DECUS IT-Symposium 2004

Informationssicherheit Christian Scheucher

PROTECTION · DETECTION · REACTION

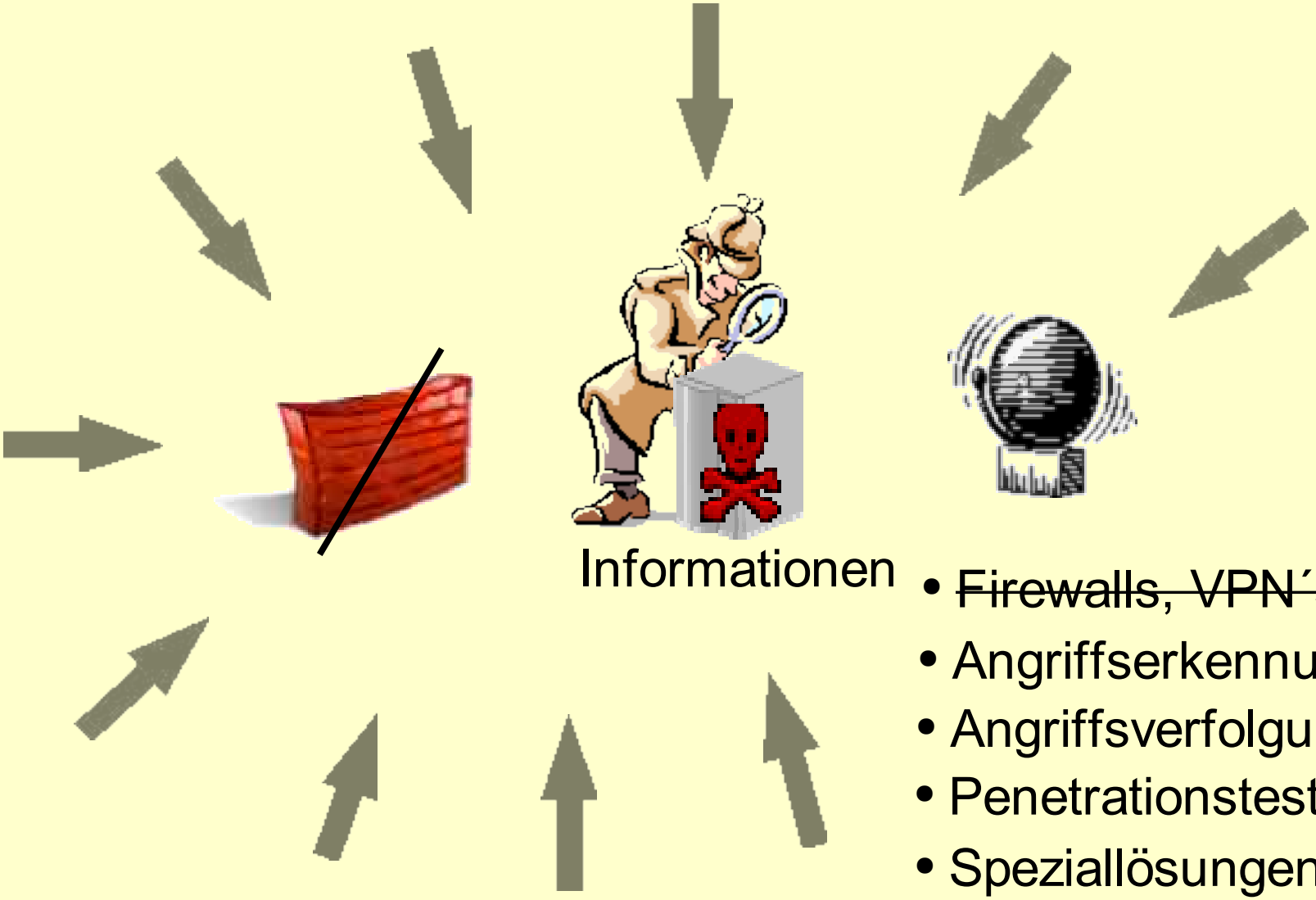
Angriffserkennung mit Honeypots und Honeynets

Session 3N07

Christian M. Scheucher

http://www.scheucher.net
☎ +49(0)89-61208591 +49(0)89-61208593
christian.scheucher@scheucher.net

