Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

- Vorlesung -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- Idee eines EWS
- Aufbau eines EWS
- Sensoren
- Analysekonzepte
- Zusammenfassung

→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Angriffspotentiale
- Idee eines EWS
- Aufbau eines EWS
- Sensoren
- Analysekonzepte
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung

→ Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

- Gutes Verständnis für mögliche **Angriffspotentiale** und Maßnahmen zum Entgegenwirken.
- Erlangen der Kenntnisse über die **Idee**, den **Aufbau** und den **Prozessen** von Cyber-Sicherheit-Frühwarn- und Lagebildsystemen.
- Gewinn von praktischen Erfahrungen durch die Analyse von konkreten **Sensoren**.

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Angriffspotentiale**
- Idee eines EWS
- Aufbau eines EWS
- Sensoren
- Analysekonzepte
- Zusammenfassung

Angriffspotentiale
→ Einleitung (1/2)

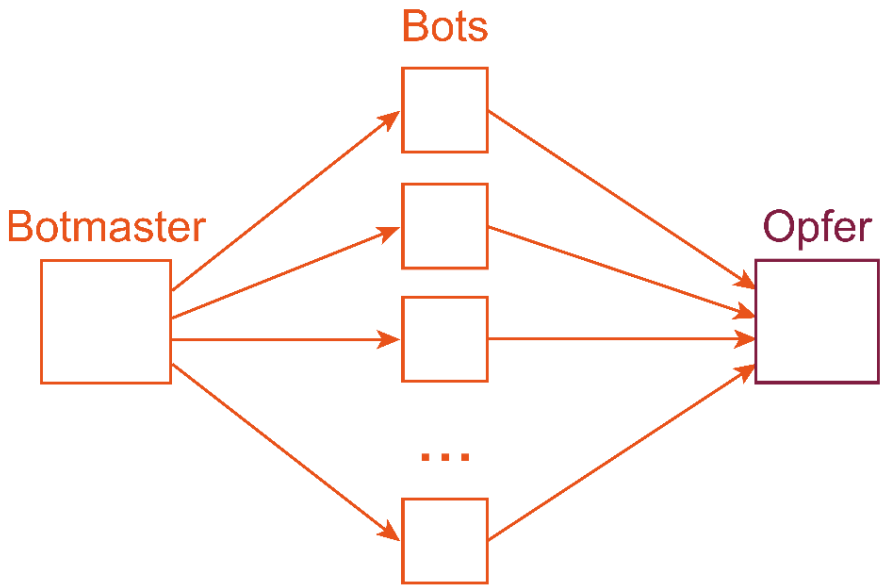
- Alle Organisationen sind zunehmend von der Verfügbarkeit der eigenen und öffentlichen IT-Infrastruktur abhängig.
- Ausfälle und Störungen können zu unkalkulierbaren Schäden führen.
- Hilfe durch: **Cyber-Sicherheit-Frühwarn- und Lagebildsysteme** (im englischen „Early Warning Systems“, kurz EWS).
- **Wichtigste Eigenschaften:**
  - Aktuelle **Cyber-Sicherheitslage** aufzeigen.
  - **Angriffspotentiale** und **reale Angriffe** (möglichst früh) erkennen.
  - Rechtzeitig **Warnhinweise** geben.
  - **Minimierung** oder **Verhinderung** von Schäden.

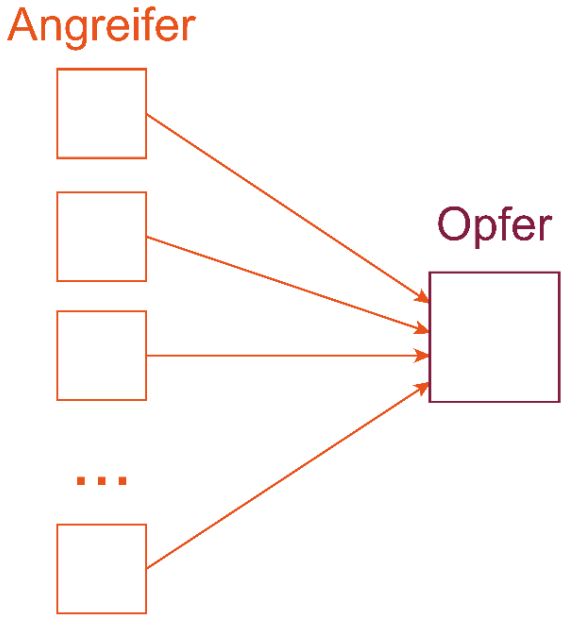
Angriffspotentiale
→ Einleitung (2/2)

- Ein Angriff ist ein Versuch,
  - einen Wert zu stehlen,
  - zu verändern,
  - zu löschen oder
  - sich unbefugten Zugriff auf ein IT-System und deren Ressourcen zu verschaffen.

- Mögliche Kriterien für die Unterscheidung von Angriffen:
  - Anzahl Angreifer
  - Anzahl Opfer
  - Kommunikationsstruktur

Durchführung von Angriffen
→ **M:1-Angriff** (M Angreifer und ein Opfer)



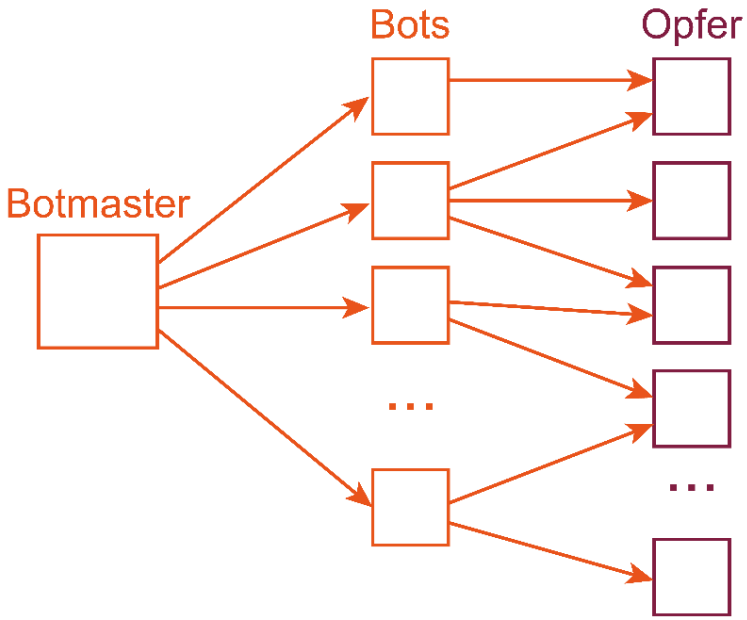


- **M:1-Angriff mit Hilfe eines Botnetzes:**
  - Bots ≙ kompromittierte IT-Systeme mit Malware.
  - Teil eines Botnetzes.
  - Gesteuert von einem Botmaster.

- **M:1-Angriff – Aktivisten**

- **Ausprägung:** Distributed Denial of Service (DDoS)

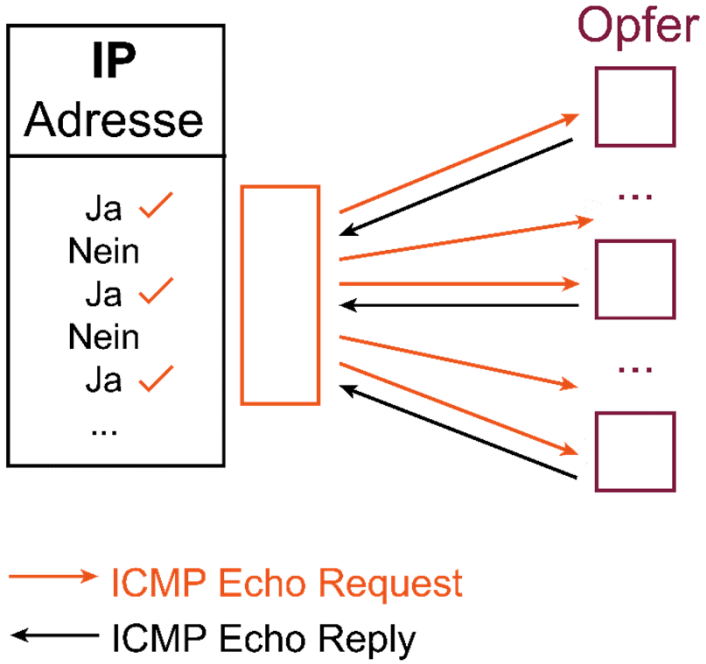
Durchführung von Angriffen
→ **M:N-Angriff** (M Angreifer und N Opfer)



- **Ausprägungen:**
  - Spam-E-Mails
  - Click Fraud

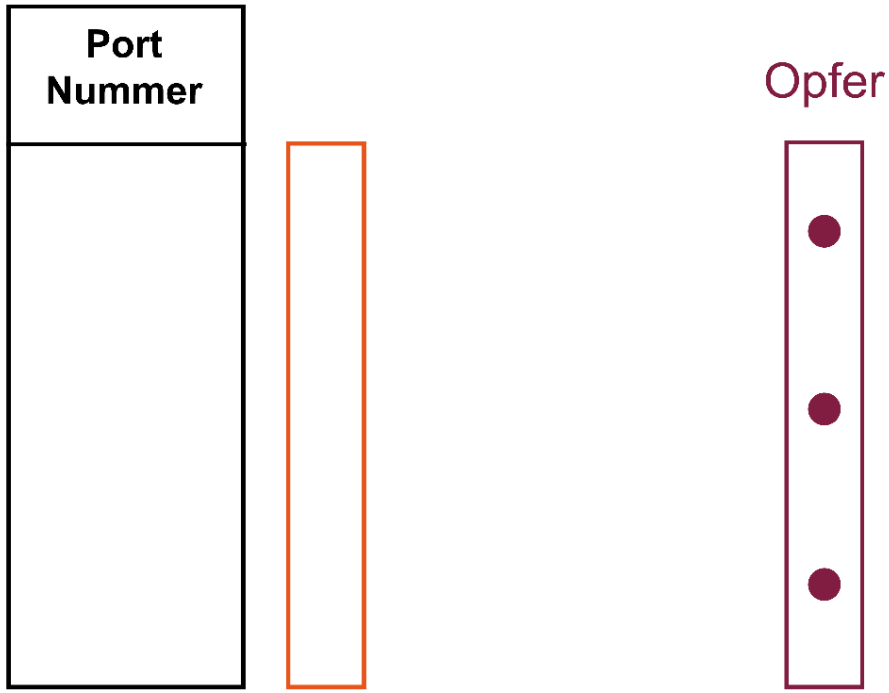
Durchführung von Angriffen
→ 1:N-Angriff (1/4) - (1 Angreifer und N Opfer)

- **Vorbereitung von gezielten Angriffen**
- **Ping Scan:**
  - Erreichbarkeit von IT-Systemen prüfen.
  - ICMP Protokoll auf Netzwerkebene.



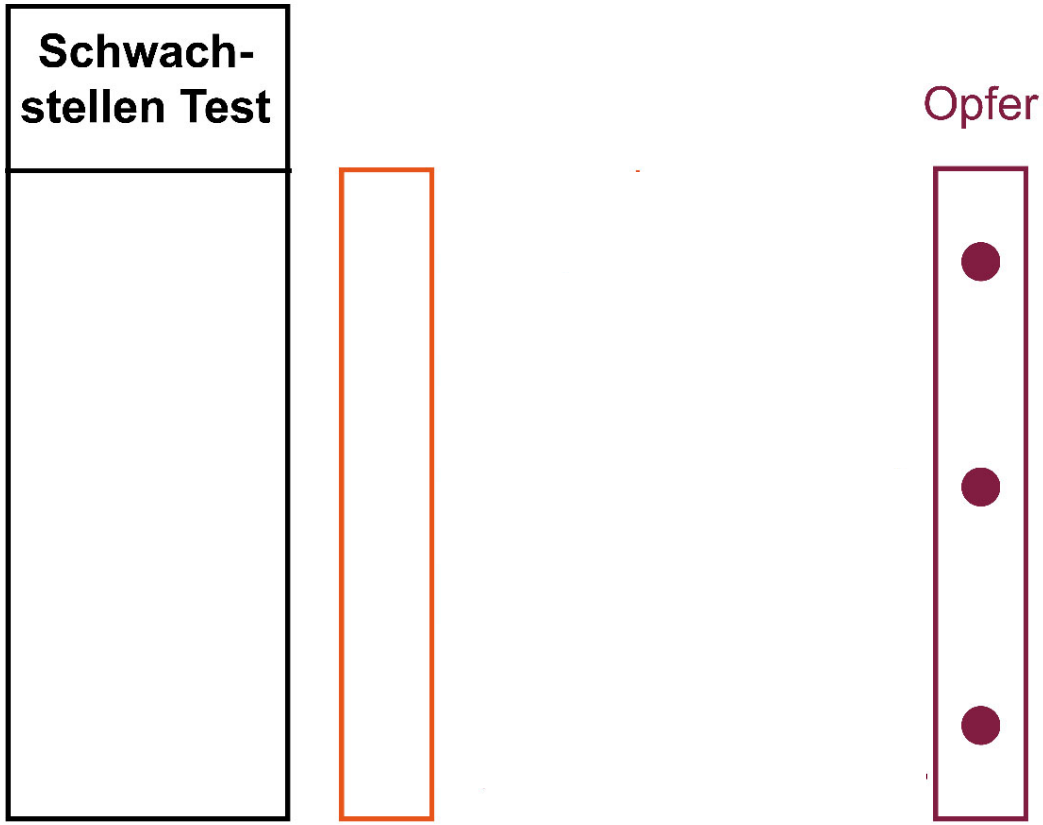
Durchführung von Angriffen
→ 1:N-Angriff (2/4) - (1 Angreifer und N Opfer)

- **Port Scan:**
  - Angebotene Anwendungsdienste prüfen (z.B. Webserver, E-Mail-Server, SIP-Server usw.).
  - Verbindungsversuch mittels SYN-Flag eines TCP-Paketes auf Transportebene (TCP-SYN-Scan).



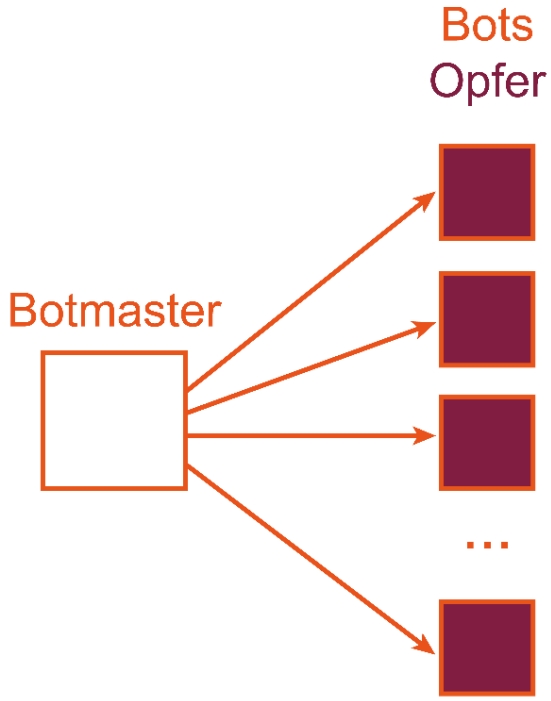
Durchführung von Angriffen
→ 1:N-Angriff (3/4) - (1 Angreifer und N Opfer)

- **Vulnerability Scan:**
  - Ausnutzbarkeit von **aktuellen**, **öffentlich bekannten** und **nicht gepatchten** Sicherheitslücken auf Anwendungsebene prüfen.



