INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH

Private Netze –
Das Nonplus-Ultra für die Sicherheit?

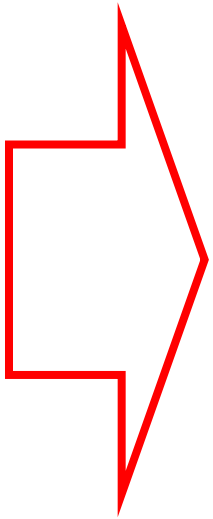
Notwendigkeit von Branchennetzen aus dem Blickwinkel Sicherheit

Dr. Thomas Stock

12. März 2013

Wozu Private Netze?
Das Internet ist doch eh da und quasi kostenfrei!

T
A
N
S
T
A
A
F
L



Angriffe auf

- **Vertraulichkeit**
- **Integrität / Authentizität**
- **Verfügbarkeit**

von Anwendungen und Daten, die über das Internet erreicht werden können, sind an der Tagesordnung

Der Trend zu gezielten Angriffen hält weiter an

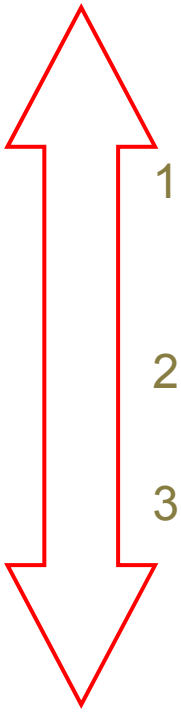
Angreifer denken anders als Entwickler, Administratoren und Anwender

- System-Entwickler, Administratoren, Anwender:
  „Es muss funktionieren!“
  - In möglichst jedem Umfeld
  - Auch bei Ausfall einzelner Komponenten
  - Möglichst „out of the Box“

- Angreifer (externe und interne):
  „Wo liegen die Schwächen des Systems und wie kann ich sie ausnutzen?“
  - Mit möglichst geringem Aufwand
  - Mit möglichst großer Wirkung
  - Möglichst ohne entdeckt zu werden

Lebenszyklus von Schwachstellen – Wettrennen zwischen gut und böse

1. Die Schwachstelle ist da, aber keiner kennt sie
2. Die Schwachstelle ist einem sehr eingeschränkten Kreis von Insidern bekannt
3. Die Schwachstelle ist einem umfangreichen Publikum bekannt
4. Security-Scanner enthalten entsprechende Module für die Erkennung der Schwachstelle



1. Die Schwachstelle kann von Einzelnen mit selbst generierten Werkzeugen ausgenutzt werden
2. Diese Werkzeuge kursieren in breiteren Kreisen und werden „generalisiert“
3. Es sind ready-to-use Tools bzw. Module verfügbar, die leicht konfigurier- und flexibel einsetzbar sind

- Entwickler/Admin/Anwender:

  Kann die Schwachstelle rechtzeitig geschlossen werden?

- Angreifer:

