SIDLER Information Security GmbH

Für BESSERE Sicherheit
IT-Sicherheit für KMU

vom Know-how zum Do-how

Netzwerksicherheit – Aktuelle Bedrohungen und Lösungsansätze

KeyNet AG – Technologieseminar - 26. Juni 2009

Ziele des Vortrages

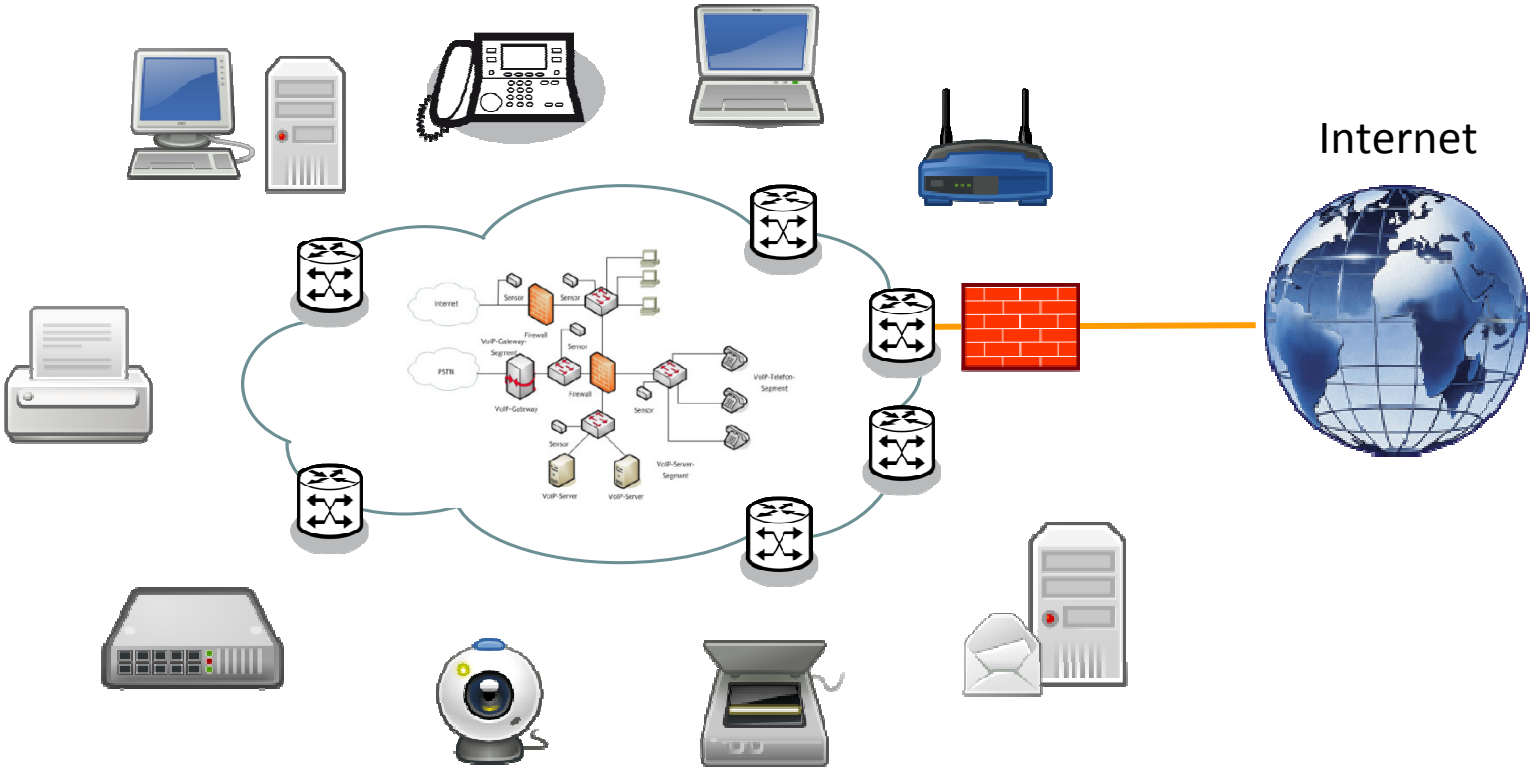
- Sie kennen die aktuellen Bedrohungen und Gefahren in Bezug auf Ihr Netzwerk
- Die möglichen Lösungsansätze für die Sicherung Ihres Netzwerkes sind Ihnen bekannt
- Sensibilisierung im Bereich Netzwerksicherheit

Das Netzwerk

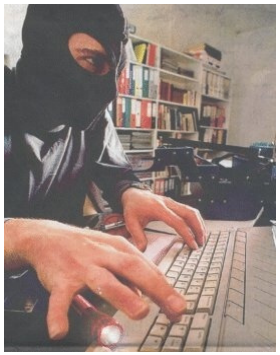
Kennen Sie die Risiken Ihres Netzwerkes?

