

Wolfgang Straßer



Unternehmenssicherheit in der Praxis

@-yet

## Daten Zahlen Fakten

- ✓ gegründet: Juni 2002
- ✓ Mitarbeiter: 25
- ✓ Umsatz: ca. 2,7 Mio €
- ✓ Standort: Leichlingen/NRW
- ✓ Aktionsradius: bundesweit/weltweit

## @-yet Geschäftsbereiche



## Agenda

- ✓ Informationssicherheit ist kein Selbstzweck
- ✓ 100% Sicherheit gibt es nicht,  
aber reichen 15-20%???
- ✓ Informationssicherheit ist bezahlbar

## Informationssicherheit ist kein Selbstzweck

### ✓ Bedeutung der IT

- Ohne IT keine Innovation
- Ohne IT keine Wertschöpfung
- Ohne IT kein Wachstum

## Informationssicherheit ist kein Selbstzweck

- ✓ Warum IT-Sicherheit?
  - Schutz vor Ausfällen
  - Schutz vor Know-How-Verlust
  - Schutz vor dem Gesetzgeber
    - Compliance

## Informationssicherheit ist kein Selbstzweck

### ✓ Warum IT-Sicherheit?

1. Deutschland ist Exportweltmeister
  - vor allem wegen des Mittelstandes
2. Deutschland im Fokus von Wirtschaftsspionage
  - ca. 50 Mrd. € Innovationswerte jährlich
    - 20 Mrd. werden gestohlen

## Informationssicherheit ist kein Selbstzweck

### ✓ Warum IT-Sicherheit?

- Auf den Servern und in den Netzen liegen
  - Produkt Know-How
    - tw. Jahrhunderte an Entwicklung
  - Produktionsprozeß Know-How
  - Kalkulationen
  - Bankverbindungen
  - u.v.m. an Unternehmenswerten

## 100% Sicherheit gibt es nicht, aber ....

- ✓ das ist kein Grund sich mit 15-20% zu begnügen
- ✓ oder gar zu resignieren

## 100% Sicherheit gibt es nicht, aber ....

✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz

- |                       |                              |
|-----------------------|------------------------------|
| 1. Alter              | > 60 Jahre                   |
| 2. Umsatz             |                              |
| 3. Anzahl Mitarbeiter | ca. 600                      |
| 4. Standorte          |                              |
| • Produktion          | 3 (2 ausländische)           |
| • Vertrieb            | 8 (7 ausländische)           |
| 5. Vertriebsgebiet    | 5000 Kunden in<br>70 Ländern |

## 100% Sicherheit gibt es nicht, aber ....

- ✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz

Auftrag: Sicherheitsüberprüfung

Ablauf:

- 3 Abende PenTest (offsite)
- 2 Tage Social Engineering
  - u.a. Phishing Angriff
- 2 Tage Infrastrukturcheck
  - mit WLAN Check
- 1 Tag PenTest (onsite)
- 1 Tag Policycheck

## 100% Sicherheit gibt es nicht, aber ....

- ✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz
- ✓ Ergebnis: technische Checks
  - Firewall/Internet/VPN/mail Gateway:
    - » beim Provider war zwar state-of-the art, aber
    - » Zugriff auf Sicherheitssysteme war möglich
    - » Passwörter wurden in Klartext übertragen
    - » reichhaltige Informationen über die IT-Infrastruktur
  - WLAN Check
    - » div. vorhanden, vor allem in der Produktion
    - » tw. noch mit WEP so gut wie ungeschützt

## 100% Sicherheit gibt es nicht, aber ....

- ✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz
- ✓ Ergebnis: Social Engineering:
  - 2 Tage ungehinderter Zugang zu
    - Produktion und Verwaltung
    - F&E Bereich
    - in der Verwaltung wurde uns auf Nachfrage der AP eines abwesenden MA zugewiesen
    - bis 23 Uhr konnten wir ungehindert im Gebäude bleiben

