Intrusion Detection Systeme

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Einleitung: Definitionen und Ziele
- Funktionen
- Einbindung von IDS
- Aufbau und Funktionsweise
- Auswertekonzepte
- Probleme
- Zusammenfassung

Einleitung
→ Definition

- **Intrusion**

  „Eine Menge von Handlungen, deren Ziel es ist, die Integrität, die Verfügbarkeit oder die Vertraulichkeit eines Betriebsmittels zu kompromittieren“

- **Intrusion Detection**

  Das Erkennen von

  - Vorbereitungen für oder
  - Durchführung von

  Kompromittierungsversuchen (Angriffen), mit dem Ziel einen Schaden zu verhindern.

Einleitung
→ Analogien

- Videoüberwachung und Alarmanlage

Einleitung
→ Ziele von Intrusion Detection Systemen

- Kompromittierungsversuche zu erkennen
- Angriffe an zuständige Personen zu melden
- Geeignete Gegenmaßnahmen zu treffen
  - Umkonfiguration oder Herunterfahren vom System (z.B. Firewall)
- Angriffsversuche zu dokumentieren (accountability)
- Die Qualität von Sicherheitsmaßnahmen zu kontrollieren
- Forensische Analysen zu unterstützen

Funktionen eines Intrusion Detection Systems
→ Übersicht

- **Informationen sammeln**
  - Network-Sensor
  - Host-Sensor
  - Applikations-Sensor
- **Informationen analysieren**
  - Erkennung des Missbrauchs (Signaturen)
  - Erkennung von Anomalien (Verhaltensmuster)
- **Reagieren**
  - Passiv (Person oder System benachrichtigen)
  - Aktiv (Informationen sammeln, Konfiguration ändern, gegen Angreifer vorgehen)

Funktionen eines Intrusion Detection Systems
→ Informationen sammeln

- **Netzwerk-Sensor**
  - Läuft auf dediziertem Computer
  - Überwacht den Datenstrom
  - Arbeitet im Stealth-Modus, daher kaum angreifbar
  - Probleme in Netzen mit Switches !
- **Host-Sensor**
  - Läuft auf Computer in Gebrauch, z.B. Server
  - Überwacht Datenstrom zum Computer und System-Logs
  - Kann angegriffen werden und belastet den Computer !
- **Applikations-Sensor**
  - Läuft auf Computer mit Applikation
  - Überwacht Applikations-Logs

Funktionen eines Intrusion Detection Systems
→ Informationen analysieren

- Analyse durch Sensor oder Management System

- **Erkennung des Missbrauchs**
  - Abgleich von Signaturen mit Datenbank
  - Datenbank muss up-to-date sein
  - Unbekannte Signaturen können nicht erkannt werden

- **Erkennung von Anomalien**
  - Lernen des normalen Betriebs
  - Erkennen von anomalen Betriebszuständen
  - Erkennt auch unbekannnte Angriffsmuster
  - Erkannter anomaler Betrieb muss individuell beurteilt werden, d.h. erhöhter Arbeitsaufwand