Ihr Netzwerk

- Wissen Sie, welche Geräte an Ihrem Netzwerk angeschlossen sind?
- Wie diese Geräte konfiguriert sind?
- Wer Zutritt und Zugriff auf diese Geräte hat?
- Was diese Geräte alles aufzeichnen?



Die klassischen Gefahren und Risiken



Höhere Gewalt

Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …

Menschlich

Bedienu

Gesetzliche

Nicht Ei

Technisches

Netzwe

Konsequenzen:

- Unterbruch der Geschäftsprozesse
- Produktions-Ausfall, Auslieferungs-Verzug
- Projekt-Verzögerung
- Verlust von vertraulichen Daten oder Know-how
- Bussen (juristische Konsequenzen)
- Image Schaden
- Wiederherstellungskosten

Organisatorische Mängel

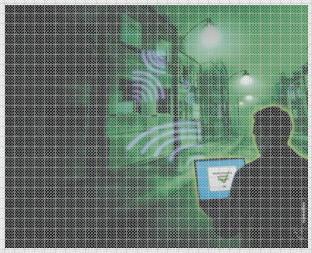
Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …

Vorsätzliche Handlungen

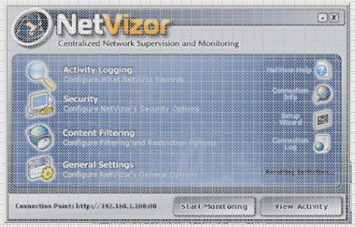
Manipulation, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Netzwerk Gefahren und Risiken I

