Aspekte der Einführung eines IDS/IPS Systems

Dr. Alexander Schinner, GCIA, GCFA

Aspekte der Einführung eines IDS/IPS Systems
Agenda

- Kurze Einführung in die Technik
  - IDS
  - IPS
- Phasen der Einführung
  - Bedarfsfeststellung
  - Anforderungsanalyse
  - Entscheidungsvorlage
  - Produktauswahl
  - Integration
  - Betrieb
  - Revision

Aspekte der Einführung eines IDS/IPS Systems
Ziele

- Es sollen neben Gartners „IDS ist tot“ und den euphorischen Werbeaussagen der Hersteller einige neutrale Aspekte dargestellt werden.
- Es sollen einige kritische Fragen beschrieben werden, mit der man die Einführung eines IDS begleiten kann.

Kurze Einführung in die Technik
Intrusion Detection Systeme

- Intrusion Detection
  - Ziel: Erkennen von Angriffen und Missbrauch
  - Aktive Überwachung von Computern oder Netzen
  - Geeignete Werkzeuge
- Intrusion Detection Systeme
  - Sensoren
  - Datenbankkomponente
  - Managementstation
  - Auswertungsstation

Kurze Einführung in die Technik
Netzbasierte Sensoren

Überwachung des Netzwerkverkehrs eines Rechners oder eines Teilnetzes

Vorteile

- Hosts bleiben unberührt
- Betriebssystemunabhängig
- Erkennen von Angriffen gegen
  - große Gruppen
  - nicht existente Ziele
- „Unsichtbar“ für Angreifer
- Möglichkeit eines separaten IDS-Netzwerks

Nachteile

- Evtl. Mangelnde Performance
- Abgriff des Netzwerkverkehrs ist nicht trivial
- Wenig Information über Reaktionen des Angriffsziels
- Probleme mit Verschlüsselung
- Angriffserkennung ist nicht exakt

Kurze Einführung in die Technik
Hostbasierte Sensoren

Überwachung des Verhaltens eines Systems (Logmeldungen, Systemcalls, Netzwerkverkehr, Useraktionen, etc.)

Vorteile

- Applikationsspezifisch
- Information über Reaktionen des Angriffsziels
- Fehlverhalten kann Nutzern zugeordnet werden
- Veränderungen am System können erkannt werden

Nachteile

- Für jeden Host notwendig
- Betriebssystemspezifisch
- Applikationsspezifisch
- Nicht unsichtbar
- Belastung des Systems
- Angriffserkennung ist nicht exakt
- Schlechte Frühwarnfunktion

Kurze Einführung in die Technik
Datenbankkomponente

- Speicherung von Ereignisdaten
- Notwendige Eigenschaften
  - Vollständige Speicherung der Ereignisse
  - Große Datenmengen
  - Möglichkeiten zur Archivierung

- Besteht die Möglichkeit zur Nutzung der firmeneigenen Datenbank?
- Wird Zugriff auf das Datenbankschema gewährt?
- Performance? Stichwort DoS

Kurze Einführung in die Technik
Managementstation

- Verwaltung der IDS-Komponenten
- Verwaltung von Netzwerkparametern
- Erstellung und Anpassung von Regeln
- Erstellen von Policies, Gruppen, etc
- Erstellen von Signaturen
- Backupmöglichkeiten

- Wie sieht die Grundkonfiguration eines Sensors aus?
- Lassen Sie sich komplexe Aktionen erklären, wie z.B.
  - Neue IP-Adressen für Sensoren, Hosts oder Managementstation
  - Hardwareaustausch von Komponenten
- Lassen Sie sich die Erstellung einer komplexen Signatur zeigen

Kurze Einführung in die Technik
Auswertungsstation

- Anzeigen eingehender Meldungen
- Sortierung der Ereignisse
- Klassifikation der Ereignisse
- Ablage für spätere Weiterverarbeitung
- Erstellung von Reports

- Wie ist die Oberfläche realisiert?
- Lässt die Oberfläche den Export von Ereignissen zu?
- Kann man nach allen Kriterien suchen?
- Zusammenarbeit mit der Managementstation?
- Unbedingt eine Teststellung verlangen und damit spielen!
- Gibt es Verweise auf weiterführende Informationen? CVE?
- Gibt es Hinweise auf Gegenmaßnahmen?
- Erstellen eigener Reports?

Kurze Einführung in die Technik
Erkennungsmethoden

- Anomalieanalyse
  - Protokollanalyse
  - Signaturbasierte Analyse
  - Statistische Analyse
  - KI
  - Heuristische Methoden
- Korrelation von Ereignisdaten

- Welche Protokolle kennt das IDS?
- Welche Signaturen gibt es? Qualität?
- Wie oft, und wie schnell gibt es neue Signaturen?
- Gibt es Lernfristen für statistische Analysen? Adaptive Anpassung? Arbeitsintervall?
- Welche Korrelationen werden bestimmt?

Kurze Einführung in die Technik
Sicherheitsaspekte

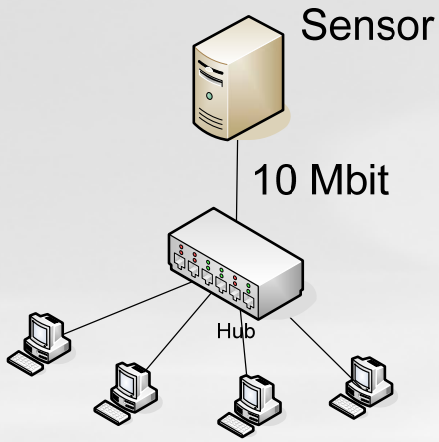
- Netzbasierte Sensoren
  - Hardwareanforderungen (auch zukünftige Entwicklung)
  - Überwachung der Sensoren
  - Bestimmung der Auslastung, Paketverlust
- Hostbasierte Sensoren
  - Was passiert bei Updates, Patches oder neuen Applikationen?
  - Überwachung der Sensoren
  - Wie lassen sich die Sensoren updaten?
- Allgemein
  - Gibt es die Möglichkeit für separate IDS-Netzwerke?
  - Wird die Kommunikation verschlüsselt?
  - Nachvollziehbarkeit des Zugriffs auf die Komponenten?
  - Zugriffskontrolle auf Management-/Auswertestation

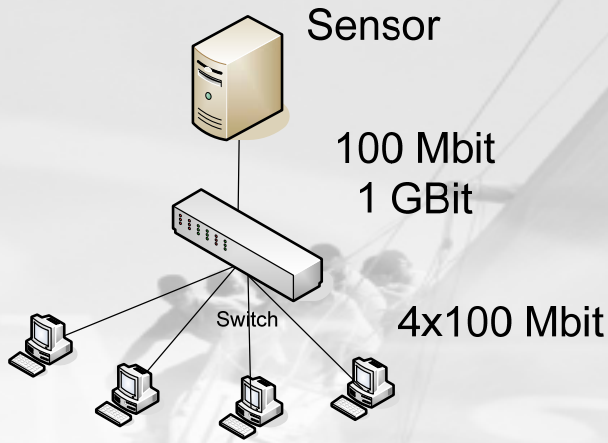
Kurze Einführung in die Technik
Abgreifmethoden im Netzwerk

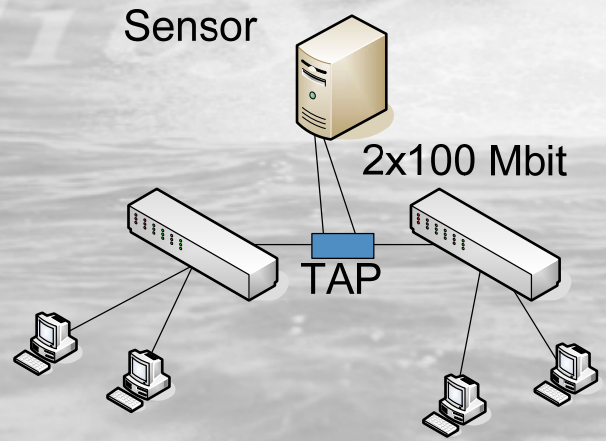
- Hub
  - Veraltet, unsicher, unbrauchbar
- Span- bzw. Mirrorport am Switch
  - Zusätzliche Last
  - Kann nicht den gesamten Verkehr erfassen
- TAP
  - Abgreifpunkte sind schwerer zu identifizieren
  - Sicherer Abgriff