Tätigkeitsschwerpunkte

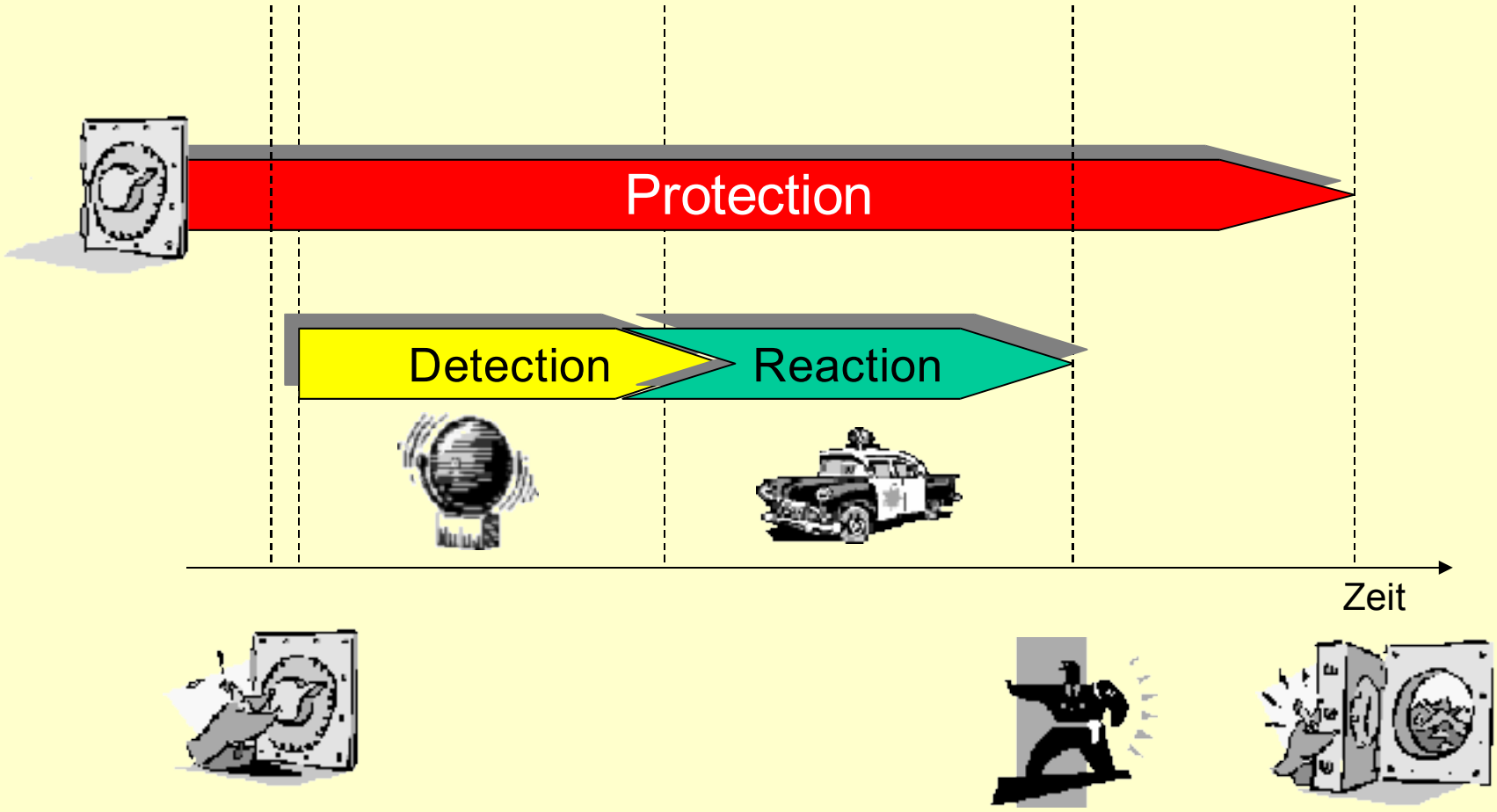


- ~~Firewalls, VPN´s, Antivirus~~
- Angriffserkennung
- Angriffsverfolgung
- Penetrationstests und Audits
- Speziallösungen
- Trainings