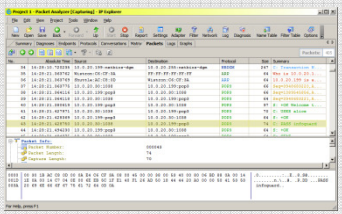
Wireless LAN Angriff



Commercial Spyware



E-Mail & VOIP Sniffing

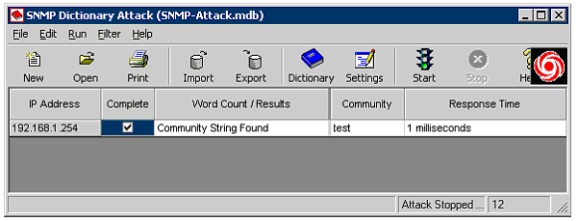


MAC-Spoofing
IP-Spoofing
DNS-Spoofing

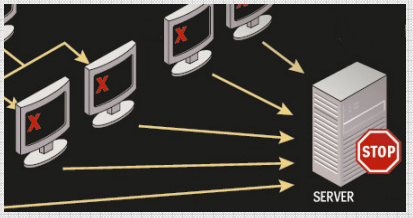
Physischer Angriff

Netzwerk Gefahren und Risiken II

SNMP-Angriffe



Denial of Service Angriffe

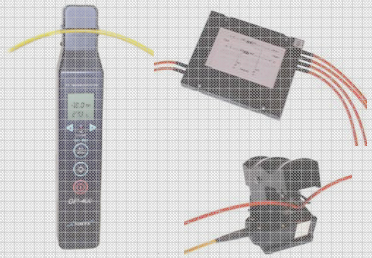


Remote Desktop und Skype

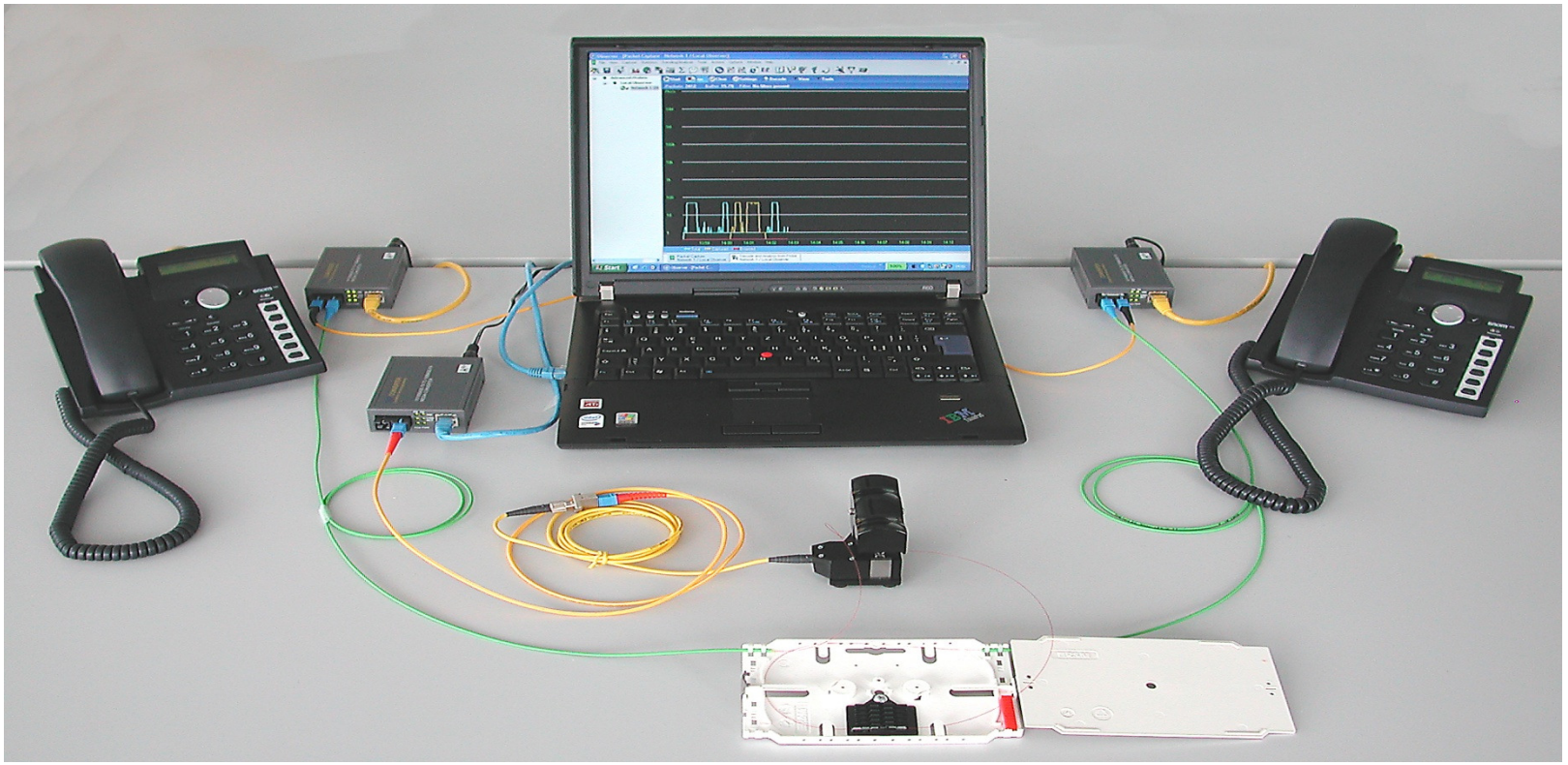
TeamViewer

skype

Fiber Tapping



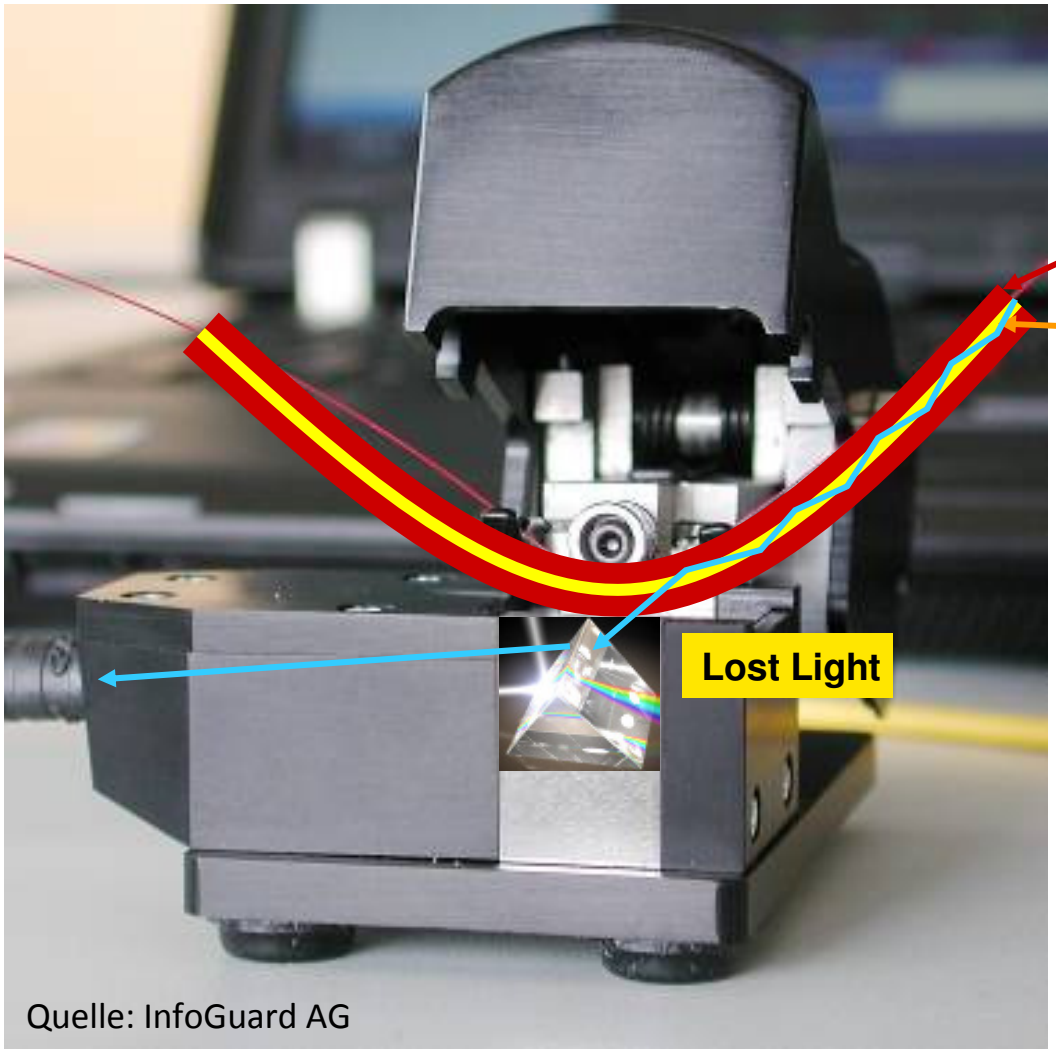
Fiber Tapping – eine Illusion?



