Ein generisches IDS/IPS

Am Beispiel des
Münchner Wissenschaftsnetz

- Ullrich Kresse -

Einführung

- Motivation
- Münchner Wissenschaftsnetz (MWN)
- Probleme und Ursachen
- Lösung
- Problemdiskussion

Motivation

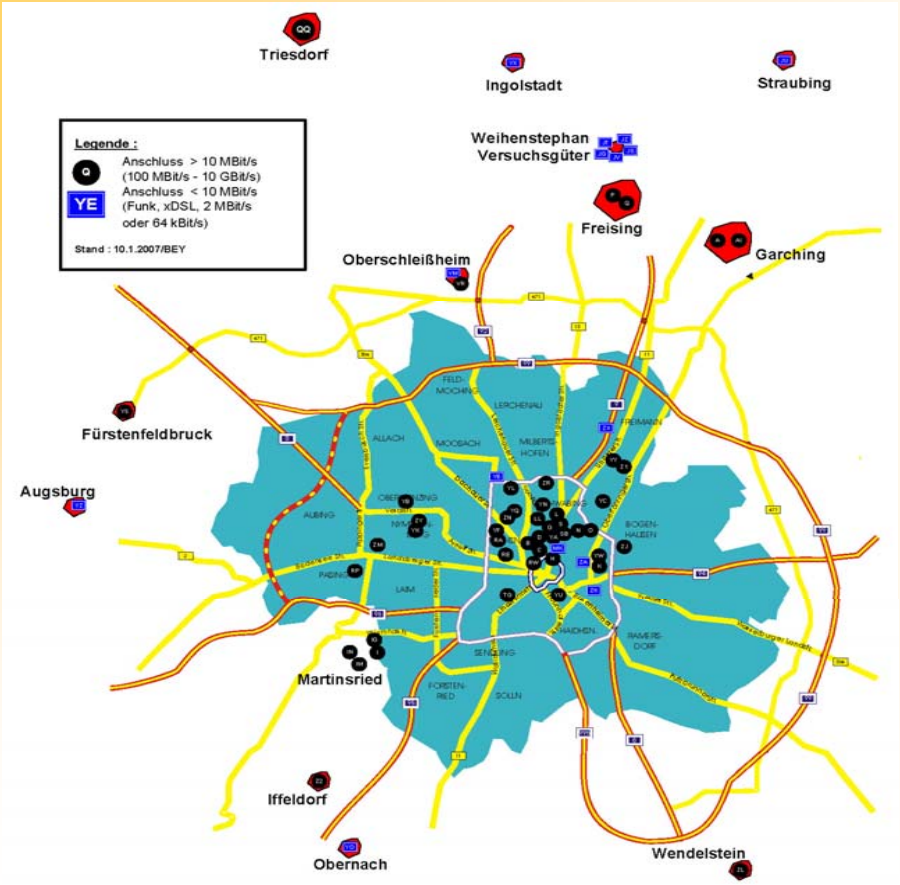
- Direkte Kontrolle der Nutzer im großen LAN möglich?
- „So viel Kontrolle wie möglich, so wenig Eingriffe wie nötig.“
- Schutz vor kompromittierten Hosts
- Intrusion Detection und Prevention

→ Am Beispiel des MWN

Kennziffern des MWN

- 60 Gebäudeareale mit <440 Gebäuden
- <55.000 Arbeitsplatzrechner (ca. 5% als Server)
- <120.000 registrierte Benutzer
- <2.000.000 Mails (inkl. SPAM)
- 7 TByte Backuptransfers innerhalb MWN

Struktur des MWN



Nutzungsbedingungen des MWN

- direkte Useridentifikation durch Registrierung
  - Einzelne Rechner oder Sub-Netze mit einem Verantwortlichen
- Keine eigenen Subnetze (NAT) erlaubt
- Kein File-Sharing

Ursachen für Probleme im MWN

- Infektion einzelner Systeme
- Übernahme der Hosts durch Malware
- Ausgehende Aktivitäten von Hosts

Auswirkungen

- Auslastung der Netze
  - Paketverzögerung
  - Überlastung der Infrastruktur
  - Überlastung von angebotenen Diensten (Backup, E-Mail, Web-Server…)

Strategien

- Lokale Kontrolle durch Virenscanner und Firewalls
- Routerfilter (Port- und Adresssperrung)
- Zentrale Kontrollinstanz
  - Analyse des Datenverkehrs
  - Beeinflussung der Bandbreite
  - Einschränkungen der Hosts