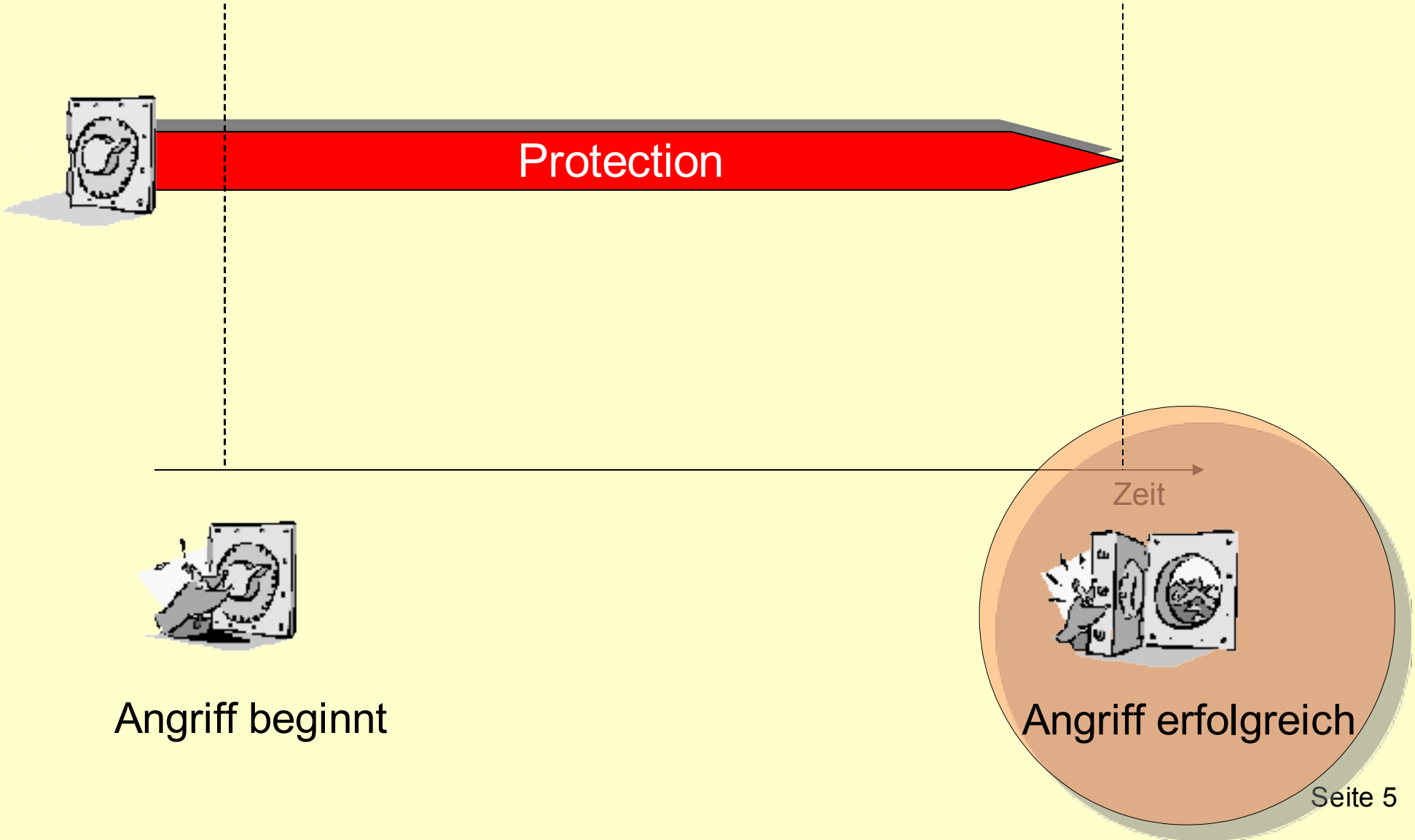
Was wir besonders gut können

- Penetrationstests und Security-Audits
- Prüfung von Wählzugängen
- Angriffe erkennen und darauf reagieren
- Angriffserkennung mit Honeypots und HIDS
- Verfolgung und Analyse von Angriffen (Incident Response, CERT und Forensics)
- Trainings im (Anti)-Hacking-Bereich

Time Based Security
Wie macht´s eine Bank?



Time Based Security
Wie sieht es in der IT aus?



Warum die Erkennung nicht funktioniert

- Man versucht, die 100% zu erreichen, schafft wegen diesem unrealistischen Anspruch in der Praxis aber nur 0%
- Wir sind zu sehr in die Technik verliebt
- Die Mentalität und Vorgehensweise des Hackers lassen wir aussen vor
- Aus Firewall-Logs lassen sich keine Angriffe erkennen
- IDS-Systeme überschütten die Anwender mit False-Positiv Alarmen und Arbeit. Sie taugen deshalb nur für bunte Grafiken

Warum IDS-Systeme nicht funktioniern

- Sie können nicht zwischen Angriffsversuch und erfolgreichem Angriff unterscheiden
- IDS kennt nur bekannte Angriffsmuster
- Man kann IDS Systeme leicht unterwandern (IDS-Evasion)
- Verhaltensbasierende IDS-Systeme können nicht zwischen der Verhaltensänderung von Benutzern oder eines Angreifers unterscheiden
- Alle Systeme erzeugen ohne immensen Tuning-Aufwand sehr viele False-Positivs
- Im lokalen Netz nicht installierbar