Wird eine Glasfaser gebogen, tritt Licht aus der Faser aus. Mit den heutigen, modernen Empfängern reichen schon 1-2% der optischen Leistung aus, um das vollständige Signal zu erhalten und in seine digitale Form zu wandeln.

Quelle: InfoGuard AG

Glasfasernetzwerke – Funktionsprinzip eines Biegekoppler



Quelle: InfoGuard AG

Aktuelle Netzwerk-Gefahr

Millionen DSL-Router sind akut gefährdet

08.04.2009 | 08:08 Uhr

Cross Site Request Forgery (CSRF) als Angriffsmöglichkeit auf Breitband-Modem wurde lange unterschätzt. Doch jetzt ist es unserer deutschen Schwesterpublikation "TecChannel" gelungen, über einfache CSRF-Attacken DSL-Router (Digital Subscriber Line) von A wie AVM Fritz!Box bis Z wie ZyXEL über das Internet von aussen anzugreifen.

(cw)

Surft man mit dem PC auf eine manipulierte Website, kann die komplette Konfiguration der DSL-Router unbemerkt modifiziert werden.

Bislang gelten Cross-Site-Scripting- und Injection-Angriffe als Haupteinfallsvektor für erfolgreiche Attacken auf Web-Server. Doch in der aktuellen Liste der gefährlichsten Fehler, die regelmässig von der OWASP (Open Web Application Security Project) herausgegeben wird, hat sich Cross Site Request Forgery (CSRF) inzwischen auf Platz fünf hochgearbeitet.

Wie gefährlich dieser bislang unterschätzte Angriffsweg tatsächlich ist, zeigen aktuelle Sicherheitstests von TecChannel. Über CSRF-Attacken ist es uns gelungen, die Konfiguration der AVM Fritz!Box, des Cisco/Linksys WAG 160 N und eines ZyXEL P-660HW beliebig zu modifizieren. Aber auch die meisten anderen DSL-Router dürften gefährdet sein. Für den Angriff genügt es, dass der Anwender eine präparierte Website besucht. Diese kann dann alle Konfigurationsarameter, die über die Web-Oberfläche des DSL-Routers zu erreichen sind, beliebig ändern. Ein Besuch einer manipulierten Seite, und alle Telefonate laufen beispielsweise über eine teure 0900er-Vorwahl.

Der Passwortschutz der Router erwies sich dabei als nicht ausreichend und kann umgangen werden.

Gefahren organisatorischer Natur

- Falsche Konfiguration der Netzwerk-Geräte und kein Backup der Konfiguration
- Keine Redundanz der kritischen Netzwerk-Komponenten
- Zutritt zu den Netzwerk-Geräten (Router, Switches etc.) ist nicht geschützt oder geregelt
- Keine Dokumentation der aktiven Netzwerk-Komponenten vorhanden
- Key-Know-how Träger hat Ihr Unternehmen ohne Know-how Transfer verlassen
- Die aktiven Netzwerk-Komponenten sind nicht genügend vor physischen Bedrohungen (wie Wasser, Klima, Staub etc.) geschützt
- Die Netzwerk-Komponenten werden nicht korrekt gewartet bzw. betrieben
- Es ist kein Change-Management Prozess vorhanden
- Nicht genügende Ausbildung der Mitarbeitenden (Netzwerk-Verantwortliche)
- Fehlerhafte Bedienung der Netzwerk-Komponenten
- Fehlende oder ungeeignete Netzwerk-Segmentierung
- Die Verkabelung wurde nicht professionell installiert und ausgemessen
- Fehlendes Risiko-Management (Sind Sie vorbereitet, wenn…?)

