

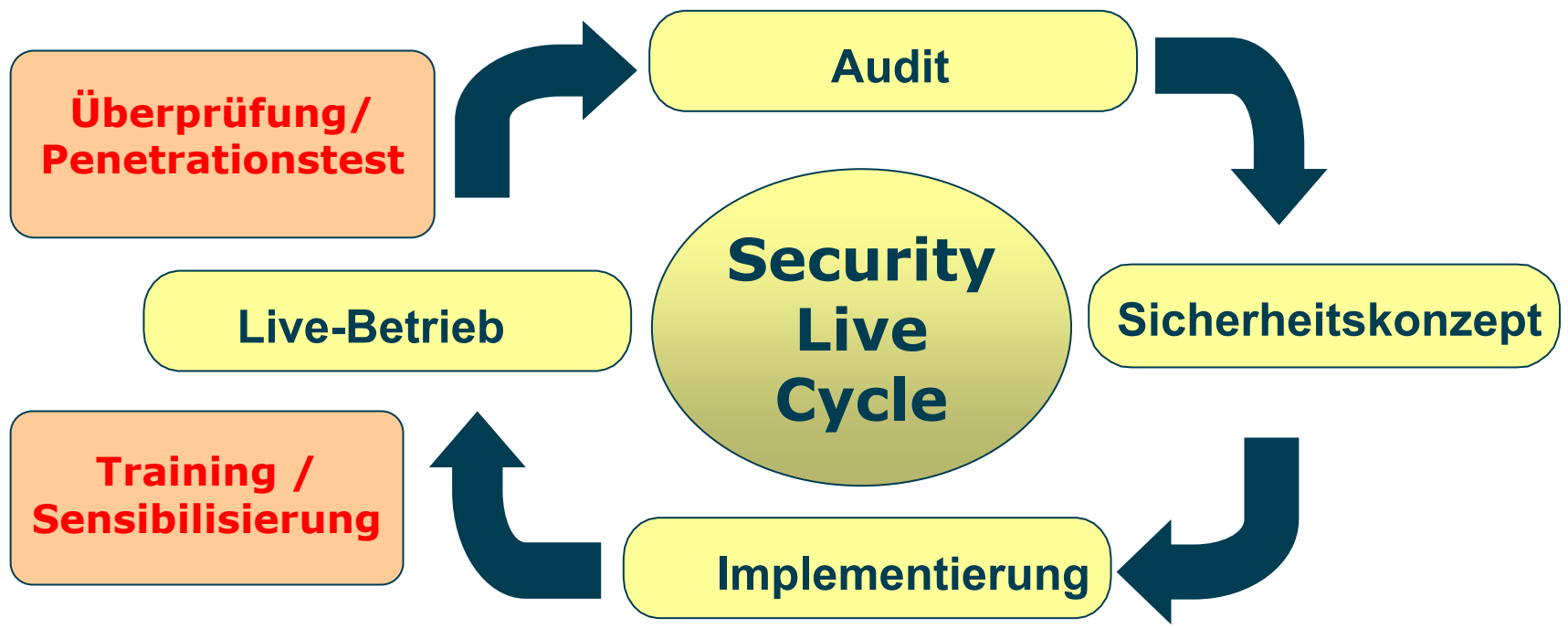
**Ihr Weg zu mehr Sicherheit**

# IT-Sicherheitsproblem

- Für IT-Sicherheit wird nicht genug getan, denn .....
  - Zwei von fünf Firmen sind pleite, wenn sie ihre Daten verlieren (CIO, 11/2001)
  - Jährliche Steigerungsraten bei IT-Sicherheitsvorfällen und -lücken von mehr als 100 Prozent in 2001 ([www.cert.org](http://www.cert.org))
  - Durch Systemabstürze verlieren 92 Prozent europäischer Führungskräfte regelmäßig wertvolle Arbeitszeit ([www.silicon.de](http://www.silicon.de), 12/2001)
  - Schäden durch erfolgreiche Hacks: 20 Milliarden US-Dollar pro Jahr in den USA (SUN News, 12/2001)

# Ihr Weg zu mehr Sicherheit

- Der Weg zur sicheren IT-Infrastruktur



# Was ist IT-Security-Consulting?



- + Gemeinsam mit Ihnen einen akzeptablen IT-Sicherheitslevel für Ihr Unternehmen erreichen
- + Ihren Blick schärfen für Gefahren und Risiken, die Ihrer IT-Infrastruktur drohen
- + Sie begleiten von der Erstellung eines IT-Sicherheitskonzepts bis hin zur Implementierung technischer Lösungen
- + Kalkulierbare Kosten, überschaubarer Zeitaufwand



Jedes einzelne Versprechen ein Pluspunkt!