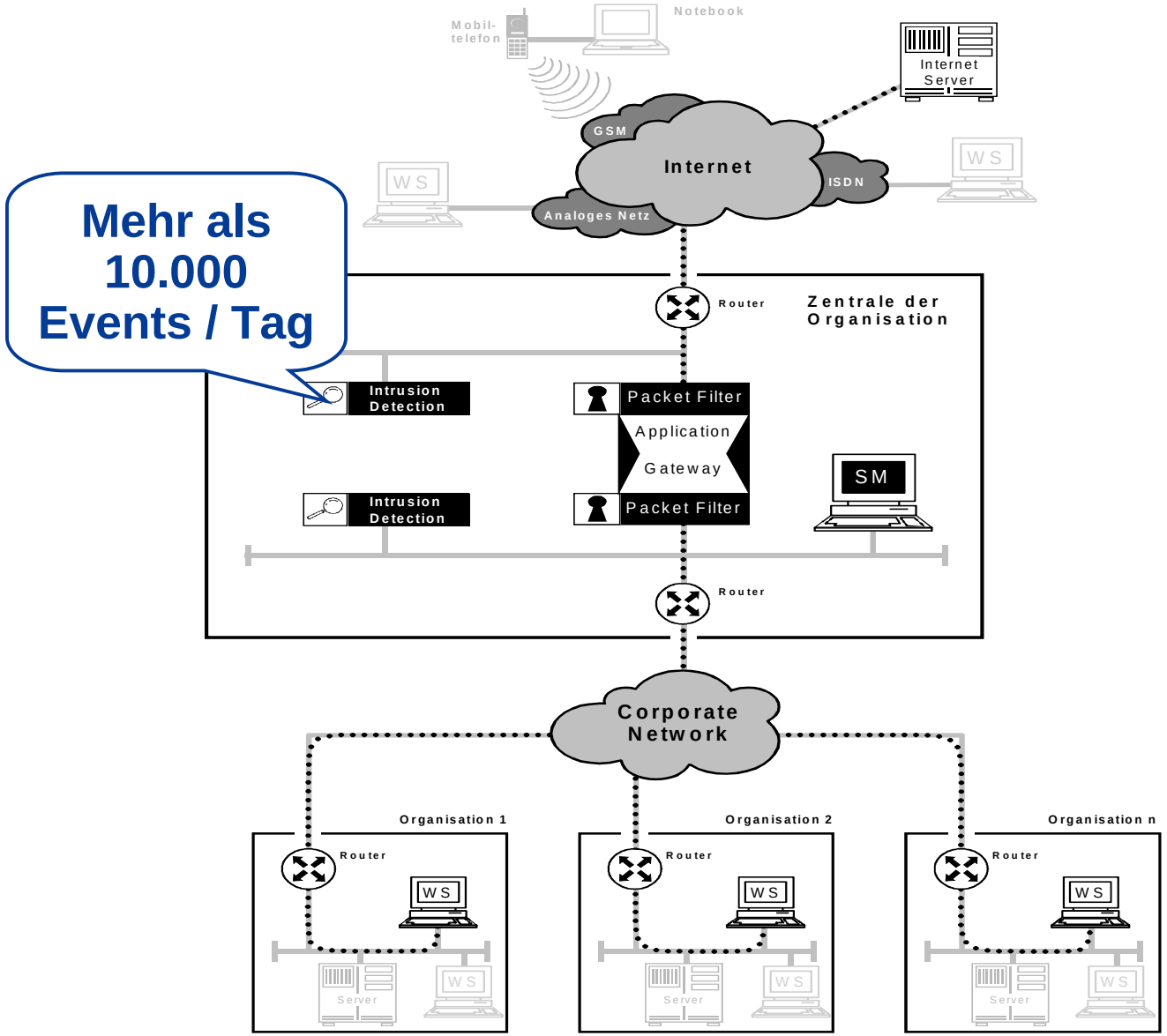
Funktionen eines Intrusion Detection Systems
→ Reagieren

- **Passiv**
  - Angriffsversuch Personen oder Systemen melden (logging, SNMP, e-mail, Pager, SMS, ...)
- **Aktiv**
  - Angriffsversuch sofort unterbrechen
  - Angreifer zu Honey-Pot leiten
  - Zukünftigen Zugriff des vermeintlichen Angreifers abblocken
  - Gegenangriff starten
  - ACHTUNG: Legalität der Aktionen ist nicht eindeutig!!!