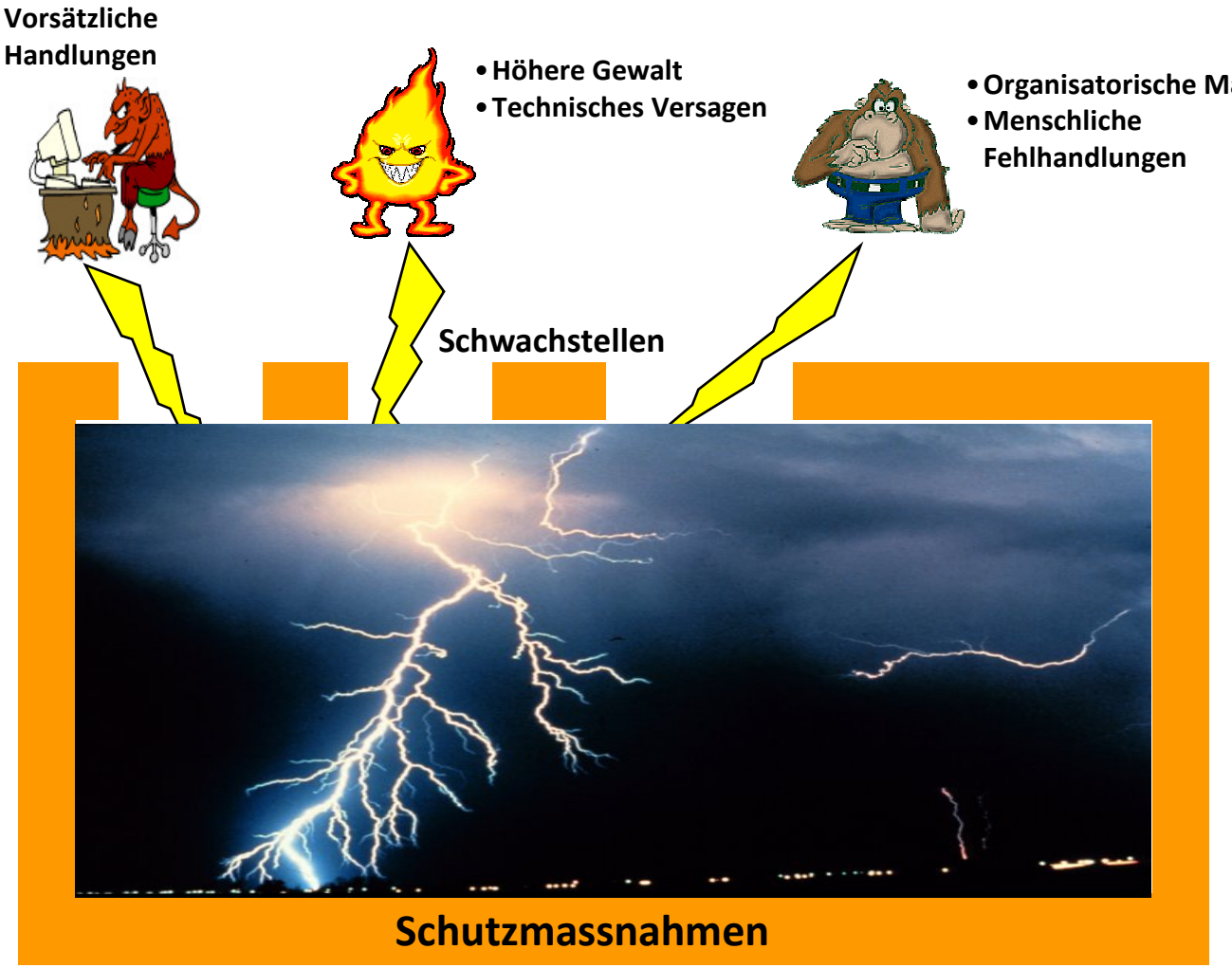
Was ist eine Gefahr – ein Risiko?