# Die NT+C-Komplettlösung für kleine und mittlere Unternehmen



- IT-Sicherheitskonzept:
  - Ermitteln der IT-Sicherheitsziele
  - Erstellen eines IT-Sicherheitskonzeptes
  - Analyse der zur Umsetzung geeigneten Produkte
  - Vergleich der Produkte (Funktionalität und Kosten)
  - Präsentation der Ergebnisse

# Die NT+C-Komplettlösung für kleine und mittlere Unternehmen



- Implementierung der technischen Lösung:
    - Beschaffung der ausgewählten Produkte
    - Installation und Konfiguration der Produkte
    - Abschlusstest
    - Know-how-Transfer für ausgewählte Mitarbeiter (Administratoren)
  - Review:
    - Überprüfung des Erfolgs (3 bis 6 Monate nach der Installation)
- + Kalkulierbare Kosten, überschaubarer Zeitaufwand

# Meilensteine auf dem Weg zur sicheren IT-Infrastruktur



- Das NT+C-Modulsystem für größere Unternehmen umfasst die wichtigsten Meilensteine auf dem Weg zu einer sicheren IT-Infrastruktur:
  - IT-Security-Workshop
  - IT-Sicherheitskonzept
  - Penetrationstest / Security Assessment
  - Implementierung der technischen Lösung
  - IT-Training

# IT-Security-Workshop

IT-Sicherheit ist kein Produkt, auch kein Zustand, sondern ein Prozess, der von allen Mitarbeitern getragen werden muss.

- Darstellung der vielfältigen Gefahren, die Ihrer IT-Infrastruktur drohen
  - Zeigen der möglichen Abwehrmaßnahmen
  - Basis für Ihre Unternehmensentscheidungen
- + Nach dem Workshop sind die Teilnehmer in der Lage, gemeinsam mit unseren Experten ihr individuelles IT-Sicherheitskonzept zu erarbeiten.