Durchführung von Angriffen
→ 1:N-Angriff (4/4) - (1 Angreifer und N Opfer)

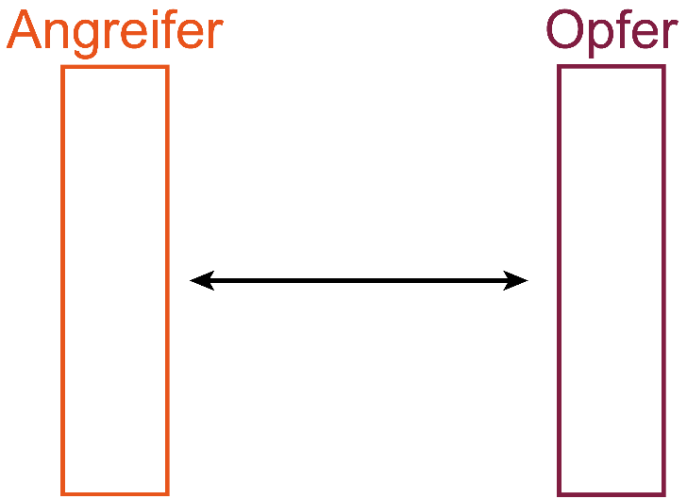
- **1:N-Angriff auf mit Malware kompromittierte IT-Systeme**
  - **Ransom-Ware:**
    - ***Verschlüsselung*** von Daten.
    - Erpressung von ***Lösegeld.***
  - **Keylogger:**
    - ***Tastatureingaben mitlesen***.
    - Speicherung in Drop Zones.
  - **Trojanisches Pferd:**
    - ***Zugriff auf die Werte*** des IT-Systems.
    - Einschleusen von weiteren Schadfunktionen.
  - **Adware:**
    - ***Unerwünschte Werbung***.
    - Profilbildung durch Werbeagenturen.



Durchführung von Angriffen
→ 1:1-Angriff - (1 Angreifer und 1 Opfer)

- **Advanced Persistent Threat (APT):**
  - Professionelle Hacker.
  - Komplexe Angriffsmethoden.
  - Viele Ressourcen (z.B. Geld, Zeit, leistungsstarke IT-Systeme, Unbekannte Softwareschwachstellen, Hacking Tools, …).
  - Große Angriffsziele (z.B. Regierungen, Kritische Infrastrukturen, Unternehmensleitung, …).

- **Social Engineering** (Vorbereitung)**:**
  - Spear-Phishing (Zielgerichtet).
  - Whaling (Führungskräfte).



Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- **Idee eines EWS**
- Aufbau eines EWS
- Sensoren
- Analysekonzepte
- Zusammenfassung

Idee eines EWS
→ Definition

„Basierend auf verlässlichen Ergebnissen und Resultaten über **Angriffspotentiale** oder bereits eingetretener **Cyber-Sicherheitsvorfälle**, die jedoch vorerst nur wenige IT-Infrastrukturen betreffen, wird ein **Cyber-Sicherheitslagebild** kontinuierlich aktualisiert, und beim Eintreten eines adäquaten und relevanten Vorfalls wird eine qualifizierte **Warnung** an potentiell **Betroffene** verbreitet, um deren voraussichtlichen **Schaden** zu **verringern** oder ganz zu **vermeiden**.“

Idee eines EWS
→ Funktionale Anforderungen (1/3)

- **Zeitpunkt:**
  - Bevor konkreter Schaden eingetreten ist.
  - Früh genug, um potentielle Schäden zu minimieren.
  - Erkennung von bereits bekannten und unbekannten Angriffen.

- **Entscheidungsprozess:**
  - Unterstützung durch Analysetools und Ergebnisvisualisierungen.
  - Einsatz von Expertensystemen.

Idee eines EWS
→ Funktionale Anforderungen (2/3)

- **Forensik:**
  - Sicherstellung von Beweismitteln für rechtliche Maßnahmen.
- **Statusinformationen:**
  - Entwicklung des Kommunikationsverkehrs beobachten.
  - Treffen von Technologieentscheidungen.
- **Cyber-Sicherheitslage:**
  - Übersicht über alle sicherheitsrelevanten Ereignisse.
  - Kontinuierliche Aktualisierung.
  - Nutzung geeigneter Visualisierungen.

Idee eines EWS
→ Funktionale Anforderungen (3/3)

- **Effektivität:**
  - Stabilität
  - Sicherheit des EWS.
  - Datenschutz
  - Wartbarkeit
  - Performanz

Idee eines EWS
→ Herausforderungen

- **Reaktionszeit:**
  - Prinzipiell gibt es nur sehr wenig Zeit für eine Frühwarnung vor einem **konkreten Angriff**.
  - Automatisierte Scans können schnell ausgeführt oder über einen größeren Zeitraum verschleiert werden.
  - Kollaborative Frühwarnsysteme können effektiver warnen.

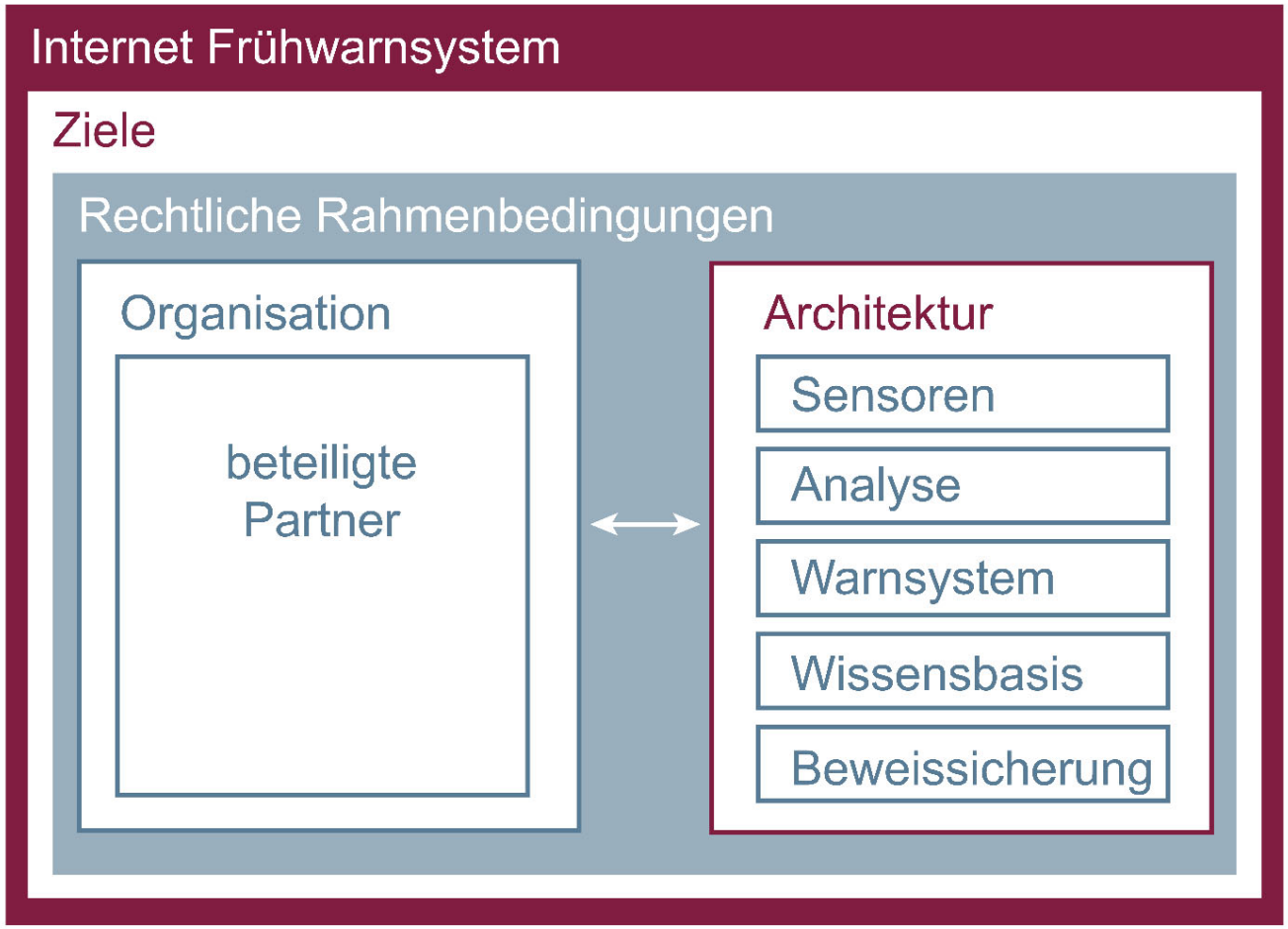
- **Asymmetrische Bedrohungen:**
  - Viele Angriffe werden **global** durchgeführt.
  - Gegenmaßnahmen werden derzeit nur **lokal** initiiert.
  - **Alle Beteiligten** müssen jedoch aktiv werden!
  - Der Gesamtaufwand multipliziert sich mit der Anzahl der betroffenen IT-Systeme und IT-Infrastrukturen.

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- Idee eines EWS
- **Aufbau eines EWS**
- Sensoren
- Analysekonzepte
- Zusammenfassung

Aufbau eines EWS
→ Modell



Aufbau eines EWS
→ Rechtlichen Rahmenbedingungen

- Rechtliche Rahmenbedingungen können sowohl einschränkend, als auch fordernd für EWS sein.
  - Datenschutz
  - Vertragsrecht
  - IT-Sicherheitsgesetze
  - Schutz von kritischen Infrastrukturen

- Rahmenbedingungen variieren von Land zu Land.

Aufbau eines EWS
→ Beteiligte Organisationen

- **Aktive Rolle (Aufbau und Betrieb des EWS):**
  - Bereitstellung von Sensoren.
  - Operativer Betrieb eines Lagezentrums.
  - Erstellung von Gegenmaßnahmen.
  - Strukturanalyse (Geschäftsprozesse, Verantwortlichkeiten, Daten, Infrastruktur, …).
  - Festlegung von Handlungsprozessen.

- **Passive Rolle (Anwender des EWS):**
  - Privatnutzer oder kleine Organisationen.

Aufbau eines EWS
→ Architektur (1/3)

- **Realisierung der technischen Komponenten unter den Voraussetzungen:**
  - Zuverlässigkeit
  - Wartbarkeit
  - Komplexität
  - Leistung
  - Datenschutz
  - Vertraulichkeit

Aufbau eines EWS
→ Architektur (2/3)

- **Zentralisierte Architektur:**
  - Alle Komponenten befinden sich in einer zentralen Betriebseinheit.
  - ***Vorteile:***
    - Einfache Wartbarkeit
    - Begrenzte Komplexität
  - ***Nachteile:***
    - könnte zu Leistungsproblemen führen
    - zentralisierte Systeme sind leichter anzugreifen, wie zum Beispiel mithilfe von DDoS-Angriffen

Aufbau eines EWS
→ Architektur (3/3)

- **Dezentrale Architektur:**
  - Alle Komponenten befinden sich in einer zentralen Betriebseinheit.
  - ***Vorteile***
    - bessere Skalierung der Leistung
    - kann nicht so leicht angegriffen zu werden
  - ***Nachteile***
    - komplexer
    - Wartbarkeit ist schwieriger

Aufbau eines EWS
→ Sensoren

- **Physikalische** oder **logische** Komponente für das **Sammeln** von Daten in einem IT-System oder einer IT-Infrastruktur.
  - Positioniert an **strategisch wichtigen Punkten**.
  - Grundlage für die Generierung des **aktuellen Status**.
  - Benötigte Anzahl hängt von den Zielen des EWS ab.

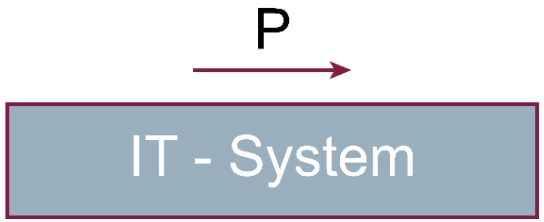
- **Rahmenbedingungen:**
  - Datenschutz
  - Forensik/Beweissicherung
  - Performanz (Zeitkritische Verarbeitung von großen Datenmengen)
  - Datengüte (z.B. Stichprobe oder Abbildung des Gesamtverkehrs)

Aufbau eines EWS
→ Analyse

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- Idee eines EWS
- Aufbau eines EWS
- **Sensoren**
- Analysekonzepte
- Zusammenfassung

Sensoren
→ Grundprinzip (1/2)



- **P: = vollständige Daten** (z.B. Kommunikationsverkehr, Anwendungsverhalten, Datenzustände, Ereignisse, ...)
- **D: = Daten, die durch den Sensor gehen** (z.B. Reduktion durch Router oder Switch)
- **Y: = Ergebnis der Verarbeitung des Sensors** (z.B. wichtige Sicherheitsrelevante Informationen - SI für ein Angriffsmuster)

Sensoren
→ Grundprinzip (2/2)

- **Qualität eines Sensors**
  Herausforderung: Den besten Sensor zu finden!