80% der Angriffe von innen

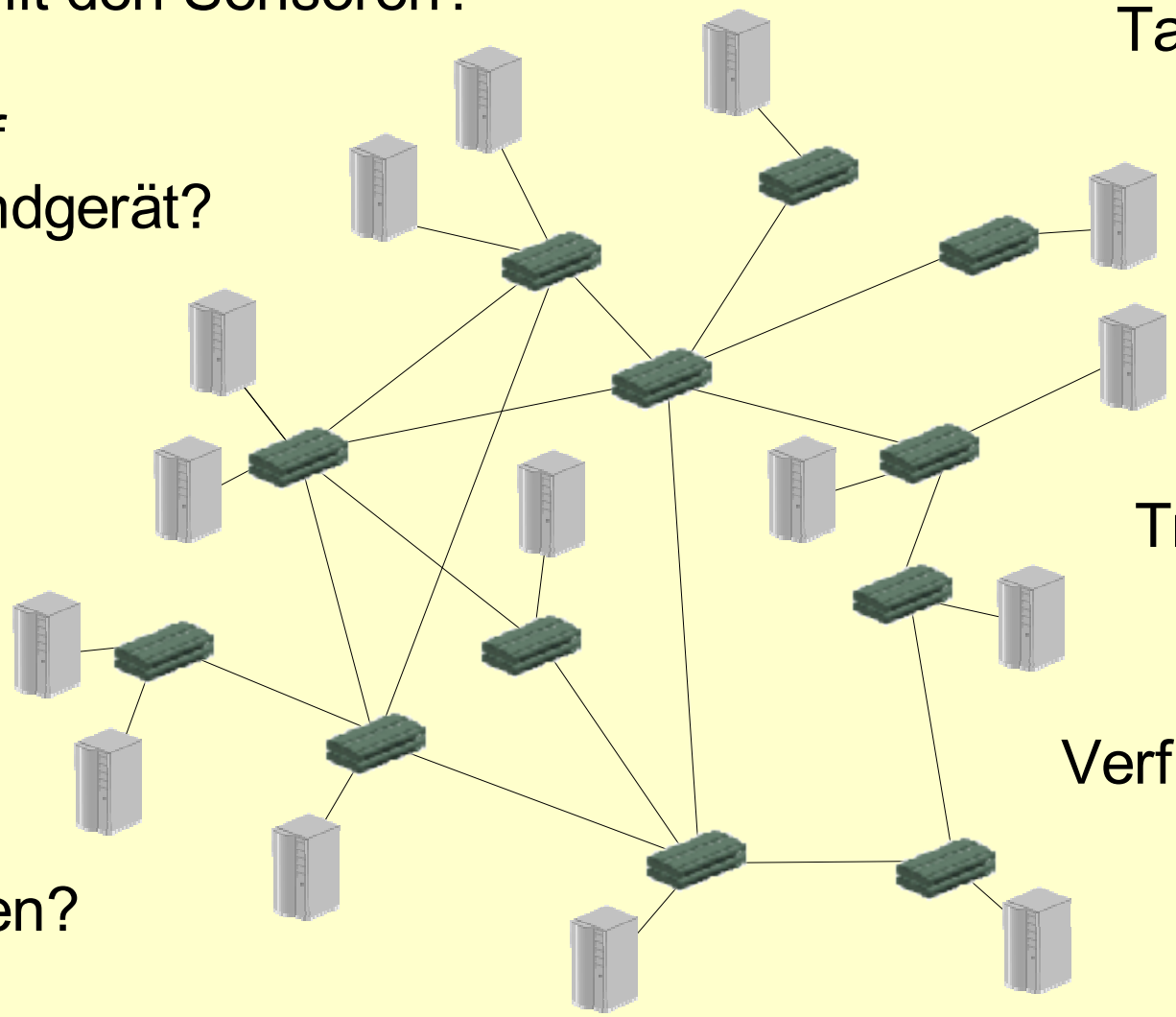
- 80% aller Angriffe werden von innen durchgeführt, nur 20% von außen (Internet, Dial-Up, WLAN)
- Fast 100% der Investitionen werden zur Abwehr von Angriffen von außen aufgewendet.
- Fast 100% davon werden in „Protection“ investiert. Fast nichts im Vergleich dazu in „Detection“ und „Response“
- Noch weniger in die Security Awareness
- Nur etwa 5% aller internen Angriffe werden erkannt, nur jeder fünfte davon konnte aufgeklärt werden

Flächendeckende Überwachung mit IDS möglich oder aussichtslos?

Wohin mit den Sensoren?

Taps?

IDS auf
dem Endgerät?



Trunking?

Verfügbarkeit?

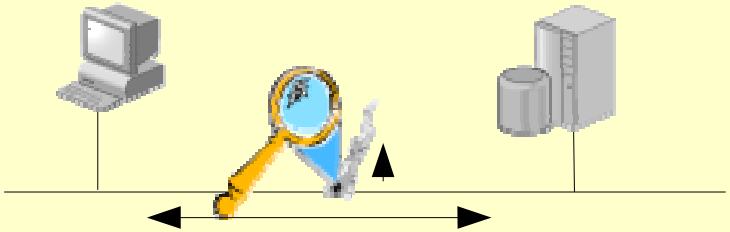
Kosten?

Wird mit Intrusion Prevention Systemen (IPS) alles besser?

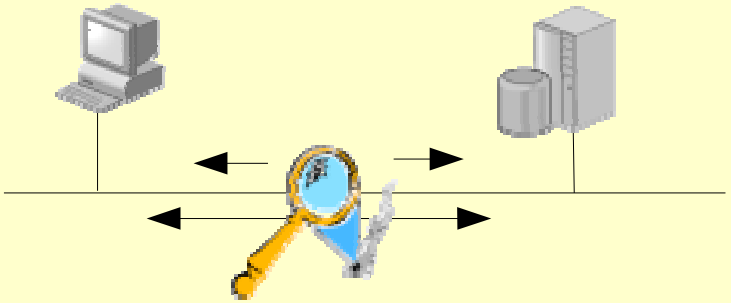
- IPS ist seit längerer Zeit verfügbar, nur der Begriff ist neu
- Es wird versucht, die Erkennung und Reaktion in einem Gerät zu vereinigen
- Und das, obwohl die Erkennung (s. IDS) nach wie vor mit den bekannten Ansätzen nicht funktioniert
- Noch schwerer und teuer als IDS zu integrieren, da sie aktiv in den Datenstrom eingreifen müssen

IDS/IPS im Netzwerk

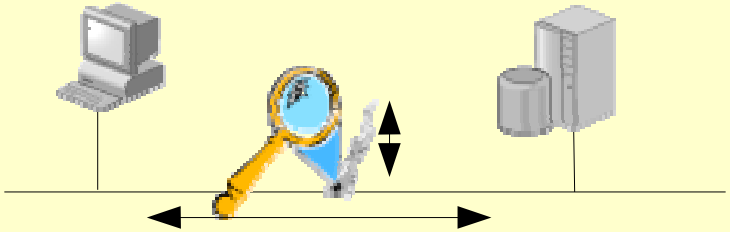
IDS - Sniffing am Netz



Inline - IPS



IPS - Sniffing am Netz mit Response



Know your enemy

Wenn du deinen Feind und auch dich kennst, brauchst du nicht die Ergebnisse von 100 Kämpfen zu fürchten.