Bedrohung

Schwachstelle

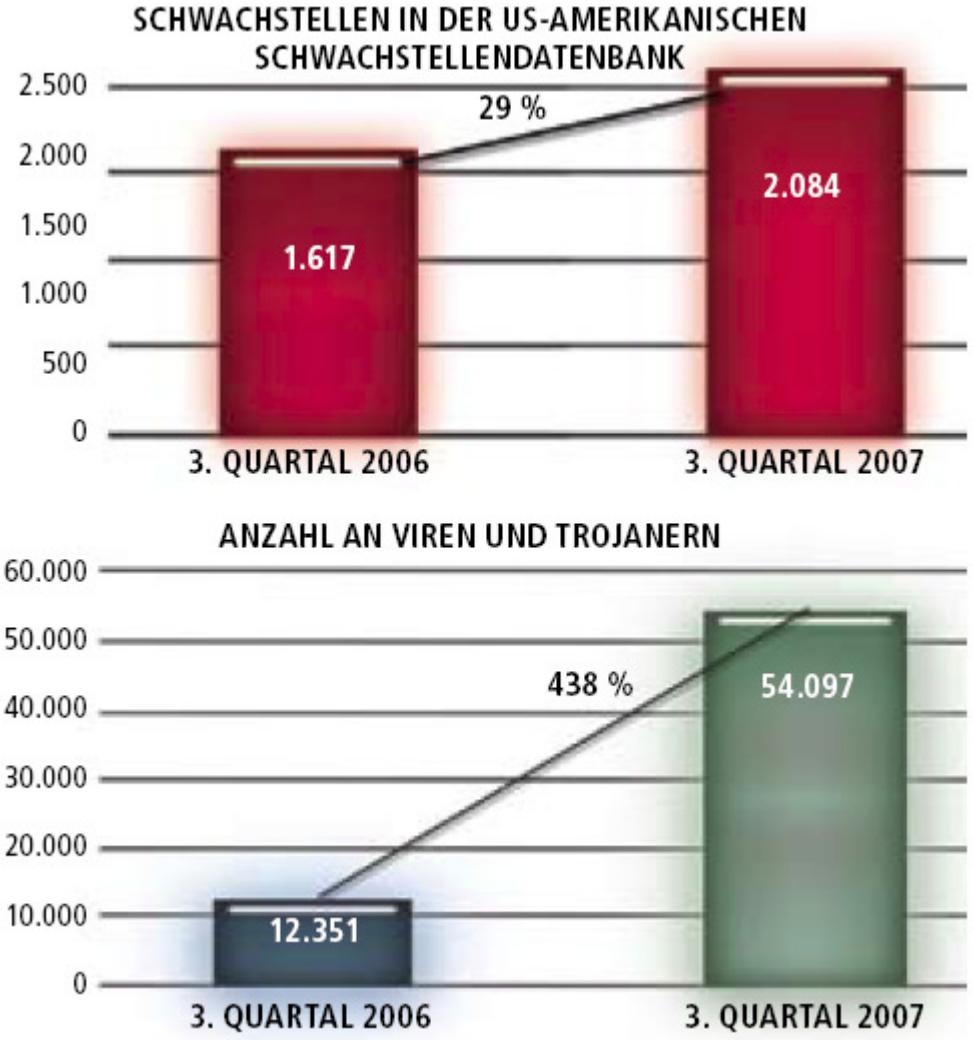
Gefahr

Risiko



R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

Global Threat Report 2008 von MacAfee

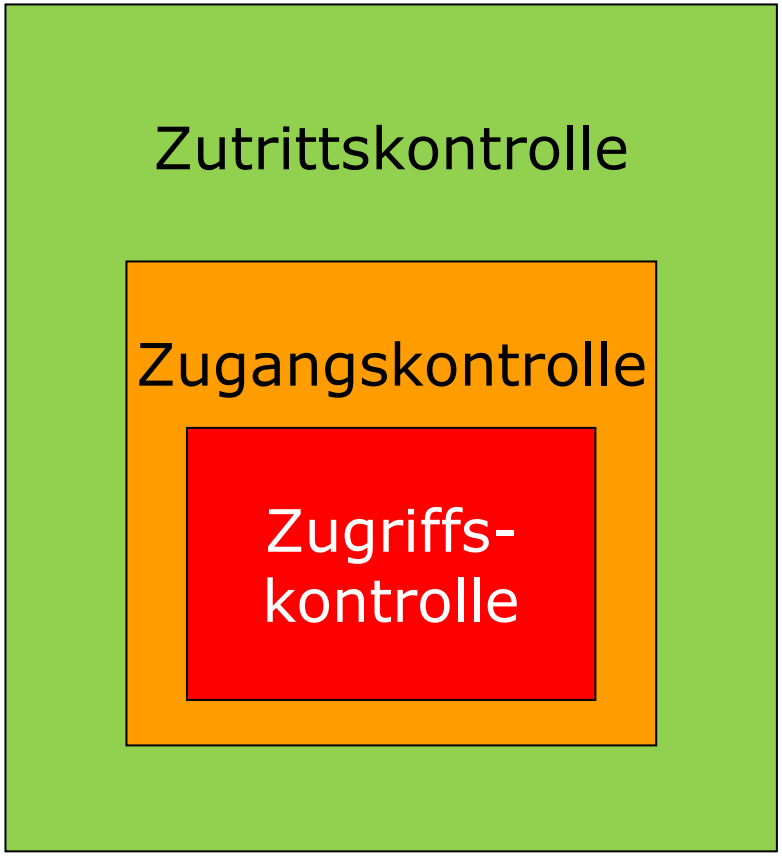


Die 4 Layer des Sicherheits-Managements Verteidigungsstrategie

Layer 1	**Technologie (20%)** **Firewall, Virenschutz, IDPS, NAC, DMZ**
Layer 2	**Management (20%)** **Netzwerk-Management, Vulnerabiliy Management, Audit, Pentest**
Layer 3	**Organisation (20%)** **Weisungen, Prozesse (ITIL), Kontrolle, BCM/DR**
Layer 4	**Mensch (40%)** **Ausbildung, Sensibilisierung**

Zutritts-, Zugangs- , Zugriffskontrolle

- Zutrittskontrolle
  - gerätebezogen
  - Schutz des physischen Systems (Firewall, Router etc.)
- Zugangskontrolle
  - personenbezogen
  - Schutz des logischen Systems (Firewall, Router etc.)
- Zugriffskontrolle
  - „Daten“-bezogen (Konfigurationen)
  - Schutz der Operationen (RBAC)



Wie sieht es bei Ihnen aus?