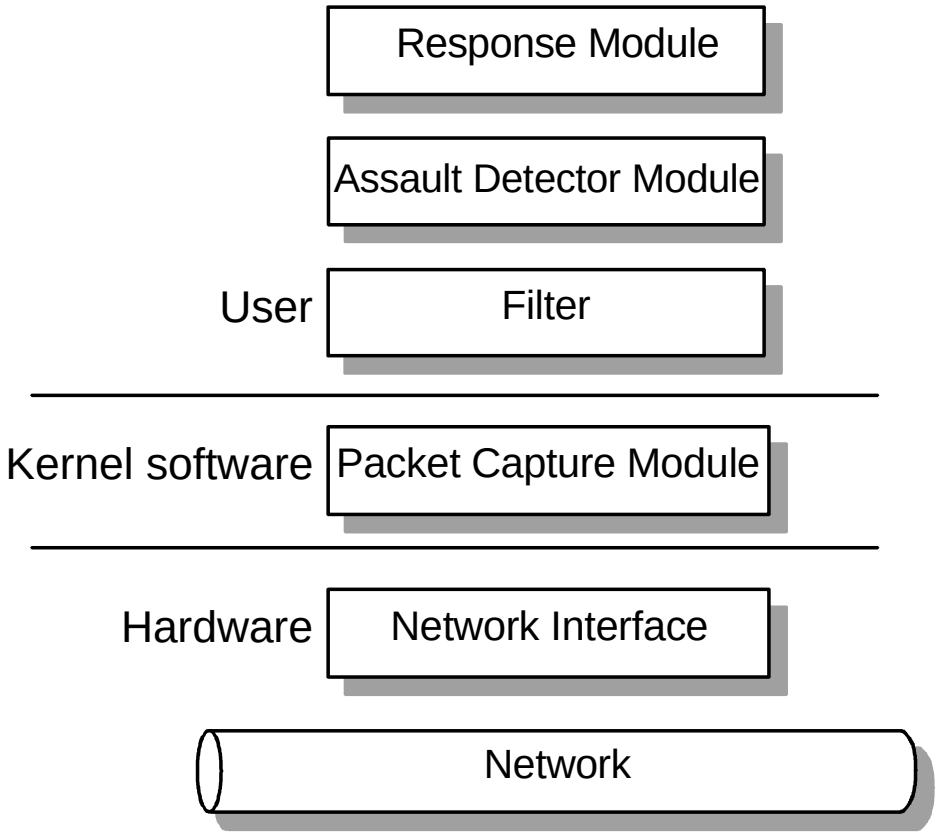
Erkennbare Angriffe

- Netzwerk- und Portscanning
  - Ping-Sweeps
  - ...
- Denial-of-Service-Angriffe (DOS)
  - Fehlerhafte Datenpakete
  - ICMP-, UDP-, TCP-SYN-Flooding
  - ...
- Penetrationsangriffe
  - Bekannte Dienstmissbräuche
  - Unauthorisierte Zugriffsversuche
  - Trojanische Pferde / Backdoors
  - ...

