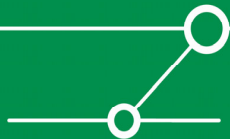


# Sicherheit per Quarantäne – Moderne Ansätze beim Design sicherer Netze

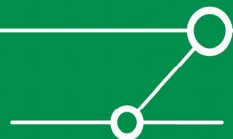
Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)  
CISSP, CISA



# ERNW GmbH



- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell neun Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Penetrations-Tests, Risiko-Bewertung & -Management, Security Research
- Kunden: Industrie, Banken, Behörden, Provider
- [www.ernw.de](http://www.ernw.de)



# Agenda

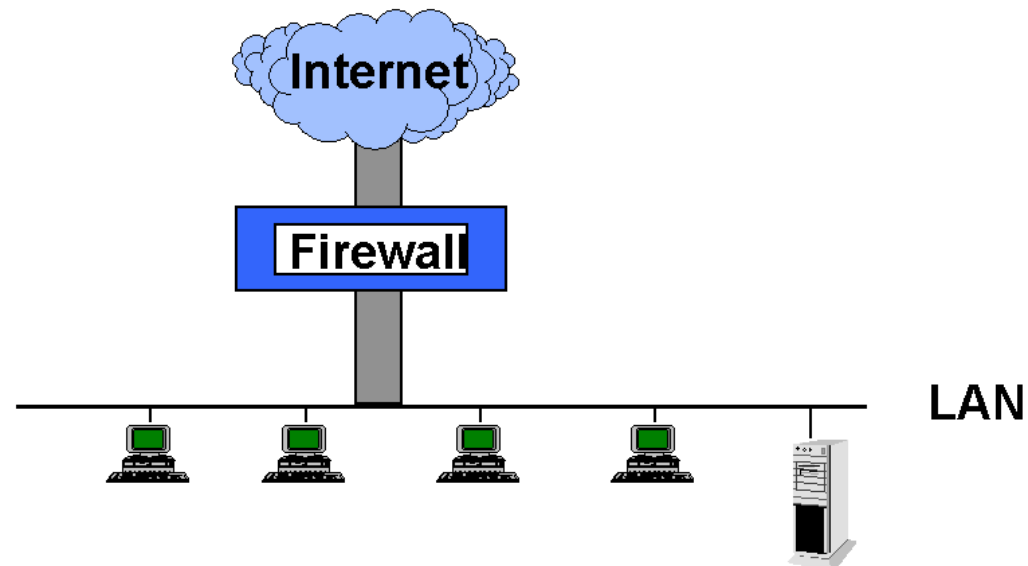


- Das klassische Firewall-Modell
- Netzwerk-Segmentierung mit Zonen
- Konzept & Technologie des Quarantäne-Ansatzes



# Das klassische Firewall-Modell

entnommen aus einem Foliensatz von 1997



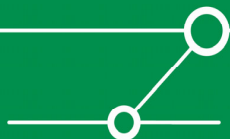
# Das klassische Firewall-Modell



- Noch immer entspricht dies in etwa dem in vielen Organisationen anzutreffendem Design.
- Die hier symbolisierte 'Firewall' kann dabei durchaus aus mehreren Einzelkomponenten bestehen (inkl. AV-Gateway, Content Filter etc.).

Zentrale Konzepte sind hier:

- *Perimeter Defense/Border Defense*: Gefahren-Abwehr an der Netzwerk-Grenze
- *Choke Point*: der gesamte Netzwerk-Verkehr muss über diese(n) Punkt(e) fließen, um dort geprüft/kontrolliert/geregelt zu werden.

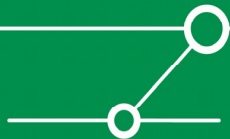


# Grundannahmen des klassischen Firewall-Modells



Dieses Design setzt implizit u.a. voraus:

- Alle internen Hosts sind vertrauenswürdig (*trusted*).  
[siehe etwa Architektur der *Cisco PIX*].
- Alle internen Systeme haben denselben Schutzbedarf.
- Es gibt eine klare Grenze zwischen 'innen' und 'außen'.
- Gefahren kommen in erster Linie 'von außen'.
- Die Firewall kann diese Gefahren erkennen und abwehren.