- Passwörter der Firewalls, Switches, Router etc. sind nicht vor unbefugtem Zugriff geschützt
- Zutritt zu Gebäuden und Netzwerk-Schränken ist kaum gesichert und fremde Personen können sich unbehelligt bewegen
- Mitarbeitende sind hilfsbereit und geben bereitwillig Auskunft
- Notebook und andere Netzwerk-Geräte können einfach ins bestehende Netzwerk angeschlossen werden und erhalten eine gültige IP-Adresse
- Vertrauliche Dokumente (Konfigurationen, Netzwerk-Zeichnungen etc.) liegen auf dem Arbeitsplatz
- Dokumente und Datenträger werden nicht korrekt vernichtet

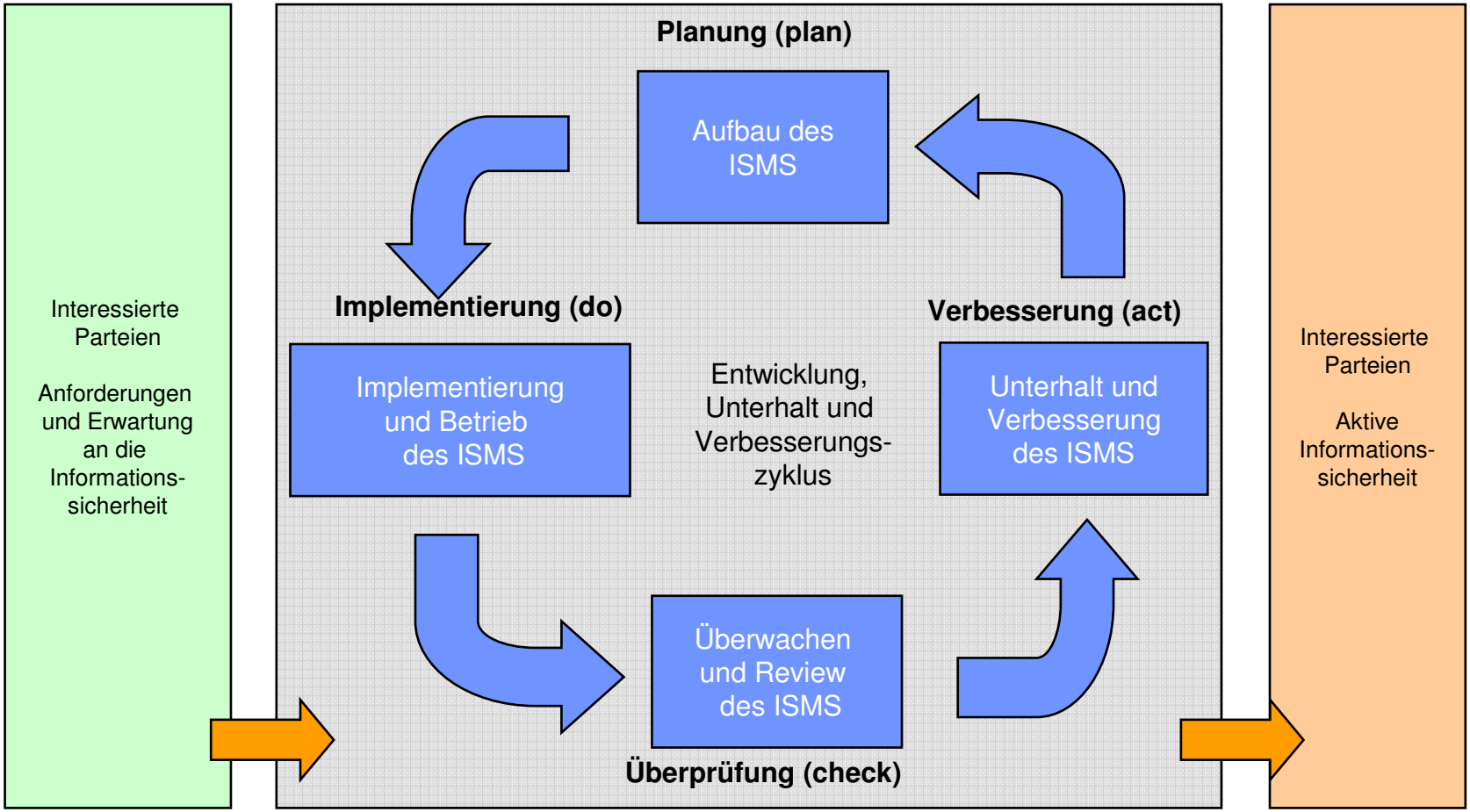
Lösungsansätze für ein sicheres Netzwerk

