Bot-Netz ohne Fritz – Ein Frühwarn- und Abwehrsystem für ISPs basierend auf in DSL-Routern platzierten Sensoren

Björn Stelte und Robert Koch

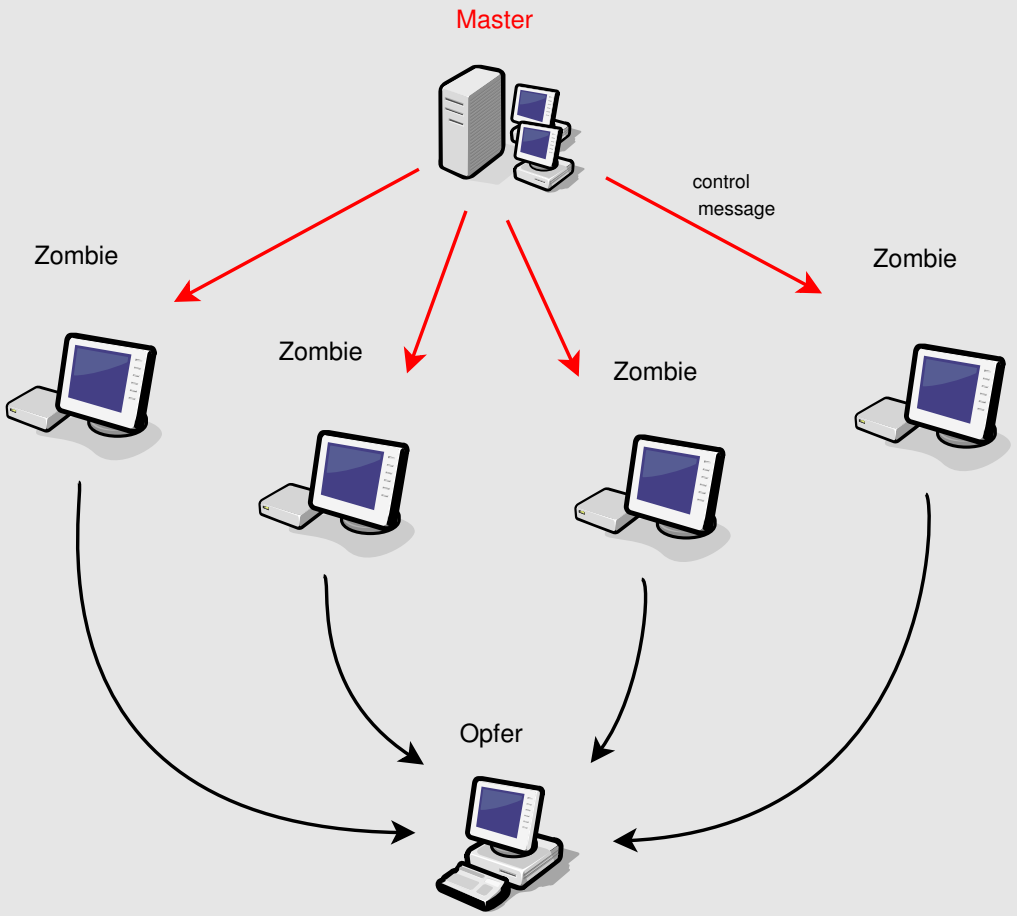
Fakultät für Informatik
Institut für Technische Informatik
der Bundeswehr Universität München

15.2.2011

Outline

Bot-Netz

Schemata eines aktiven DDoS Angriffs



Motivation

Definition

Botnetze sind Netzwerke aus COMPUTERN, die nach der **Infektion mit Schadsoftware** zusammengeschlossen werden. Ist Ihr Computer Teil eines Botnetzes, kann er unbemerkt auf **ferngesteuerte** Befehle von Cyberkriminellen reagieren und zum Beispiel Spam versenden oder andere Computer infizieren, wenn Sie online sind.[a]

[a] Quelle: Anti-Botnet Beratungszentrum

Motivation

Wie detektieren?