## 100% Sicherheit gibt es nicht, aber ....

- ✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz
- ✓ Ergebnis: Social Engineering:
  - Phishing Angriff:
    - viele Anwender haben brav mit Passwort geantwortet
  - unerkanntes anbringen eines WLAN AccessPorts
  - keine Meldung an Geschäfts- oder IT-Leitung

## 100% Sicherheit gibt es nicht, aber ....

- ✓ Beispiel: mittelständischer Lackhersteller in der deutschen Provinz
  
- ✓ Ergebnis: PenTest onsite
  - unerkanntes einloggen ins Firmennetz
  - „barrierefreies“ arbeiten, kopieren und manipulieren möglich von und mit
    - FI-Daten
    - HR-Daten
    - F&E Daten
    - etc. war möglich

## 100% Sicherheit gibt es nicht, aber ....

✓ Beispiel: mittelständischer Lackhersteller  
in der deutschen Provinz

✓ Fazit:

Wir hätten das Unternehmen komplett

- ausrauben und
- stilllegen können

## 100% Sicherheit gibt es nicht, aber ....

### ✓ Fazit vieler Überprüfungen:

1. bei der Firewall hört die Informationssicherheit auf
2. organisatorische Sicherheit ist meist unterentwickelt
3. physische Sicherheit (Gebäudezugänge etc.) wurde vor Jahren abgebaut
4. vorhandene Policies werden nicht gelebt
5. Bewusstsein bei Geschäftsleitung und folglich auch bei den Mitarbeitern ist nicht vorhanden
6. die Bedeutung wird total unterschätzt
  - immer wieder die Aussage: wer interessiert sich schon für uns??

## Sicherheit muß nicht teuer sein,

- ✓ wenn Sie es
  1. gezielt angehen
  2. strukturiert betreiben
  3. als Prozeß betrachten
  4. als unternehmensweite Aufgabe ansehen
  
- ✓ wenn Sie es als notwendig für den Schutz Ihrer
  1. Unternehmenswerte und
  2. Wettbewerbsfähigkeit halten

## Sicherheit muß nicht teuer sein

- ✓ Vorgehensweise:
  - Riskassessment
    - Bestimmung der Daten und Prozesse, die für die Wertschöpfung sorgen
    - Klassifizierung und Bewertung der Daten und Prozesse
      - Was bedeutet der Verlust von Know-How in €?
      - Was bedeutet der Stillstand von Prozessen in €?

## Sicherheit muß nicht teuer sein

- ✓ Vorgehensweise:
  - Bestimmung des Status Quo durch
    - Sicherheitsüberprüfung
    - Verfügbarkeitscheck
    - Compliancecheck
  - Abgleich Soll/Ist
  - Maßnahmen

## Sicherheit muß nicht teuer sein

✓ Aufwand (dicker Daumen):

- |    |                                  |          |
|----|----------------------------------|----------|
| 1. | Riskassessment                   | 2-5 MT   |
| 2. | Bestimmung des Status Quo        | 12-20 MT |
|    | • off-site PenTest               | 6-9 MT   |
|    | • Social Engineering             | 2-4 MT   |
|    | • on-site PenTest                | 2-3 MT   |
|    | • Policycheck                    | 1-2 MT   |
|    | • Infrastruktur-Bewertung (grob) | 1-2 MT   |
| 3. | Maßnahmenkatalog                 |          |
| 4. | Umsetzung                        |          |

## 100% Sicherheit gibt es nicht, aber ....

- ✓ das ist kein Grund sich mit 15-20% zu begnügen
- ✓ oder gar zu resignieren

## Finale

- ✓ Herzlichen Dank  
für Ihre  
Aufmerksamkeit!
- ✓ Fragen Sie bitte jetzt!

Wolfgang Straßer  
@-yet GmbH  
Schloß Eicherhof  
42799 Leichlingen