**Man muss ein System verstanden haben, um es zu bewerten.**

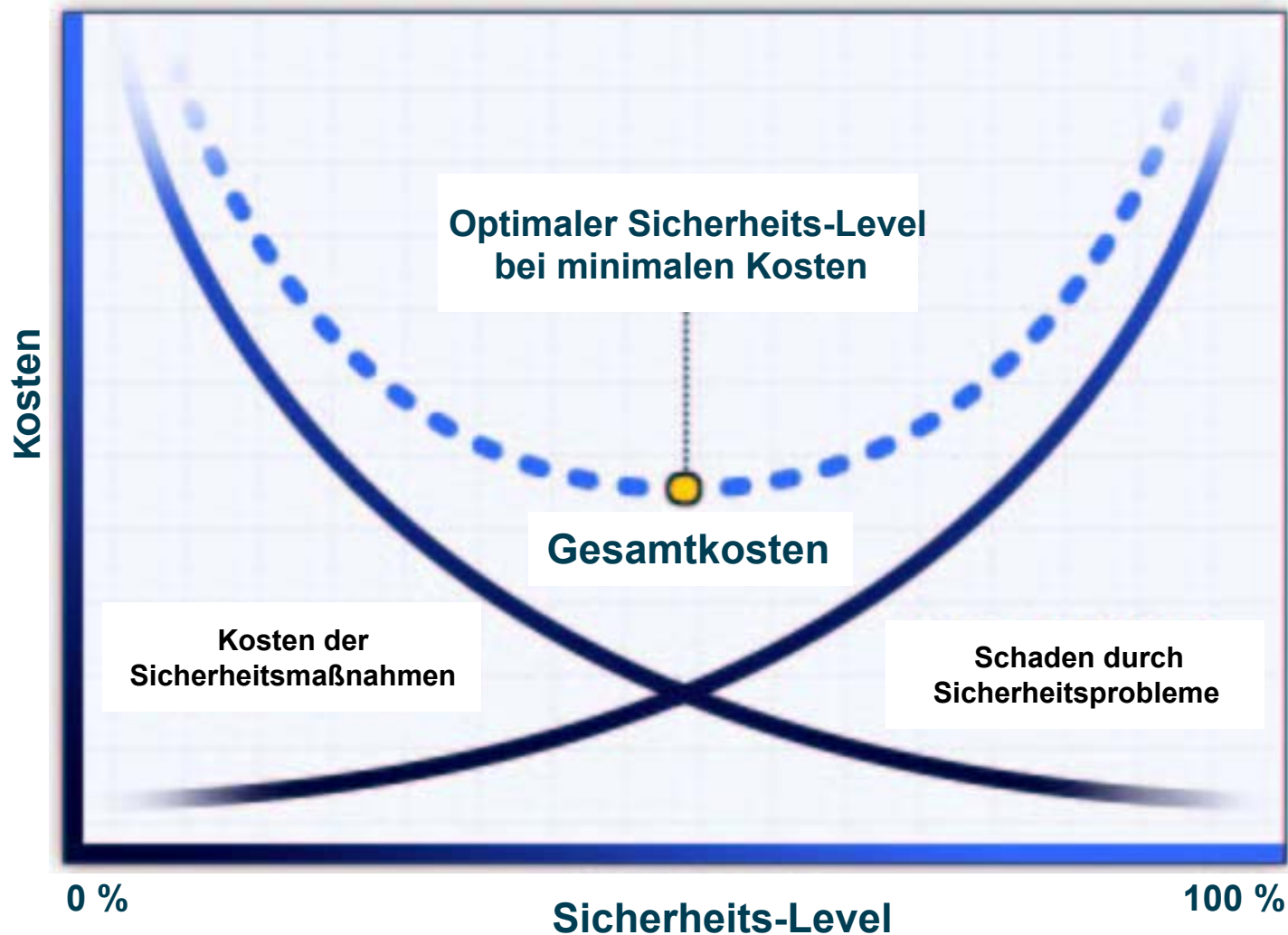
# IT-Sicherheitskonzept

- Erstellen und implementieren eines IT-Sicherheitskonzepts (Security-Policy) für Ihr Unternehmen **oder** überprüfen eines vorhandenen Konzepts
- Ausgehend vom Schutzbedarf des Unternehmens wird eine Policy entwickelt,
  - + die nicht so viel IT-Sicherheit wie möglich, sondern soviel IT-Sicherheit wie nötig bringen soll,
  - + die implementierbar und anwendbar ist
  - + und gewohnte Arbeitsabläufe nicht beeinträchtigt.