Einbindung von Intrusion Detection-Systemen



Aufbau und Funktionsweise einer Network Engine

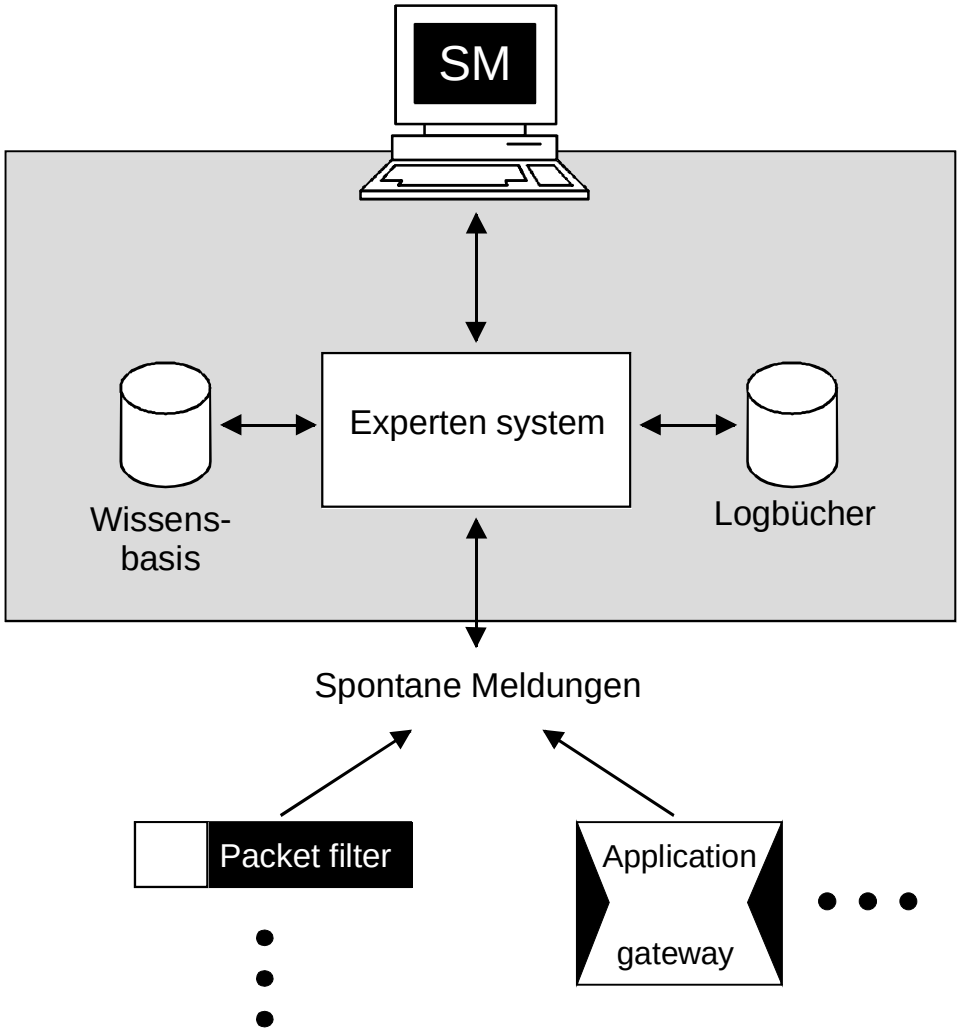


- **Response Modul**
  Gegenmaßnahmen wie »Verbindung blocken« oder »Alarm senden«
- **Angriffsdetektor**
  untersucht den Datenstrom nach bekannten Angriffsmustern (Signaturdatenbank)
- **Filterung**
  Analyse der Pakete
- **Packet Capture Modul**
  organisiert den Transport von Paketen vom Netzwerk zum Analyse Modul.
- **Netzwerkadapter**
  Die Netzwerkadapter werden im Promiscuous Mode betrieben.

Auswertungskonzepte
→ Signaturanalyse (1/3)

- Auf der Grundlage von bekannten und hypothetischen Angriffsszenarien werden **Signaturen für verschiedene Angriffe** erstellt und in einer Datenbank hinterlegt.

- Die Übereinstimmung spezifischer Nutzungsverhalten im Betrieb mit hinterlegten Signaturen deuten auf eine eventuelle **Sicherheitsverletzung** hin.



Auswertungskonzepte
→ Signaturanalyse (2/3)

- **Strategie bei der Bewertung Sicherheitsverletzungen**
  - Wenn ein Benutzer einmal einen Fehler macht, wird dieser als **Versehen** bewertet;
  - Falls der Benutzer zweimal eine falsche Aktion durchführt, wird dies als **unglücklicher Zufall** bewertet;
  - Falls der Benutzer aber dreimal dieselbe falsche Aktion innerhalb eines bestimmten Zeitraumes durchführt, wird diese Ereignisfolge als **Angriff** bewertet, und entsprechende Schritte werden eingeleitet.

Auswertungskonzepte
→ Signaturanalyse (3/3) Beispiele / Firewall-Systemen

- Fehlerhafte Authentikation eines Benutzers mit dem Firewall-System
- Jemand verwendet den Befehl »debug« (SMTP-Proxy)
- Jemand versucht einen Hopping-Angriff (Telnet-Proxy)
- Verwendung des Befehls »del«, obwohl dieser verboten wurde (FTP-Proxy)
- Adressierung eines nicht initialisierten Port des Application Gateway, obwohl dieser im Packet Filter als »nicht erlaubt« definiert ist (Application Gateway bei einer High-level Security Konfiguration)
- Nicht erlaubter Versuch eines Verbindungsaufbaus zu einem Rechnersystem im zu schützenden Netz

Auswertungskonzepte
→ Anomalieerkennung (1/4)

- Das Nutzungsverhalten eines Anwenders bzw. eines Rechners wird über einen bestimmten Zeitraum gemessen.
- Aus den Messdaten werden die Parameter für ein „Normalverhalten“ ermittelt.
- Im Betrieb erfolgt ein Vergleich der aktuellen Messdaten mit denen des „Normalverhaltens“.
- Abweichungen deuten auf eine eventuelle Sicherheitsverletzung hin.

Auswertungskonzepte
→ Anomalieerkennung (2/4)

- Bei diesem Auswertungskonzept sollen über das Erkennen von Anomalien – eine Abweichung vom Normalen – Sicherheitsverletzungen entdeckt werden.