Und im Gegensatz zu analogen Internetverbindungen fällt bei DSL-Anschlüssen kaum auf, ob der Computer HEIMLICH DINGE MACHT, weil die Verbindungsgeschwindigkeit nicht merklich langsamer wird.
Studien zufolge werden pro Tag weltweit mehrere Tausend neue Computer gekapert und für fremde Zwecke missbraucht.[a]

[a] Quelle: BSI für Bürger Portal

Gegenmaßnahmen

Gegenmaßnahmen

- verstärkte Kooperation zwischen Providern, CERTs und IT-Sicherheitsexperten
- Maßnahmen zur Aufklärung und Sensibilisierung der Privatanwender
  - auf Dektop-PCs werden Firewalls immer konsequenter eingesetzt
  - Virenscanner sind quasi Standard geworden
  - Updates werden auf PCs (regelmäßig) installiert
- Fokus auf **privat betriebene PCs**
- Rechnernetze/Computer in Firmen sind meist gut geschützt

Ausblick

. . . NEXT STEPS

Reicht das? Was ist ein Computer???

Auch **Netzkomponenten**, wie Router, WLAN AccessPoint, Switch, VoIP Telefon . . . sind COMPUTER!
Merkmale: 24/7 Betrieb, Updates nur selten, . . .

Angriff auf Embedded Network Devices

Untersuchung

- Studien zeigen, dass viele netzwerkfähige Geräte schlecht gesichert sind [a]
- Ports (TELNET oder SSH) sind öffentlich erreichbar
- Standard-Passwörter werden nicht geändert
- Ergebnis einer Studie (2010) [b]
  - 3,223,358,720 total IPs untersucht
  - 3,912,574 identifizierte Geräte
  - 540,435 angreifbare Geräte (13.81%)

---

[a] Heffner, Blackhat'10: `https://spreadsheets.google.com/pub?key=0Aupu_01ythaUdGZINXQ5Vi16X3hXb3VPYkszNXM0YXc`

[b] Ang Cui et al.:'A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan', ACSAS'10, Dez 2010.

Ergebnis der Studie: Problem Alternative Firmware (OpenWRT,. . .)

Land	gefährdete Router
Japan	75%
Kanada	60%
Indien	57%
Korea	57%
Ungarn	54%
Australien	50%
Niederlande	48%
USA	38%
Frankreich	34%

Tabelle: Prozentual angreifbare Router der Firma LinkSys im Internet, Untersuchung von Ang Cui et al. RAID 2009 Konferenz

Angriff auf DSL-Router: Provider Firmware

Psyb0t

- Angriff auf NetComm NB5 Router (SSH Port)
- Device Provisioning (Nutzer konfiguriert selber nichts)
- psyb0t ist der erste bekannte Wurm (Bot-Client)
- wurde von DroneBL analysiert
  - attack shell scripts - brute force
  - 30 unterschiedliche LinkSys Modelle
  - 10 Netgear Modelle
  - einige mehr
  - Liste mit 6000 Usernames und 13000 Passwörtern

Angriff auf DSL-Router

Psyb0t

- kein Anti-Virus Programm auf dem Router verfügbar
- Möglichkeiten der Detektion
  - Beobachtung des Datenverkehrs (in/out)
  - verdächtige Nachrichten nur auf dem WAN abgreifbar
  - Nutzer bemerkt (leicht) reduzierte Datenrate
  - IT-Forensik

