologie

- Erkennung von **neuen und gezielten Angriffen** durch Verhaltensanalysen
- **Verhinderung von Angriffen** durch Steigerung der **Netzwerk-Resistenz**
- Aufdecken und Beseitigen von **Schwachstellen**

Das Wertversprechen

- **Priorisierung** und **Handlungsempfehlungen**
- **Hocheffiziente** und **intelligente** Netzwerkanalyse in Deutschland entwickelt **ohne Backdoors**
- Extreme **Detailtiefe** bei **geringen Datenmengen**, ewig speicherbar und **Datenschutzkonform**
- **Einfach zu implementieren mit geringstem Pflegeaufwand**

Identifikation/Authentifikation - Signatur → XignQR

- Einfach, schnell, **benutzerfreundlich** & **sicher**
- Adaptive **Authentifizierung** und rechtlich bindende **e-Unterschriften ohne Passwort**, TAN oder Zusatzhardware
- Identity- & Accessmanagement **as a Service** oder **on-premise**
- **Flexibel** und **schnelle Integration**
- **Unzählige Anwendungsfälle** vom Login an PC oder Webseite, über Transaktionen und Dokumentensignaturen
- **Modernste Identifikationsverfahren**, z.B. Video-Ident oder Gebrauchsmuster

Eine moderne Kommunikationsplattform → smart, effizient und sicher

- Effizientere Kommunikation (Chat)
- Verschlüsselung der Kommunikation (geht nicht ohne)
- Organisations-orientierung
  → jede Firma verwaltet die eigene Kommunikation
- Aber, auch sichere Inter-Organisationskommunikation möglich

- **Features**
  - Identity-Management (vertrauenswürdig)
  - Verfügbarkeitsstatus (Auto, Flugzeug, Urlaub, …)
  - Knowhow Attribute – wie Ressourcen und Wissen
  - Nachweisbarkeit von Geschäftsprozessen
    - Urlaubsanträge
    - Dienstreisen
    - Budget
    - Usw.

Quvert

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyberkriminalität

→ Wie kann ich mich schützen?

IT ist unsicher, aber wir haben Möglichkeiten uns zu schützen!

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.