  - **Hoher Grad an Reduzierung der Bytes**
    → Speicherung von großen Datenmengen über einen langen Zeitraum.

    $$Y <<< P$$

  - **Geringe Reduzierung der SI** (Sicherheitsrelevante Informationen)
    → Erkennung von Angriffen und Angriffspotentialen.

    $$SI(Y) < SI(P)$$

  - **Optimaler Sensor**

    $$\mathbf{SI(Y) = SI(P)}$$

Sensoren
→ Idealer Sensor

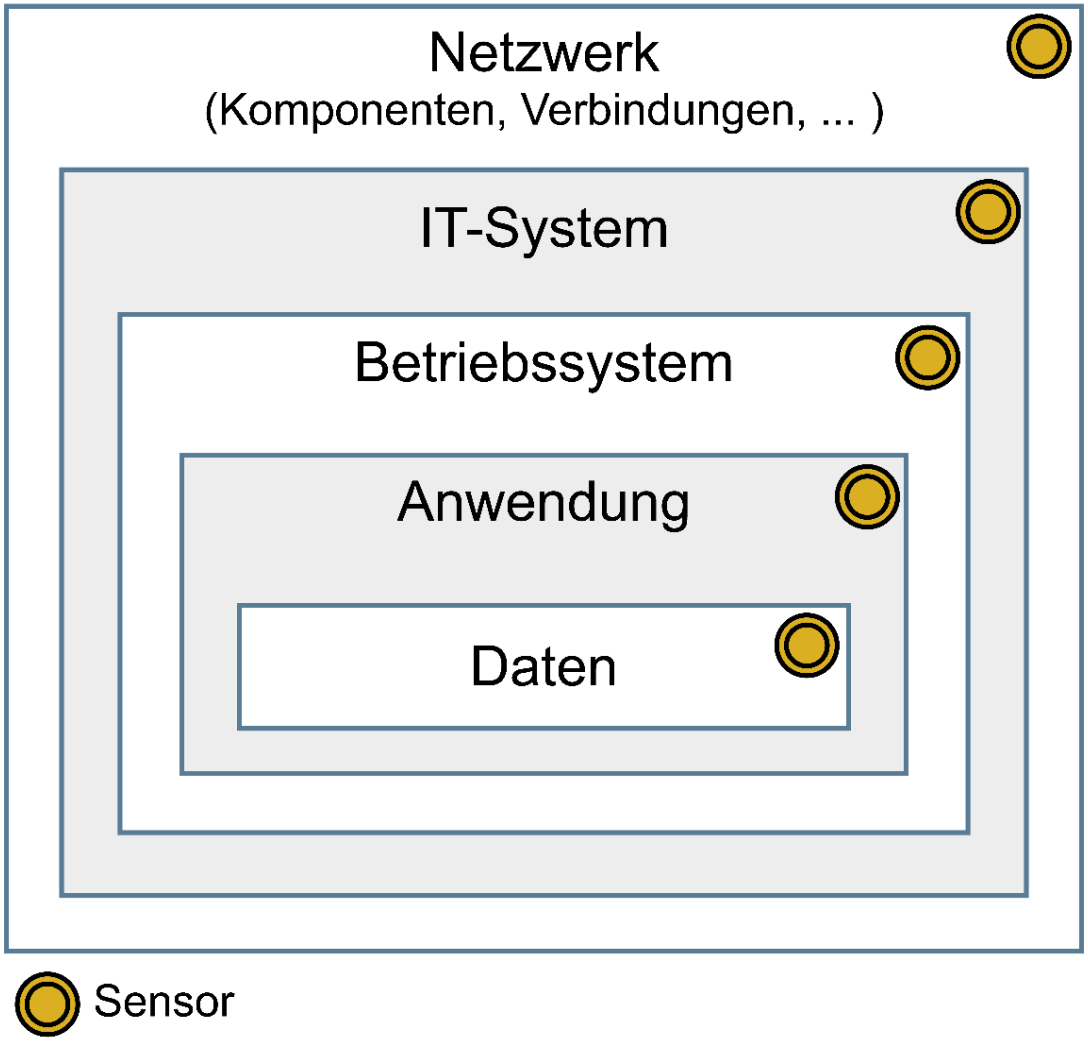
- Ein **idealer Sensor**
  - hat **Zugriff auf alle Daten** und
  - **extrahiert** daraus alle **sicherheitsrelevanten Informationen** so, dass diese für das **Erkennen aller Angriffe** und **Angriffspotentiale** genutzt und
  - von der notwendigen Speichergröße **langfristig gespeichert** werden können.

Sensoren
→ Messmethoden

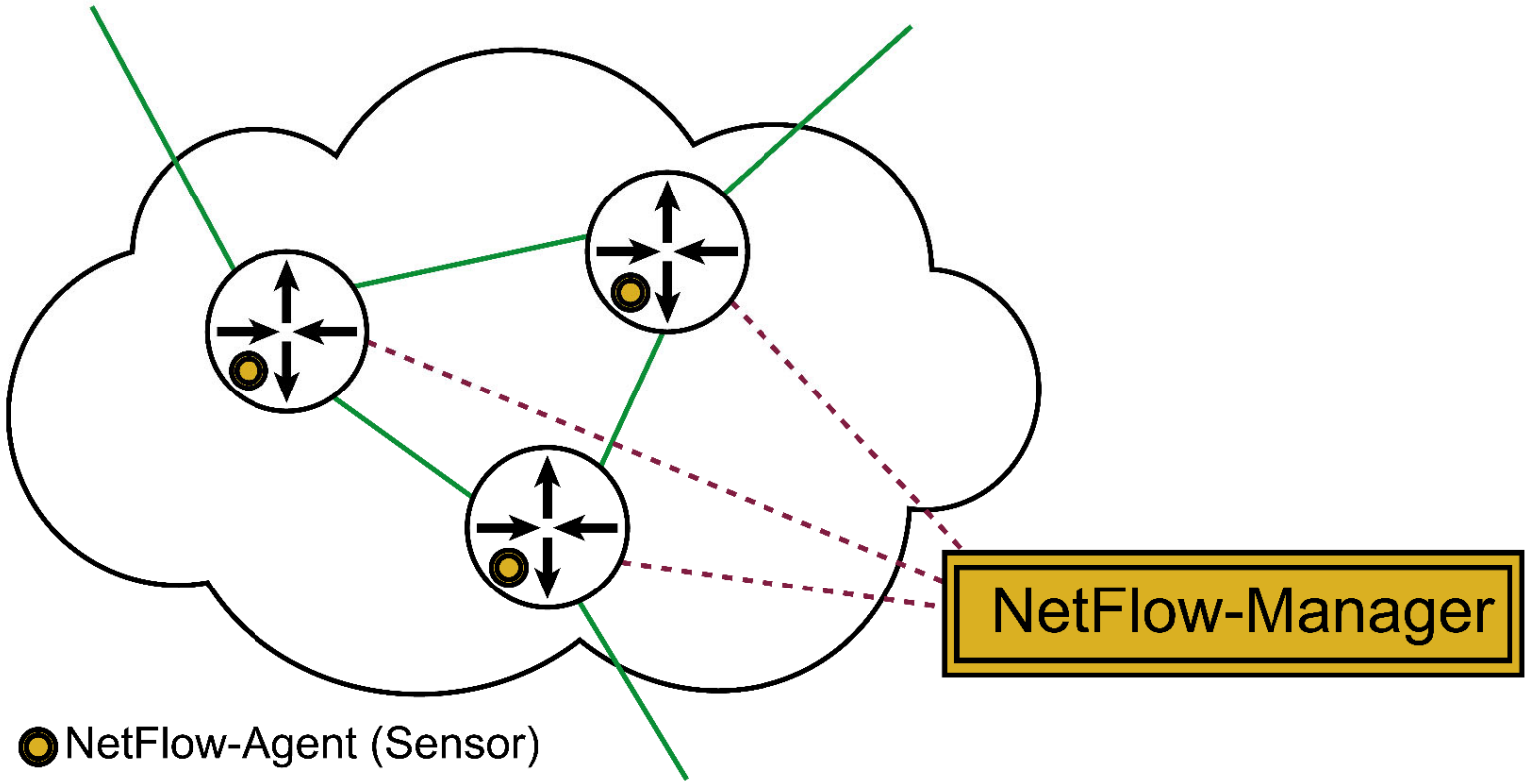
- **Aktive Messung:**
  - Erzeugung von Daten und/oder Aktionen.
  - Messung des resultierenden Verhaltens.
  - z.B. mittels Ping, Trace-Route, Ausführung von Anwendungen/Diensten, …

- **Passive Messung:**
  - Abgreifen von Daten während des Betriebes.
  - z.B. abhören von Kommunikationsleitungen, Messen von Ereignissen in einem IT-System, …

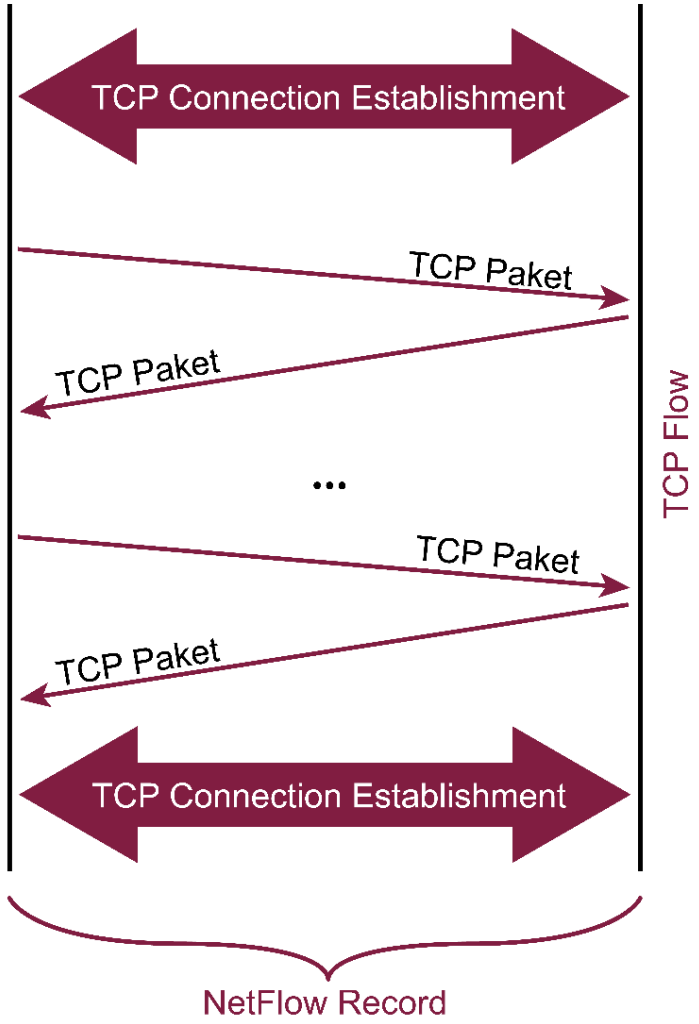
Sensoren
→ Ort der Messung



Sensoren
→ Beispiel: NetFlow-Sensor (1/4)



Sensoren
→ Beispiel: NetFlow-Sensor (2/4)



{
...
Zeitstempel,
Byte- und Paketzähler,
Quell- und Ziel-IP-Adressen,
Quell- und Ziel-IP-Ports,
TOS-Informationen,
AS-Nummern,
TCP-Flags,
Protokoll-Typ,
...
}

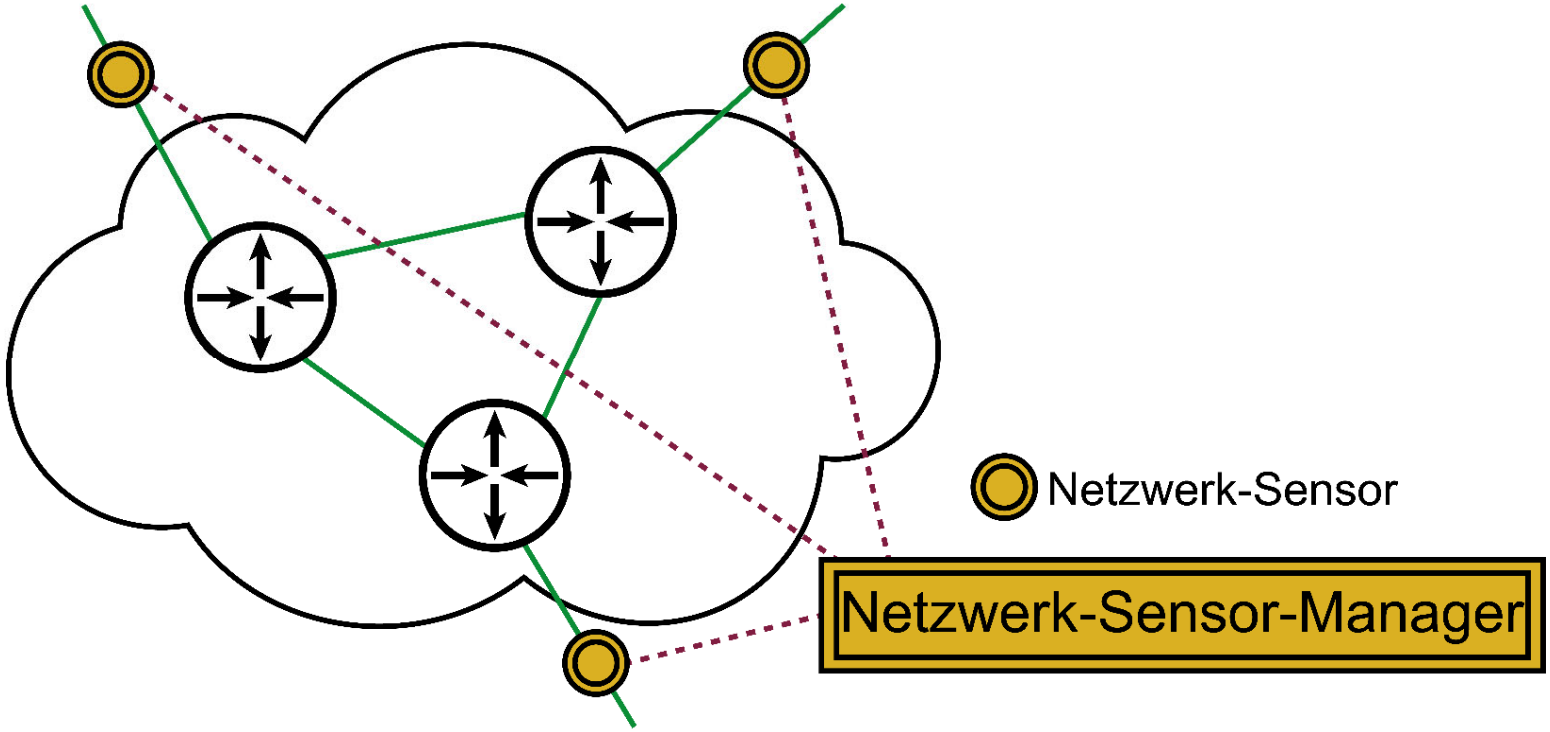
Sensoren
→ Beispiel: NetFlow-Sensor (3/4)

- **Grundprinzip:**
  - P: = alle IP-Pakete
  - D: = P
  - SI (D): = Auswahl der NetFlow-Rekords und deren Inhalt
  - Y: = NetFlow-Rekords
  - Analyse der SI findet im NetFlow-Kollektor statt.
- **Genereller Aspekt:**
  - Ursprünglich für die Abrechnung des Netzwerkverkehrs konzipiert.
- **Ort der Messung:**
  - Netzwerk, Funktion in Routern

Sensoren
→ Beispiel: NetFlow-Sensor (4/4)

- **Sicherheitsinformation:** + (wenig)
  - Wenige SI im NetFlow-Rekord enthalten.
- **Vorteile:**
  - Bereits als eine Funktion im Router verfügbar.
  - Sehr schnell und keine Probleme mit hoher Bandbreite.
- **Nachteile:**
  - Nur wenige Sicherheitsinformationen (SI) verfügbar.

Sensoren
→ Beispiel: Netzwerk-Sensor (1/4)



Sensoren
→ Beispiel: Netzwerk-Sensor (2/4)

- **Grundprinzip:**
  - P: = alle IP-Pakete
  - D: = P
  - SI (D): = **Deep Packet Inspection** (erkannte Ereignisse) oder ***Intrusion Detection*** (erkannte Signaturen) oder **statistische Ansätze** (Statistiken über Kommunikationsparameter)
  - Y: = Rohdaten/Sicherheitsereignisse
  - Analyse der SI im Sensor und/oder Analysesystem.