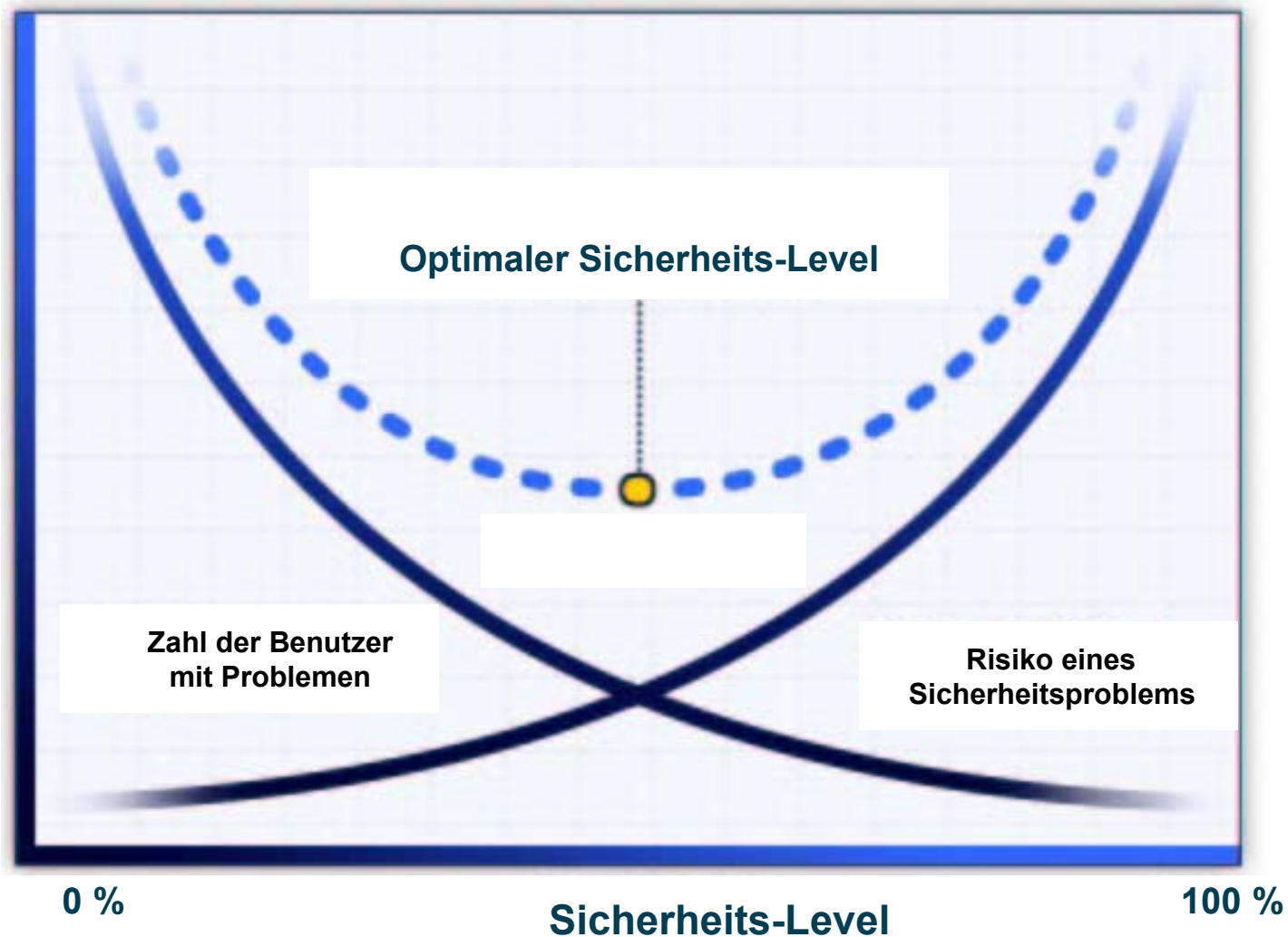
# IT-Sicherheitskonzept

- Modulares Regelwerk mit Richtlinien
  - für verschiedene Bereiche,
  - für Administratoren,
  - interne Benutzer
  - und externe Mitarbeiter
- Analysebericht der IT-Risiken
  - + Verwendbar für das Risk-Management-System nach dem KonTraG
  - + Verwendbar für Basel II