Wenn du dich kennst, aber nicht deinen Feind, wirst du für jeden Sieg eine Niederlage erleiden.

Wenn du weder dich noch deinen Feind kennst, wirst du in jeder Schlacht versagen.

Sun-Tzu (Chinesischer General, ca. 50 v. Chr.)

Know your enemy

Angreifer und deren Motive

Profis
- Industrie-Spionage
- Wettbewerbs-Spionage
- Politische Interessen

(Externe) Mitarbeiter
- Diebstahl
- Sabotage
- Frust und Langeweile

Hacker
- „Ruhm und Ehre“
- Währung
  - Kreditkartennummern
  - Identitäten
  - root-Accounts
  - Exploits
  - Speicherplatz

Art des Angriffs

gezielt — unspezifisch

Ein paar Begriffe...

- **Honeypot** – „A honeypot is a system who's value is being probed, attacked, or compromised, you want the bad guys to interact with your honepyot“ aus „The Honeynet Project FAQ“
- **Honeynet** – Mehrere Honeypots, die ein typisches Netzwerk aus Produktivsystemen (nach)bilden
- **Honeytoken** - ist alles, was ein Honeypot auch ist, außer dass es sich dabei explizit nicht um einen Computer handelt.

Vorgehensweise von Hackern

1. Footprinting
2. Scanning (ICMP, Ports, Betriebssysteme)
3. Enumeration (Connects, User, Software)
4. Gaining Access
5. Escalating privilege
6. Pilfering (Vertrauensbeziehungen, Passwörter)
7. Backdoors
8. Spuren verwischen
9. Denial of Service

Arten von Honeypots

Low interaction Honeypots

- Bieten (fast) keine Interaktionsmöglichkeiten
- Einfach aufzubauen und zu pflegen
- Kostengünstig
- Durch die Einfachheit kaum ein Risiko für den Honeypot selbst
- Emulation der ersten Phasen von Protokollen einfach umsetzbar

Beispiele

- Specter
- Honeyd
- BackOfficer Friendly

High Interaction Honeypots

- Reelle komplexe Systeme
- Studium von fortgeschrittenen Angriffstechniken möglich
- Risikoreich im Einsatz
- Für den Angreifer schwer von einem echten Produktivsystem zu unterscheiden

Beispiele

- ManTrap

Risiken von Honeypots

- Keine 100%-ige Erkennung aller Angriffe möglich
- Hoher Aufwand bei der Auswertung von High-Interaction Honeypots, dadurch wird die Auswertung nicht immer durchgeführt
- Rechtliche Situation
- Honeypots werden selbst zu Jump-Points für Hacker

Was können Sie mit Honeypots?

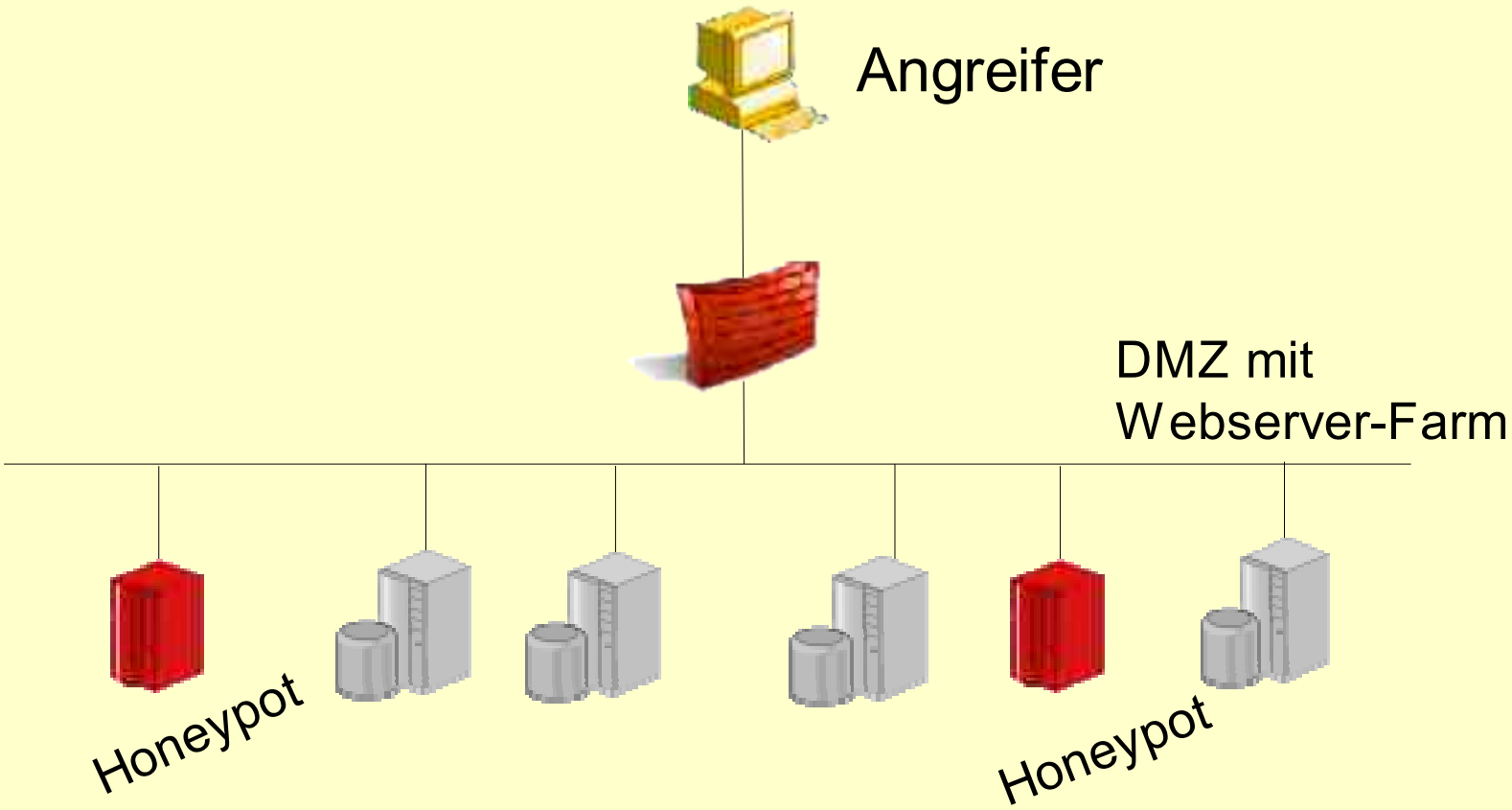
- Angriffe erkennen
- Eine Menge über die Angreifer lernen
- IDS und IPS in weiten Teilen ersetzen
- Endlich das interne Netzwerk flächendeckend überwachen
- Gegnerische Kräfte binden
- Angreifer von produktiven Systemen auf Honeypots umlenken
- Bisher in der Öffentlichkeit noch unbekannte Angriffe entdecken und analysieren

