



# Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz: Maßnahmen und Handlungsempfehlungen

Maik Pommer, Landesinitiative »secure-it.nrw«

Essen, 29.10.2009

## »secure-it.nrw«: Kommunikationsinitiative für mehr IT-Sicherheit

### neutral und unabhängig:

- gefördert vom NRW-Innovationsministerium
- angesiedelt bei der IHK Bonn/Rhein-Sieg

### Ziele:

- Sensibilisierung, Information und Qualifizierung zu IT-Sicherheit und Datenschutz
- Prävention durch Medienkompetenz
- Impulsgeber in den Zielgruppen: Unternehmen, Schulen, Bürgerinnen und Bürger



## Maßnahmenbereiche für den Mittelstand

### • Informationen „live“

- Mittelstandsforen
- Fachkonferenz  
IT-Sicherheitstag NRW



### • Informationen zum Selbststudium

- Themenbroschüren
- Newsletter
- [www.secure-it.nrw.de](http://www.secure-it.nrw.de)
- Best Practice:  
IT-Sicherheitspreis NRW



### • Lösungshilfe: Branchenbuch

- [www.Branchenbuch-IT-Sicherheit.de](http://www.Branchenbuch-IT-Sicherheit.de)



### • Beratung: Basisprüfung IT-Sicherheit

- kostenfreies Kurzaudit
- angelehnt an BSI-Grundschutz
- Ziel: Aktuelle Einschätzung  
des Sicherheitsniveaus  
im Unternehmen



## Warum IT-Sicherheit?

- Schutz von Daten, Prozessen und unternehmerischer Handlungsfähigkeit
- Gewährleistung von Verfügbarkeit, Korrektheit und Vertraulichkeit von Daten und Informationen im Unternehmen

## Lösungsansatz: technische Basis-Schutzmaßnahmen

- Antivirensoftware einsetzen und täglich aktualisieren
- Firewalls einsetzen
- Betriebssystem und Standardsoftware aktuell halten
  - Patches (automatische Softwareupdates) installieren
- Daten und Dokumente durch Berechtigungskonzepte schützen
- Internet: Filtersoftware einsetzen
- Datensicherung und -rücksicherung

## Und was macht der Mensch?

- Passwörter auf Post-its am Arbeitsplatz
- „Verlassene“ Computer ohne Schutzmaßnahme (sichere Bildschirmschoner)
- Öffnen von E-Mail-Anhängen unbekannter Sender
- Auswahl schwacher Passwörter
- Betriebsfremde unbegleitet in Büros, Rechenzentrum, ... lassen
- „Ausplaudern“ von Passwörtern oder Firmeninformationen
- Datenträger ausrangiert im Müll



## Lösungsansatz: Sicherheitsrichtlinie

- Definition des angestrebten Sicherheitsniveaus
- Sicherheitsziele und die Sicherheitsstrategie
- Maßnahmen: Organisation und Umsetzung von Sicherheit
- Verantwortlichkeiten (auch von Mitarbeitern!)
- Verhaltensregeln für Mitarbeiter
- Sanktionen bei Sicherheitsverstößen

## Aber: mangelnde Akzeptanz bei Mitarbeitern

- Sicherheit als Behinderung bei der Arbeit
  - IT-Sicherheitsmaßnahmen beeinträchtigen die Performance
  - Komplexe Passwörter sind schwer zu merken
  - Daten sind nicht unmittelbar zugänglich
- Risikoannahmen „realitätsfern“
  - Bedrohungen erscheinen unrealistisch („Meine Daten sind doch nichts Besonderes!“)
  - Sicherheitsmaßnahmen erscheinen überzogen (z. B. Passwortlänge, Passwortwechsel)

## Mangelndes Verantwortungsgefühl

- Verantwortung wird Anderen zugeordnet
- Lösung von IT-Sicherheitsproblemen ist Aufgabe der IT-Abteilung
- Man für sich durch Sicherheitsvorfälle nicht unmittelbar betroffen
- Bedeutung des eigenen Verhaltens wird unterschätzt