# Wirtschaftliche Ausgewogenheit



# Nicht vergessen: Benutzerakzeptanz!



# Penetrationstests, Security Assessments

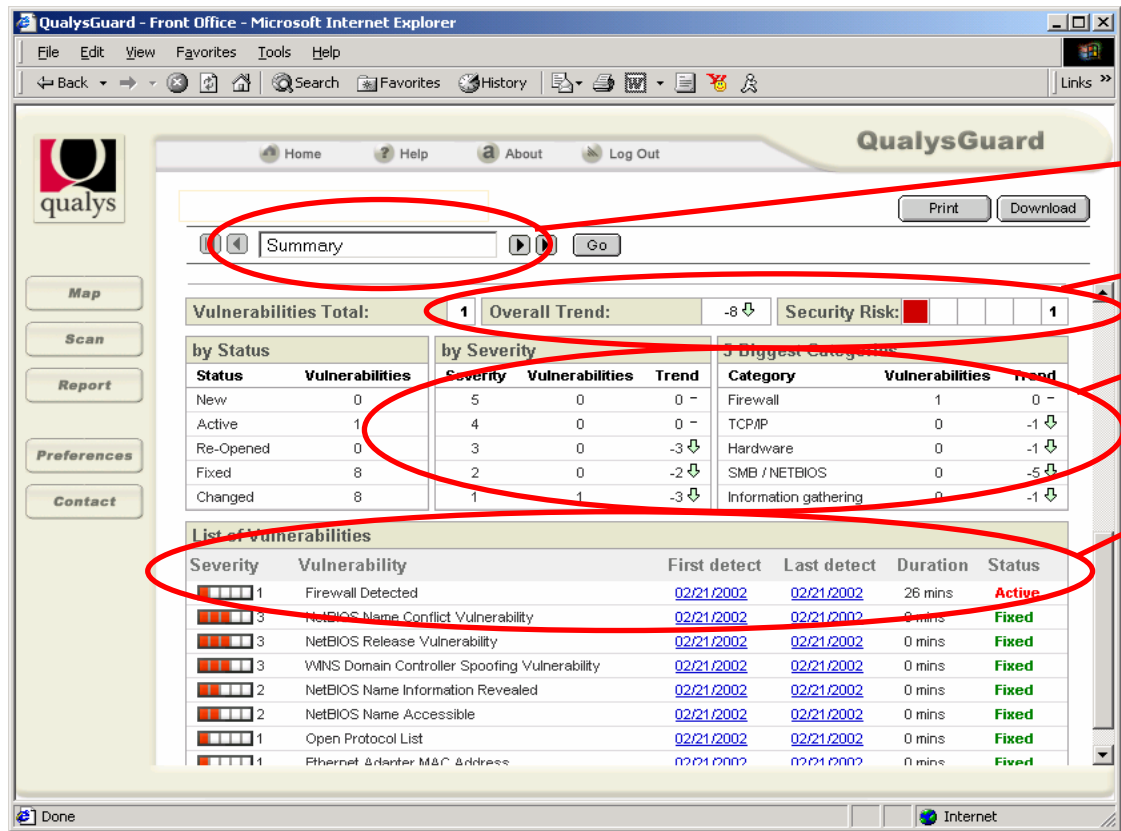


- Viele Verantwortliche glauben, dass ihre IT-Infrastruktur sicher ist, wissen es aber nicht.
- Wir analysieren die Sicherheitsschwächen Ihrer IT-Infrastruktur.
- Zwei Phasen Test:
  - Aus Hacker-Perspektive greifen wir Ihr Netzwerk an:
    - Zero-Knowledge-Test (ohne Information über Ihr Netzwerk)
    - Unter Verwendung einer vorgegebenen IP-Adresse
  - Aus interner Sicht analysieren wir, welche Elemente der IT-Infrastruktur Angriffsziele für Innentäter Ihres Unternehmens darstellen.

**Vertrauen ist gut, Kontrolle besser**

# Penetrationstest

## Grafischer HTML-Report



Reporttyp

Zusammenfassung

Trendanalyse

Schweregrad,  
Schwachstelle,  
Erstes & letztes Auftreten,  
Dauer  
Status (Aktiv/Gefixt)

# Penetrationstest

## Technik- und Managementreport

Report: **Report Sorted by Vulnerability** | Print | Download | Edit

Vulnerabilities Total: 41 | Overall Trend: 4 ↕ | Overall Security Risk: [Red] 4

**Report Summary**

Account:	quays_ts	Filter Severity:	None
IPs Scanned:	4	Filter Status:	New, Fixed, Re-Opened
Total Scans:	6	Include Detailed Results:	No
Dynamic Analysis:	Last 8 weeks	Date:	01/21/2002 to 01/22/2002
Sort by:	Host		
IP / Range:	123.123.123.123, www.qualys-test.com		

by Status		by Severity			5 Biggest Categories		
Status	Vulnerabilities	Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	34	5	6	+3 ↗	SMBNETBIOS	8	+3 ↗
Active	20	4	2	+4 ↗	Info. Gathering	3	+1 ↗
Re-Opened	4	3	14	-5 ↘	TCP/IP	4	-2 ↘
Fixed	18	2	9	+2 ↗	FTP	0	-1 ↘
Changed	0	1	10	-4 ↘	Web Server	2	+2 ↗

**Readable SNMP Information**

**SEVERITY** [Red] 3

**CATEGORY** SNMP

**DIAGNOSIS** Unauthorized users can read all SNMP information because the access password is not secure.

**CONSEQUENCES** Read-access to all SNMP information can give unauthorized users an incredible amount of valuable information about your network. See the "Information Gathered" section of the report for a demonstration.