Angriffe mit Honeypots erkennen

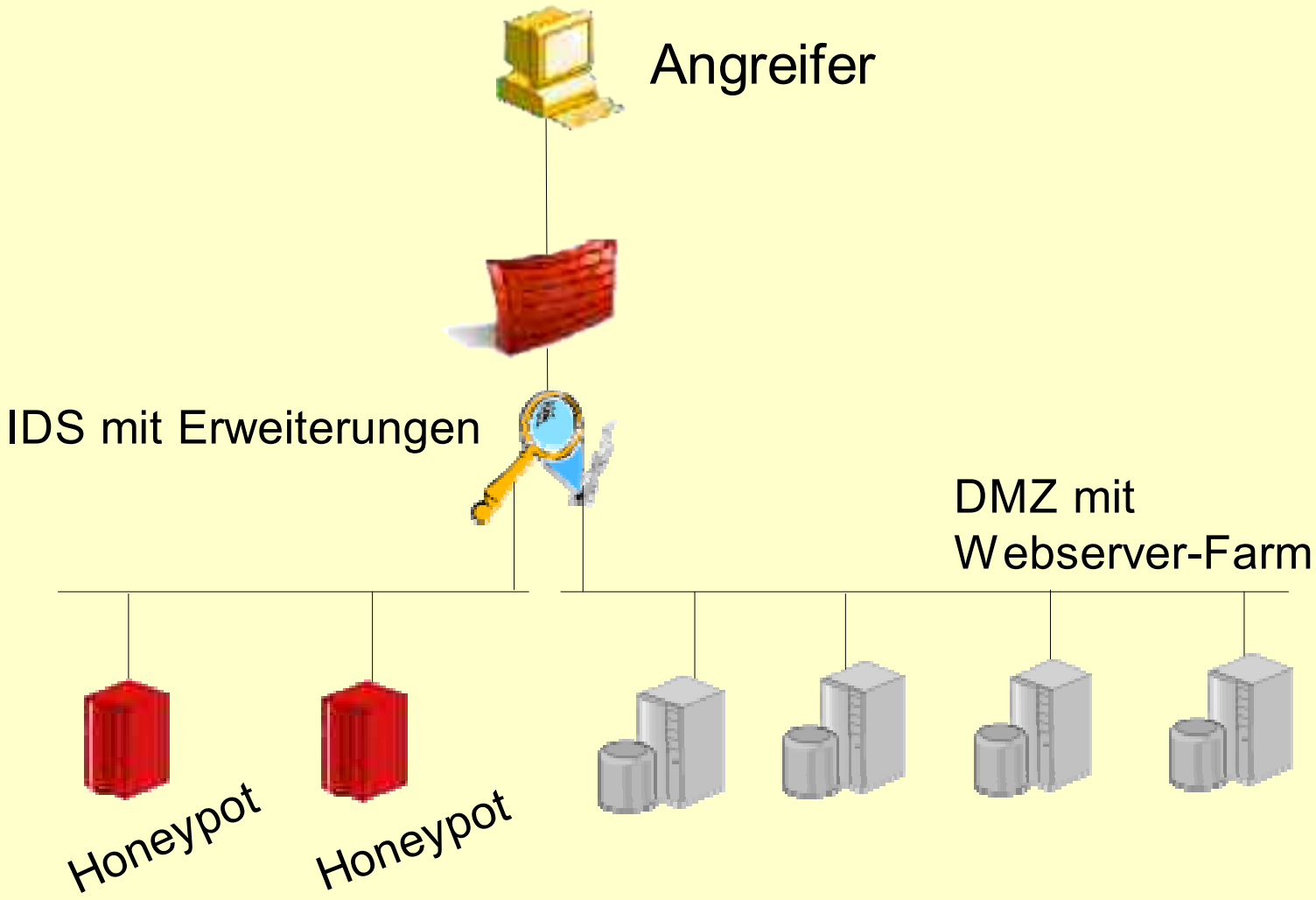
1. Footprinting *Low Interaction Honeypots*
2. Scanning (ICMP, Ports, Betriebssysteme)
3. Enumeration (Connects, User, Software)
4. Gaining Access
5. Escalating privilege
6. Pilfering (Vertrauensbeziehungen, Passwörter)
7. Backdoors
8. Spuren verwischen
9. Denial of Service