Weiterführende Literatur

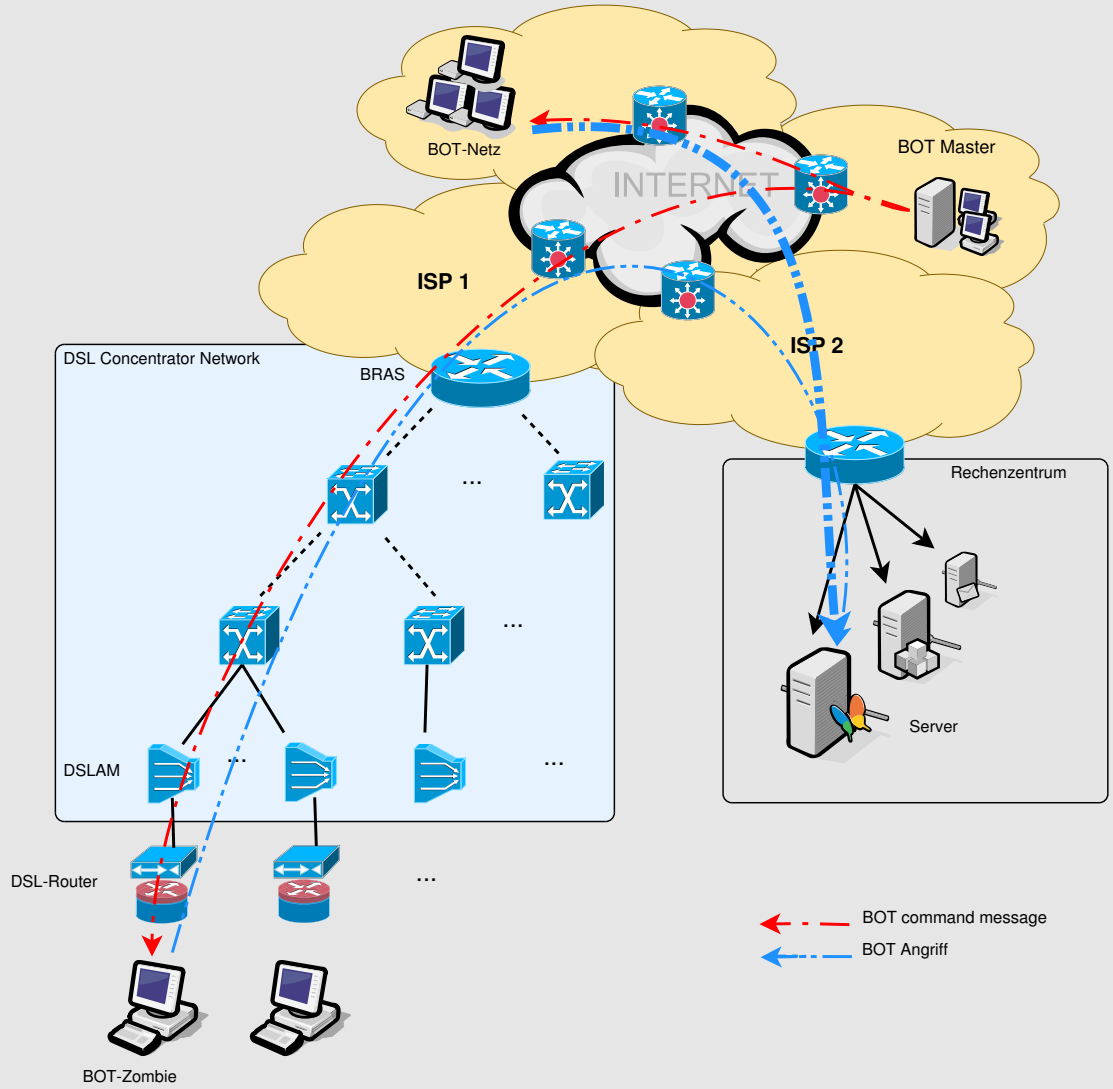
Emmanouil Karamanos: “Investigation of home router security”, KTH, Schweden 2010

Angriff auf DSL-Router II

Angriff auf geschützte DSL-Router

- “vernünftige” DSL-Router haben keine offenen Ports (WAN)
- Angriff auf die Managment-Webseite des Routers dennoch möglich (`http://router.ip`)
  - Cross-Site Request Forgery (CSRF) Angriff
  - Cross-Site Scripting (XSS) Angriff
  - UPnP Protokoll (wenn über WAN errreichbar)
  - SNMP (trap handling)
- Craig Haffner, Blackhat’10: **DNS Rebinding**

Pfad eines DDoS Angriffs in einer DSL Umgebung



Gefahrenpotential DSL-Router

- Betriebssysteme, wie Linux, VxWorks, ...
- 24/7 Betrieb
- Knotenpunkt, Internet-Datenverkehr des Nutzers kontrollierbar
- kein Viren-Scanner, Malware-Scanner, etc.
- Geräte sind nicht Tamper-Resistent, kein hardend OS (bspw. SELinux)
- **fehlendes Sicherheitsbewusstsein**, Geräte werden nicht als Computer angesehen
- Fazit: Angriffe sind möglich und werden zunehmen

Idee

- Absichern des DSL-Routers (SELinux)
- Integritätstest (Software-based Firmware Attestation)
- Bot-Client hinter dem Router (internes Netz)
  - Verbindungsdaten auf dem Router sammeln
  - in Traffic-Klassen einteilen
  - anhand von verschiedener Faktoren erfolgt Gewichtung
- Zentraler Instanz (ISP) melden – dort wird bewertet und Lagebild erstellt – bessere Abwehr von DDoS
- verteilte Sensorik vor dem DSL-Konzentratornetz
- **Sensorik auf dem Router platzieren!**

Konzept Sensorik

Datensammlung: Was ist möglich?