**SOLUTIONS**

- Brute force of community names:** Replace the default password (often "public" or "private") with a secure one. The password should be hard to guess, and should not be derived from the hostname of the machine or from its model name (e.g., "sun" or "ibm").
- Eavesdropping of community names:** SNMP Version 3 agents, as well as some of the SNMP Version 2 agents (not those named SNMPv2c for "community based SNMP version 2") include authentication using hashing functions, such as MD5.
- Eavesdropping of information retrieved by authorized users:** Use the privacy function, such as DES-encryption, of the protocols described above.
- Replay of legitimate SNMP message by unauthorized users:** The protocols described above provide a simple replay protection using a timestamp and a message sequence number.

Host	First detect	Last detect	Duration	Status
123.123.123.123	01/21/2002	01/22/2002	< 1 day	Active

**Open UDP Services List**

**SEVERITY** [Red] 1

Report: **Executive Report** | Print | Download | Edit

Vulnerabilities Total: 41 | Overall Trend: 4 ↕ | Overall Security Risk: [Red] 4

**Report Summary**

Account:	quays_ts	Filter Severity:	None
IPs Scanned:	4	Filter Status:	New, Fixed, Re-Opened
Total Scans:	6	Include Detailed Results:	No
Dynamic Analysis:	Last 8 weeks	Date:	01/21/2002 to 01/22/2002
Sort by:	Host		
IP / Range:	123.123.123.123, www.qualys-test.com		

by Status		by Severity			5 Biggest Categories		
Status	Vulnerabilities	Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	34	5	6	+3 ↗	SMBNETBIOS	8	+3 ↗
Active	20	4	2	+4 ↗	Info. Gathering	3	+1 ↗
Re-Opened	4	3	14	-5 ↘	TCP/IP	4	-2 ↘
Fixed	18	2	9	+2 ↗	FTP	0	-1 ↘
Changed	0	1	10	-4 ↘	Web Server	2	+2 ↗

**Number of Vulnerabilities by Severity**

Your Network had:

- 6 Severity 5 (Urgent)
- 2 Severity 4 (Critical)
- 14 Severity 3 (Serious)
- 9 Severity 2 (Medium)
- 10 Severity 1 (Minimal)

41 Total

**Vulnerabilities by Severity and Time**

Total Number of Vulnerabilities vs Days Ago (3.0 to 1.0)

Legend: Severity 5 (Urgent), Severity 4 (Critical), Severity 3 (Serious), Severity 2 (Medium), Severity 1 (Minimal)