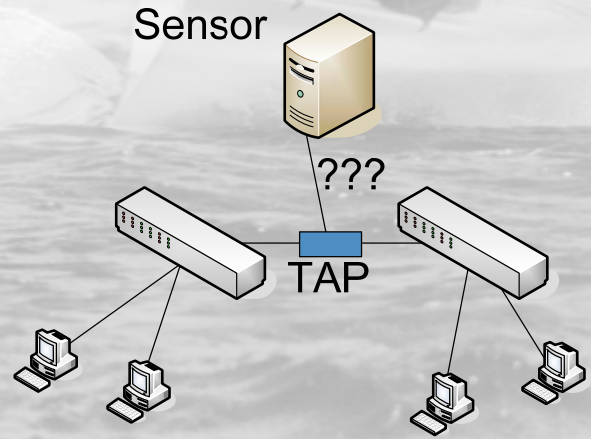
- Lassen sie den Berater die Abgreifmethoden erklären!
- Wenn er „Aggregating Taps“ ohne große Einschränkung empfiehlt, werden Sie misstrauisch!
- Wenn er Hubs empfiehlt,...☠

Kurze Einführung in die Technik
Abgreifmethoden im Netzwerk









Kurze Einführung in die Technik
Intrusion Prevention Systeme

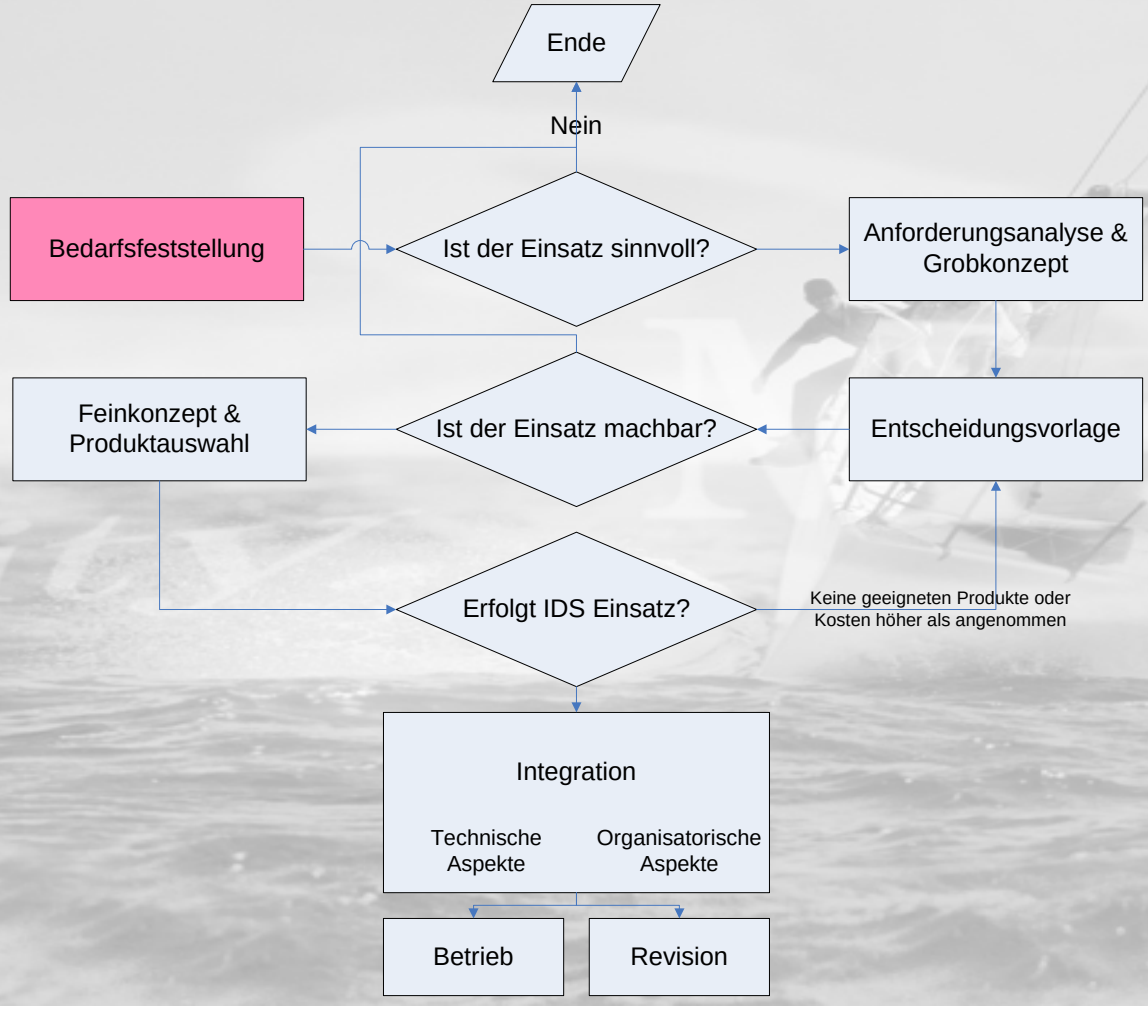
- Erkennungsmethoden ähnlich den IDS
- Blockierung gefährlicher Aktionen
  - Hostbasiert
  - Blockieren von Netzwerkpaketen (arbeiten als Bridge)
  - Rekonfiguration von Firewalls ☠
  - Senden von RST-Paketen ☠ ☠ ☠

- Wie werden Angriffe blockiert?
- Welche Reaktionszeiten hat das System?
- Lassen sie den Berater die Probleme bei Fehlalarmen erklären!
- Was passiert beim Ausfall von netzwerkbasierten IPS Sensoren?

Keine kurze Einführung in die Technik
Was ist ein IDS nicht?

- Low-maintenance
- Ein Ersatz für
  - Netzwerk Monitoring
  - Logging
  - Firewalls
- IPS ist keine Verteidigung gegen alle unbekannten Angriffe
- so was ähnliches wie ein Virenscanner
- einmal installiert und läuft dann ewig
- wartungsarm
- unbedingt notwendig

Phasen der Einführung
Bedarfsfeststellung



Phasen der Einführung
Bedarfsfeststellung

Ist der Einsatz eines IDS zur ergänzenden Absicherung sinnvoll?