- Routen-Tabelle (/PROC/NET/ROUTE)
- ARP-Tabelle (/PROC/NET/ARP)
- IP-Verbindungsinformationen (/SYS/CLASS/NET/...)
- Hauptspeicherinhalt (/PROC/KCORE)
- Informationen zu geladenen Kernelmodulen
- allgemein das /PROC Verzeichnis
- `http://fritz.box/cgi-bin/webcm?getpage=../html/capture.html`
- ...[a]

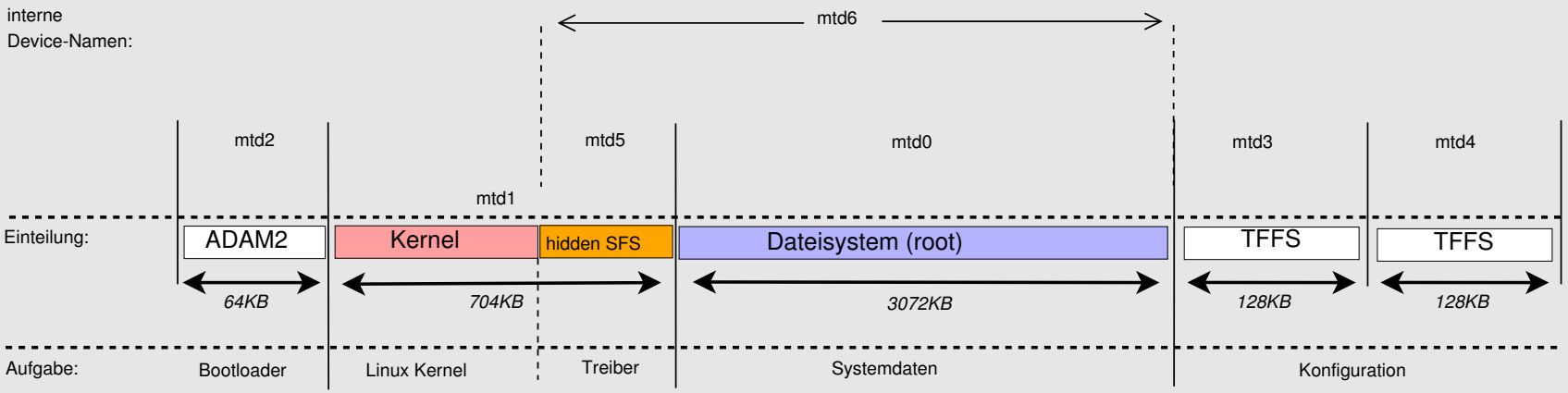
[a] weiterführende Informationen: BSI Leifaden IT-Forensik, 2010

Umsetzung

Konzept Sensor

- nur begrenzte Ressourcen auf dem Router
- daher minimaler Ressourcenbedarf gefordert
- autarke Funktionalität
- keine Einschränkung der gewohnten Nutzung und Wartungsfreiheit ohne erforderliche Nutzeraktion