High Interaction Honeypots

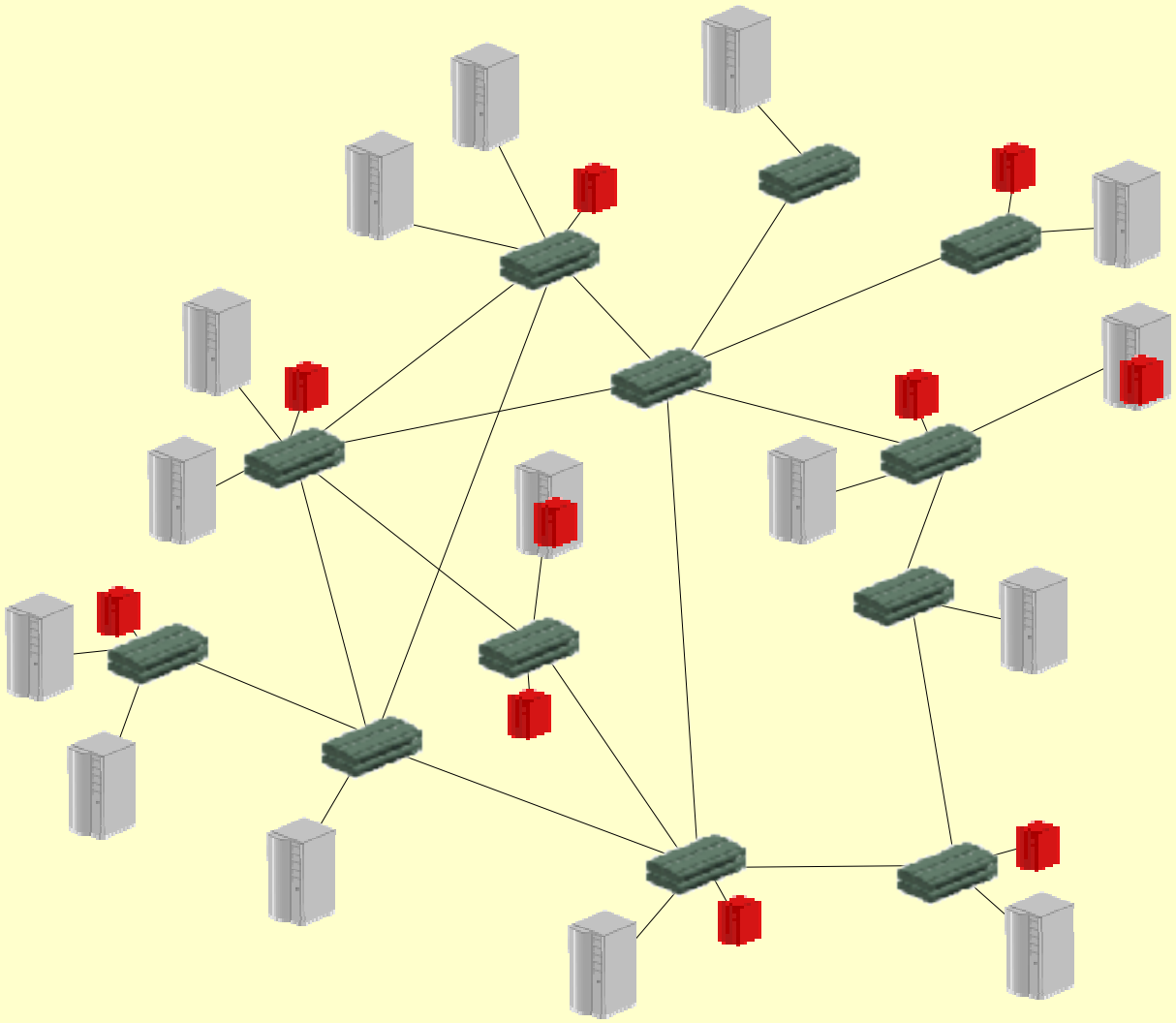
Ablenkung der Angreifer



Umleitung der Angreifer



Honeypots im LAN



Angriff erkannt – und jetzt?