Sensoren
→ Beispiel: Netzwerk-Sensor (3/4)

- **Genereller Aspekt:**
  - Jedes IP-Paket kann analysiert werden.
- **Ort der Messung:**
  - Separater Sensor (Netzwerkkomponente).
  - Integriert in Netzwerkkomponenten (Router, Switch, ...).

Sensoren
→ Beispiel: Netzwerk-Sensor (4/4)

- **Sicherheitsinformation:** +++ (hoch)
  Sonde hat Zugriff auf alle Kommunikationsdaten.

- **Vorteile:**
  - unabhängig von Netzwerkkomponenten
  - beste Erkennungsfähigkeiten, arbeiten auf allen Kommunikationsebenen

- **Nachteile:**
  - Höhere Kosten
  - Datenschutzprobleme
  - Sehr hohe Leistungsanforderung

Sensoren

→ Herausforderungen bei Netzwerk-Sensoren (1)

- **Kompletter Datenverkehr (P):**
  - DE-CIX ist größter öffentlicher Austauschpunkt der Welt.
  - Im Peek bis zu 7 TBit/s (2019).
  - Durchschnittlich bis zu 5 TBit/s (2019).
  - Vollständige Analyse nicht möglich.

- **Reduktion:**
  - Durchsatz von 100 MBit/s → 1 TByte in 24 h.
  - Viel Rechenpower benötigt (CPU, RAM, …).
  - Geringer Verlust von Sicherheitsrelevanten Informationen (SI).

Sensoren

→ Herausforderungen bei Netzwerk-Sensoren (2)

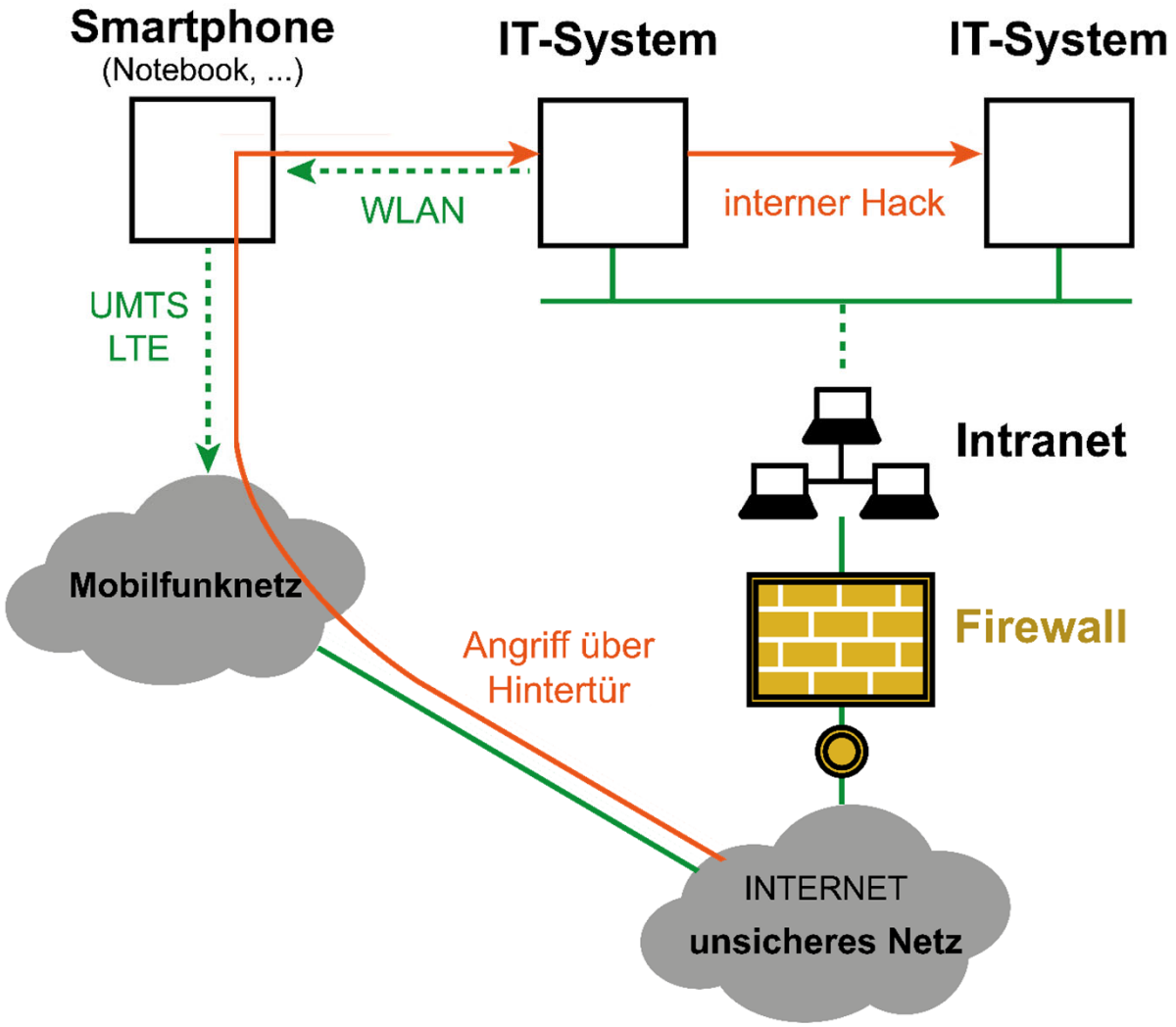
- **Rechtliche Bedingungen für den Zugriff.**

- **Ergebnis durch den Sensor (Y):**
  - Sensor muss SI kennen.
  - SI sollten langfristig gespeichert werden.
  - Effektive Datenstrukturen benötigt.
  - Ggf. zusätzliche Pseudonymisierung oder Anonymisierung.

Sensoren

→ Herausforderungen bei Netzwerk-Sensoren (3)

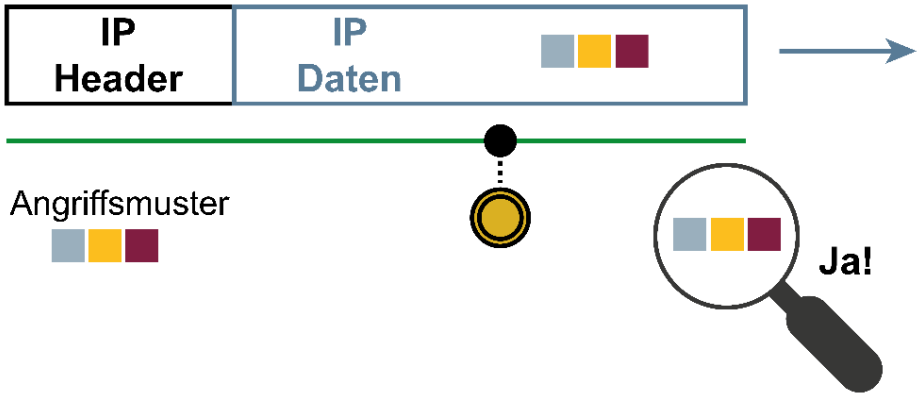
- **Nutzung von Hintertüren:**



Sensoren

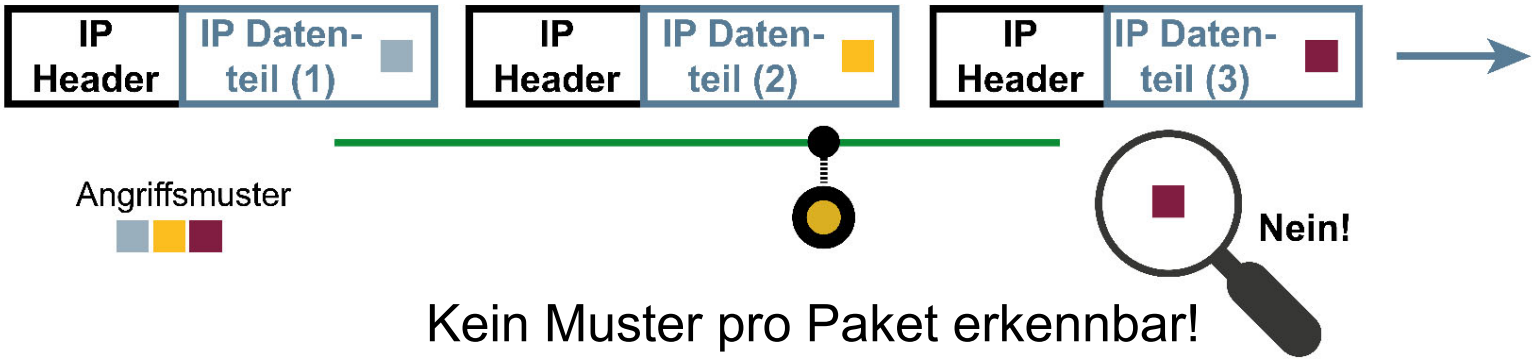
→ Herausforderungen bei Netzwerk-Sensoren (4)

- **Advanced Evasion Techniques (AET):**
  - Techniken zum Umgehen eines Netzwerksensors.
  - z.B. mittels IP-Fragmentierung.



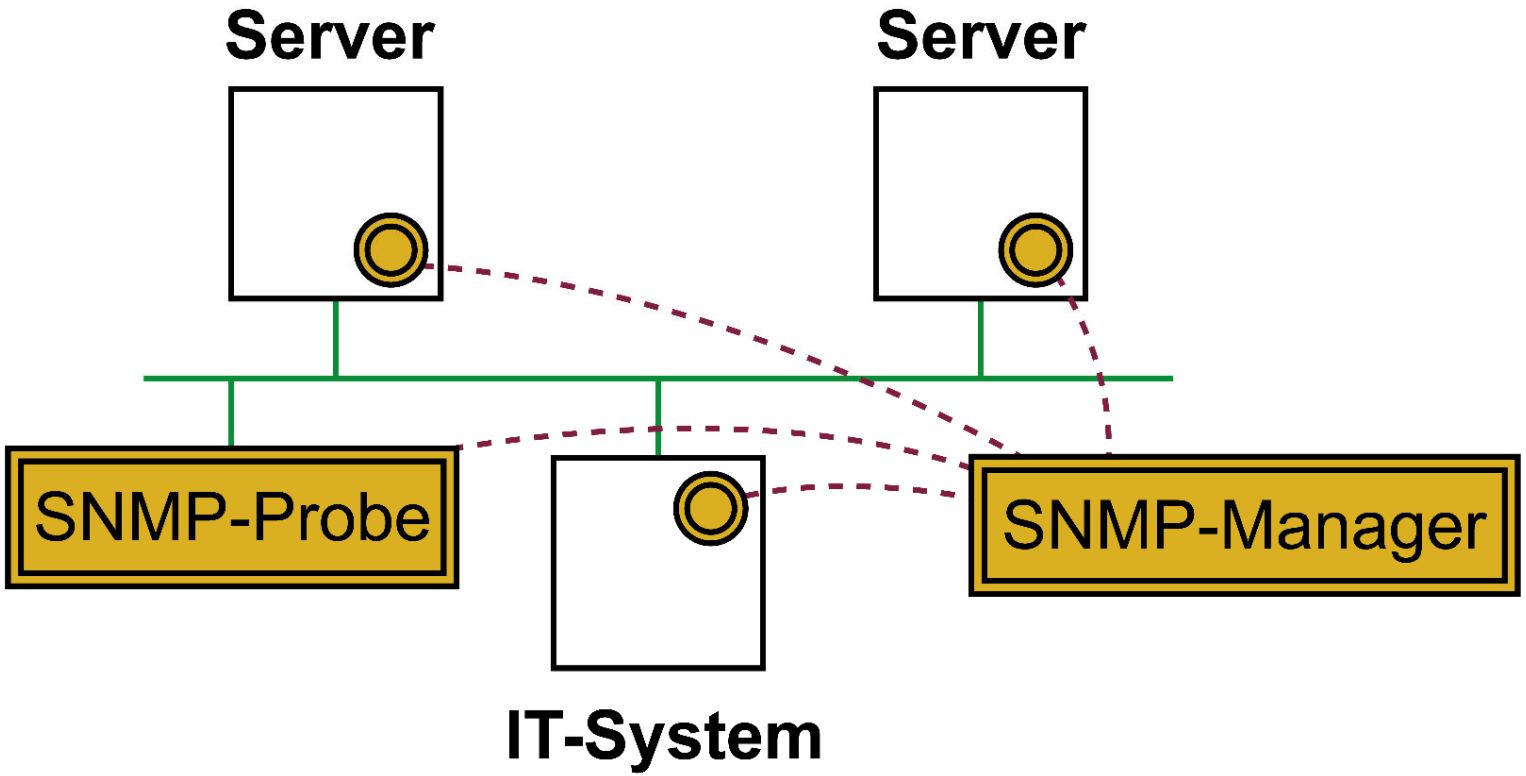
Angriffserkennung auf der Basis eines Musters in einem Paket (Signatur)

IP-Fragmentierung teilt die Daten eines Paketes auf mehrere Pakete auf!

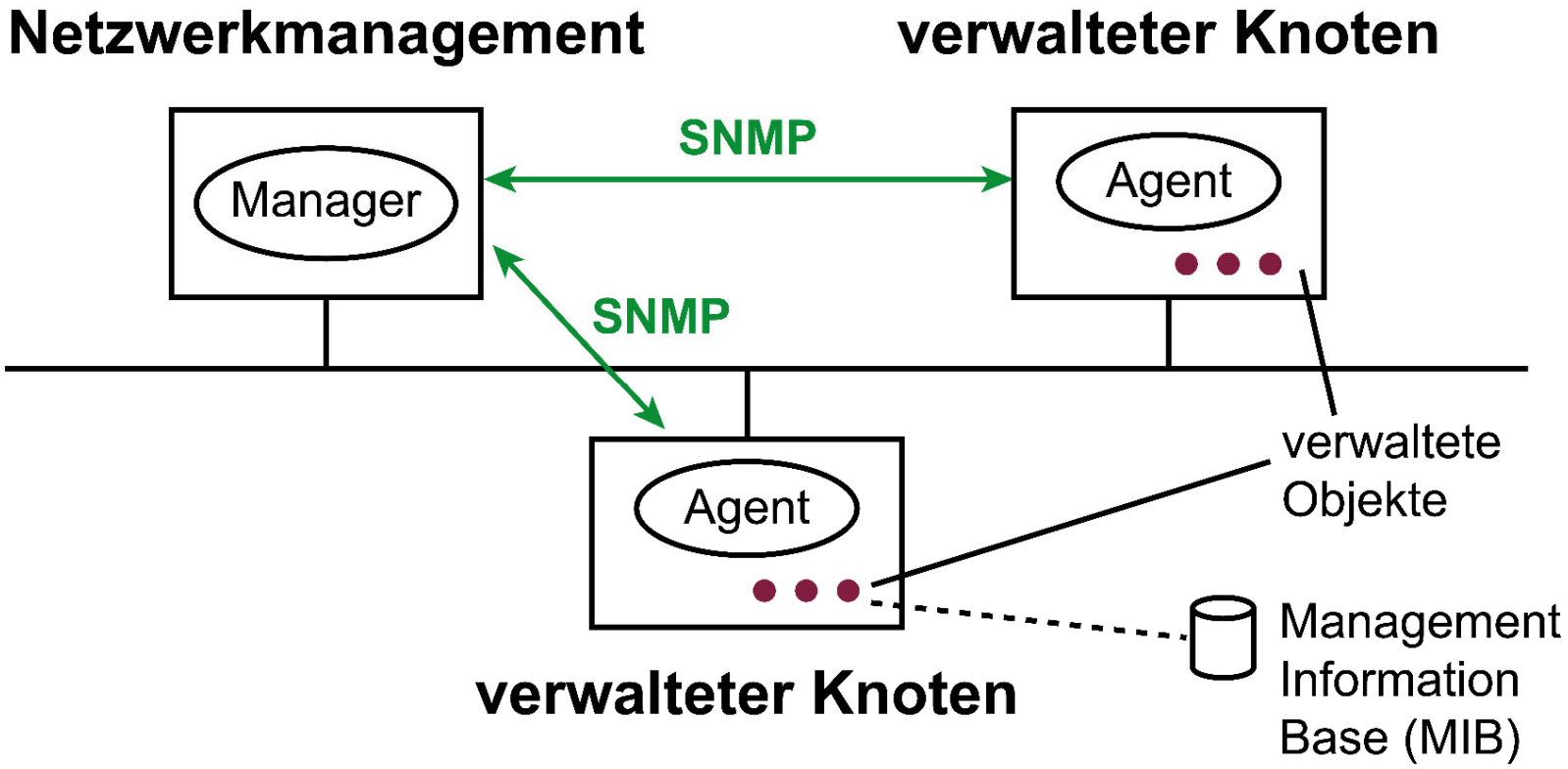


Kein Muster pro Paket erkennbar!