Typischer Aufbau einer AVM FritzBox



Kriterien Sensor

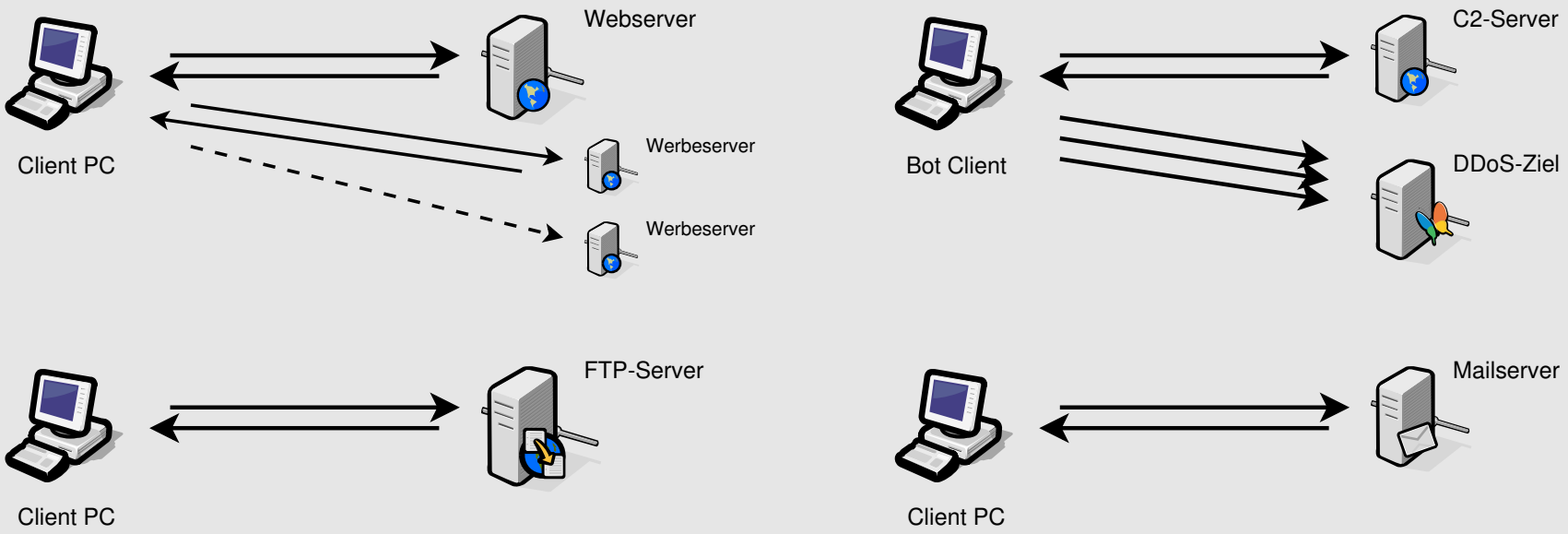
Es werden folgende Attribute vom Sensor aufgezeichnet:

- Anzahl der Verbindungen zu einer Ziel-IP
- Übertragene Datenmenge zu einer Adresse
- Empfangene Datenmenge von einer Adresse
- Dauer der Verbindungen

Mögliche Bot-Client Aktivitäten erkennen.

Schematischer Ablauf der Kommunikation

Die Anzahl von aufgebauten Verbindungen sowie die Datenmengen und Transportrichtungen können Aufschluss über das Vorhandensein unerwünschter Kommunikation geben.



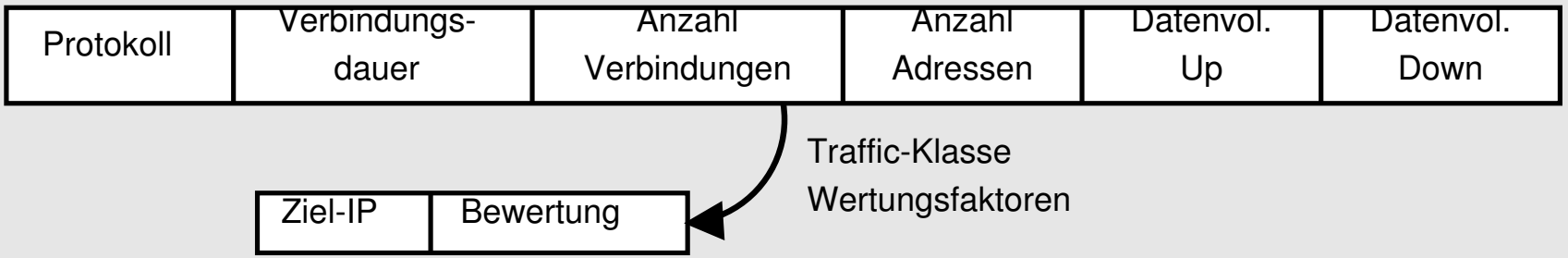
Anhand verschiedener Faktoren erfolgt die weitere Gewichtung:

- Uplink- zu Downlink- Verhältnis (Datenmenge)
- Anzahl Verbindungen und Verbindungsdauer zu Anzahl versch. IP-Adressen
- Verhältnis übertragene Datenmengen zur durchschnittlichen Datenmenge des Routers
- Kommunikationsbeziehungen (einseitig, etc.)