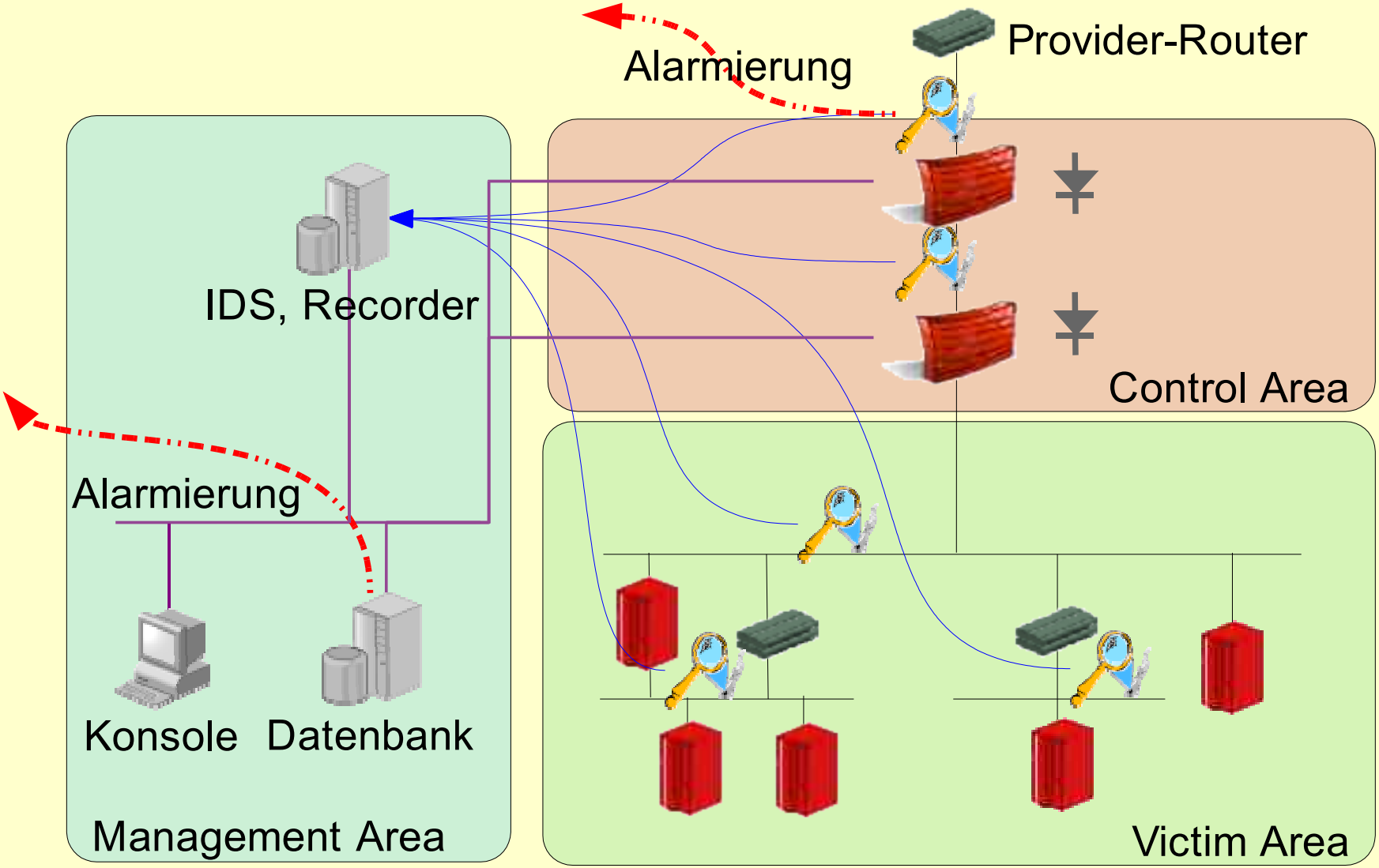
Was üblicherweise passiert:

- Panik
- Däumchendrehen
- Ratlosigkeit

Was Sie stattdessen tun sollten:

- Die ersten Schritte, die sie regelmäßig trainiert haben, durchführen
- Intern die vorhandenen Prozesse anstoßen
- Bei komplexen Fällen auf externe Partner zurückgreifen, die mit Ihnen bereits die Trainings durchgeführt haben

HoneyNet für Forschung



Wie können Sie das Thema Erkennung und Reaktion angehen?

- Sie müssen sich selbst ein Commitment zur Informationssicherheit geben
- Sie müssen bereit sein, „es durchzuziehen“, mit allen Konsequenzen
- Sie müssen es wollen
- Starten Sie im internen Netzwerk
- Sie sollten mit Überraschungen rechnen
- Und rechnen Sie mit Menschen!

Zusammenfassung

- Wirksame Informationssicherheit können wir nur erreichen, wenn Protection, Detection und Reaction funktionieren
- Wir haben nur gegen einen Teil der Angreifer eine echte Chance
- IDS und IPS sind für Detection schlecht geeignet
- Honeypots ermöglichen eine zuverlässige Angriffserkennung
- Honeynets ermöglichen Forschung
- Incident Response und Forensik sind die nächsten Schritte

Vielen Dank für Ihre Aufmerksamkeit

Informationssicherheit Christian Scheucher

PROTECTION · DETECTION · REACTION

Angriffserkennung mit Honeypots und Honeynets

Session 3N07

Christian M. Scheucher

http://www.scheucher.net
☎ +49(0)89-61208591 +49(0)89-61208593
christian.scheucher@scheucher.net