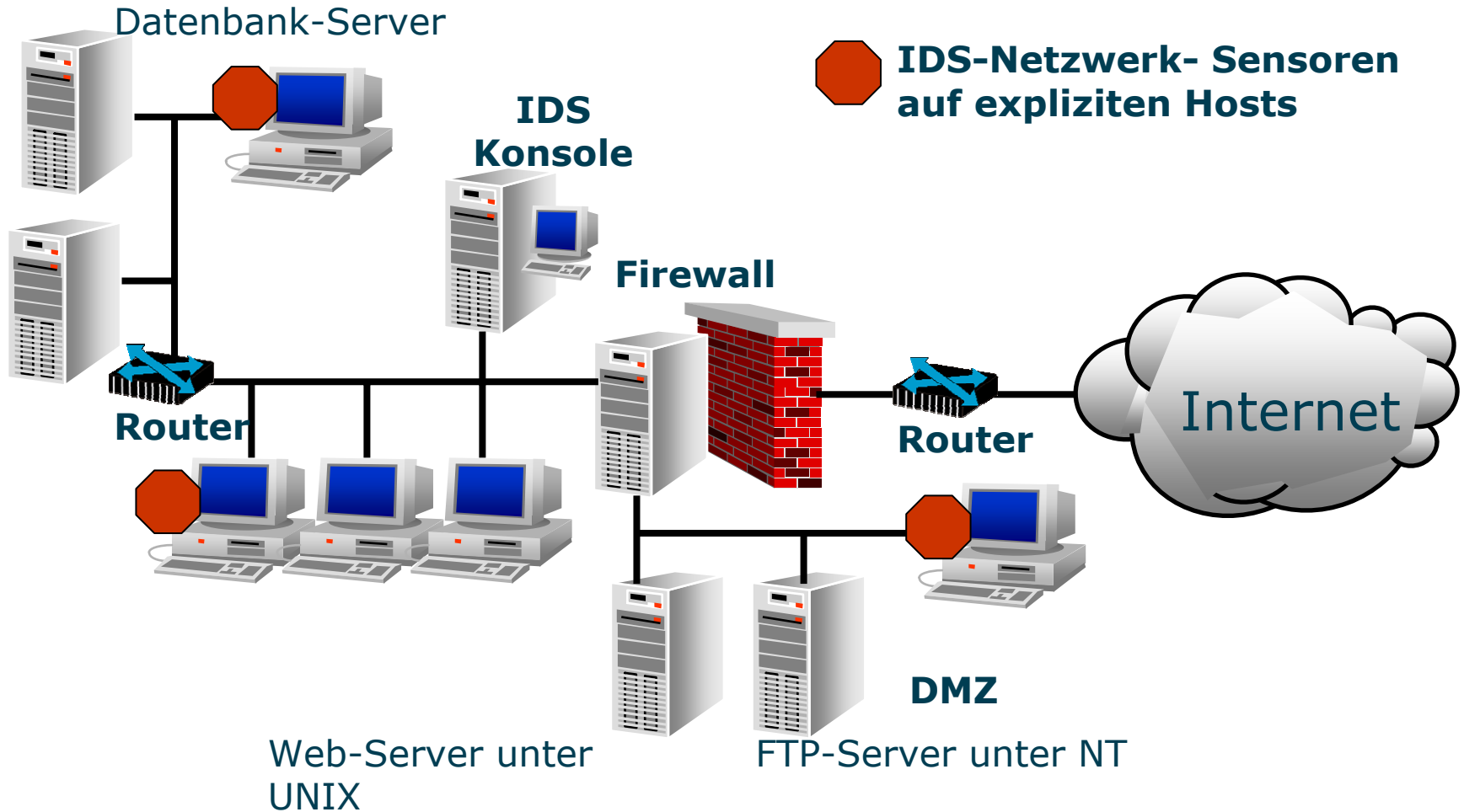
# Implementierung

- Security Policy oder die Ergebnisse der Penetrationstests verlangen nach technischen Lösungen
  - Auswahl und Einrichtung von Firewall-Systemen
  - Firewall-Add-ons, wie Anti-Viren- und Content-Security-Systeme
  - Ausfallsichere IT-Infrastruktur

# Implementierung

- Eine Firewall schützt nach außen.
- Es bleiben Möglichkeiten, die Firewall zu überwinden, und es bleibt das Risiko der Innentäter.
- Wir helfen Ihnen bei der Auswahl und Implementierung von Security-Scannern und Intrusion Detection-Systemen, die Sicherheitsbeeinträchtigungen frühzeitig erkennen.

# Implementierung



# Training

- Administratorenschulung („Training on the Job“), in kundenindividuellen Workshops und Standardseminaren
- Anwenderschulung
- Erarbeitung von mittel- und langfristigen Weiterbildungsprogrammen
- Sensibilisierung der Mitarbeiter durch spezielle Maßnahmen oder in speziellen Workshops

**Sicherheit muss „gelebt“ werden**

# Training

- + Jeder Mitarbeiter kennt und leistet seinen Beitrag zur IT-Sicherheit.
- + In Ihrem Unternehmen existieren Mitarbeiter, die die Verantwortung für die IT-Sicherheit tragen.
- + Vom Anfänger bis zum Experten, von der Assistenzkraft bis zum Sachbearbeiter, vom Systemadministrator bis zum IT-Manager:

**NT+C bietet für jede Zielgruppe maßgeschneiderte Kurse: für kleine, mittlere und große Unternehmen sowie Behörden.**

# Training



- Die IT-Security-Ausbildung beginnt bei den NT+C-Trainings zu Anwendungen, Betriebssystemen und Netzwerken.

# Wir freuen uns über Ihr Feedback



Network Training and Consulting GmbH  
Weidenauer Straße 15  
57078 Siegen  
siegen@networktraining.de

Network Training and Consulting Südwest GmbH  
Gutenbergstraße 13  
70771 Leinfelden-Echterdingen  
stuttgart@networktraining.de

**Bundesweite Infoline: 0180 11 77 333**  
(Festnetz / Telekom 4,6 Cent / Minute)



**it networks – because we do**