Sensoren
→ Beispiel: SNMP-Sensor (1/5)

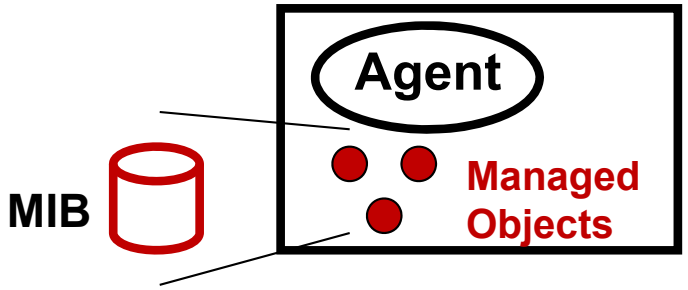


Sensoren
→ Beispiel: SNMP-Sensor (2/5)



Sensoren
→ Beispiel: SNMP-Sensor (3/5)

- **Grundprinzip des Sensors:**
  - P: = alle IP-Pakete und/oder
    zusätzliche Daten abhängig von den verwendeten MIBs
    (Festplatte, CPU, ...)
  - D: = eine Reduktion von P
  - SI (D): = Auswahl der Objekte in der MIB
  - Y: = SNMP-Nachricht (Inhalt der verwalteten Objekten)
  - Analyse von Sicherheitsinformationen nur im Analysesystem (SNMP-Manager)



- **Genereller Aspekt:**
  - Überwachen und/oder Verwalten einer Gruppe von IP-fähigen IT-Systemen in einem Netzwerk.

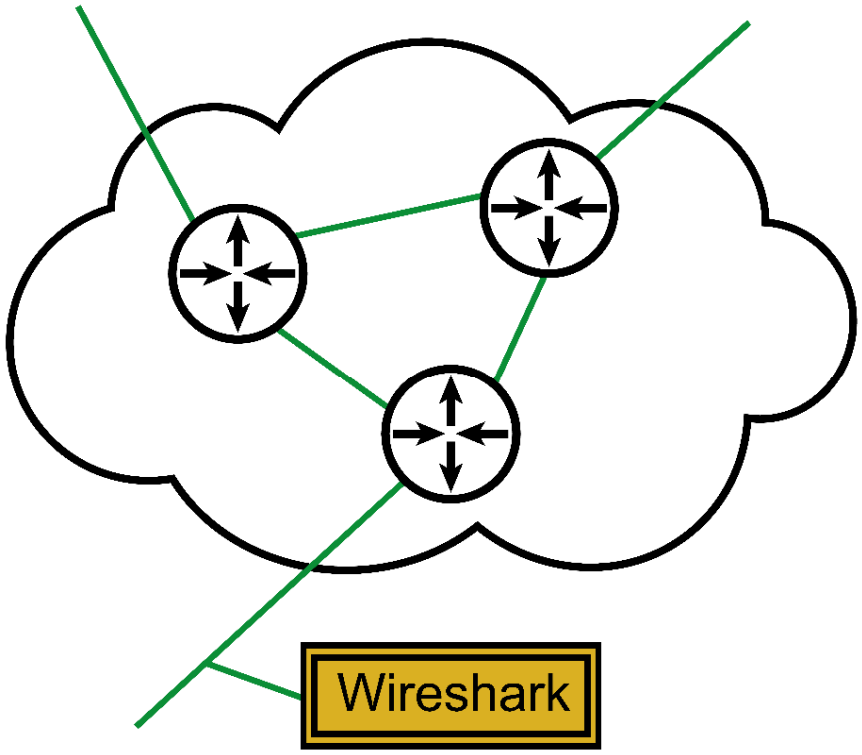
Sensoren
→ Beispiel: SNMP-Sensor (4/5)

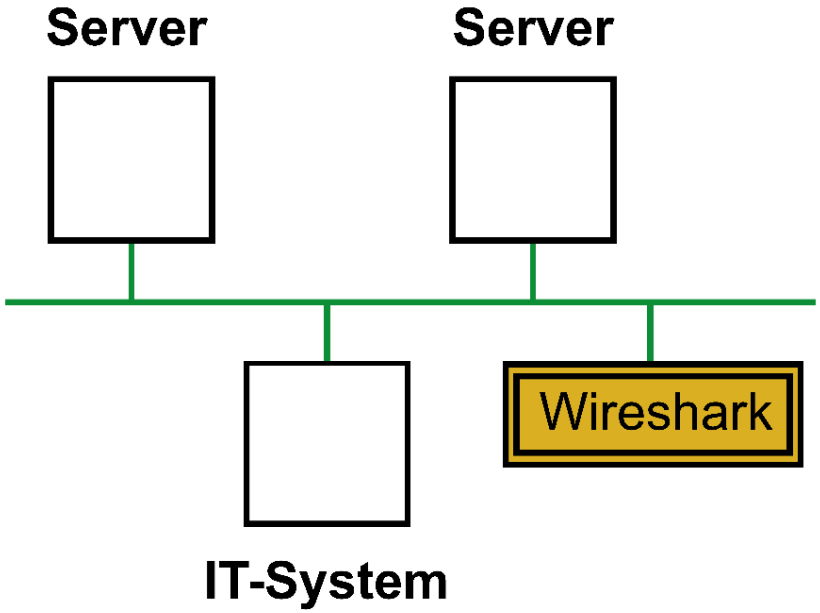
- **Ort der Messung:**
  - Netzwerk, SNMP-Agent ist eine Anwendung in IP-fähigen IT-Systemen.
- **Sicherheitsinformation:** + (wenig)
  Nur wenig SI in den MIBs von SNMP.
- **Vorteile:**
  - Der Sensor ist bereits als ein Feature in den IP-fähigen IT-Systemen verfügbar.
  - Perfekt zum Testen der Verfügbarkeit von lokalen Netzwerkgeräten, Servern, Diensten, ...

Sensoren
→ Beispiel: SNMP-Sensor (5/5)

- **Nachteile:**
  - Wenig Sicherheitsinformationen in den MIBs verfügbar.
  - SNMP ist eher ein Netzwerkmanagement als ein IT-Sicherheits-Tool.

Sensoren
→ Beispiel: Wireshark-Sensor (1/4)





Sensoren
→ Beispiel: Wireshark-Sensor (2/4)

- **Grundprinzip des Sensors:**
  - P: = alle IP-Pakete
  - D: = P
  - SI (D): = Auswahl der Filter durch den Cyber-Sicherheitsexperten
  - Y: = Interpretation durch einen Cyber-Sicherheitsexperten
  - Die Analyse der Sicherheitsinformationen erfolgt lokal durch einen Cyber-Sicherheitsexperten mithilfe der Wireshark-Anwendung.

Sensoren
→ Beispiel: Wireshark-Sensor (3/4)

- **Genereller Aspekt:**
  - Wireshark ist sehr nützlich für die detaillierte Analyse eines Angriffs.

- **Ort der Messung:**
  - Netzwerk, integriert als Anwendungstool in ein IT-System (Notebook, PC).

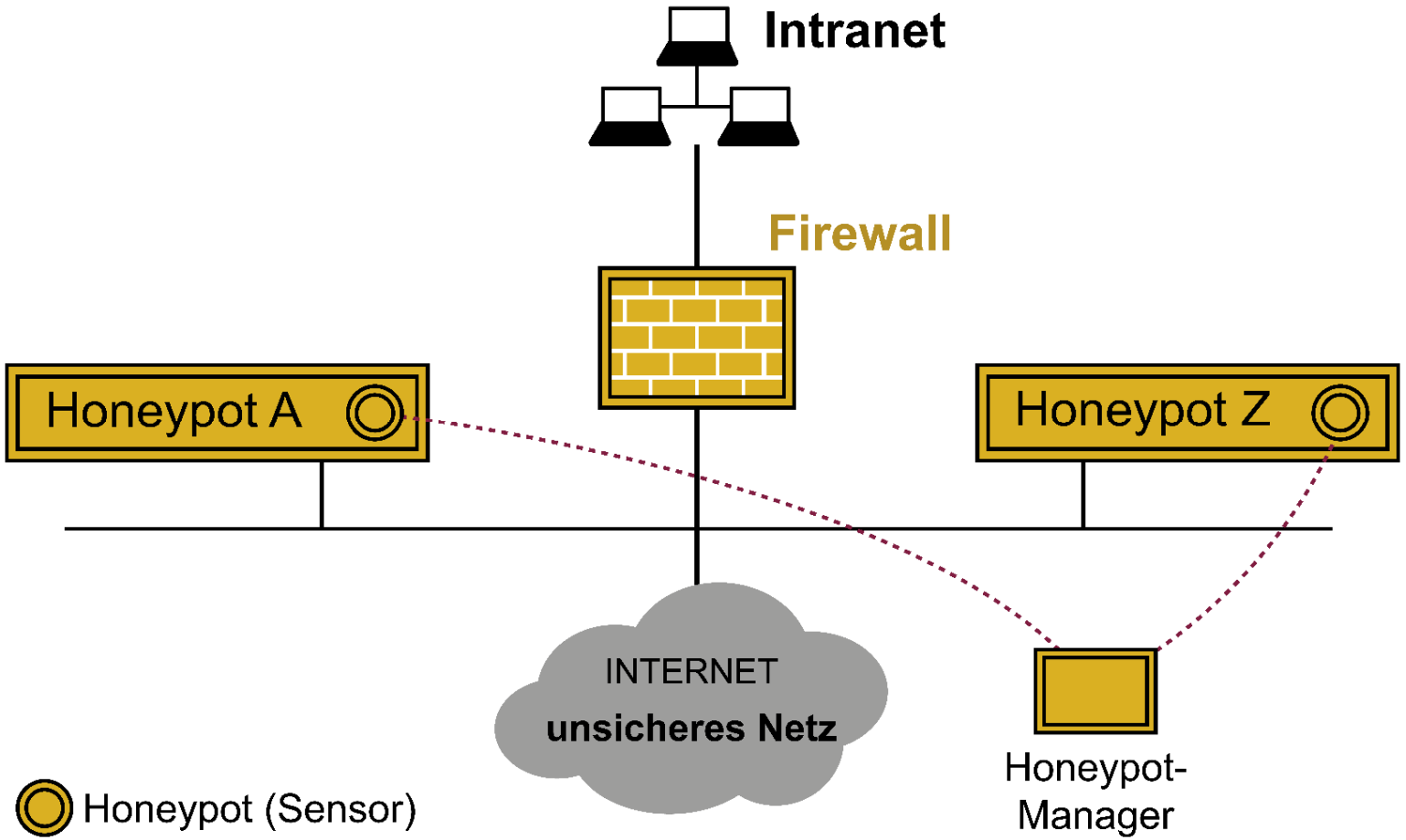
- **Sicherheitsinformation:** +++ (hoch)
  Zugriff auf alle Pakete der unterschiedlichen Protokolle.

Sensoren
→ Beispiel: Wireshark-Sensor (4/4)

- **Vorteile:**
  - Alle Sicherheitsinformationen verfügbar.
  - Nicht nur IT-Sicherheit, sondern auch Netzwerkinformationen.

- **Nachteile:**
  - Zu viele Informationen
    – Größe der Daten (100 M Bit/s … ca. 1 T Byte / 24 h).
  - Sehr komplex; nur manuelle Analyse (hohe Kosten).

Sensoren
→ Beispiel: Honeypot-Sensor (1/4)



Sensoren
→ Beispiel: Honeypot-Sensor (2/4)

- **Grundprinzip des Sensors:**
  - P: = alle IP-Pakete und Ereignisse im IT-System (Betriebssystem, Anwendung, Daten, …)
  - D: = Teilmenge der Netzwerkdefinition der Regeln für die Protokollierung
  - SI (D): = Auswahl der Nutzung und Anzahl der Honeypot-Systeme
  - Y: = detaillierte Angriffsspuren (Netzwerk/Host)
  - Analyse von Sicherheitsinformationen im Sensor- und Analysesystem.

Sensoren
→ Beispiel: Honeypot-Sensor (3/4)

- **Genereller Aspekt:**
  - Alle Interaktionen mit Honeypots als „Fake-Services“ sind Angriffspotentiale, die der Angreifer auch auf einem echten IT-System durchgeführt hätte.

- **Ort der Messung:**
  - Netzwerk, separater Sensor.