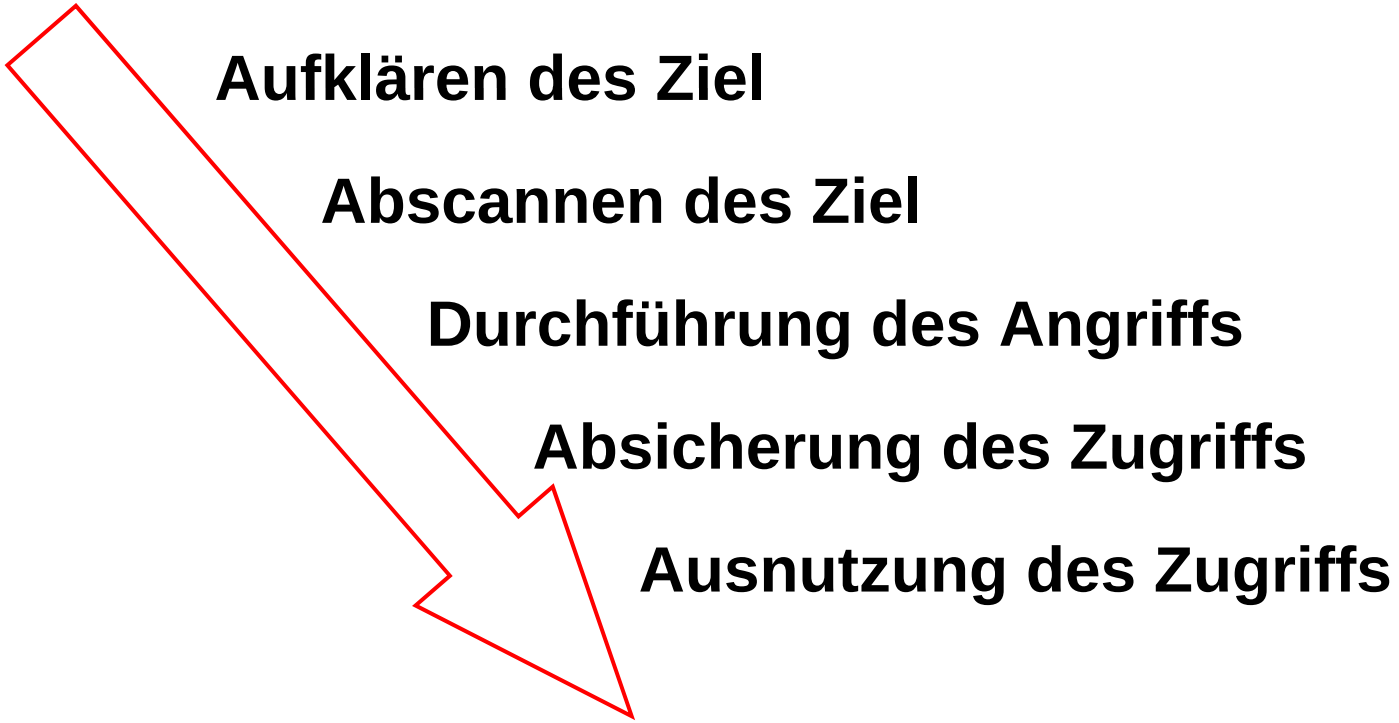
  Kann die Schwachstelle umfassend ausgenutzt werden, bevor sie geschlossen wird?

Motive für Angriffe

- Zufall
- Neugier
- Geltungsbedürfnis
- Vandalismus
- Betrug
- Diebstahl
- Erpressung
- Industriespionage
- Politische / militärische Spionage
- Manipulation von Daten, Einschätzungen und Meinungen
- Cyber-War

- u. v. m.

(Gezielte) Angriffe im Internet folgen i.d.R. einem Standard-Schema



Private Netze können die Risiken für Vertraulichkeit, Integrität & Authentizität reduzieren

- Reduzierte Menge an potenziellen Angreifern
- Reduzierte Angriffsfläche
- Zusätzliche Sicherungsverfahren
  - Gateways/Proxies für Authentisierung und Verschlüsselung
- Zentrales Monitoring im Allg.
  - Network Intrusion Detection Funktionen im Speziellen

Private Netze können Verfügbarkeitsrisiken reduzieren

- Reduzierte Angriffsfläche (im Hinblick auf DoS, DDoS)
- SLAs mit hohen Verfügbarkeitsgarantieren
- Architekturell „garantierte“ Redundanz
- Garantierte Bandbreiten
- Quality/Type-of-Service
- Zentrales Monitoring im Allgemeinen
  - Performance-Monitoring im Besonderen

Private Netze – Das Nonplus-Ultra für die Sicherheit?

- Absolute Sicherheit gibt es nicht!
- Maximale Sicherheit ist in der realen Welt [nie, selten, ab und an, …] umsetzbar: Kosten, Akzeptanz der Anwender, …
- Private Netze für geschlossene Benutzergruppen bieten für sensitive B2B-Dienste im Vergleich zum Internet einen wirtschaftlich guten Kompromiss bezüglich der Sicherheit:
  - Geringe Angriffsfläche
  - Hohes Vertrauensniveau
  - Hohe Verfügbarkeit
- Sie stellen daher in sensitiven B2B-Szenarien [oft, meist, ...] die bessere Alternative zum Internet dar

Fragen? Anmerkungen?

INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH

Dr. Thomas Stock

Simrockstr. 4

53113 Bonn

Telefon: +49 (228) 4495 7 363

Telefax: +49 (228) 4495 7 555

E-Mail:

Thomas.Stock@SIZ.de

Internet:
http://www.siz.de