Empfohlenes Vorgehen

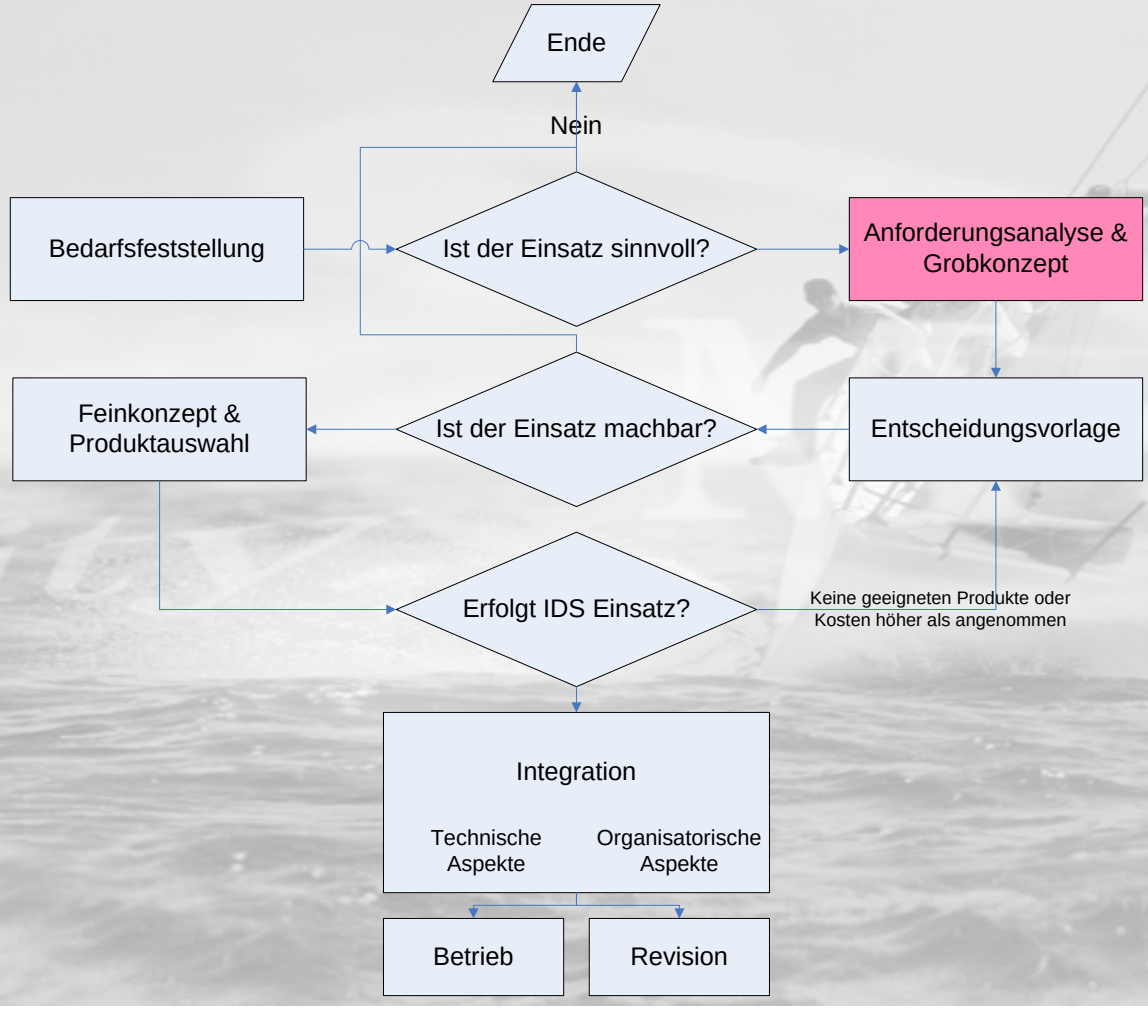
- Ist-Aufnahme von IDS relevanten Faktoren
  - Risikobereitschaft und Risk-Management der Organisation
  - Infrastruktur und Schutzmaßnahmen der Organisation
  - Organisation und Infrastruktur am Netzübergang
  - Art und Anwendung der angebotenen Kommunikationsdienste
- Ermitteln, ob der Einsatz grundsätzlich sinnvoll ist
  - Ergibt sich ein Zusatznutzen?
  - Ist ein höherer Nutzen mit vergleichbarem Aufwand durch andere Maßnahmen erzielbar?

Phasen der Einführung
Bedarfsfeststellung

- Sensibilisierung der Entscheider
  - Management
  - Systemadministration und –betrieb
  - Revision
  - Datenschutzbeauftragter
  - Personalvertretung
- Bereitstellung von Ressourcen zur Erstellung einer Entscheidungsvorlage

- „Das können die Firewalljungs ja noch nebenbei machen“ ist ein KO-Kriterium

Phasen der Einführung
Anforderungsanalyse & Grobkonzept



Phasen der Einführung
Grobkonzept und Anforderungsanalyse

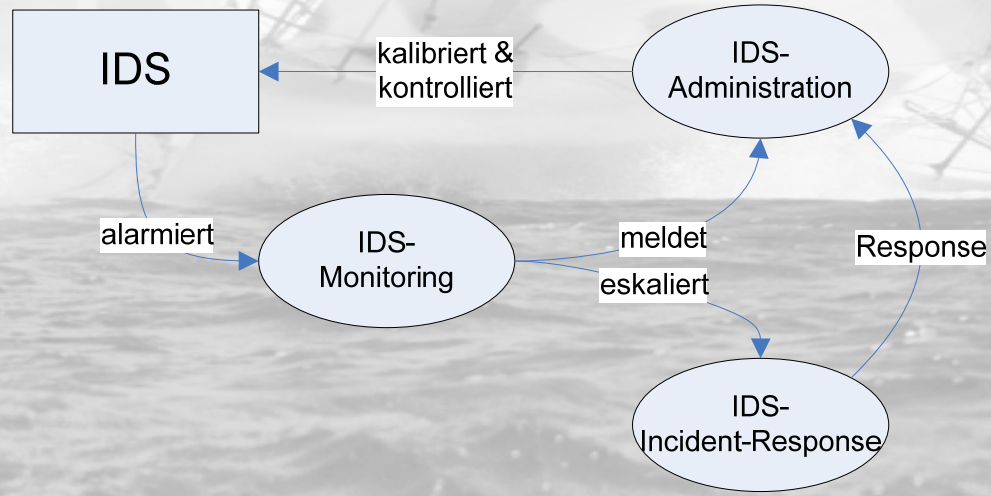
In welcher Weise ist das IDS in die technisch-organisatorische Umgebung integrierbar und welche Anforderungen muss es erfüllen, um die Zielsetzungen zu erreichen?

Empfohlenes Vorgehen

- Ist-Aufnahme der technischen Infrastruktur
  - Ziel ist die Sensorplatzierung
  - Netzwerkdiagramm
- Ist-Aufnahme der bestehenden Incident-Response-Organisation
  - Wie ist die Vorgehensweise zur Verfolgung von Sicherheitsvorfällen?
  - Gibt es ein System-Management, das Serverausfälle erkennt?
  - Gibt es eine zentrale Stelle, bei der Probleme und Alarme auflaufen?

Phasen der Einführung
Grobkonzept und Anforderungsanalyse

- Konkretisierung der Ziele des IDS-Einsatzes
- Anforderungsanalyse
  - Basis sind die Ist-Analyse und die Zielsetzungen
  - Festlegung der Gewichte
  - Ableitung der Anforderungen
  - Dokumentation der Anforderungen
- Festlegung einer geeigneten Organisation
  - IDS-Manager
  - IDS-Administration
  - IDS-Monitoring
  - Incident-Response