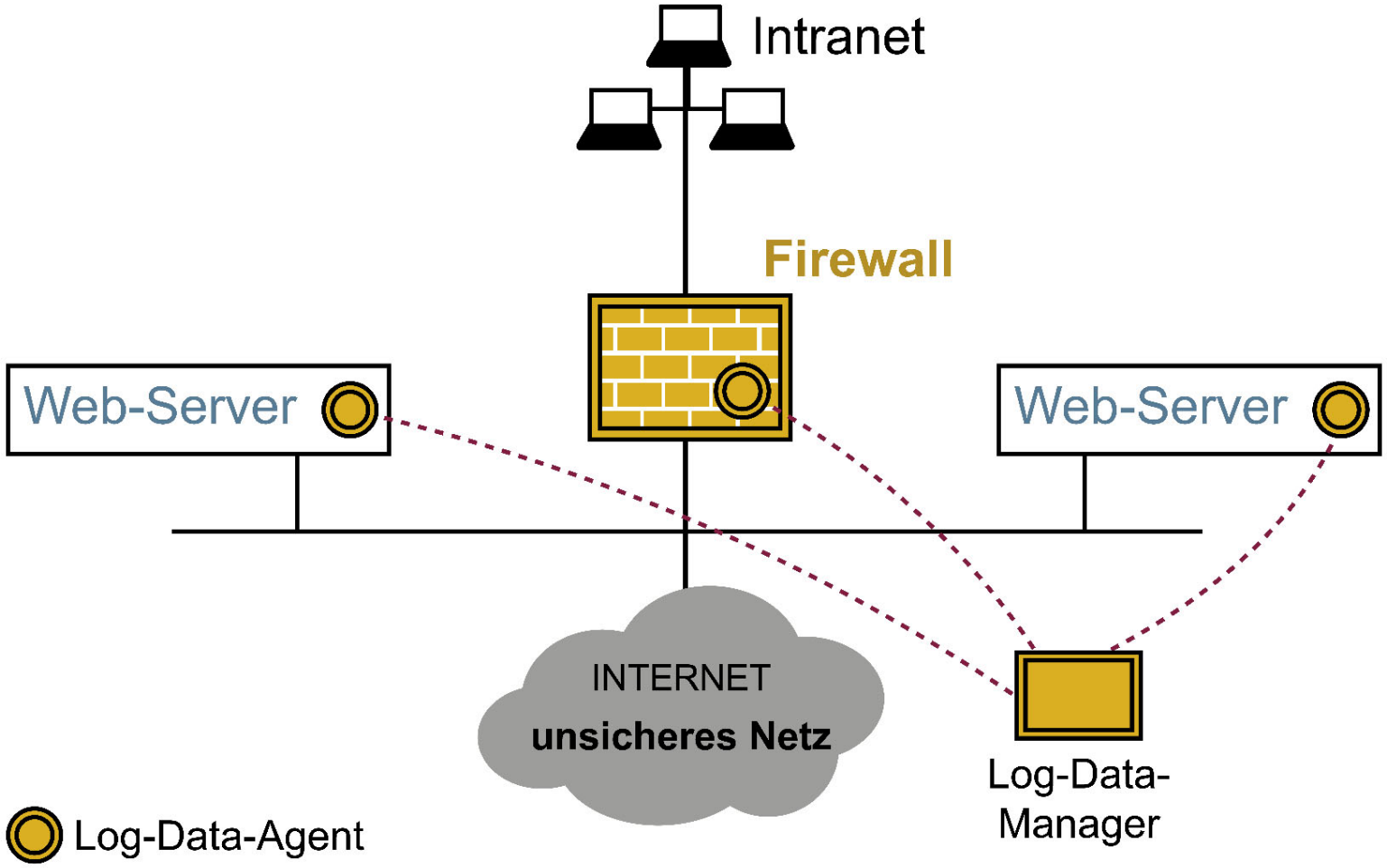
- **Sicherheitsinformation:** ++ (mittel)
  Angriffspotential gut erkennbar.

Sensoren
→ Beispiel: Honeypot-Sensor (4/4)

- **Vorteile:**
  - Qualitative Sicherheitsinformationen.
  - Angriffsmuster werden identifiziert und können genutzt werden, um sich besser zu schützen.

- **Nachteile:**
  - Wartungsintensiv
  - Angreifer sind in der Lage, Honeypots zu erkennen.

Sensoren
→ Beispiel: Logdaten-Sensor (1/5)



Sensoren
→ Beispiel: Logdaten-Sensor (2/5)

Sensoren
→ Beispiel: Logdaten-Sensor (3/5)

- **Grundprinzip des Sensors:**
  - P: = Aktivitäten in den IT-Systemen
  - D: = Ereignisse
  - SI (D): = Hängt von der Definition des Regelwerks ab (signatur- und anomaliebasierte Analyse)
  - Y: = Logdatei (Logeinträge)
  - Analyse von Sicherheitsinformationen im Sensor- und Analysesystem.

Sensoren
→ Beispiel: Logdaten-Sensor (4/5)

- **Genereller Aspekt:**
  - Erzeugt einen Nachweis und hilft dabei, Aktivitäten (Angriffe) zu identifizieren und zu verstehen.

- **Ort der Messung:**
  - Netzwerk, Netzwerkkomponenten (Firewall, ...)
  - IT-System (Betriebssystem, Anwendungen und Daten)

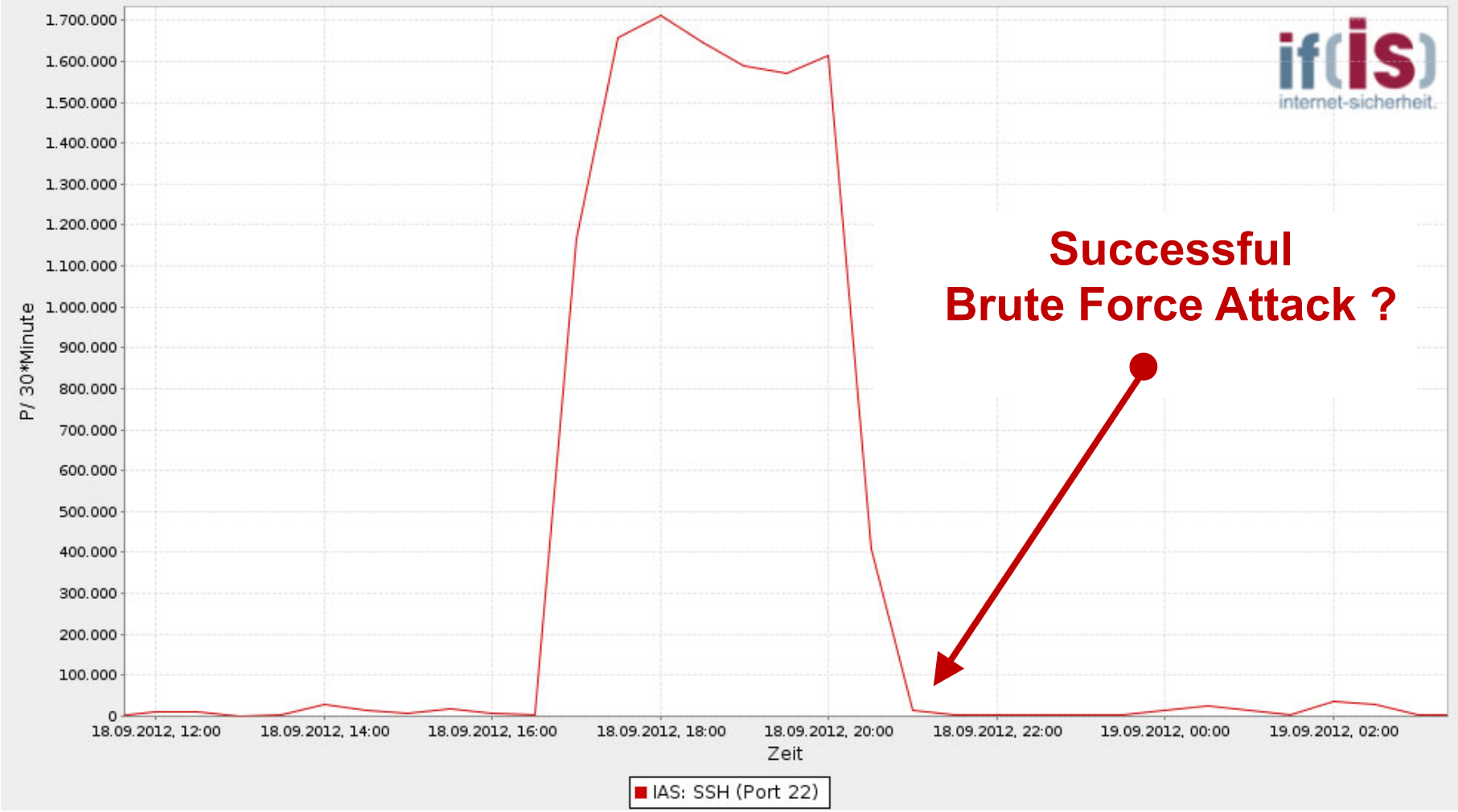
- **Sicherheitsinformation:** +++ (hoch)
  Logdaten können sehr viele SI enthalten.

Sensoren
→ Beispiel: Logdaten-Sensor (5/5)

- **Vorteile:**
  - Detaillierte Sicherheitsinformationen.
  - Angriffspfad kann analysiert werden.
  - Erfolgreiche Angriffe können gespeichert und weiter analysiert werden.
  - Die Logdaten können auch zur Beweissicherung genutzt werden.
- **Nachteile:**
  - schwierige Definition der Ereignisse und ein optimaler Regelsatz
  - Problem: in der Praxis sind nur ca. 5% der Log-Einträge wichtig (sicherheitsrelevant)
  - Protokollierung := Erfolgreiche Angriffe sind bereits umgesetzt.

Network sensor
→ Interpretation or clearly identify (1/2)

- **Network sensor**
  - Interpretation of attack pattern
    - Could be a successful attack but we do not know



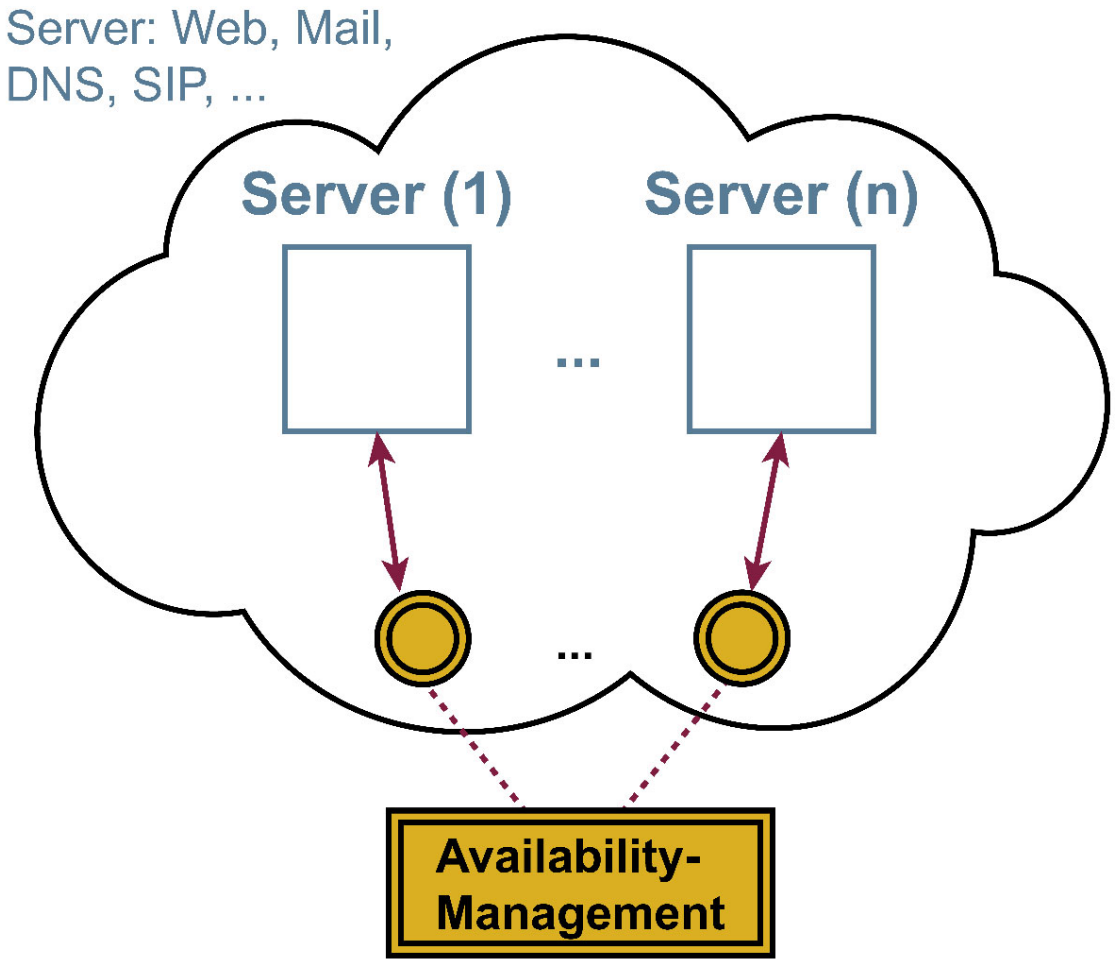
Network sensor
→ Interpretation or clearly identify (2/2)

- **LogData sensor**
  - Clear identification of events (Events identify a successful attack)

…
Sep 23 04:02:49 prometheus sshd[30395]: **Failed password** for root from 140.114.78.131 port 56003 ssh2
Sep 23 04:02:49 prometheus sshd[30396]: Received disconnect from 140.114.78.131: 11: Bye Bye
Sep 23 04:02:52 prometheus unix_chkpwd[30400]: password check failed for user (root)
Sep 23 04:02:52 prometheus sshd[30398]: pam_unix(sshd:auth): authentication failure;
Sep 23 04:02:54 prometheus sshd[30398]: **Failed password** for root from 140.114.78.131 port 57683 ssh2
Sep 23 04:02:54 prometheus sshd[30399]: Received disconnect from 140.1
Sep 23 04:02:56 prometheus unix_chkpwd[30403]: password check failed f
Sep 23 04:02:56 prometheus sshd[30401]: pam_unix(sshd:auth): authentic
Sep 23 04:02:58 prometheus sshd[30401]: **Failed password** for root from 140.114.78.131 port 59293 ssh2
Sep 23 04:02:59 prometheus sshd[30402]: Received disconnect from 140.114.78.131: 11: Bye Bye
Sep 23 04:03:01 prometheus unix_chkpwd[30406]: password check failed for user (root)
Sep 23 04:03:01 prometheus sshd[30404]: pam_unix(sshd:auth): authentication failure;
Sep 23 04:03:03 prometheus sshd[30404]: **Failed password** for root from 140.114.78.131 port 32877 ssh2
Sep 23 04:03:03 prometheus sshd[30405]: Received disconnect from 140.114.78.131: 11: Bye Bye
…
Sep 23 11:42:55 prometheus sshd[683]: **Accepted password** for root from 140.114.78.131 port 56418 ssh
Sep 23 11:42:55 prometheus sshd[683]: pam_unix(sshd:session): session opened for user root by (uid=0)

Successful Brute Force Attack !

Sensoren
→ Beispiel: Verfügbarkeitssensor (1/4)



Sensoren
→ Beispiel: Verfügbarkeitssensor (2/4)

- **Grundprinzip des Sensors:**
  - P: = Verfügbarkeitsinformationen
  - D: = Quality of Service (QoS)- und Quality of Experience (QoE)-Parameter
  - SI (D): = Auswahl der gemessenen Parameter
  - Y: = Sicherheitsereignisse und/oder QoS/QoE-Parameter?
  - Analyse von Sicherheitsinformationen im Sensor- und Analysesystem.

Sensoren
→ Beispiel: Verfügbarkeitssensor (3/4)

- **Genereller Aspekt:**
  - Hilft, die Verfügbarkeit von IT-Systemen und -Diensten zu bewerten.
- **Ort der Messung:**
  - Sensor im Netzwerk.
- **Sicherheitsinformation:** ++ (mittel)
  Für das Cyber-Sicherheitsbedürfnis „Gewährleistung der Verfügbarkeit“ werden hilfreiche Sicherheitsinformationen zur Verfügung gestellt.