Umsetzung

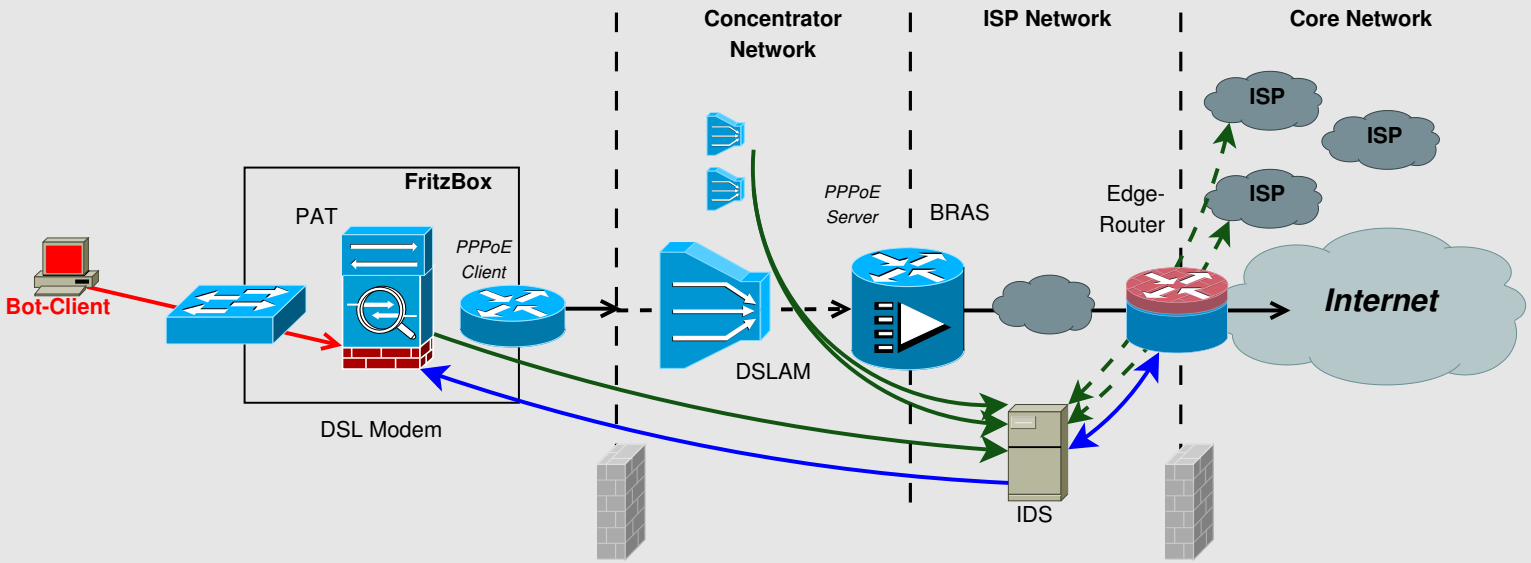
Auswertung des Datenverkehrs auf dem Router

Für jede Verbindung wird ein Datagramm mit Ziel-Adresse und einem Bewertungsfaktor erzeugt.
Je höher der Wert, desto wahrscheinlicher handelt es sich um eine unerwünschte Verbindung.



Mögliche Architektur des IDS zur Detektion von Bot-Aktivitäten.

- Sensorik ist bei den Endkunden in den DSL-Routern installiert
- Minimale Auswertungsdaten werden zur zentralen Auswertung an den IDS/EWS-Server beim ISP übermittelt.
- IDS sammelt Informationen sämtlicher Teilnehmer und kann bei der Detektion eines Angriffes entsprechend reagieren.
- Konfiguration der eigenen Firewall oder des Routers anpassen.



Zusammenfassung

- Netzwerkfähige Embedded Devices sind als Computer anzusehen.
- Sicherheitsbewusstsein der Nutzer muss hier geschärft werden.
- Es ist mit bekannten Technologien möglich diese Geräte zu sichern.
- . . . wir sollten ein Schritt weitergehen und Sensorik in die Router mit einbauen.
- **Idee:** Vorbewertung auf dem Router, Verbesserung der Detektion beim Provider.
- **Ziel:** Early Warning System beim Provider mit feedback Möglichkeit zum Kunden.

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:

Dipl.-Inf. Björn Stelte
Fakultät für Informatik
Institut für Technische Informatik
Universität der Bundeswehr München
BJOERN.STELTE@UNIBW.DE

der Bundeswehr Universität München