- VPN (Virtual Private Network) -> Schutz der Vertraulichkeit und Integrität
- NAC (Network Access Control) und UTM (Unified Threat Management)
- DMZ (Demilitarized Zone) und VLANs (Virtual Local Area Network)
- Sichern Sie Ihre Wireless-Netzwerke (DMZ, Config-Passwort, Verschlüsselung, SSID, MAC-Adressen etc.)
- Sind Sie vorsichtig mit der SNMP-Konfiguration
- Erstellen Sie ein IP-Konzept (Zonen, Adresse-Bereiche für Clients, Server etc.)
- Konfigurieren Sie Ihre Firewall richtig. Und überprüfen Sie regelmässig die Rules und die Logs
- Definieren Sie die Benutzer-Accounts bei den Routern, Switches korrekt
- Verwenden Sie starke Passwörter bei den Routern, Switches etc.
- Verschlüsselung von Netzwerk-Verbindungen, welche über den öffentlichen Grund oder öffentliche Netzwerke gehen. (z.B. Verbindung vom RZ zum Backup-RZ, Zugang über Internet (VPN)
- Setzen Sie ein Netzwerk-Management System zur Überwachung ein

Lösungsansätze für ein sicheres Netzwerk

- Network Intrusion Detection System (NIDS) mit Alarm-Funktion
- Scannen Sie regelmässig Ihr Netzwerk
- Führen Sie jährlich einen unabhängigen Netzwerk-Audit durch

Information Security Management Prozess



Plan – Do – Check - Act

Plan

Netzwerk-Konzept (Netzwerk-Topologie, Netzwerk-Protokolle, Schnittstellen, WAN, Internet-Anbindung, Firewall, IDPS, Proxy, SAN, Drucker, Scanner, URL-Filter, Antivirus-Lösung, SPAM-Filter, DMZ, Redundanz, VLAN‘s, WLAN, Support, NAC, VPN, VOIP, physische Sicherheit, Management (SNMP), Monitoring, USV, Verkabelung etc.

Do

Änderung der Default-Passwörter, sichere Fernwartung, Notfallvorsorge (DR), Backup der Konfigurations-Daten, Dokumentation (Betriebshandbuch, Konfiurations-Manual, Beschriftung, Kabelmanagement etc.)

Check

Überprüfen der Log-Files, Netzwerk-Audit (Scanning), Update/Upgrade der Firmware und Betriebssysteme

Act

Netzwerk-Lösung stetig verbessern und erweitern, ITIL-Prozesse einführen (Change Management, Configuration Management, Incident Management etc.)

Herausforderungen an die Netzwerksicherheit

- Mobile Mitarbeiter mit Notebooks, iPhones etc.
- Remote-Access für die Mitarbeitenden und für den Fernsupport
- Nicht bewilligte wireless Access Points
- Umsetzung der eigenen Informationssicherheits-Strategie
- Aufbau eines zentralen Netzwerk-Sicherheits-Cockpits (Dashboard) inkl. Alarmierung
- Sicherung der Geschäfts-Prozesse (BCM und DR)
- Einhaltung der Gesetze und Verordnungen (DSG, IKS, etc.)
- Das Unternehmen und das Management vor Haftungsklagen schützen
- Kennen und akzeptieren der Rest-Risiken
- Komplexe Netzwerk-Technologie professionell umsetzen und warten

Ihr Nutzen

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Positive Audits (interne und externe Revision)
- Einhalten aller Gesetze (IKS, Datenschutz, etc.)
- Wettbewerbsvorteil -> Sicherheit = Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter (Sicherheitskultur)
- Steigert die Möglichkeit die Netzwerk-Architektur sicher und schneller zu erweitern

Trends und Ausblick

- Trends im Netzwerkbereich:
  - NAS
  - Netzwerk-Monitoring Lösungen (SIEM Security Information Event Monitoring)
  - NAC Lösungen (Verteilung der Sicherheits-Policy, Health-Check des Clients, zentrales Management, Scanning-Funktion etc.) -> Endpoint Security!
  - Trennung Unternehmens-Netzwerk und Internet (Citrix/Tarantella)
- Weiter wachsende Mobilität / “Intelligente” Geräte / Spontane Netzwerke (GPS, RFID, WLAN, UMTS, Bluetooth etc.)
- Erhöhte Abhängigkeit von komplexer Technologie (Virtualisierung & Miniaturisierung der Hardware, Cloud-Computing)
- Kommunikations-Tools (Skype, Teamviewer , Peer-to-Peer, etc.)
- Erhöhte Abhängigkeit von komplexer Technologie
- Erhöhte rechtliche / regulatorische Anforderungen
- Die Trojaner werden raffinierter und tarnen sich z.B. als Microsoft oder Java Update
- Einführung von ITIL-Prozessen (Change Management etc.)

KeyNet AG Seminar Angebot

Sie erhalten heute das **„IT-Sicherheitshandbuch“** für nur

CHF 80.- **(statt 98.-)**

IT-Sicherheitshandbuch für die Praxis ISBN: 3-9521208-3-9