Sensoren
→ Beispiel: Verfügbarkeitssensor (4/4)

- **Vorteile:**
  - Echte Sicherheitsinformationen für den Aspekt Verfügbarkeit
- **Nachteile:**
  - Kosten für zusätzlichen Netzwerkverkehr, CPU, ...

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

→ Inhalt

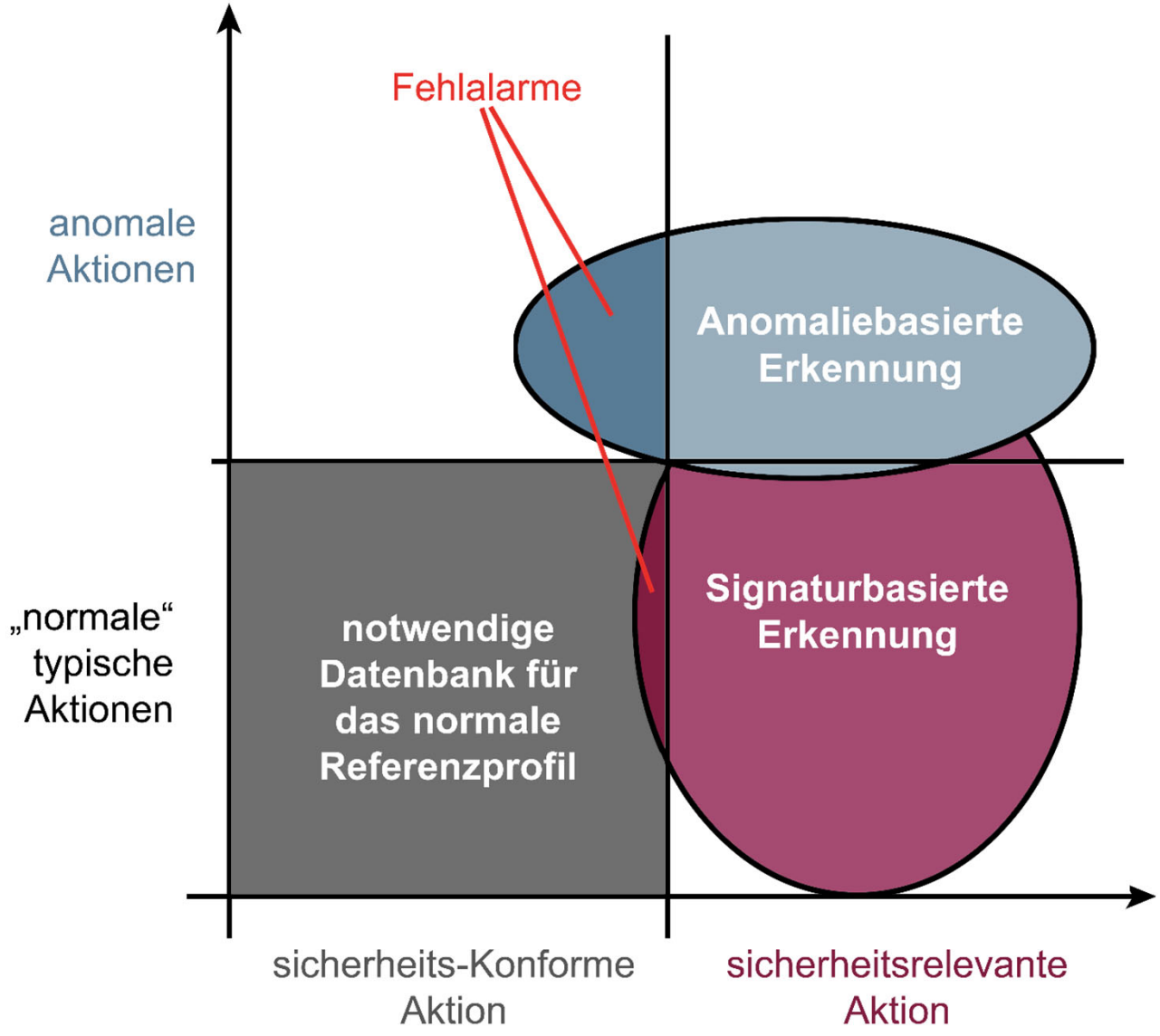
- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- Idee eines EWS
- Aufbau eines EWS
- Sensoren
- **Analysekonzepte**
- Zusammenfassung

Analysekonzepte
→ Auswertung (1/2)

- **Erkennen von bekannten sicherheitsrelevanten Aktionen:**
  - Festhalten von bereits **bekannten/hypothetischen Ereignissen/Abläufen**.
  - Erzeugung einer **Signatur**.
  - Problem: **Zeitverzögerung** zwischen Erkennung und Erzeugung der Signatur.

- **Erkennen von Anomalien:**
  - Definition eines „normal“-Zustandes.
  - Erkennung von gravierenden Verhaltensabweichungen (Statistiken, Erfahrungswerte, Systemzustände, …)
  - Erkennung von unbekannten Angriffen möglich.

Analysekonzepte
→ Auswertung (2/2)



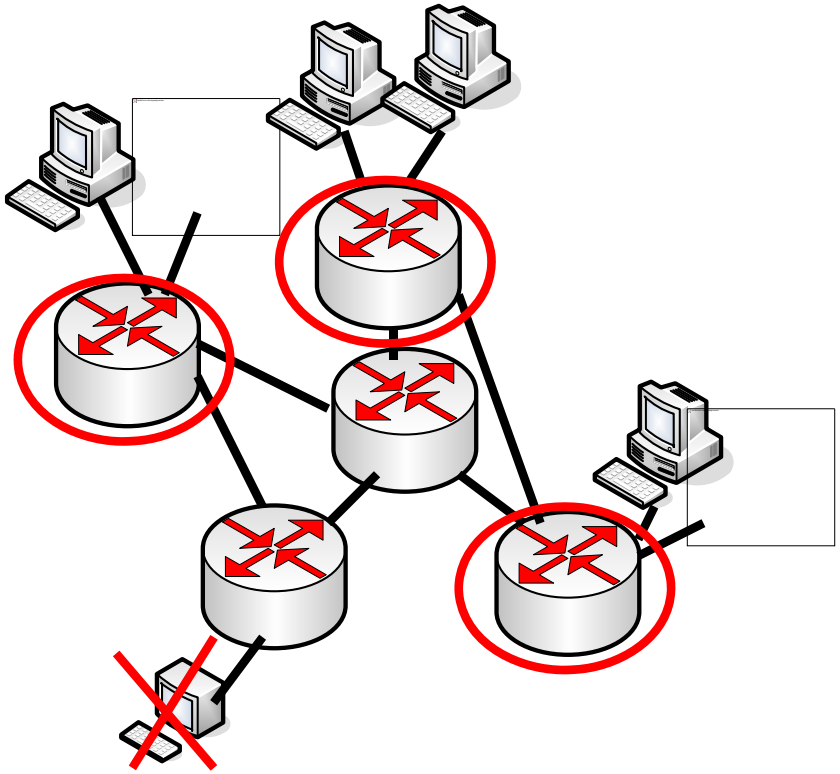
Analysekonzepte
→ Frühwarnprozess

Analysator

- **Private users / enterprises**
  - Reduction of the possibilities (firewall, …)
  - Increasing security mechanisms
  - Selective shut-down (cut-off) of affected systems
    (without destroying evidence for possible criminal prosecution (forensics))
  - Complete deactivation of the uplink to the internet

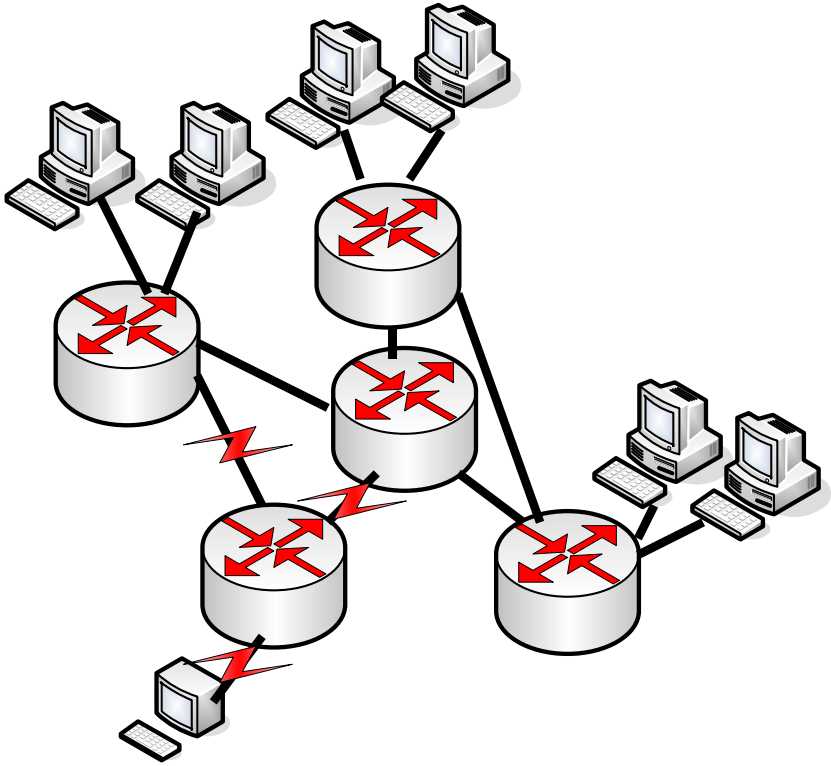
- **Internet Service Provider**
  - Access Control Lists
  - Rate-Limiting
  - Blackholing
  - Off-Ramping / Sinkholing

Access Control Lists



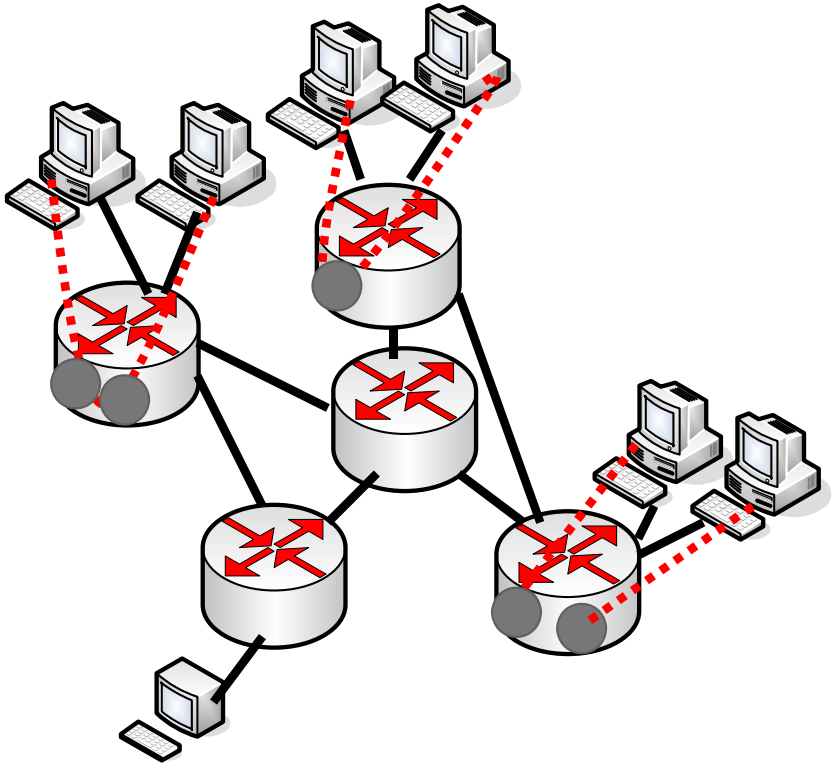
e.g. black-, white- or grey-List

Rate-Limiting



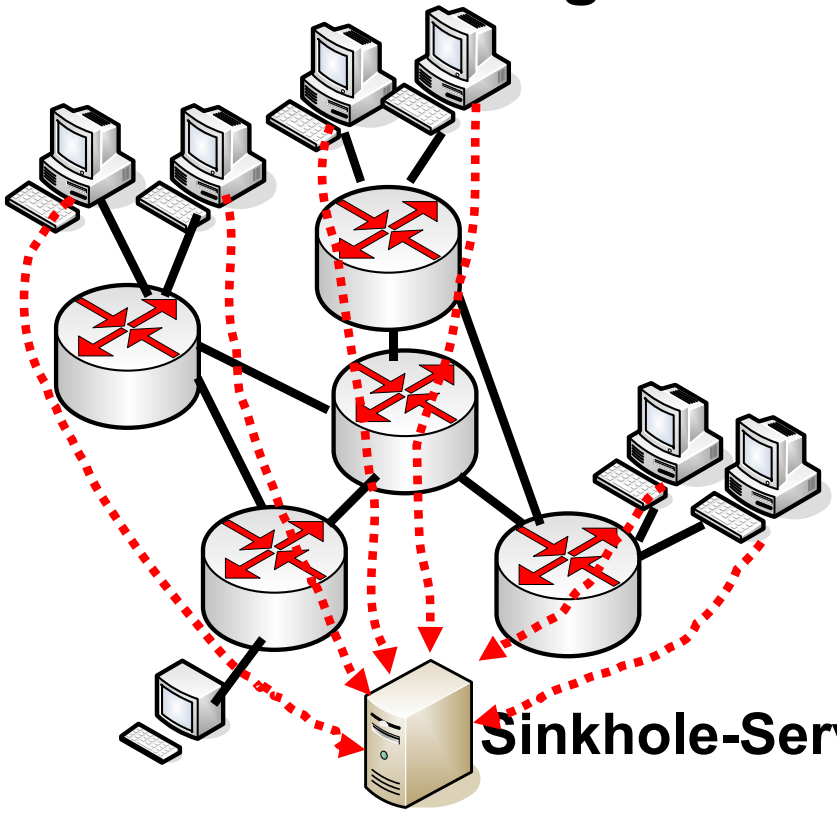
e.g. traffic shaping, packet shaping, bandwidth throttling, …

Blackholing

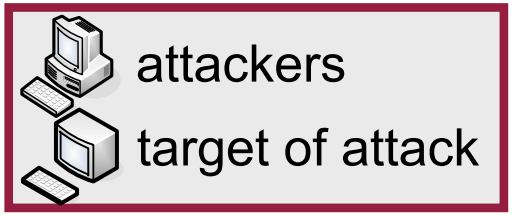


a null route (blackhole route) is a network route (routing table entry) that goes nowhere