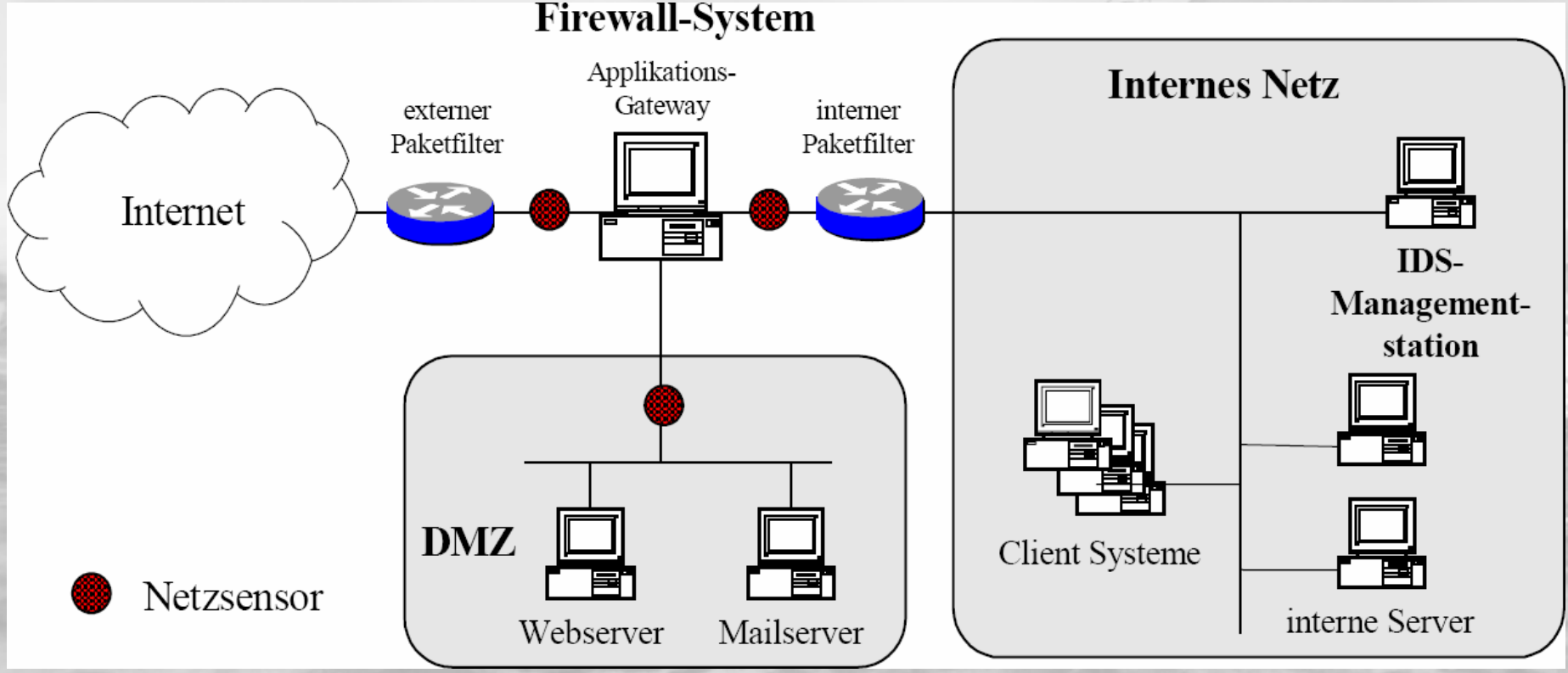


Phasen der Einführung
Grobkonzept und Anforderungsanalyse

- Platzierung der Management- und Auswertungsstation
  - Kommunikationswege berücksichtigen (Sensoren, Management, Updates vom Hersteller, Alarmierungen)
  - Zum Teil abhängig vom Hersteller
- Dokumentation der Ergebnisse

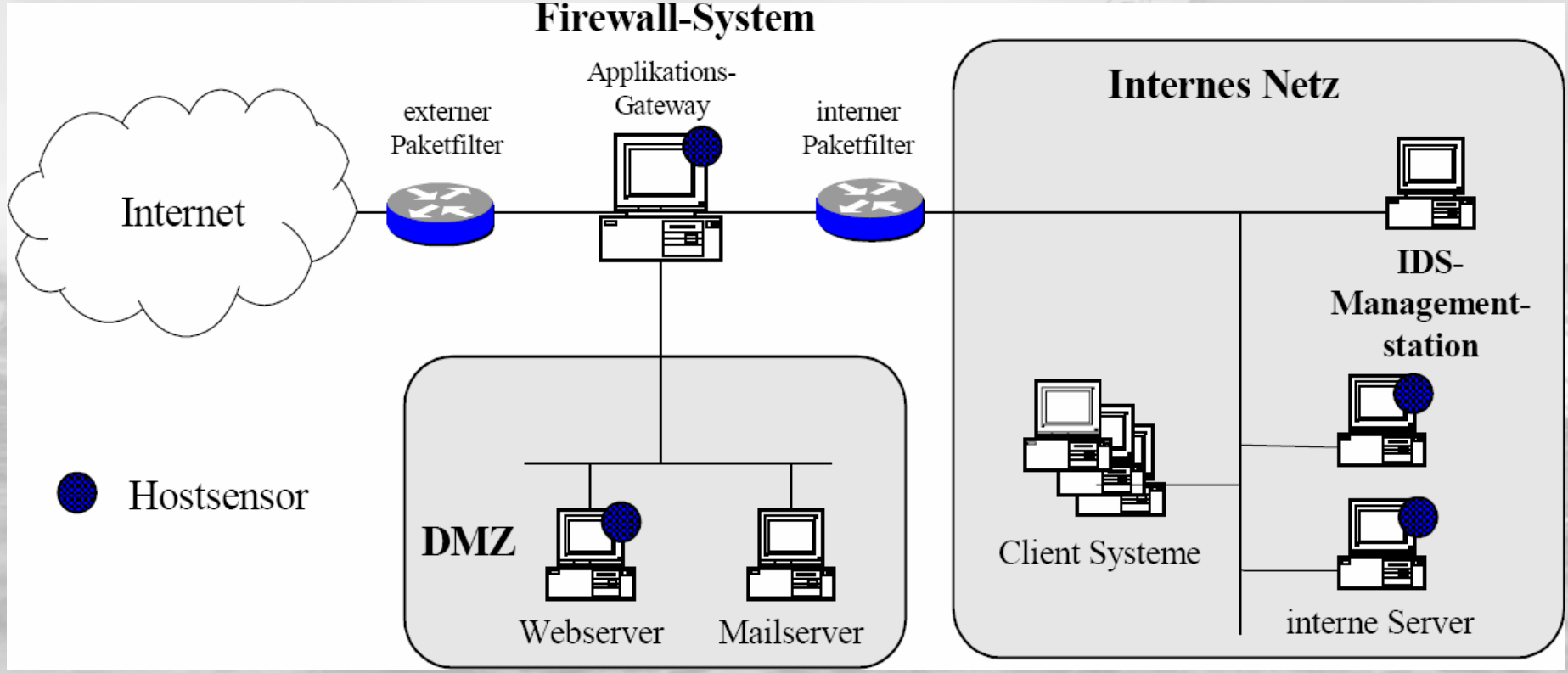
Phasen der Einführung
Sensorplatzierung

Absicherung von Netzübergängen



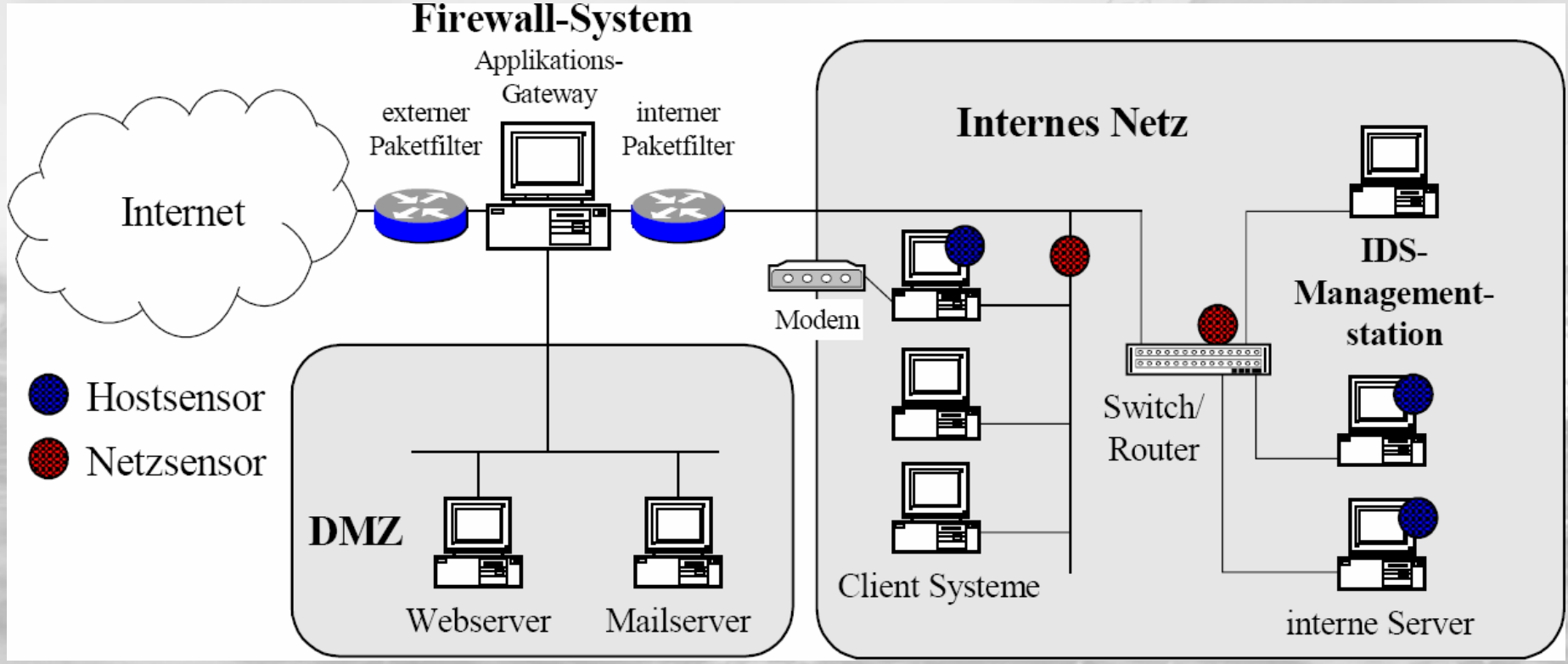
Phasen der Einführung
Sensorplatzierung

Überwachung spezifischer Systeme und Anwendungen

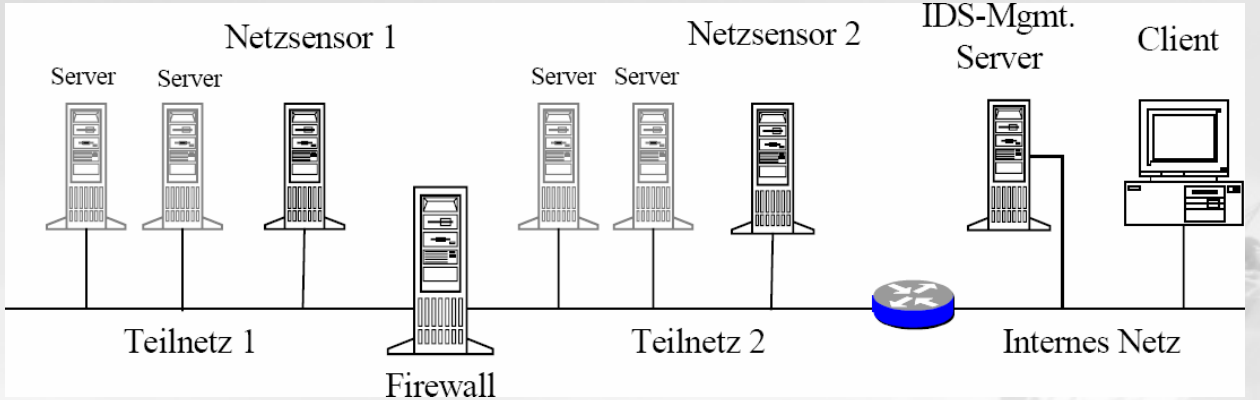


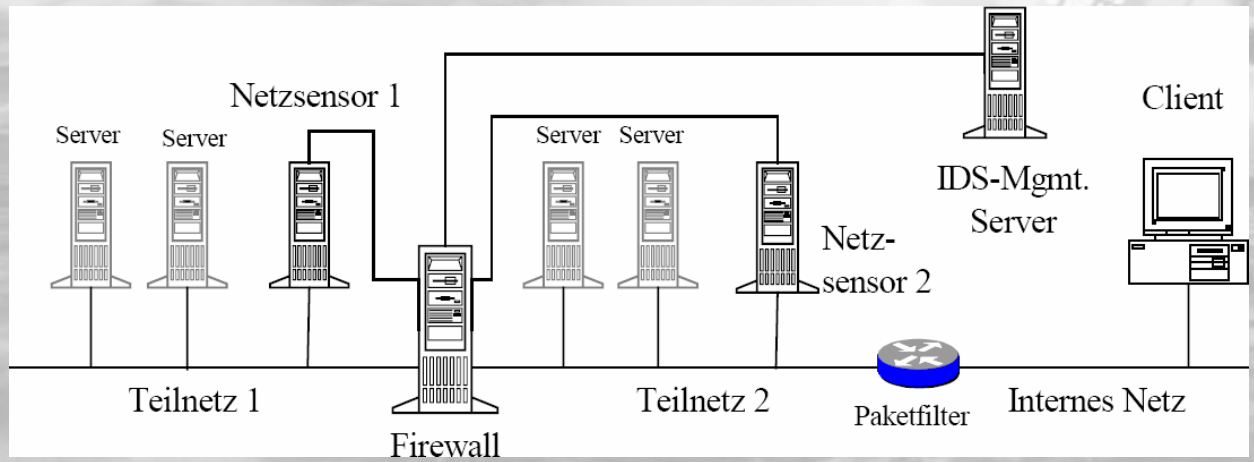
Phasen der Einführung
Sensorplatzierung

Überwachung interner Netze



Phasen der Einführung
Kommunikation zwischen IDS-Komponenten

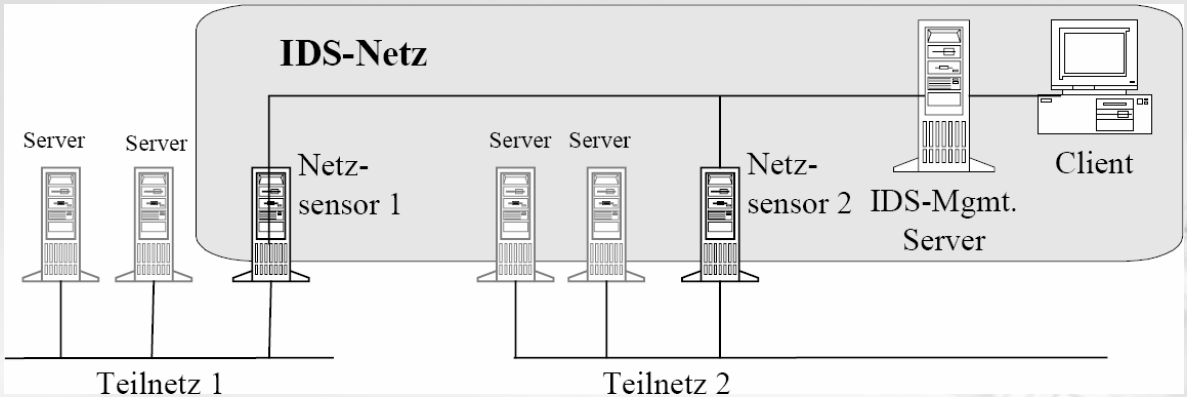


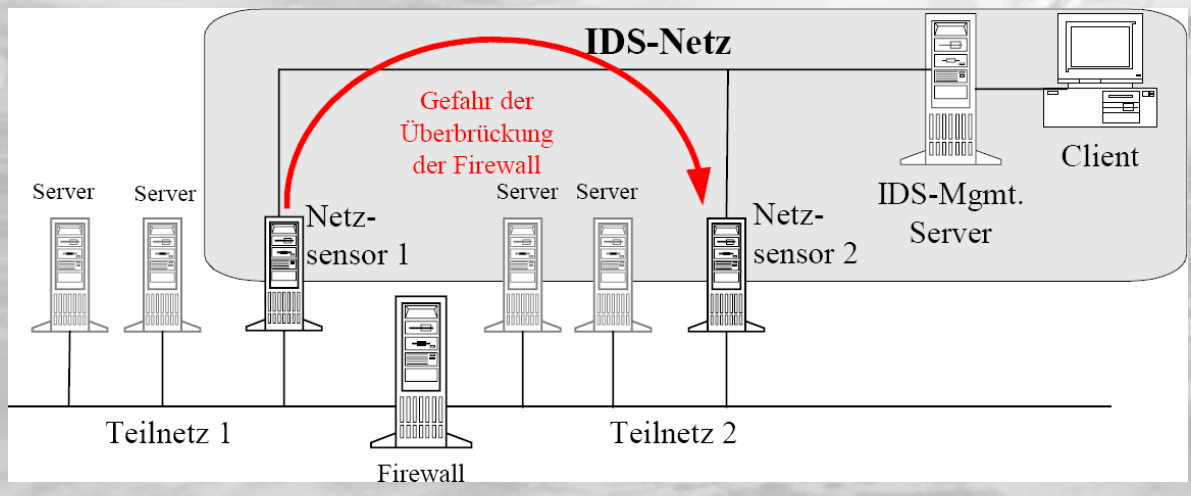


Problem

- Komponenten sind identifizierbar
- IDS angreifbar
- IDS-Traffic analysierbar

Phasen der Einführung
Kommunikation zwischen IDS-Komponenten





Vorteile

- IDS ist unsichtbar
- IDS ist schwer angreifbar

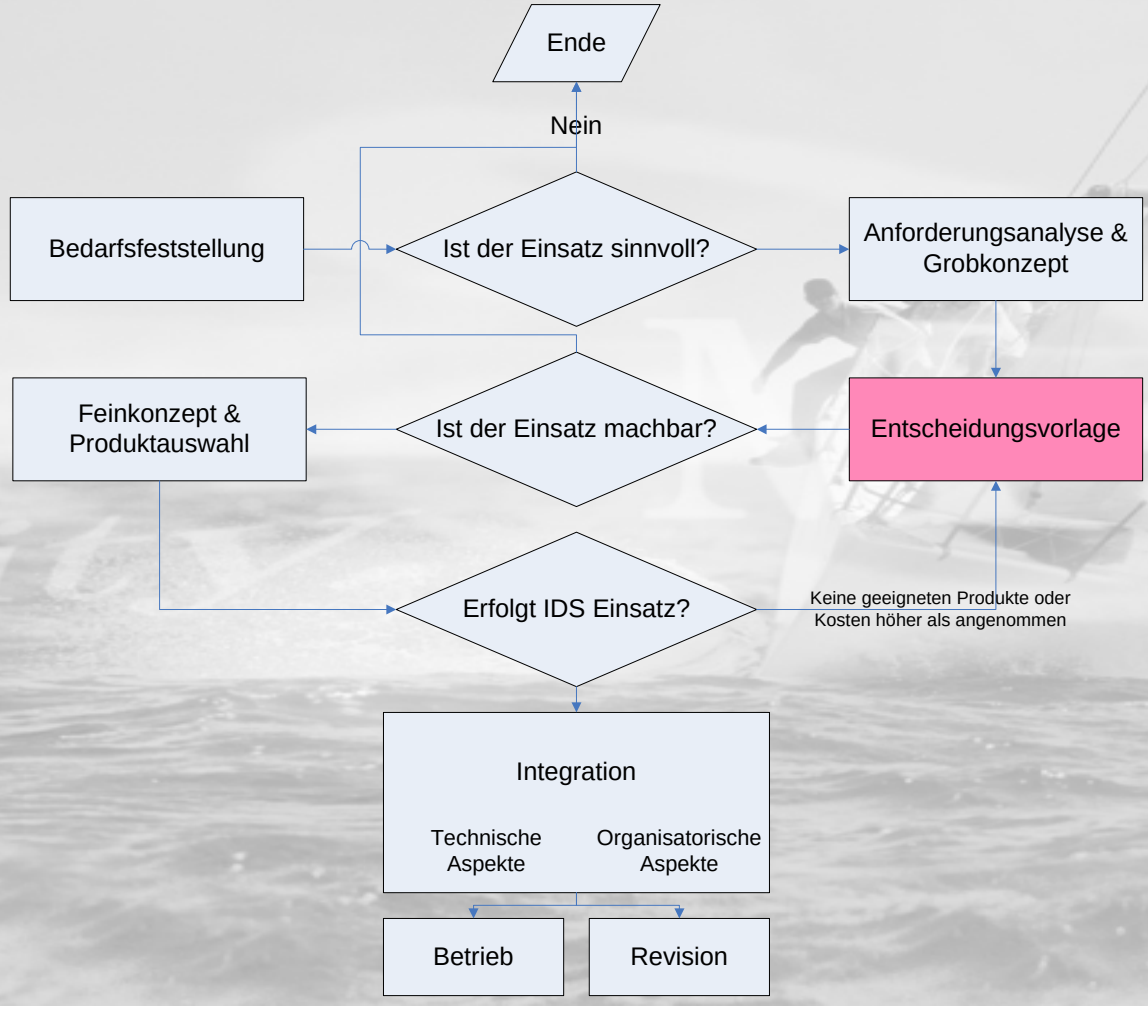
Nachteile

- Bypass der Firewall

Lösung

- Einsatz von Taps

Phasen der Einführung
Entscheidungsvorlage



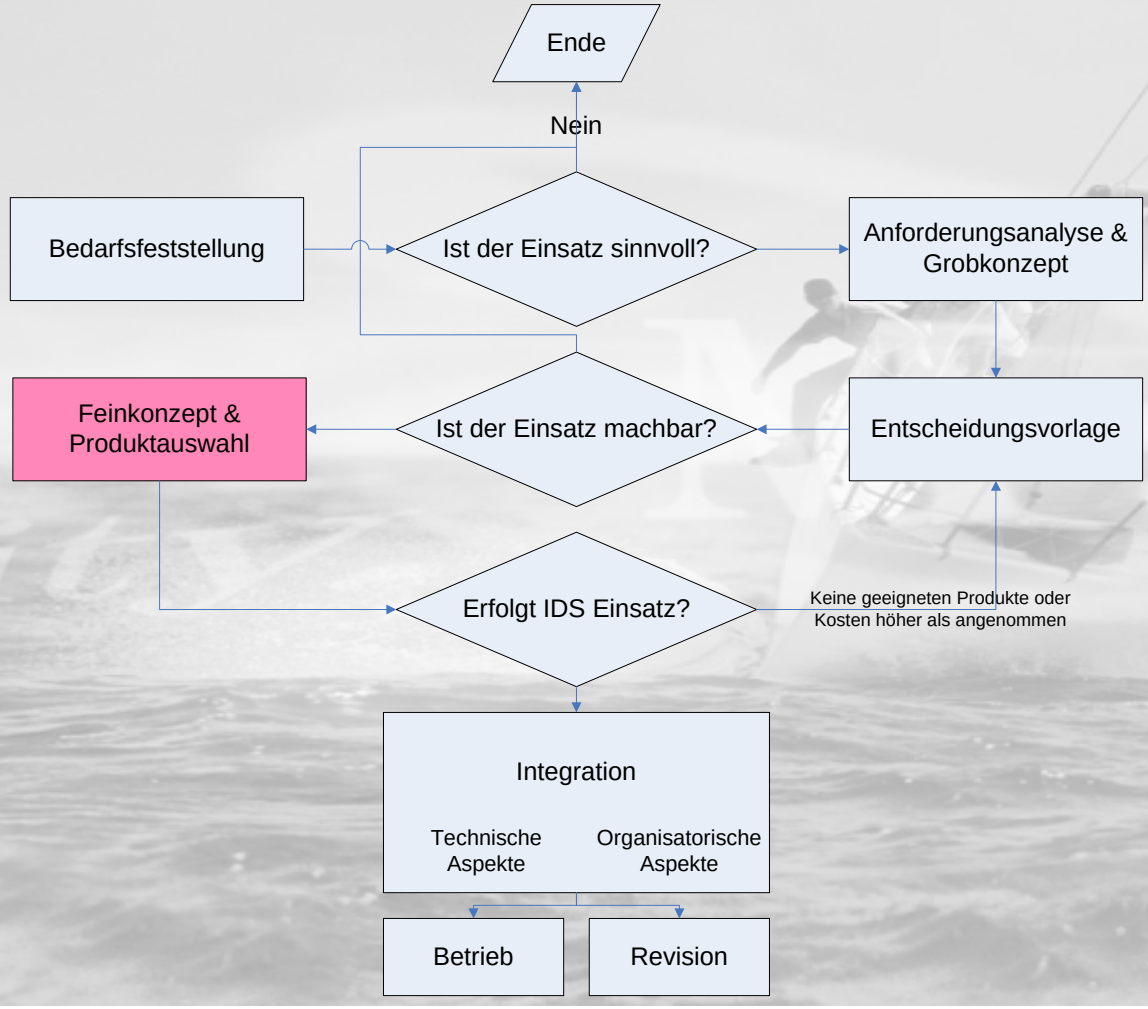
Phasen der Einführung
Entscheidungsvorlage

Verifikation der Machbarkeit des IDS-Einsatzes und Abschätzung des finanziellen und personellen Aufwands.