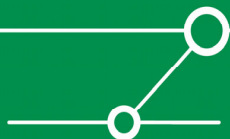


# Kritik dieser Grundannahmen



“Alle internen Hosts sind vertrauenswürdig (*trusted*).”

- In den internen Netzen sind zunehmend Geräte, die dort nur temporär sind & die sich oft auch ‘außerhalb’ befinden (Laptops, PDAs, ggf. private PCs).
- Die Systeme werden bedient von Menschen (*Usern*)...
- Die Vertrauenswürdigkeit der Systeme hängt weiterhin von ihrer Konfiguration ab (Patch-Level, Aktualität der Viren-Signaturen, System-Konfiguration etc.).
- Dies alles können die FW-Admins üblicherweise überhaupt nicht einschätzen... weil unterschiedliche Abteilungen für Firewalls & Desktop-Rechner zuständig sind.
- Wer & wo ist ‘intern’?

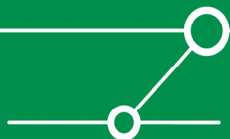


# Kritik dieser Grundannahmen



“Es gibt eine klare Grenze zwischen innen und außen.”

- Diese Grenze wird aufgeweicht eben durch Systeme, die nur temporär im internen Netz sind (s.o.).
- Interne Netze werden logisch erweitert durch VPNs... mit ggf. unkontrollierbaren Endpunkten.
- Sie werden möglicherweise auch physisch erweitert durch Wireless-Technologien (WLANs, Bluetooth etc.).
- Es gibt immer mehr ‘Partner-Anbindungen’, Wartungszugänge etc.  
Diese sind zwar durchaus ‘kontrollierbar’, machen aber die Regelsätze dann unübersichtlicher und damit meist fehlerhaft(er).

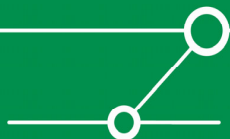


# Kritik dieser Grundannahmen



“Gefahren kommen in erster Linie von außen.”

- S.o.: die Systeme werden bedient von Menschen (*Usern*)...
- Gestattet *Ihre* Firewall eingehend Port 135 oder 1433?  
Und trotzdem haben sich SQL-Slammer und W32/Blaster in Unternehmensnetzen ausgebreitet...
- Selbst wenn dem so *wäre... könnten* Sicherheits-Probleme ja auch intern entstehen... und damit jenseits der Zuständigkeit einer *Border Defense*-Firewall.

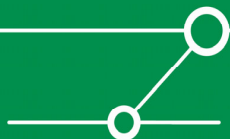


# Kritik dieser Grundannahmen



“Die Firewall kann diese Gefahren erkennen und abwehren.”

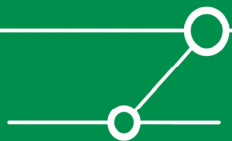
- Firewall-Technologie und –Implementierung hinken der technischen Entwicklung (von Übertragungs-Mechanismen/Protokollen) deutlich hinterher (siehe Instant Messaging, VoIP, SOAP etc.).
- Sicherheits-relevanter Verkehr kann leicht getunnelt werden (insbesondere über HTTP oder auch SSL/TLS).
- Firewalls können nur (stark) beschränkt mit verschlüsseltem Verkehr umgehen.
- Ausblick: Diese Probleme werden mit IPv6 noch größer.



## Weitere Probleme



- Eine *Border Defense/Choke Point* Firewall bildet oft einen Flaschenhals für die Kommunikation... und verlockt dadurch, sie zu umgehen.
- Es wird ggf. ein falsches Bewusstsein von Sicherheit erzeugt ("wir haben doch eine Firewall").



# Segmentierung als typischer Lösungsansatz



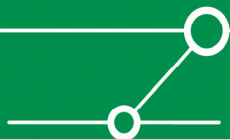
- Eine geeignete Segmentierung des Netzes mit Regeln für die Netzübergänge und geeigneten Massnahmen innerhalb der Segmente kann viele der o.g. Probleme lösen.
- Nachfolgend ein Beispiel aus einer deutschen Provider-Umgebung (“Zonen-Modell”).



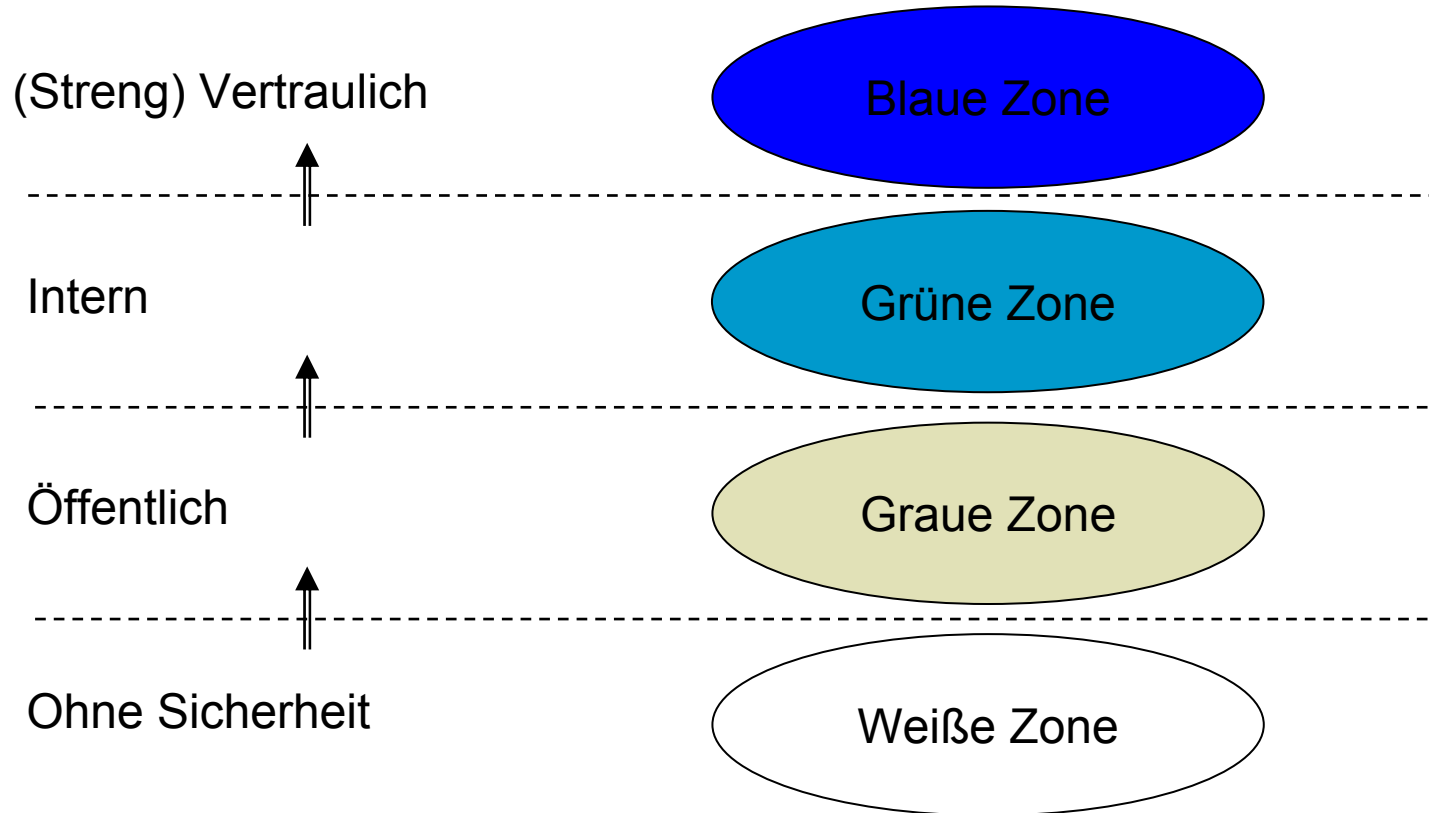
# Grundlegendes Konzept



- Das gesamte Netzwerk wird in Segmente (“Zonen”) mit unterschiedlichen Sicherheits-Anforderungen unterteilt. Die Zonen sind physisch voneinander getrennt und können in sich nochmals (etwa anhand von Anwendungen) unterteilt werden (z.B. mit VLANs).
- Alle Netzwerk-Entitäten im weitesten Sinn (etwa Applikationen, Systeme, User) werden durch ihre jeweiligen Owner/Verantwortlichen je einer Zone zugeordnet.
- Pro Zone gelten bestimmte Massnahmen zu Installation/Konfiguration/Betrieb der Systeme (bspw. Richtlinien hinsichtlich Dokumentation, User-Verwaltung, Zugriffsregelung, Hardening, Logging, Business Continuity etc.).
- Die Kommunikationsbeziehungen zwischen den Zonen sind genau geregelt; im Beispiel sind etwa nur Kommunikationsbeziehungen zwischen benachbarten Zonen gestattet und bestimmte Kommunikationsvorgänge müssen zwingend verschlüsselt werden.

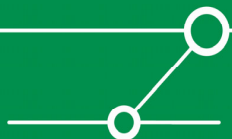


# Beispiel zur Netz-Segmentierung



# Beispiel zur Netz-Segmentierung, Kommunikationsbeziehungen

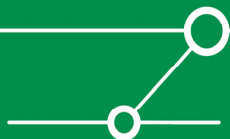
Datenquelle in Zone	Applikation in Zone	Übergang zu Zone	Verschlüsselung
Blau	Grün	Grau	Ja
Blau	Grün	Grün	Ja
Grün	Grün	Grau	Ja
Grün	Grün	Grün	Ja
Grün	Grau	Weiß	Ja
Grün	Grau	Grau	Ja
Grau	Grau	Weiß	Nein
Grau	Grau	Grau	Nein



# Segmentierung, Vorteile



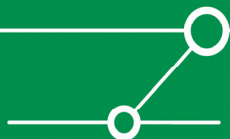
- Den Grundprinzipien einer solchen Segmentierung zu folgen, kann auch in Unternehmensnetzen viele der o.g. Probleme lösen.