Sinkholing

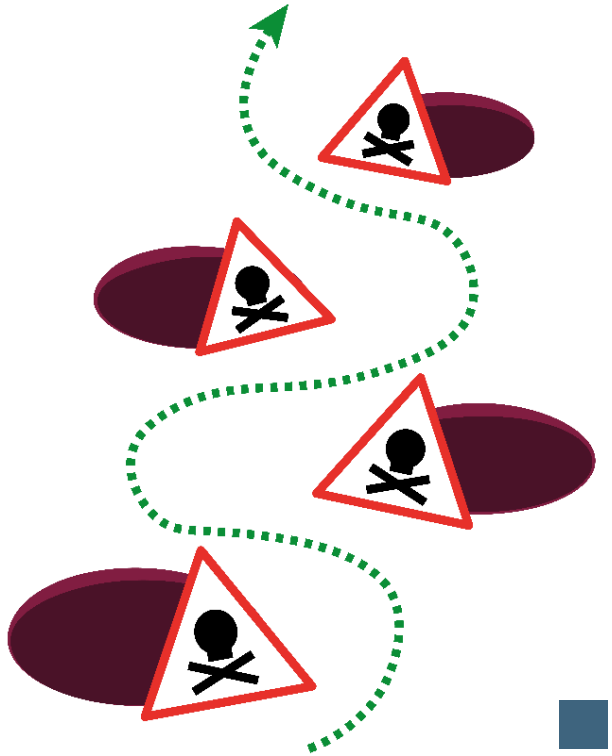


e.g. darknet (unused regions of IP address space), flow collectors, backscatter detectors, packet sniff…



Analysekonzepte
→ Kommunikationslagebild (1/3)

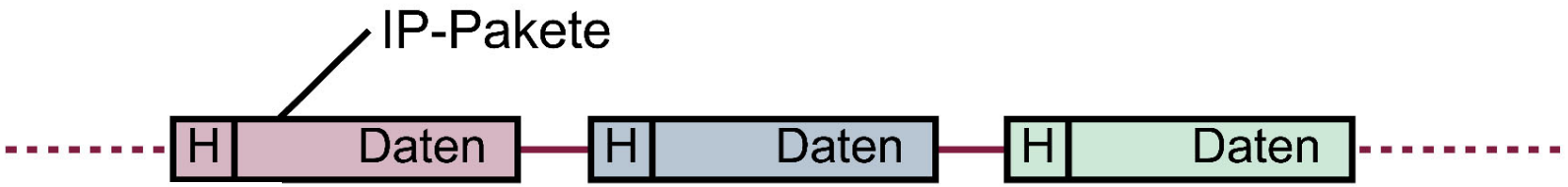
- **Herausforderungen:**
  - Sehr gute Sichtweise über die gesamte Kommunikationslage erlangen.
  - Wissen über die eigene Kommunikation und die verwendeten IT-Technologien aufbauen und nutzen.
  - Aus der Vergangenheit lernen.
  - Mit anderen zusammenzuarbeiten.
  - Angemessene Gegenmaßnahmen einleiten.



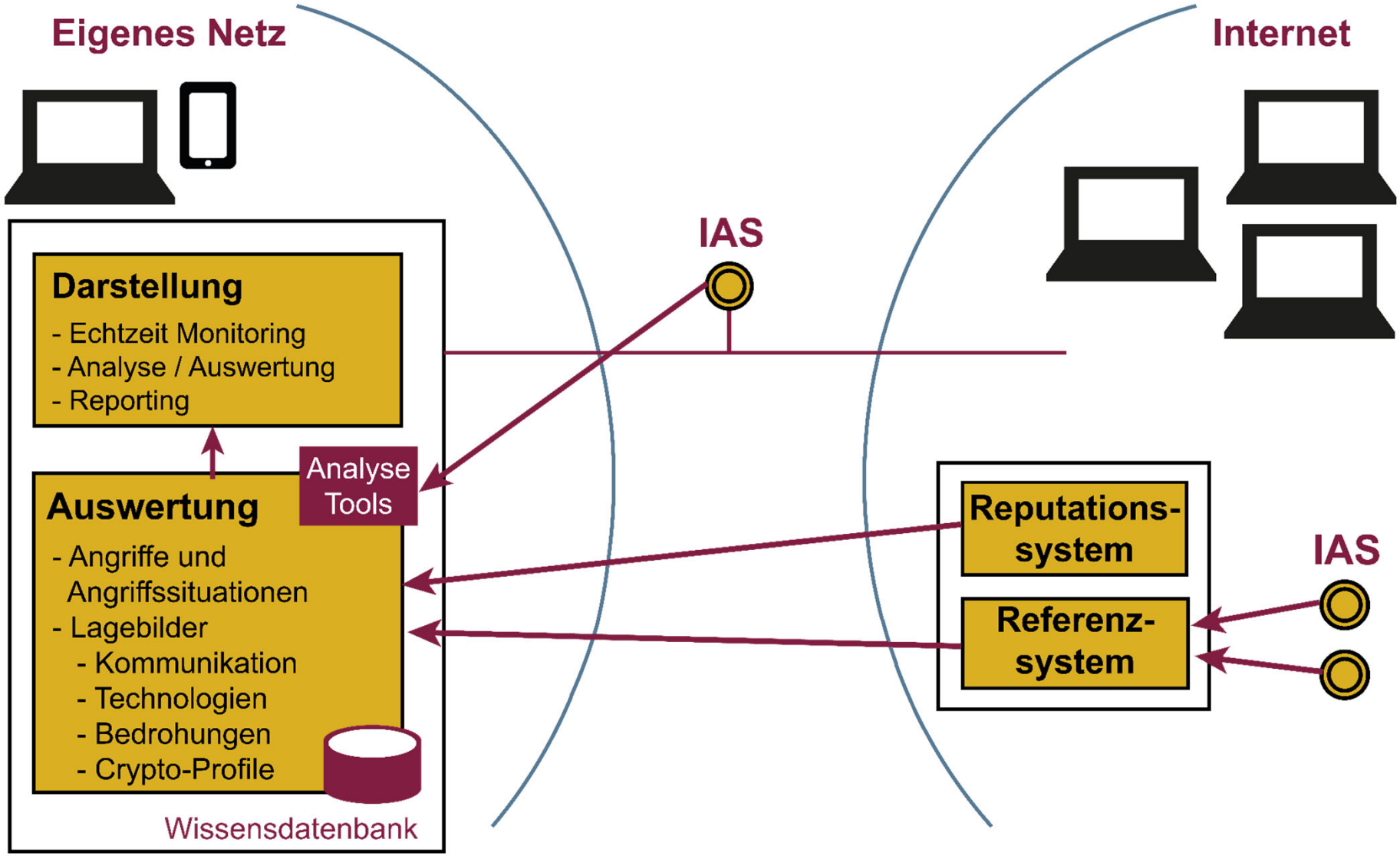
Analysekonzepte
→ Kommunikationslagebild (2/3)

- **Erkennen von Angriffspotentialen:**
  - Angriffe und Schwachstellen zuerst identifizieren.
  - Resultierende Angriffspotentiale bewerten.
  - Risiken gezielt auf ein angemessenes Maß minimieren.

Analysekonzepte
→ Kommunikationslagebild (3/3)



Analysekonzepte
→ Internet-Analyse-System



Analysekonzepte

→ Bewertung der Kommunikationslage (1)

- **Genutzte TLS/SSL-Technologie:**

TLS-Version	Pakete	
	Anzahl	%
SSL Version SSL 2.0	0	0,00
SSL Version SSL 3.0	25.989	0,12
SSL Version TLS 1.0	10.154.344	48,42
SSL Version TLS 1.1	608.026	2,90
SSL Version TLS 1.2	10.182.293	48,55
SSL Version Other	0	0,00
Gesamt	**20.970.652**	**100,00**

Analysekonzepte

→ Bewertung der Kommunikationslage (2)

- **Verteilung der IP-Portnummern:**

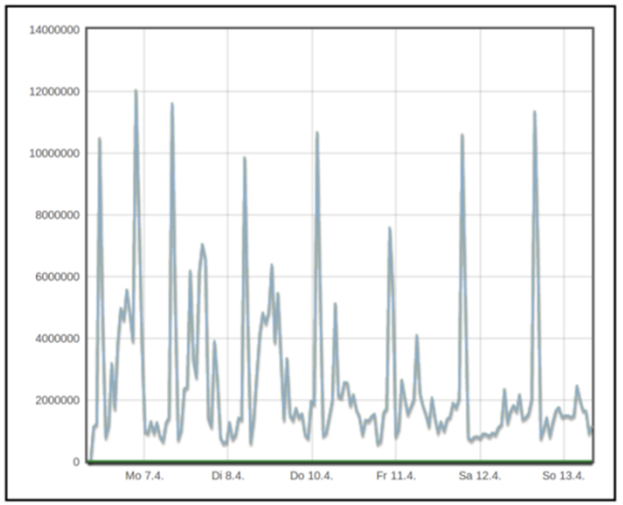
IP Protokollnummer	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Protocol number 6 (TCP)	468.472.020	64,62	358.462	4,74	86,63
Protocol number 17 (UDP)	237.139.295	32,71	53.729	0,71	12,99
Protocol number 1 (ICMP)	18.914.729	2,61	1.582	0,02	0,38
Protocol number 50 (ESP)	5.799.799	0,8	<1	<0,01	<0,01
Protocol number 2 (IGMP)	4.431	<0,01	2	<0,01	<0,01
Protocol number 132 (SCTP)	12	<0,01	<1	<0,01	<0,01
Protocol number 46 (RSVP)	1	<0,01	<1	<0,01	<0,01
Rest	0	0,00	0	0,00	0,00
Gesamt	**724.974.918**	**100,00**	**413.776**	**5,47**	**100,00**

Analysekonzepte

→ Bewertung der Kommunikationslage (3)

- **Nutzung und Verteilung von Protokolle:**

Port	Richtung	Pakete Anzahl	Pakete %	Traffic MB	Bandbreite Mbps	Bandbreite %
80 (HTTP)	DST	64.684.674	15,53	6.247	<0,01	1,87
	SRC	119.764.297	28,76	152.480	2,02	45,53
	Alle	**184.448.971**	**44,29**	**158.726**	**2,10**	**47,39**
22 (SSH)	DST	36.189.875	8,69	6.821	<0,01	2,04
	SRC	73.040.334	17,54	98.176	1,30	29,31
	Alle	**109.230.209**	**26,23**	**104.997**	**1,39**	**31,35**
443 (HTTPS)	DST	30.334.171	7,28	5.568	<0,01	1,66
	SRC	47.446.836	11,39	49.740	<0,01	14,85
	Alle	**77.781.007**	**18,68**	**55.308**	**<0,01**	**16,51**
993 (IMAPS)	DST	13.320.318	3,20	1.285	<0,01	<0,01
	SRC	20.612.130	4,95	9.649	<0,01	2,88
	Alle	**33.932.448**	**8,15**	**10.934**	**<0,01**	**3,26**
25 (SMTP)	DST	3.681.795	<0,01	2.341	<0,01	<0,01
	SRC	2.759.396	<0,01	260	<0,01	<0,01
	Alle	**6.441.191**	**1,55**	**2.602**	**<0,01**	**<0,01**
873 (rsync)	DST	394.331	<0,01	35	<0,01	<0,01
	SRC	853.234	<0,01	1.225	<0,01	<0,01
	Alle	**1.247.565**	**<0,01**	**1.259**	**<0,01**	**<0,01**
53 (DNS)	DST	769.144	<0,01	59	<0,01	<0,01
	SRC	658.873	<0,01	408	<0,01	<0,01
	Alle	**1.428.017**	**<0,01**	**467**	**<0,01**	**<0,01**
143 (IMAP)	DST	316.425	<0,01	93	<0,01	<0,01
	SRC	295.037	<0,01	176	<0,01	<0,01
	Alle	**611.462**	**<0,01**	**270**	**<0,01**	**<0,01**
99 (WIP Message)	DST	103.532	<0,01	6	<0,01	<0,01
	SRC	199.528	<0,01	287	<0,01	<0,01
	Alle	**303.060**	**<0,01**	**293**	**<0,01**	**<0,01**
110 (POP3)	DST	104.942	<0,01	10	<0,01	<0,01
	SRC	105.330	<0,01	46	<0,01	<0,01
	Alle	**210.272**	**<0,01**	**56**	**<0,01**	**<0,01**
Rest	DST	206.309	<0,01	13	<0,01	<0,01
	SRC	628.887	<0,01	9	<0,01	<0,01
	Alle	**835.196**	**<0,01**	**22**	**<0,01**	**<0,01**



	Pakete Anzahl	Pakete %	Traffic MB	Bandbreite Mbps	Bandbreite %
Gesamt	725.009.432	100,00	413.780,64	5,47	100,00
VLAN	724.973.419	>99,99	413.776,38	5,47	>99,99
IPv4	724.970.615	>99,99	413.776,38	5,47	>99,99
IPv6	36.013	<0,01	4,25	<0,01	<0,01
Teredo	36.013	<0,01	4,25	<0,01	<0,01
ARP	2.804	<0,01	<0,01	<0,01	<0,01

Analysekonzepte

→ Bewertung der Kommunikationslage (4)

- **Nutzung und Verteilung von Übertragungsarten:**

Traffic-Art	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Src >= 1024 and Dst >= 1024 ("P2P") - client-to-client	49.922.825	10,66	23.096	0,31	6,44
Src < 1024 and Dst < 1024 ("B2B") - server-to-server	326.388	0,07	22	<0,01	<0,01
Src >= 1024 and Dst < 1024 ("P2B") - client-to-server	152.183.466	32,49	22.752	0,30	6,35
Src < 1024 and Dst >= 1024 ("B2P") - server-to-client	266.037.102	56,79	312.589	4,13	87,20
Gesamt	**468.469.781**	**100,00**	**358.458**	**4,74**	**100,00**

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Angriffspotentiale
- Idee eines EWS
- Aufbau eines EWS
- Sensoren
- Analysekonzepte
- **Zusammenfassung**

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme
→ Zusammenfassung (1/3)

- **Generelle Vorgehensweise eines Angreifers:**
  - Erreichbarkeit prüfen → Ping Scan
  - Verfügbare Dienste prüfen → Port Scan
  - Schwachstellen prüfen → Vulnerability Scan

- **Wichtigste Eigenschaften eines EWS:**
  - Aktuelle Cyber-Sicherheitslage aufzeigen.
  - Angriffspotentiale und reale Angriffe (möglichst früh) erkennen.
  - Rechtzeitig Warnhinweise geben.
  - Minimierung oder Verhinderung von Schäden.

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme
→ Zusammenfassung (2/3)

- **Bestandteile eines EWS:**
  - Rechtliche Rahmenbedingungen
  - Sensoren
  - Analysetools
  - Warnsystem
  - Wissensbasis
  - Beweissicherung

- Es gibt verschiedene **Analysekonzepte**, die unterschiedliche **sicherheitsrelevante Aktionen** erkennen können.
  - **Anomalie** Erkennung
  - **Signatur** Erkennung

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme
→ Zusammenfassung (3/3)

- Sensoren und EWS können an verschiedenen Stellen von IT-Systemen und IT-Infrastrukturen platziert werden.

- Wichtige Stellschrauben für die Analyse sind unteranderem:
  - Verwendete Technologien
  - Platzierung von Sonden und EWS
  - Anzahl von Sonden

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

- Vorlesung -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

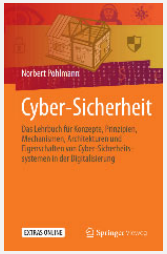
Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum
- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/
- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
- https://norbert-pohlmann.com/cyber-sicherheit/



Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/