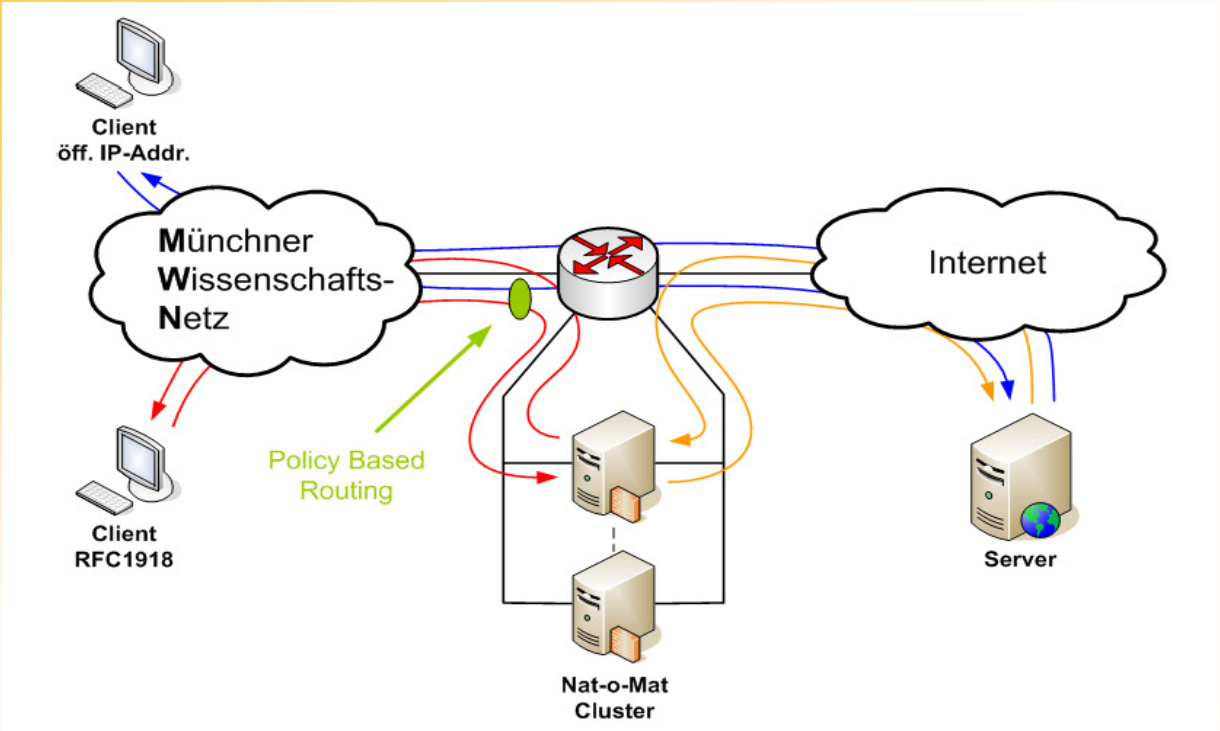
Das Sicherheitssystem im MWN
- das Nat-O-Mat -

- Idee
- Struktur
- Sicherheitskonzept

Idee

- Kontrolle des Netzverkehrs
- Automatisierung statt manuellem Eingreifen
- Schutz der Infrastruktur
- Intrusion Detection/ Prevention

Struktur


Client
öff. IP-Addr.
Münchner
Wissenschafts-
Netz
Internet
Client
RFC1918
Policy Based
Routing
Server
Nat-o-Mat
Cluster

Analyse des Datenverkehrs

- Statisch
  - Anzahl der Kommunikationspartner
  - Paketrate und Bandbreite
- Signatur
  - Bitmuster in Paketen

Sicherheitskonzept

- protokollabhängige Beschränkungen
- Stufenbasierte Einschränkung der Benutzer/ Hosts
- Punktekonto und „sanfte Sperrung“

Effekte durch Nat-O-Mat

- Intern-Extern-Kommunikation wird untersucht
  - Paketverzögerung
  - Beschränkung der Bandbreite / Unterbindung

Punktesystem

- Abweichungen vom Normverhalten belasten Konto
- Normverhalten als parametrisierte Erfahrungswerte aus vorausgegangenen Untersuchungen (Eingewöhnungsphase)

Eskalationsstufen

- Stufe 1: kurzzeitige Abweichung
  → Keine Beschränkung
- Stufe 2: längere Abweichung von Burst-Bedingung bis zum Soft-Limit
  → Verwerfen der Pakete, Strafpunkte

Eskalationsstufen

- Stufe 3: Überschreitung des Hard-Limits
  → Sperrung, http-requests werden umgeleitet
- Stufe 4: organisatorische Eskalation

Informationsmanagement

- Benachrichtigung der User

Status Report for 129.187.47.34 (gesperrt/blocked)

Überschreitungen Number of hits	Protokoll Protocol	Zielport und Grund der Sperrung Destination port and suspension reason
105	ICMP	Zu viele Pings
63	TCP	25 SMTP, Versenden von zu vielen Spam- oder Virenmails
33	TCP	6600-6699 WinM / Napster Filesharing
21	TCP	53 DNS, Zu viele DNS Anfragen

Technische Realisierung

- Komponenten:
  - Parallele Rechnersysteme mit heartbeat
  - Netfilter/ iptables
  - Bro
  - RRDTools

Zusammenfassung

- übergeordnete Instanz zur Aktivitätskontrolle
- verbesserter Schutz des Netzes vor Eingriffen
- geringer manueller Aufwand durch Automatisierung
- Nat-O-Mat als IPS/IDS

Problemdiskussion

- Wirkungsbereich
- Ausfallsicherheit des Systems
- Benutzerakzeptanz
- Qualität der Parameter

Ende

Vielen Dank für Ihre Aufmerksamkeit ☺