Empfohlenes Vorgehen

- Marktsichtung
  - Erfüllung der definierten Anforderungen
  - Preise der Komponenten, Wartungskosten, Kosten für Installation, Schulung, laufende Kosten
- Darstellung der Lösungsansätze
- Erstellung der Entscheidungsvorlage für das Management

Phasen der Einführung
Feinkonzept & Produktauswahl



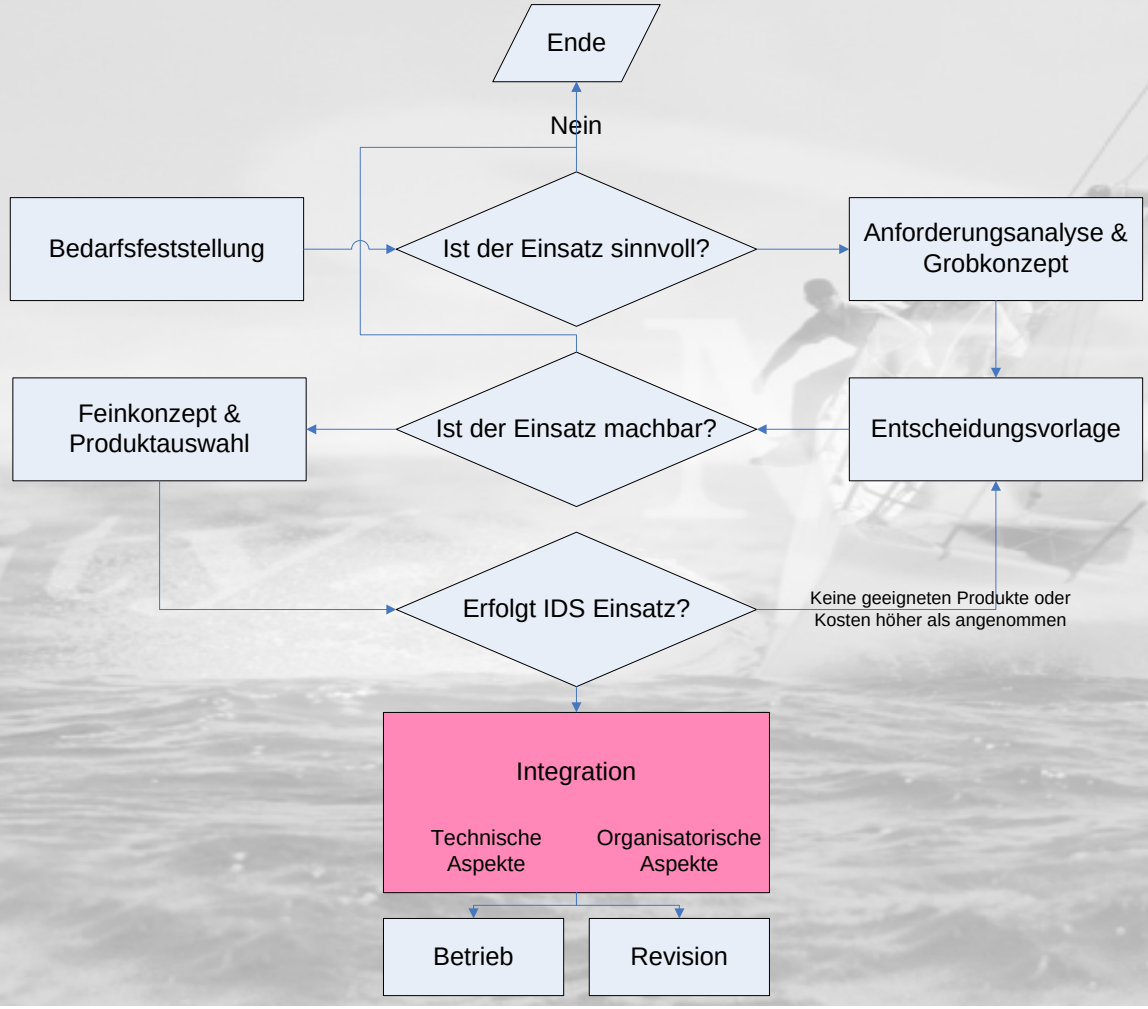
Phasen der Einführung
Feinkonzept und Produktauswahl

Festlegung der Einzelheiten zum IDS-Einsatz.

Empfohlenes Vorgehen

- Feinkonzept (unabhängig vom gewählten Produkt)
  - Ggf. Änderungen in der Infrastruktur; neue Infrastruktur
  - Endgültige Festlegung der Abgriffpunkte
  - Festlegung der Zuständigkeiten
- Produktauswahl
- Beschaffung

Phasen der Einführung
Integration



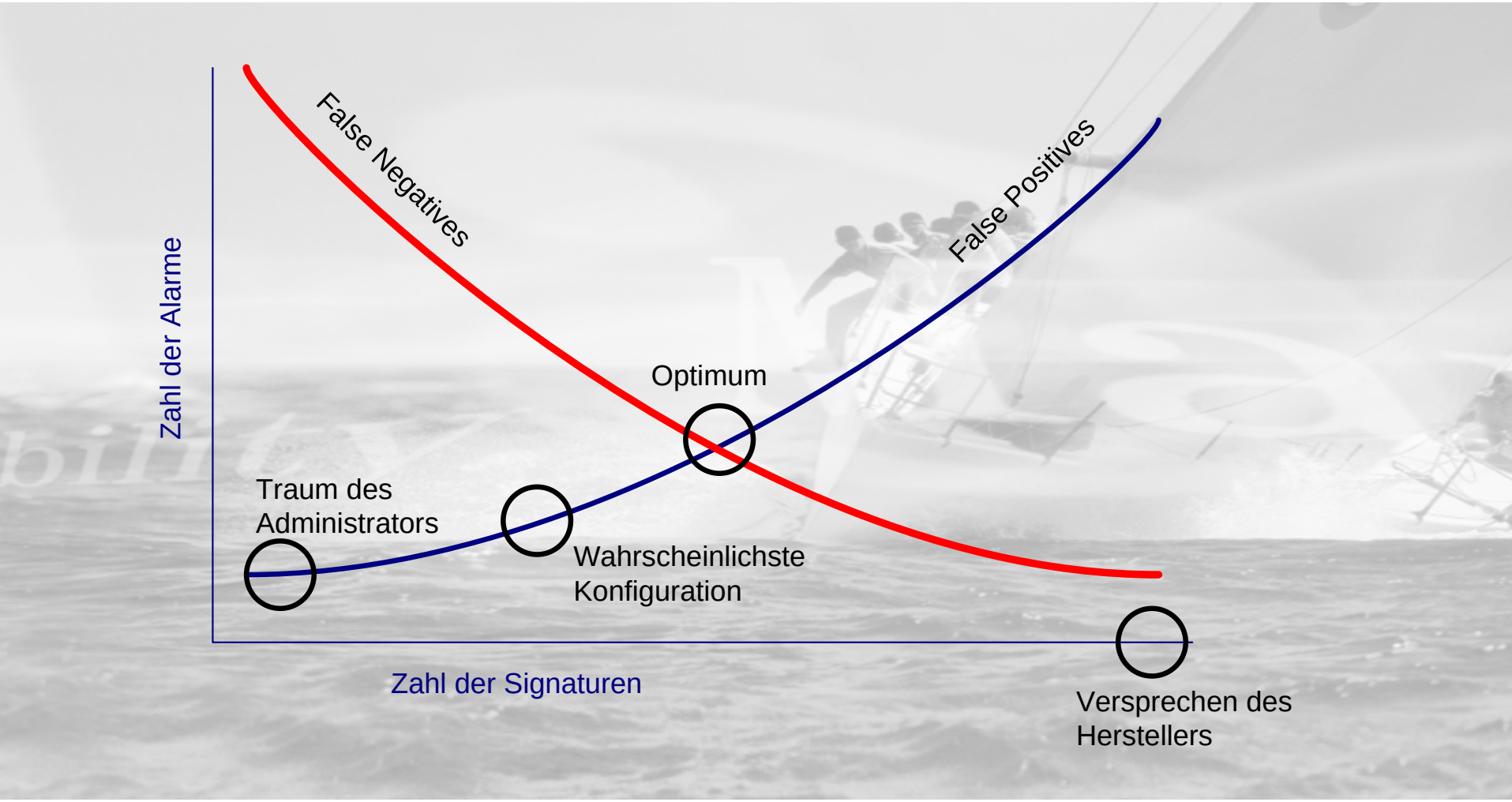
Phasen der Einführung
Integration

- Vorbereitung der technischen Infrastruktur auf die Integration
- Integration und Inbetriebnahme des IDS
- Kalibrierung der Sensoren
- Aufnahme der Überwachungsziele in den Sicherheitsstandard
- Zuweisung der IDS-Funktionen an die Organisationseinheiten
- Festlegung der Eskalation bei IDS-Alarmen
- Schulung der IDS-Funktionsträger
- Vereinbarungen über den IDS-Betrieb mit dem Betriebs- bzw. Personalrat
- Integration in das Change-Management
- Festlegung von Verfahrensweisen zur Prüfung der Funktionsfähigkeit der Sensoren
- Und so weiter und so fort...

Phasen der Einführung
Kalibrierung der Sensoren

- Basiskalibrierung
  - Findet statt im Rahmen der Installation
  - Unnötige Signaturen deaktivieren
  - Fehlalarme reduzieren
- Verfeinerung der Kalibrierung
  - Ist ein laufender Prozess
  - Erstellen neuer Signaturen
  - Verändern existierender Signaturen
  - Nehmen Sie einen Berater des Herstellers dazu!

Phasen der Einführung
Kalibrierung der Sensoren



Phasen der Einführung
Schulung

- Schulung beim Hersteller
- Allg. Schulung zum Thema IDS (z.B. SANS)
- Am Anfang gelegentlich einen Berater des Herstellers/Resellers hinzuziehen

Warum?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
(msg:"FTP CWD overflow attempt";
flow:to_server,established; content:"CWD";
nocase; isdataat:100,relative;
pcre:"/^CWD\s[^\n]{100}/smi"; sid:1919;
rev:19;)
```

Phasen der Einführung
Schulung – Warum?

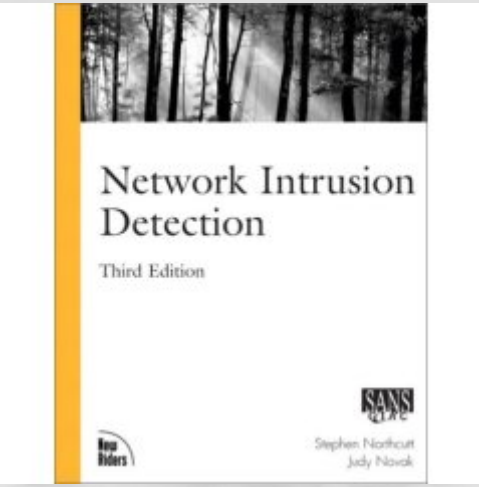
```
03:09:06.526507 00:03:e3:d9:26:c0 > 00:00:0c:04:b2:33, ethertype IPv4 (0x0800),
 length 574: IP (tos 0x0, ttl 45, id 55450, offset 0, flags [DF], length: 560,
 bad cksum 9bb8 (->516e)!) 195.232.55.6.1701 > 207.166.87.42.21: P
[bad tcp cksum 7135 (->25e2)!] 2184450005:2184450513(508) ack 1127458918 win
5840 <nop,nop,timestamp 1040178 3948516>

0x0000: 0000 0c04 b233 0003 e3d9 26c0 0800 4500 .....3....&...E.
0x0010: 0230 d89a 4000 2d06 9bb8 c3e8 3706 cfa6 .0..@.-.....7...
0x0020: 572a 06a5 0015 8234 0fd5 4333 a866 8018 W*.....4..C3.f..
0x0030: 16d0 7135 0000 0101 080a 000f df32 003c ..q5.........2.<
0x0040: 3fe4 4357 4420 3030 3030 3030 3030 3030 ?.CWD.0000000000
0x0050: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
[…]
0x0120: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
0x0130: 3030 3030 3030 3030 3030 3030 3030 3030 0000000000000000
0x0140: 3030 3030 3030 f0fc 4031 0708 985f 0808 000000..@1..._..
0x0150: eb0c eb0c eb0c eb0c eb0c eb0c eb0c eb0c ................
[…]
0x01e0: eb0c eb0c eb0c eb0c eb0c eb0c eb0c eb0c ................
0x01f0: eb0c eb0c eb0c 9090 9090 9090 9090 9090 ................
0x0200: 9090 31db 43b8 0b74 510b 2d01 0101 0150 ..1.C..tQ.-....P
0x0210: 89e1 6a04 5889 c2cd 80eb 0e31 dbf7 e3fe ..j.X......1....
0x0220: ca59 6a03 58cd 80eb 05e8 ed0a ca59 6a03 .Yj.X........Yj.
0x0230: 58cd 80eb 05e8 edff ffff ffff ff0a uX..............
```

Phasen der Einführung
Schulung –Warum?

```
00000000: 31DB xor bx,bx
00000002: 43 inc bx
00000003: B80B74 mov ax,740B
00000006: 51 push cx
00000007: 0B2D or bp,[di]
00000009: 0101 add [bx+di],ax
0000000B: 0101 add [bx+di],ax
0000000D: 50 push ax
0000000E: 89E1 mov cx,sp
00000010: 6A04 push (w) +04
00000012: 58 pop ax
00000013: 89C2 mov dx,ax
00000015: CD80 int 80
00000017: EB0E jmps
          file:00000027
00000019: 31DB xor bx,bx
0000001B: F7E3 mul (w) bx
0000001D: FECA dec dl
0000001F: 59 pop cx
00000020: 6A03 push (w) +03
00000022: 58 pop ax
00000023: CD80 int 80
00000025: EB05 jmps file:0000002C
00000027: E8ED0A calln +0AED
0000002A: CA596A retf 6A59
0000002D: 0358CD add bx,[bx+si-
33]
00000030: 80EB05 sub bl,+05
00000033: E8EDFF calln
file:00000023
00000036: FFFF ??? (w) di
00000038: FFFF ??? (w) di
0000003A: FF0A dec [bp+si]
```

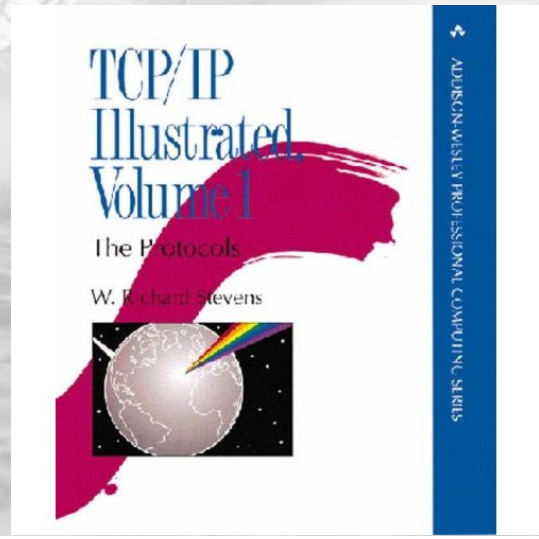
Dies ist Shellcode des TESO 7350wurm.c Exploits.

Phasen der Einführung
Schulung –Bücher



Network Intrusion Detection (New Riders)
Stephen Northcutt, Judy Novak

TCP/IP Illustrated I. The Protocols
(Addison-Wesley)
W. R. Stevens



Phasen der Einführung
Zusammenfassung

- Ein IDS kann eine sehr gute Ergänzung der bestehenden Sicherheitsinfrastruktur darstellen
- Ein IDS ist wesentlich komplexer im Management und Betrieb als eine Firewall
- Ein IPS braucht sehr lange, bis man es wirklich produktiv nehmen sollte
- Ein gut gepflegtes IDS in den Händen von gut geschulten und erfahrenen Personal kann überragende Ergebnisse bringen

Firewall immer –
IDS wenn möglich

Rechtliche Aspekte
Gesetzliche Grundlagen

- Wichtig! Es ist eine Vielzahl von rechtlichen Vorschriften zu beachten
- Personenbezogene Daten: BDSG erlaubt IDS durch §14
  - §14 (2): Das Speichern, Verändern oder Nutzen [...] ist [...] zulässig, wenn es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten [...] erforderlich ist.
  - - §14 (4), §31: Personenbezogene Daten, die ausschließlich [...] zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage genutzt werden, dürfen nur für diesen Zweck verwendet werden.

Rechtliche Aspekte
Umsetzung

- Datenschutzbeauftragter, Personal- und Betriebsrat müssen in den Prozess eingebunden werden.
- Datenschutzbeauftragter, Personal- und Betriebsrat sollen Anforderungen mit abstimmen
- Alle Mitarbeiter werden über den Zweck informiert
- Alle IDS-Mitarbeiter werden auf das Datenschutzgesetz verpflichtet.
- Daten werden nur gemäß §14 BDSG aufgezeichnet
- Geregelte Weitergabe der Daten
- Geregeltes Löschen der Daten
- Änderungen der Einsatzweise erfordert Zustimmung von Personal- und Betriebsrat


Vielen Dank für Ihre
Aufmerksamkeit!
Fragen?
T Systems