- Dieses Konzept basiert auf der Annahme, dass Sicherheitsverletzungen anhand gravierender Verhaltensabweichungen erkannt werden können.

- Solche Verhaltensabweichungen werden auf
  - einzelne Benutzer,
  - auf einzelne Programme,
  - auf bestimmte Dienste oder auch
  - auf Kommunikationsabläufe bezogen erkannt.

Auswertungskonzepte
→ Anomalieerkennung (3/4)

- Grundlage der Anomalie-Erkennung ist die Beschreibung des »normalen«, für einen Aspekt typischen, regulären Verhaltens in sogenannten Referenzprofilen.
- Diese Referenzprofile sind charakteristische Verhaltensmuster, die anhand von objektiv überprüfbaren Merkmalen beschrieben werden.
- Diese Merkmale können dann entweder
  - mit Hilfe von Statistiken über das tägliche Verhalten oder
  - aufgrund individueller Erfahrungswerte ausgewählt werden

Auswertungskonzepte
→ Anomalieerkennung (4/4) Beispiele / Firewall-Systemen

- Überdurchschnittliche Fehlerrate bei der Identifikation und Authentikation
- Art und Umfang der Inanspruchnahme von Diensten (FTP, Telnet, SMTP, HTTP, ...)
- Überdurchschnittliche lange Zeit, die Benutzer über das Firewall-System arbeiten
- Außergewöhnliche Zeiten, Wochentage, wann und wie über das Firewall-System kommuniziert wird
- Überdurchschnittlich häufiges Auftreten von sicherheitsrelevanten Ereignissen
- Verstoß gegen das Regelwerk
- Angriffsversuche auf das Firewall-System
- Fehlverhalten der Firewall-Software und -Hardware

Vergleich der verschiedenen Auswertungskonzepte (1/2)

Erkennen von bekannten sicherheitsrelevanten Aktionen (Signaturen)

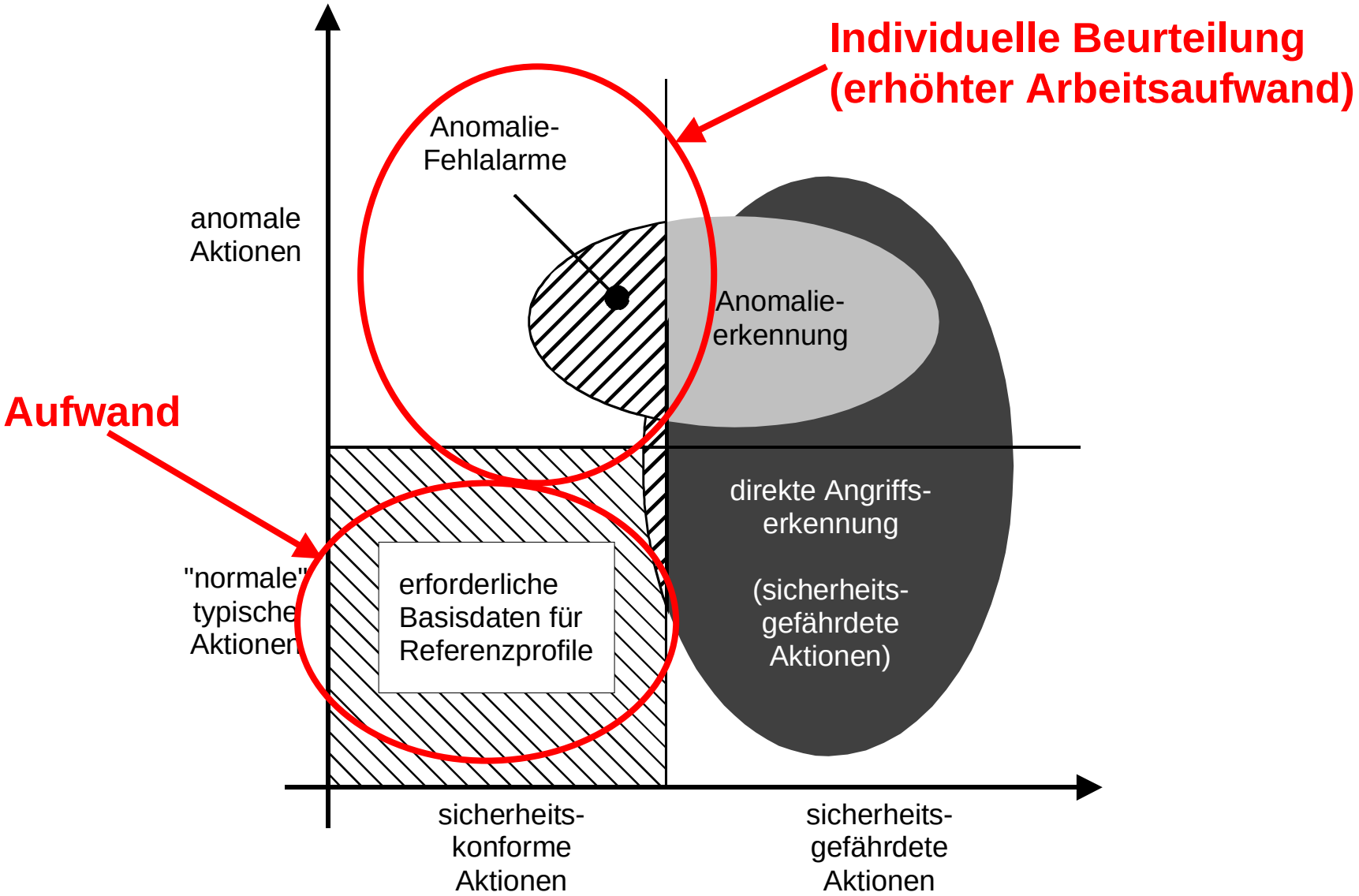
- Beim Auswertungskonzept »Erkennen von bekannten sicherheitsrelevanten Aktionen« erhält man als Ergebnis klare Aussagen darüber, ob und welche Sicherheitsverletzung auftrat und erkannt wurde.
- Daraufhin können definierte Reaktionen eingeleitet werden.