- Sicherheitsprobleme (etwa Würmer) werden bei geeigneter Kommunikation auf einzelne Segmente beschränkt.
- Verbindliche Richtlinien pro Zone gewährleisten (idealerweise) die einheitliche Konfiguration von Systemen.
- Es gibt definierte Kommunikationsbeziehungen *innerhalb* des Netzes.
- etc.



# Mögliche Probleme einer solchen Segmentierung



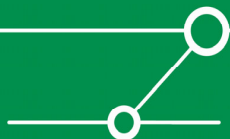
- Das klassische Problem: organisatorischer Soll-Zustand versus ggf. technischer Ist-Zustand.
- Die vorgenommene Zonen-Einstufung bestimmt *anschliessend* ein administratives (menschliches) Handeln, das zu einer bestimmten Systemkonfiguration führen *soll*.
- Wäre nicht vielleicht der umgekehrte Weg (konkrete Konfiguration eines Systems führt wiederum zu Zonen-Plazierung) angesichts aktueller Gefahren (z.B. Würmer) vielversprechender?
- Kann eine sinnvolle Re-Evaluierung beim schnellen Technologie-Wandel in modernen Netzen gewährleistet werden?



# Der Quarantäne-Ansatz



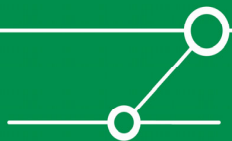
- Diese Fragestellungen haben zu einem weiteren Design-Ansatz geführt, in dem der Begriff *Quarantäne* eine grosse Rolle spielt.
- Theoretische Erörterung im (bis Januar 2005 gültigen) IETF-Draft *Quarantine Model Overview for IPv6 Network Security [draft-kondo-quarantine-overview-01]*. [1]
- Produkte etwa:  
*Cisco Network Admission Control*  
*Alcatel OmniSwitches mit Automated Quarantine Engine*



# Der Quarantäne-Ansatz, grundlegende Methodik



- Untersuchung/Bewertung des Security Levels von jedem Knoten
- Segmentierung des Netzes anhand dieses Security Levels
- Anwendung einer Policy auf jedes Netzwerk-Segment

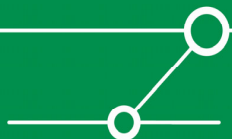


# Der Quarantäne-Ansatz, Ermittlung des Security Levels



Zugrundeliegende Parameter können hier etwa sein:

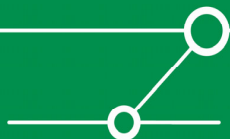
- OS & Software-Versionen
- Installierte Patches
- Installierte Security Software (Anti-Virus, Lokale Firewall etc.)
- Konfiguration & Einstellungen



# Der Quarantäne-Ansatz, Segmentierung anhand des SecLevels



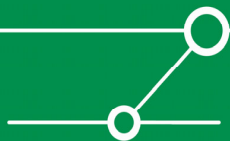
- Die Segmentierung wird durch Netzwerk-Devices vorgenommen.
- Beteiligte Technologien können etwa sein: 802.1x, VMPS, DHCP Option 82 etc.
- Segmentierung wird z.B. gewährleistet durch: VLANs, IP-Subnetze, MPLS u.a.



# Der Quarantäne-Ansatz, Policy-Anwendung



- Bestandteile einer Policy können sein:  
Authentifizierungs-Erfordernisse (etwa von Knoten mittels Zertifikaten)  
Paketfilter  
Routing-Pfade  
Bandbreiten-Begrenzungen (Wurm-Traffic!)  
usw.





# Der Quarantäne-Ansatz, notwendige Komponenten o. Mechanismen

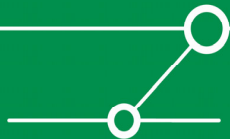


Damit ein solches Modell (Hersteller-unabhängig) funktioniert, müssten u.a. folgende Komponenten oder Mechanismen vorhanden/funktional sein:

- Server, die Informationen über Sicherheitslücken oder Viren/Würmer bereitstellen.
- Ein standardisiertes Format/Protokoll zur Übertragung solcher Informationen.
- Ein standardisiertes Format/Protokoll zur Bestimmung des Security Levels (QA <-> QS).
- Eine standardisierte *Security Policy Definition Language*.
- OS-Support für den QA, insbesondere auch für mobile Endgeräte.
- Ein Kommunikations-Mechanismus zwischen QS und PE.

Alle dies ist (noch) nicht in standardisierter Form vorhanden.

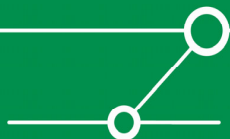
=> zur Zeit existieren nur Hersteller-proprietäre Implementierung des Quarantäne-Modells.



# Fazit



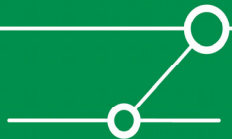
- Das klassische Firewall-Modell kann die Sicherheits-Anforderungen moderner Netze nicht erfüllen.
- Eines der wichtigsten Prinzipien zur Gewährleistung adäquater Netzwerk-Sicherheit ist die Segmentierung von Netzen.
- Diese Segmentierung kann anhand von Risiko-Analysen oder organisatorischen Strukturen/Anforderungen stattfinden und administrativ umgesetzt werden.
- Sie kann aber auch dynamisch anhand von Konfigurationsinformationen von Netzwerk-Knoten erfolgen. Dies geschieht im Rahmen des *Quarantäne-Modells*.
- Ein solches Modell könnte geeignet sein, eine Reihe aktueller Probleme zu lösen.
- Zur Zeit existieren jedoch nur erste theoretische Konzepte und Hersteller-proprietäre Implementierungen.



**Fragen?**



**Danke für Ihre Aufmerksamkeit!**



# Quellen



- [1] *Quarantine Model Overview for IPv6 Network Security*:  
<http://community.roxen.com/developers/idoocs/drafts/draft-kondo-quarantine-overview-01.html>
  
- Allgemeiner Literaturhinweis zu Angriffstechniken:  
Dominick Baier/Enno Rey/Michael Thumann: Pen-Tests – Durch Risiko-Abschätzung IT-Sicherheit optimieren [Vieweg-Verlag, ISBN 3528058390].