## Grenzen von Technik und Regeln

- Benutzerfehler sind möglich und menschlich
    - Bei der Mehrzahl der IT-Schäden sind Mitarbeiter beteiligt
    - Technische Sicherheitslösungen ersetzen Benutzermitwirkung nicht
  - Trugbild technischer Beherrschbarkeit
    - Unflexibilität technischer Schutzmaßnahmen
    - Regeldurchsetzung ohne Verständnis führt zu Umgehungsversuchen
- Eine Erhöhung des Sicherheitsniveaus ist nur bei Anhebung des Sicherheitsbewusstseins möglich.**

## Sensibilisierung – was bringt es?

- Vorsorgemaßnahmen sind preiswerter als Schadensbeseitigungen
  - Wiederherstellungs- und Anlaufkosten beschädigter IT
  - Produktionsausfallkosten aufgrund irreparabler IT-Schäden
  - Unkalkulierbare Image- und Vertrauensschäden
- Sensibilisierung erhöht Sicherheitsniveau
- Hohes Maß an IT-Sicherheit ist Qualitätsmerkmal und Imagefaktor
- Kosten für Sensibilisierung sind skalierbar

## Sensibilisierung als nachhaltiger Prozess

- Sicherheitsmaßnahmen erläutern und Verständnis schaffen
- zum eigenverantwortlichen Handeln motivieren
- Sicherheitsbegriff positiv besetzen – Nutzen herausstellen
- Informationssicherheit als Qualitätsziel verständlich machen
- sicherheitsbewusstes Verhalten fördern und belobigen
- dauerhafte Verhaltensänderungen bewirken
- Wichtig: alle Unternehmensbereiche ansprechen


## Motivieren und üben!

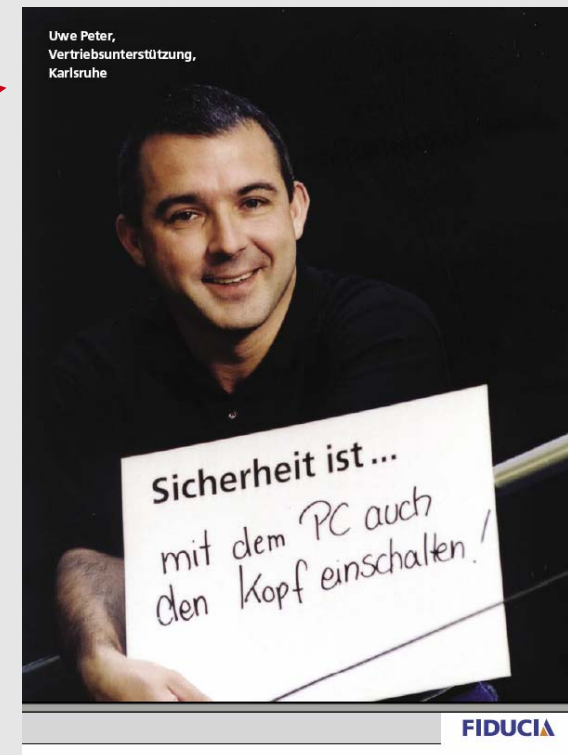
- unkommentierte Vorschriften werden oft nicht verstanden und missachtet
- Regeln sind nötig, aber ...
- Regeln müssen verständlich sein und verständlich gemacht werden
- Sicherheit positiv deuten: Der Mitarbeiter ist ein Funktionsträger für Sicherheit ( ... und kein Sicherheitsrisiko)
- Erklären Sie kreativ: Erkenntnisse dürfen auch Spaß machen
- Dranbleiben und üben: Wiederholungen stärken den Lerneffekt
- **Führungskräfte sind die Vorbilder im Sensibilisierungsprozess**

## Sensibilisierung nachhaltig planen

- Themenbereiche festlegen
- Beteiligte identifizieren – intern und extern
- Motto und/oder Logo entwerfen
- Kommunikationskanäle bestimmen
- Gremien einbeziehen
- Unternehmenskultur würdigen
- Und vor allem: **Fangen Sie an!**
- Auch mit vielen kleinen Schritten kann man zum Erfolg kommen!

## Instrumente für die Umsetzung

- Intranet
- Mitarbeiterzeitung
- E-Mail-Newsletter
- Rundbrief
- Informationsbroschüren
- Gewinnspiel
- Gegenständliches (z.B. „Passworthalter“)
- ...
- Poster 
- Schwarzes Brett
- Besprechungen
- Betriebsversammlung
- Interne Schulungen
- Wissensquiz



## Themen für eine Awareness-Kampagne

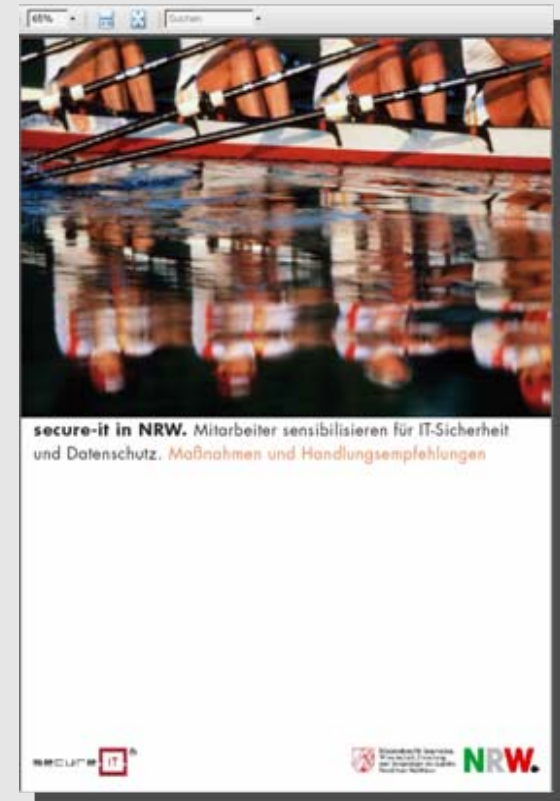
- Passwortsicherheit
- Mobile Sicherheit: Laptops, Organizer, Handys und Co.
- Dokumente und Datenträger: Erstellung, Weitergabe, Vernichtung
- Sichere Nutzung von Internet und E-Mail: Virenabwehr, Verschlüsselung
- Schutz vor schädlichen Webseiten, Phishing
- Social Engineering: Gespräche mit Fremden, Handy-Telefonate
- Weitergabe von Informationen
- Unternehmenssicherheit: Umgang mit Besuchern, Verschluss von Büros
- Datenschutz

## Erfolgsfaktoren

- Einbeziehung der Führungskräfte
- Konzentration auf das Wesentliche
  - Welche Themen und Regelungen sind am wichtigsten?
  - Nur ein Thema je Umsetzungs-Modul
- Integration betroffener Unternehmensbereiche
- Modularer Aufbau der Maßnahmen (Themenmodule)
- Ansprechende Mischung von Maßnahmenarten
- positive emotional-affektive Ansprache

## Praxisbeispiele und kostenfreie Lösungshilfen

- Broschüre mit:
  - Handlungsempfehlungen
  - Praxisbeispielen
- Plakatmotive mit Sensibilisierungscharakter
- alles kostenfrei bei »secure-it.nrw«



**- (IT-)Sicher ist Ihre Firma nur, wenn alle mitmachen!**

## Sprechen Sie uns an! Landesinitiative »secure-it.nrw«

Agentur »secure-it.nrw« bei der IHK Bonn/Rhein-Sieg

Bonner Talweg 17, 53113 Bonn

Tel.: +49 - 2 28 - 22 84-184

Fax.: +49 - 2 28 - 22 84-5184

E-Mail: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)

[www.secure-it.nrw.de](http://www.secure-it.nrw.de)

und

[www.branchenbuch-it-sicherheit.de](http://www.branchenbuch-it-sicherheit.de)