Vergleich der verschiedenen Auswertungskonzepte (2/2)

Erkennen von Anomalien

- Das Auswertungskonzept »Erkennen von Anomalien« hat den großen Vorteil, dass es durch die Art der Analyse von Protokolldaten der Logbücher gelingen kann, auch bislang unbekannte Sicherheitsverletzungen aufzuspüren, die von der direkten Angriffserkennung als solche nicht klassifiziert werden konnten.
- Damit kann dem Problem vorgebeugt werden, dass es sehr schwierig sein wird, ständig Informationen über neueste, hochaktuelle Angriffszenarien in Erfahrung zu bringen, diese zu analysieren, und für die direkte Angriffserkennung zu modellieren und in der Wissensbasis festzuhalten.
- Ein Nachteil dieses Auswertungskonzeptes ist, dass auch Fehlalarme generiert werden.

Vergleich der verschiedenen Auswerteskonzepte



Probleme von Intrusion Detection Systeme (IDS)

- **IDS Lösungen liefern**
  - ungenaue Daten
  - sehr viel davon
  - und auch viele „False Positve“

- **IDS ist ein Überwachungssystem, welches viel Manpower benötigt**
  - möglichst ständig
  - zur Analyse zweifelhafter Events
  - anspruchsvolle Tätigkeit

Zusammenfassung
→ Intrusion Detection

- IDS bieten keine hundertprozentige Sicherheit
- Zu jedem Verfahren zur ID sind (zumindest theoretisch) raffinierte Angriffsszenarien denkbar, die vom IDS nicht entdeckt werden können.
- Angriffe, die im statistischen Grundrauschen des IDS untergehen, wie etwa der sogenannte slow-scan, ein Portscan, der sich über Wochen und Monate erstreckt.
- Beimischung von deformierten Netzwerkpaketen in den Angriff. Diese Pakete stören die Mustererkennung des IDS und werden im günstigen Fall vom angegriffenen Zielsystem weggeworfen, so dass sich wieder der ursprüngliche Angriff ergibt.
- Manipulation der Anomalieentdeckung durch langsame Verschiebung der Profile, der Selbstlernmechanismus vieler IDS (neuronale Netze!) unterstützt dieses Vorgehen.

Intrusion Detection Systeme

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen