Überblick: Wozu braucht man Agenten



Themenübersicht

- Definition des Agentenbegriffs
- Anwendungsgebiete für Agenten
- Angriffserkennung
  - Nachteile des klassischen Modells
  - Agentenbasierter Schutz
- Zusammenfassung

Literatur

Cheong, F.C. (1996) *Internet Agents (Spiders, Wanderers, Brokers and Bots).* USA, New Riders, ISBN 1-56205-463-5.

Northcutt, S. Zeltser, L. Winters, S. Frederick, K.K. Ritchey, R.W. (2003) *Inside Network Perimeter Security.* USA, Indiana, Indianapolis, New Riders, ISBN 0-7357-1232-8.

Russel, S. Norvig, P. (2003) *Artificial Intelligence (A Modern Approach).* USA, Prentice Hall, ISBN 0-13-080302-2.

Tanenbaum, A. Marten van Steen. (2003) *Verteilte Systeme (Grundlagen und Paradigmen).* München, Pearson Education Deutschland GmbH, ISBN 3-8273-7057-4.

Wooldridge, M. (Februar 2002) *An Introduction to MultiAgent Systems.* Chichester, England, John Wiley & Sons, ISBN 047149691X.



Themenübersicht

- Definition des Agentenbegriffs
- Anwendungsgebiete für Agenten
- Angriffserkennung
  - Nachteile des klassischen Modells
  - Agentenbasierter Schutz
- Zusammenfassung



Was ist ein Softwareagent?

Agent: ein Programm, das auf Anforderung und Eingabe von Daten hin eine Dienstleistung erbringt.

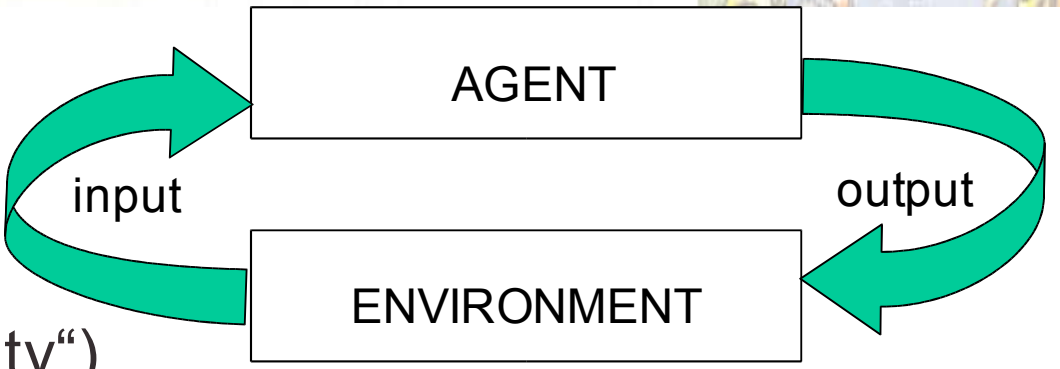
Ein Agent muss in der Lage sein,

- autonom zu handeln (agent design)

- mit anderen Systemen zu kooperieren
- mit anderen Systemen zu verhandeln

(society design)

Was ist ein Softwareagent?



Reaktivität („reactivity“)

Agenten können ihre Umgebung wahrnehmen und in akzeptabler Zeit auf deren Veränderungen reagieren.

Pro-Aktivität („pro-activeness“)

Agenten sind in der Lage, zielorientiert zu agieren („goal directed behaviour“), d.h. aus eigenem Antrieb Aktionen auszuführen.

Soziale Fähigkeiten („social-ability“)

Intelligente Agenten können mit anderen Agenten bzw. Personen kommunizieren.

Was ist ein Softwareagent?

Reaktiv: Berücksichtigung der Umgebungsänderung

- Umgebung kann sich während der Aktionsausführung verändern.
- Misserfolge müssen berücksichtigt werden (Lohnt es sich trotzdem, die Aktion auszuführen?)
- Ständige Überwachung der Umgebungsbedingungen. Gegebenenfalls – Planänderung.

Proaktiv:

- Berücksichtigung eines Ziels bei der Entscheidungsfindung (globales Optimum).
- Bewertung von Aktionen.

Es ist schwierig, das Gleichgewicht zwischen den beiden Anforderungen zu finden.

Was ist ein Softwareagent?

Kommunikativ

- Manche Ziele können nur in Zusammenarbeit mit anderen Systemen erreicht werden.
- Fähigkeit, mit anderen Agenten zu kommunizieren (gemeinsames Kommunikationsprotokoll).

Weitere Eigenschaften eines Agenten:

- Mobilität: Kann von einem System auf ein anderes migrieren
- Adaptivität: Lernfähig



Was ist ein Softwareagent?

Abgrenzung zu Objekten

- Agenten sind autonom und entscheiden für sich selbst, ob sie eine Aktion ausführen oder nicht.
- Agenten sind reaktiv, proaktiv und kommunikativ. Objekte besitzen diese Eigenschaften nicht.

Abgrenzung zu Expertensystemen

- Expertensysteme besitzen keine Sensoren.
- Expertensysteme können nicht agieren.

Agenten und Künstliche Intelligenz (KI)

- Agentensysteme bedienen sich der Errungenschaften der KI-Forschung.
- Ein Agent muss nicht unbedingt ein intelligentes Verhalten nachahmen.



Themenübersicht

- Definition des Agentenbegriffs
- Anwendungsgebiete für Agenten
- Angriffserkennung
  - Nachteile des klassischen Modells
  - Agentenbasierter Schutz
- Zusammenfassung

Anwendungsgebiete

1) Dienstleistungen in einem komplexen verteilten System:

- einfache Dienste: Datenbankabfragen
- komplexere Dienste: Planungsaufgaben

2) Bau komplexer Softwaresysteme

Vorteile von Agenten:

- Modularisierung
- Skalierbarkeit
- Erweiterbarkeit



Anwendungsgebiete

Global Computing

- Milliarden von Computern
- Unausgeglichene Ressourcen (Numbercruncher vs. Handy)
- Zentralisierte Verwaltung ist nicht möglich

Agenten – ein neues Softwareentwicklungsmodell

(Im Vordergrund steht die Kommunikationsfähigkeit von Softwaresystemen.)



Anwendungsgebiete

Verteilte/konkurrente Systeme

- Geschäftsprozessoptimierung
- verteiltes Sensoring
- E-Commerrce

Netzwerke

- Informationssammlung und -management.
- Systemsicherheit

Human-Computer Interfaces

- Nachrichtenassistenten
- Spam-Filtering.



Anwendungsgebiete

Geschäftsprozessoptimierung

Organisationseinheiten werden durch Agenten repräsentiert.

Agenten sind zuständig für:

- Angeboterstellung
- Verhandlungen
- Priorisierung unternehmensinterner Interessen

(Das Verhalten menschlicher Geschäftspartner wird nachgeahmt.)

Verteiltes Sensoring

- Überwachungskameras
- Verfolgung von Objektbewegungen.
- Kommunikation von Agenten untereinander



Anwendungsgebiete

Informationssammlung und -verwaltung

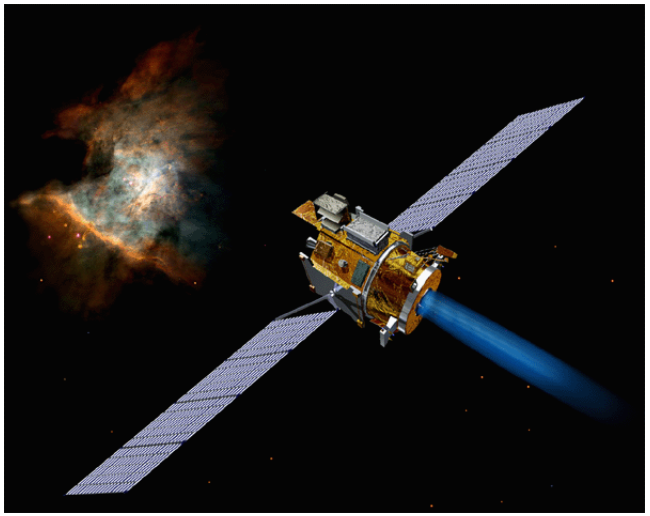
- Bekämpfung der Informationsflut
- Skalierbar
- personifizierte Suche
- relevante Informationen

E-Commerce

- Angebotvergleich
- Online-Auktionen (auction bots).

Anwendungebiete

NASA-Mission Deep Space 1



Cape Canaveral Oktober 1998

- Steuerung der Sonde durch ein Agentensystem
- Geringere Kosten durch die Einsparung des Bodenpersonals
- Erfolgreicher Abschluss der Mission im Dezember 2001

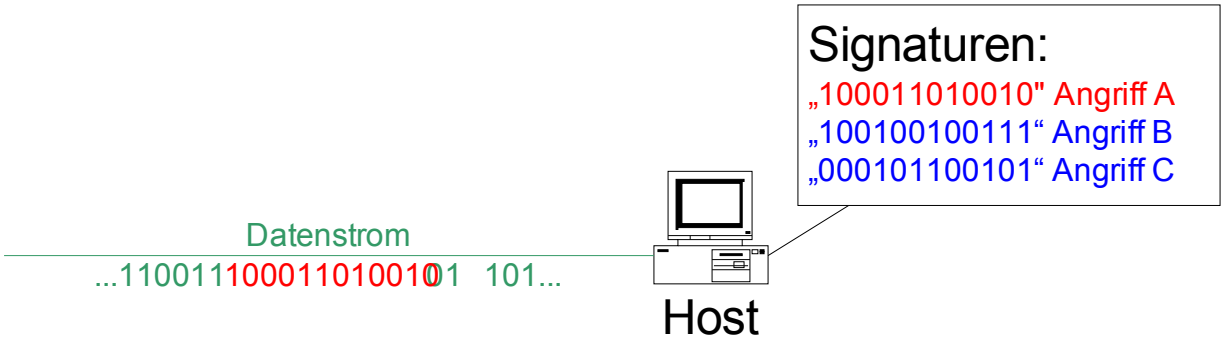
Themenübersicht

- Definition des Agentenbegriffs
- Anwendungsgebiete für Agenten
- **Angriffserkennung**
  - Nachteile des klassischen Modells
  - Agentenbasierter Schutz
- Zusammenfassung

Angriffserkennung

Methoden:

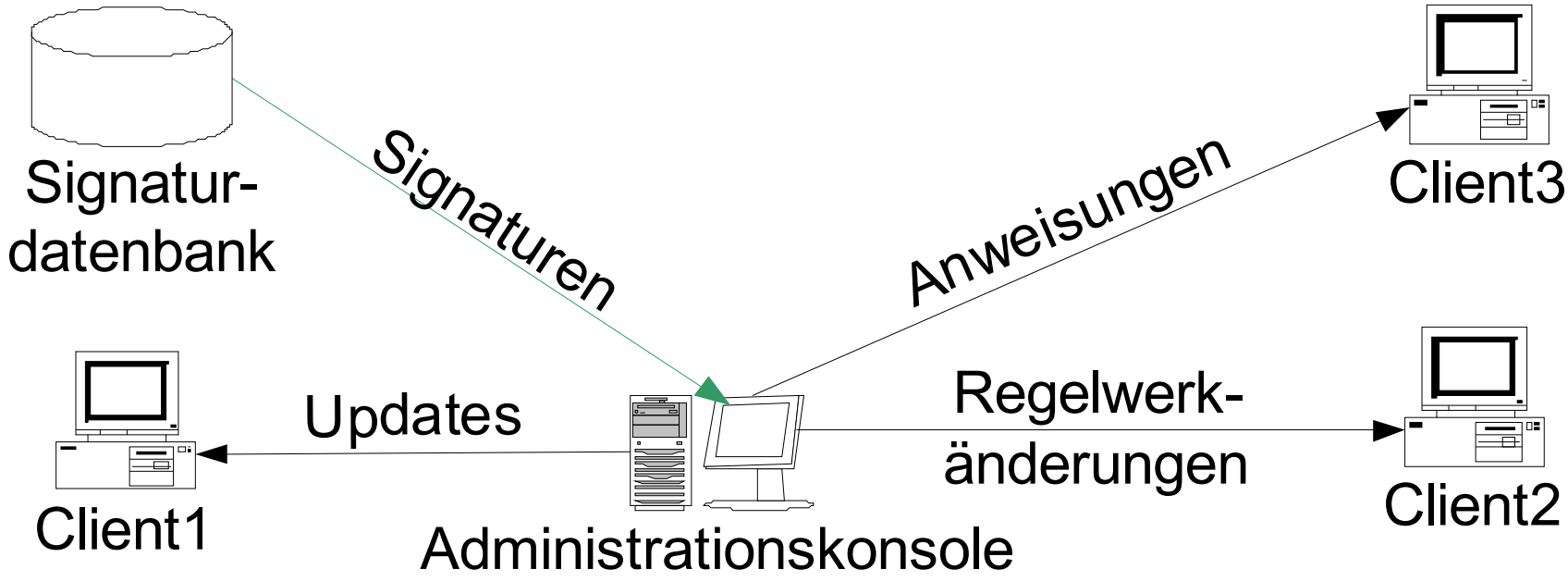
Signaturbasierte Angriffserkennung (z.B. Bitmuster, Zugriff auf einschlägig-bekannte Ports etc.)



Heuristische Methoden (Feststellung der Anomalien)

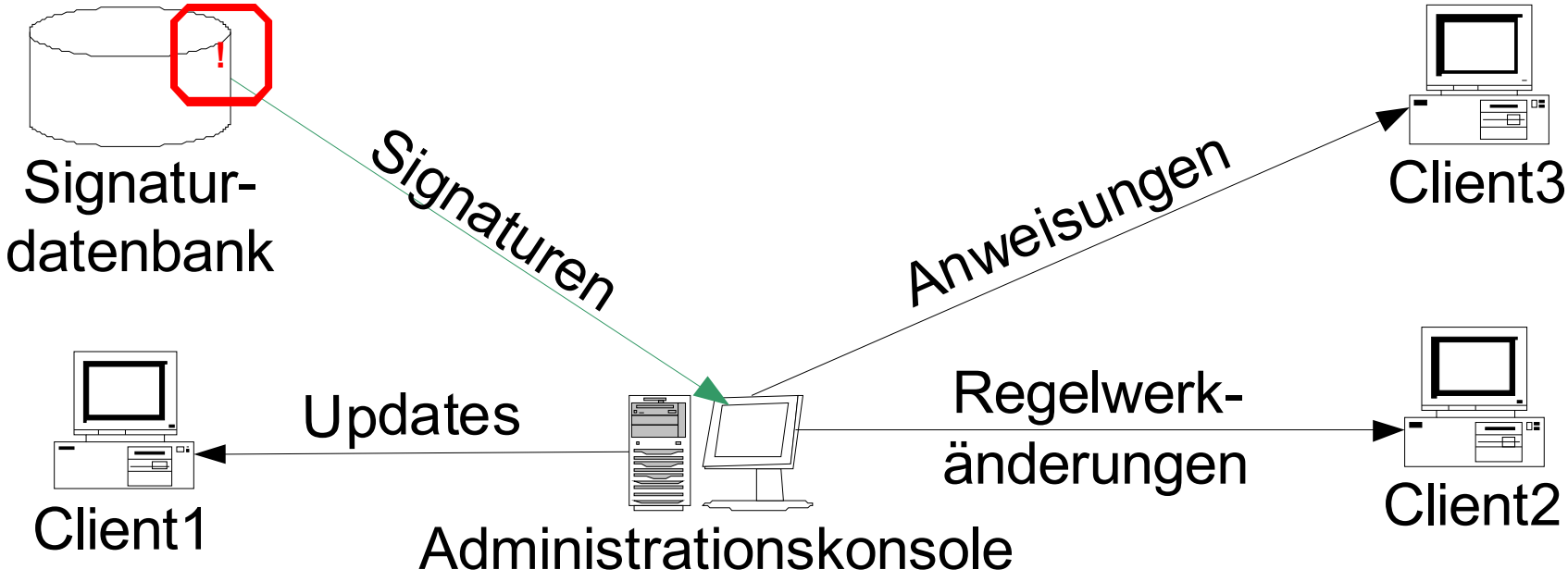
Angriffserkennung

Der klassische Aufbau einer Sicherheitsinfrastruktur:



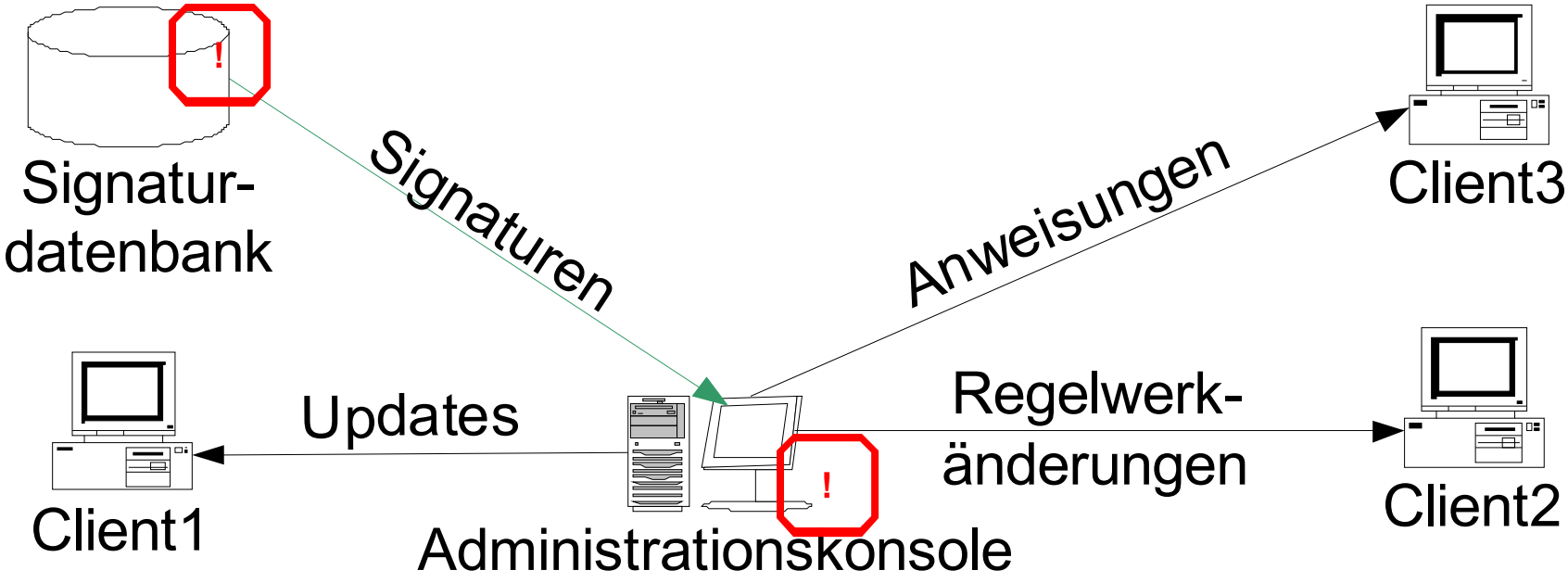
Angriffserkennung

Schwachstellen des Modells: Signatur-Upload



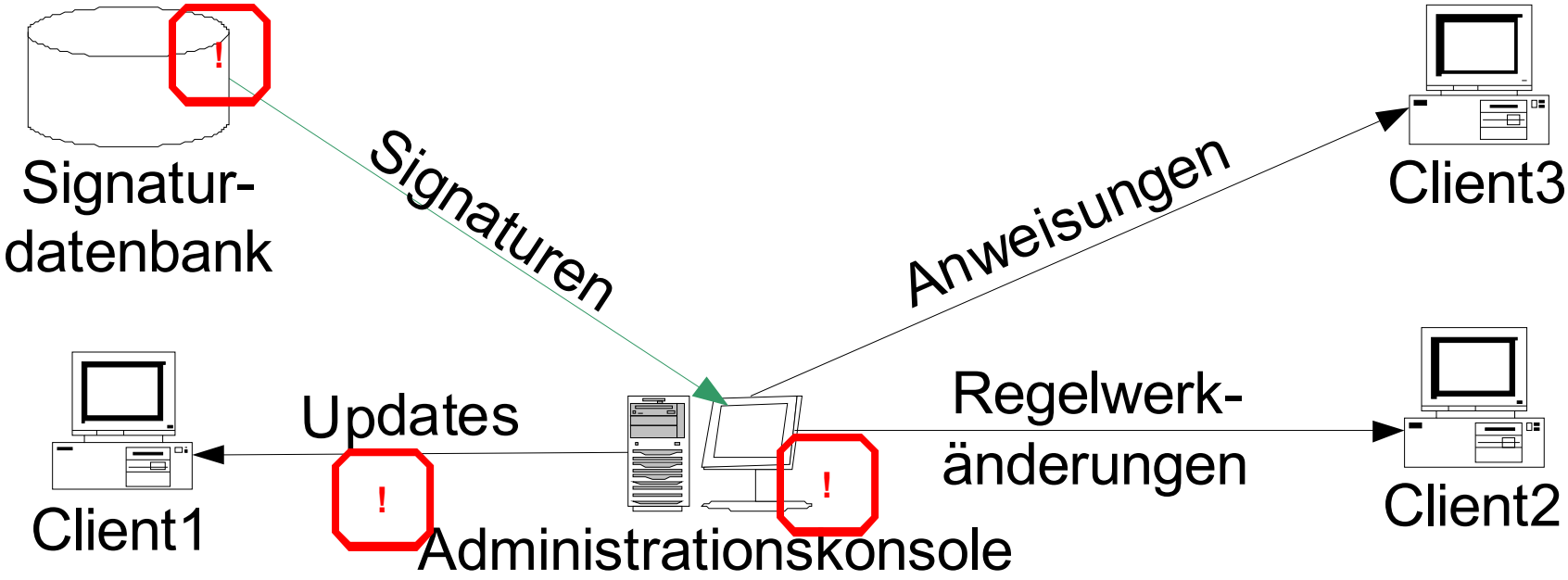
Angriffserkennung

Schwachstellen des Modells: Administrationskosnole als „single point of failure“



Angriffserkennung

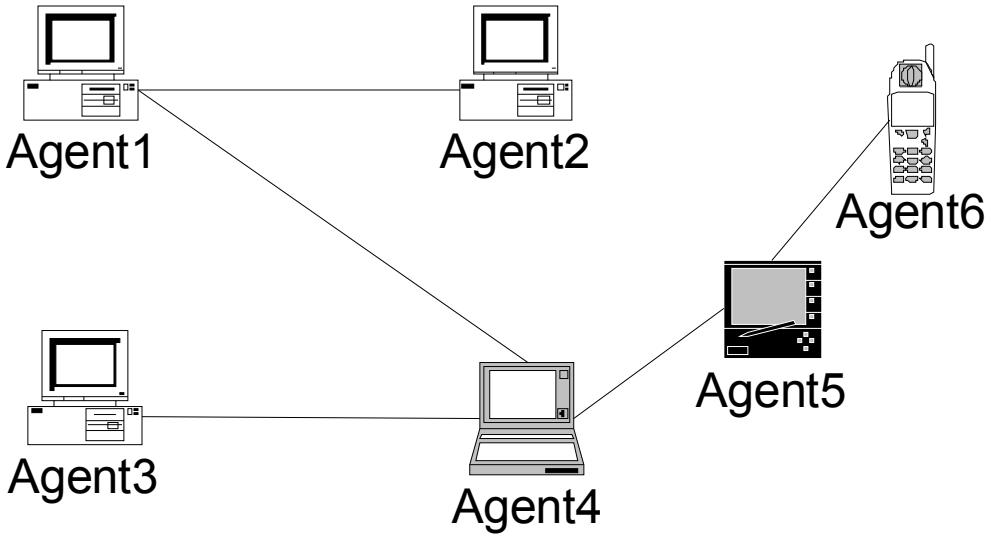
Schwachstellen des Modells: Verbreitung von Signatursätzen (updates)



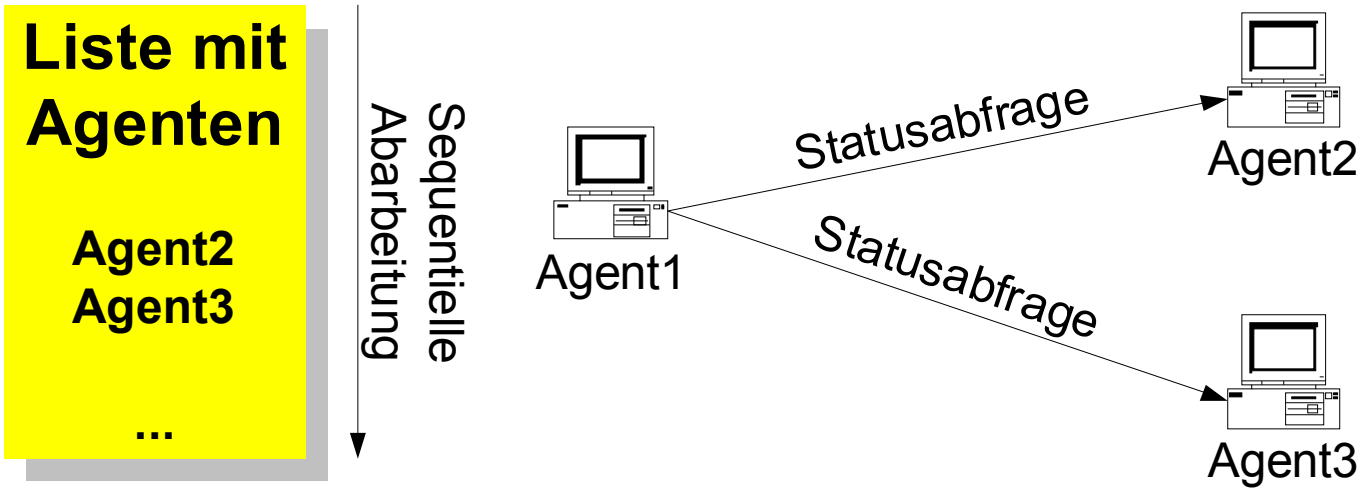
Angriffserkennung

Dezentralisierter Ansatz:

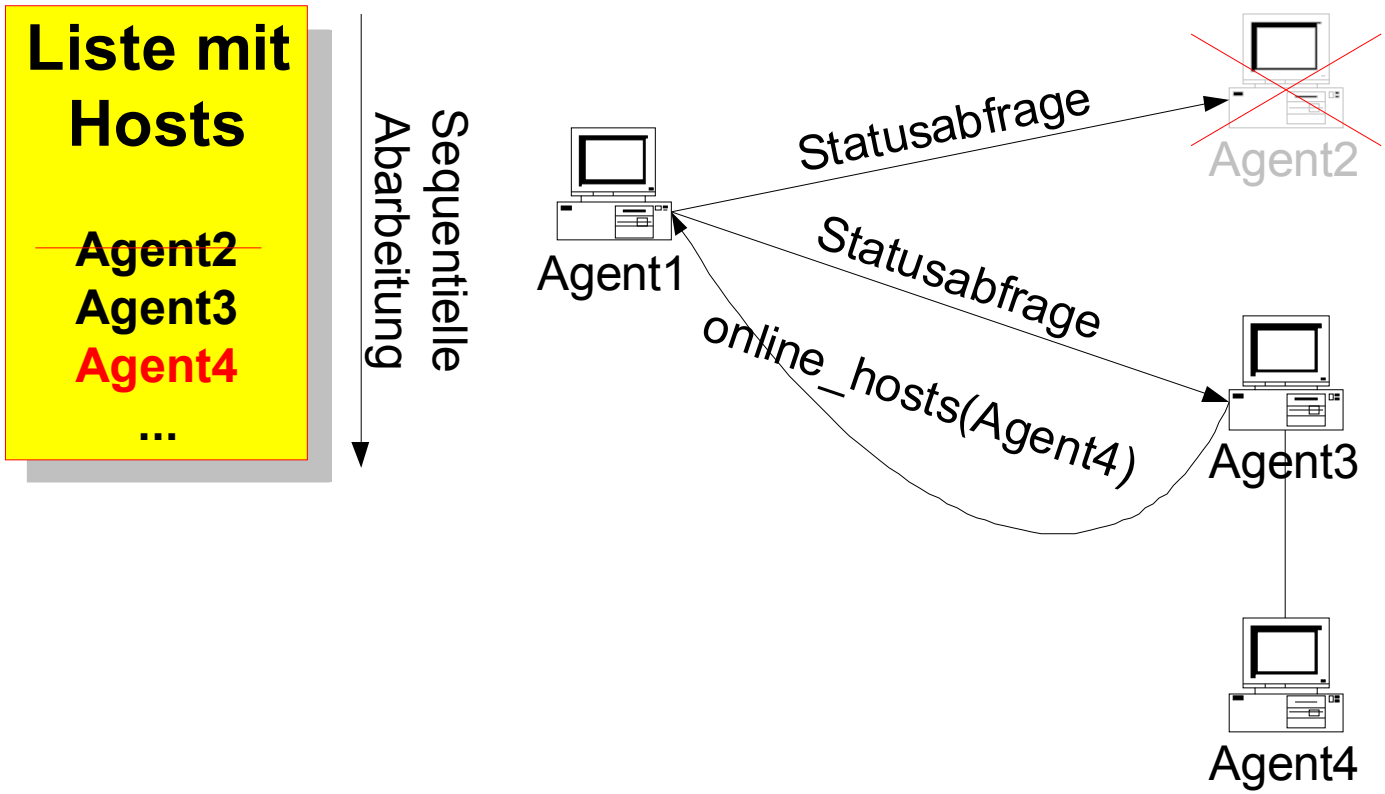
- keine zentrale Verwaltungsstelle
- keine Hierarchie
- unterschiedliche Ressourcen



Dezentralisierter Ansatz

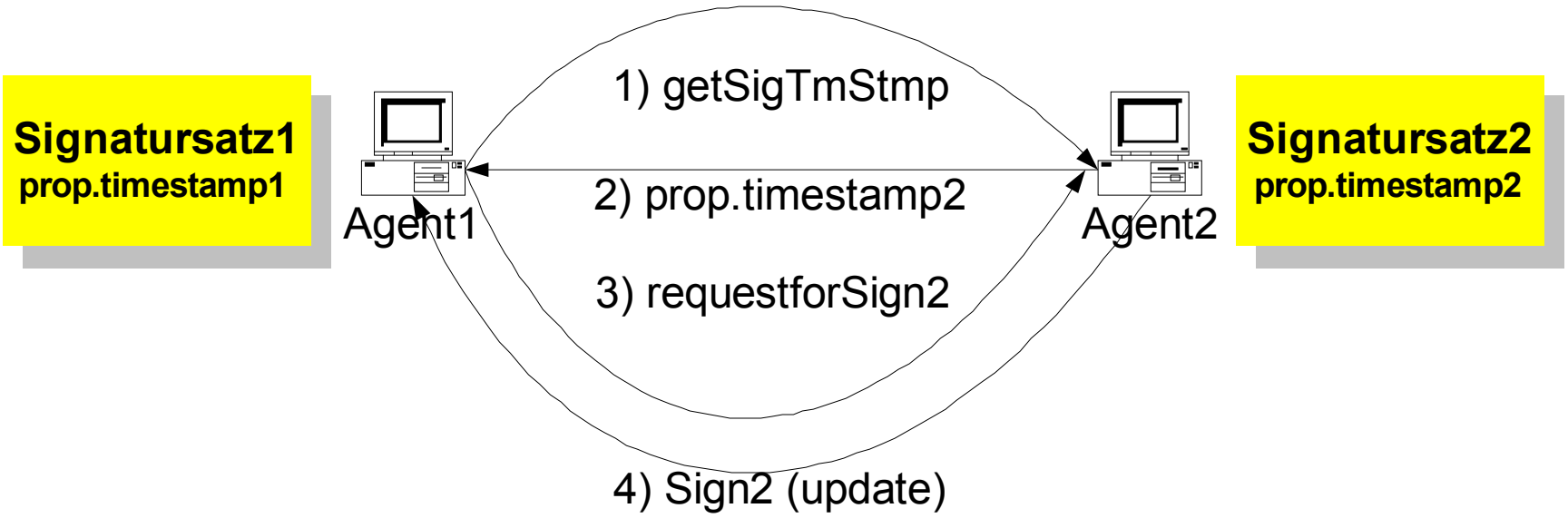


Das „lebendige“ Netz

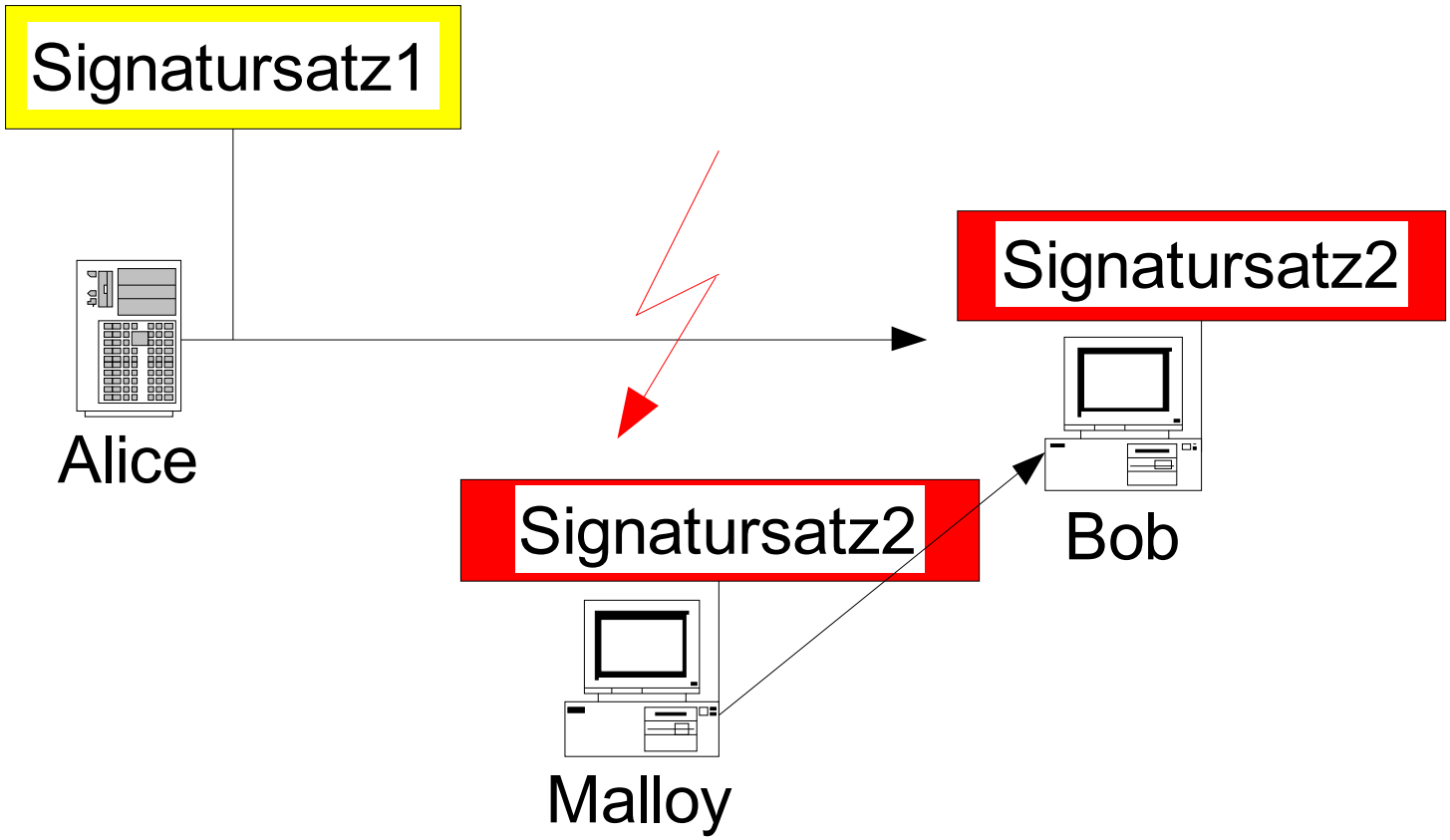


Aktualisierung von Signatursätzen

prop.timestamp2 > prop.timestamp1



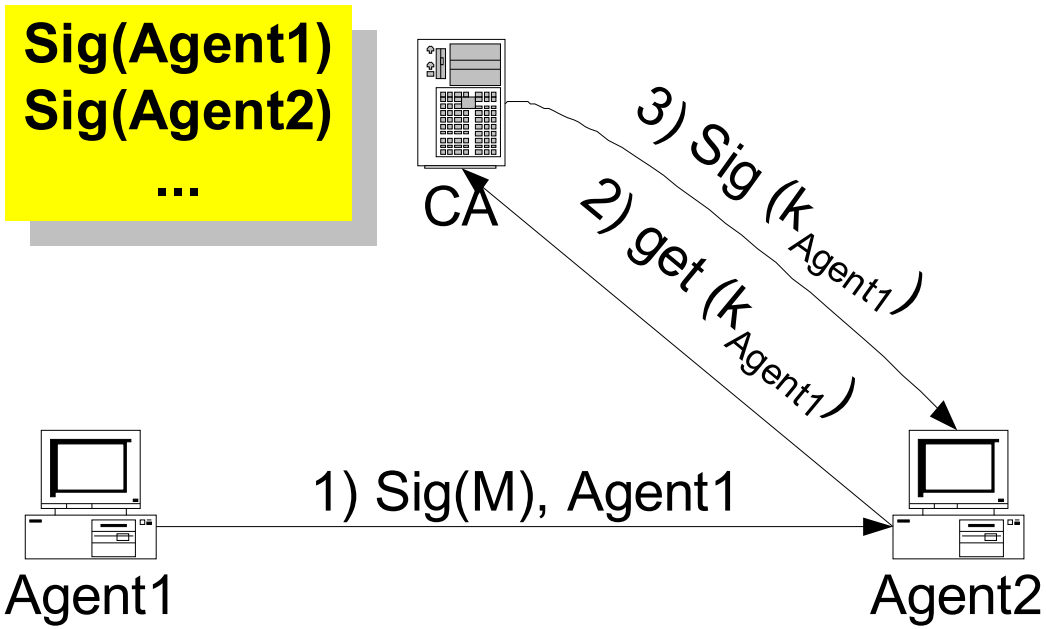
Integrität von Signatursätzen



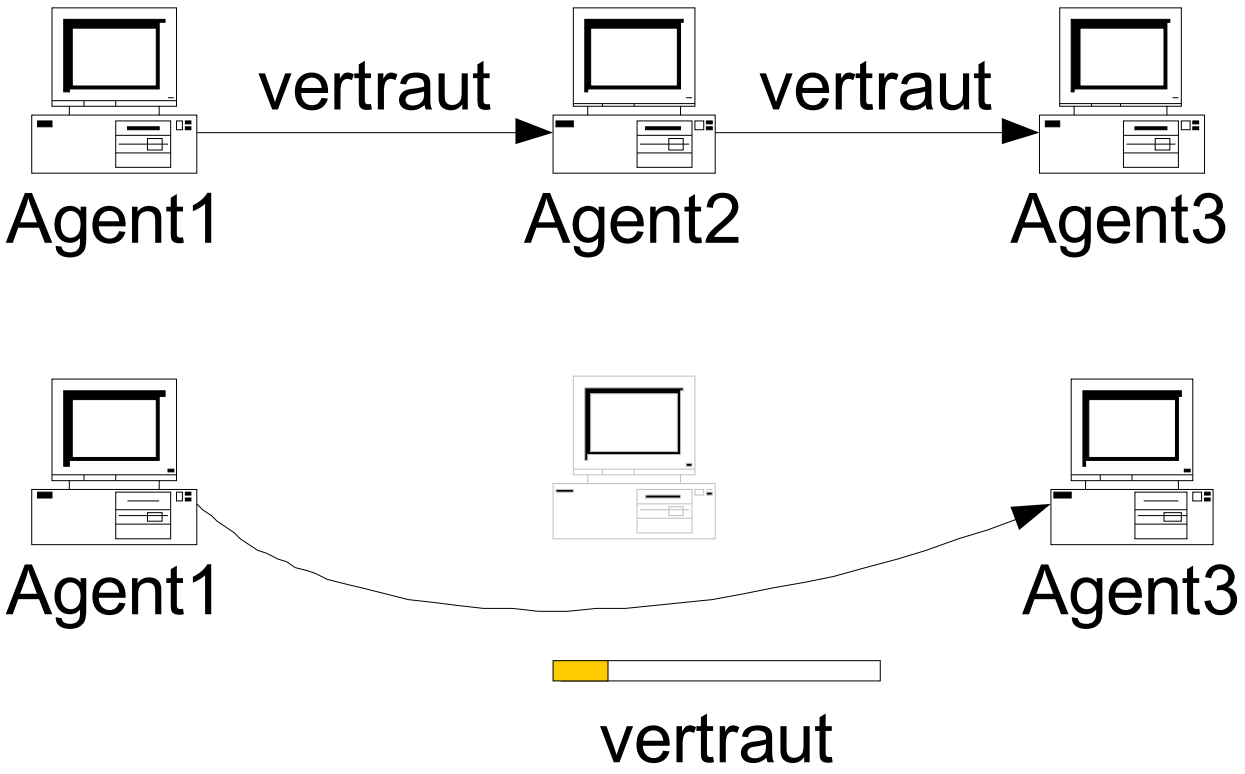
Lösung: Signieren von Daten

Identitätsprüfung: Lösung1 (Certification Authority)

k_{C4U}^{-1} [Info(this_certificate), Info(X), k_X].

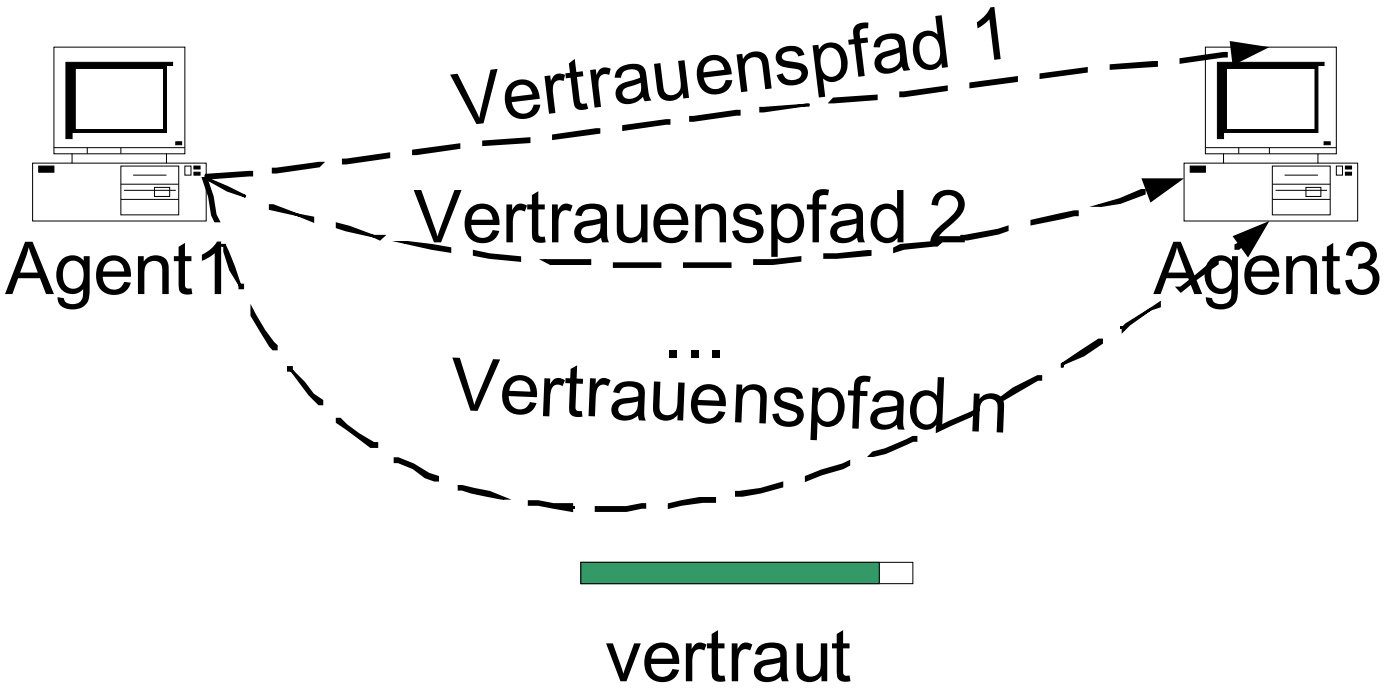


Identitätsprüfung: Lösung2 (basierend auf dem Vertrauensnetz-Modell)



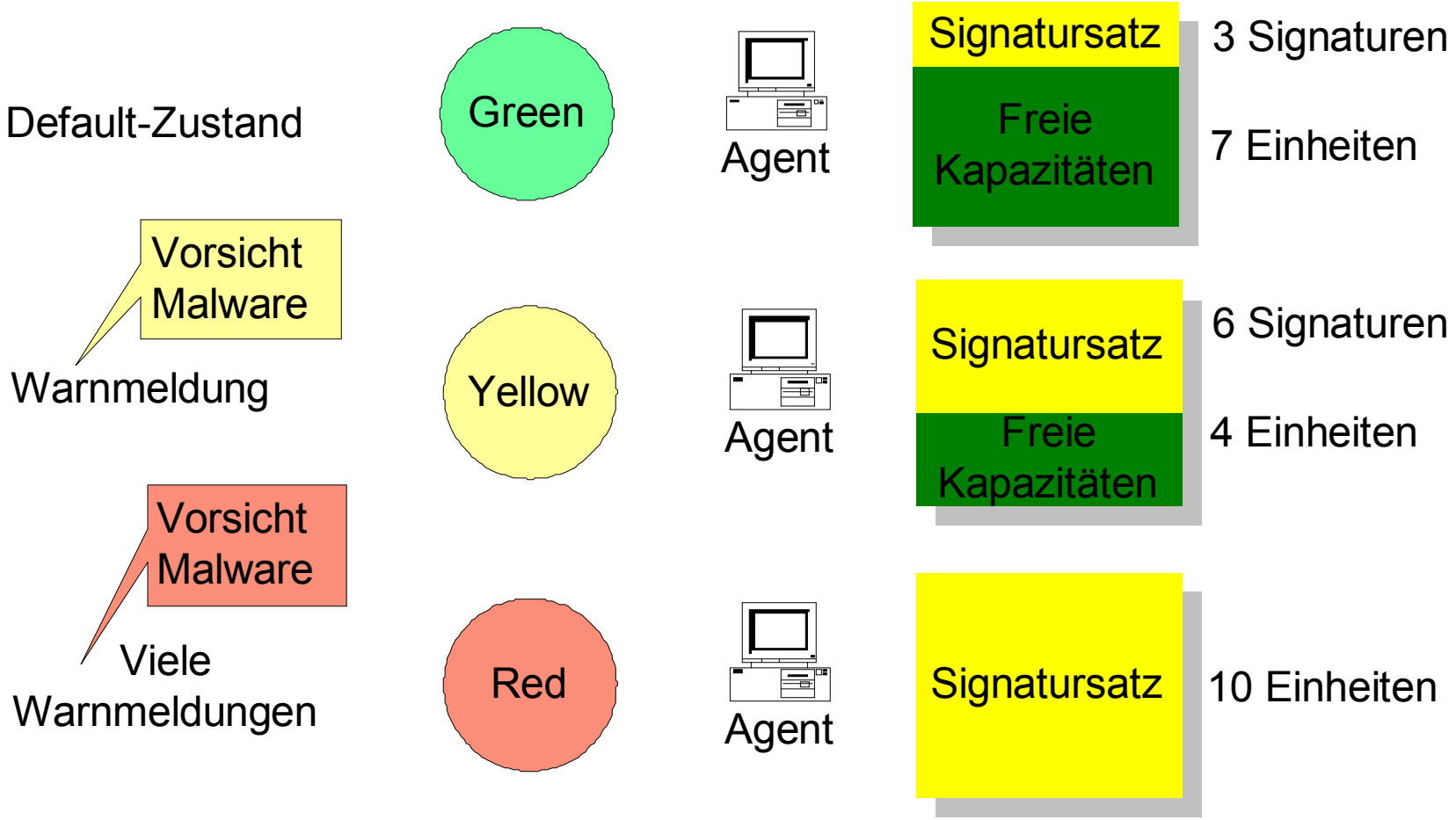
Angriffserkennung

Kurze disjunkte Vertrauenspfade erhöhen die Vertrauenswürdigkeit eines Systems.



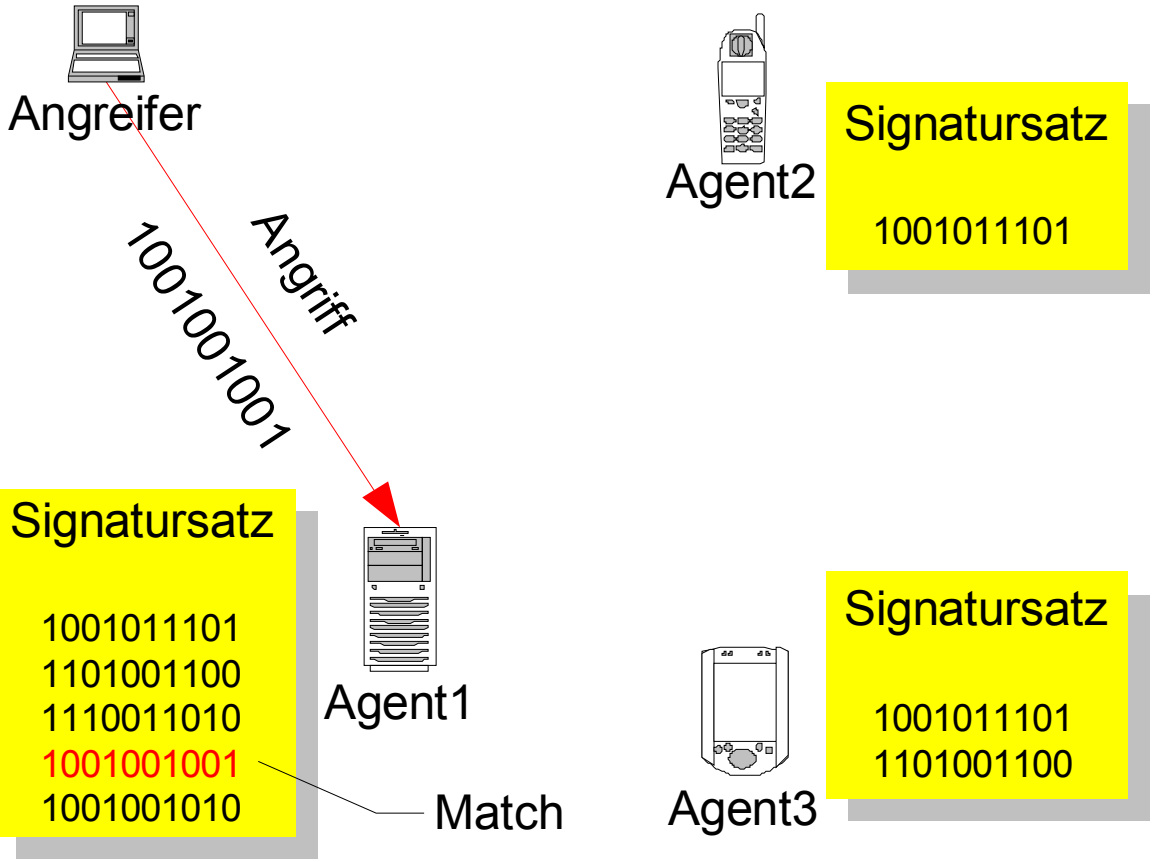
Angriffserkennung

Abhängigkeit des Signatursatzes von der aktuellen Alarmstufe:

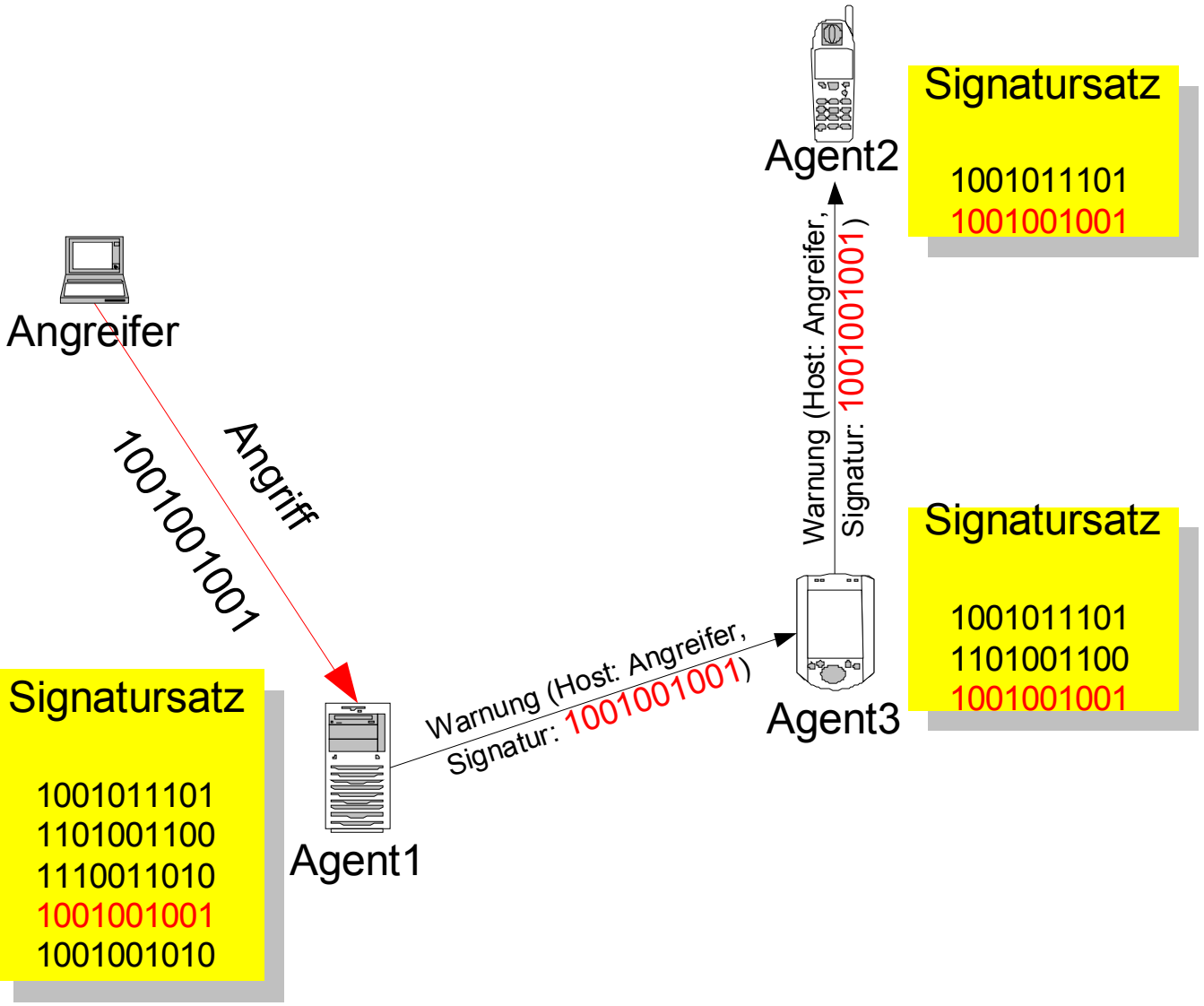


Angriffserkennung

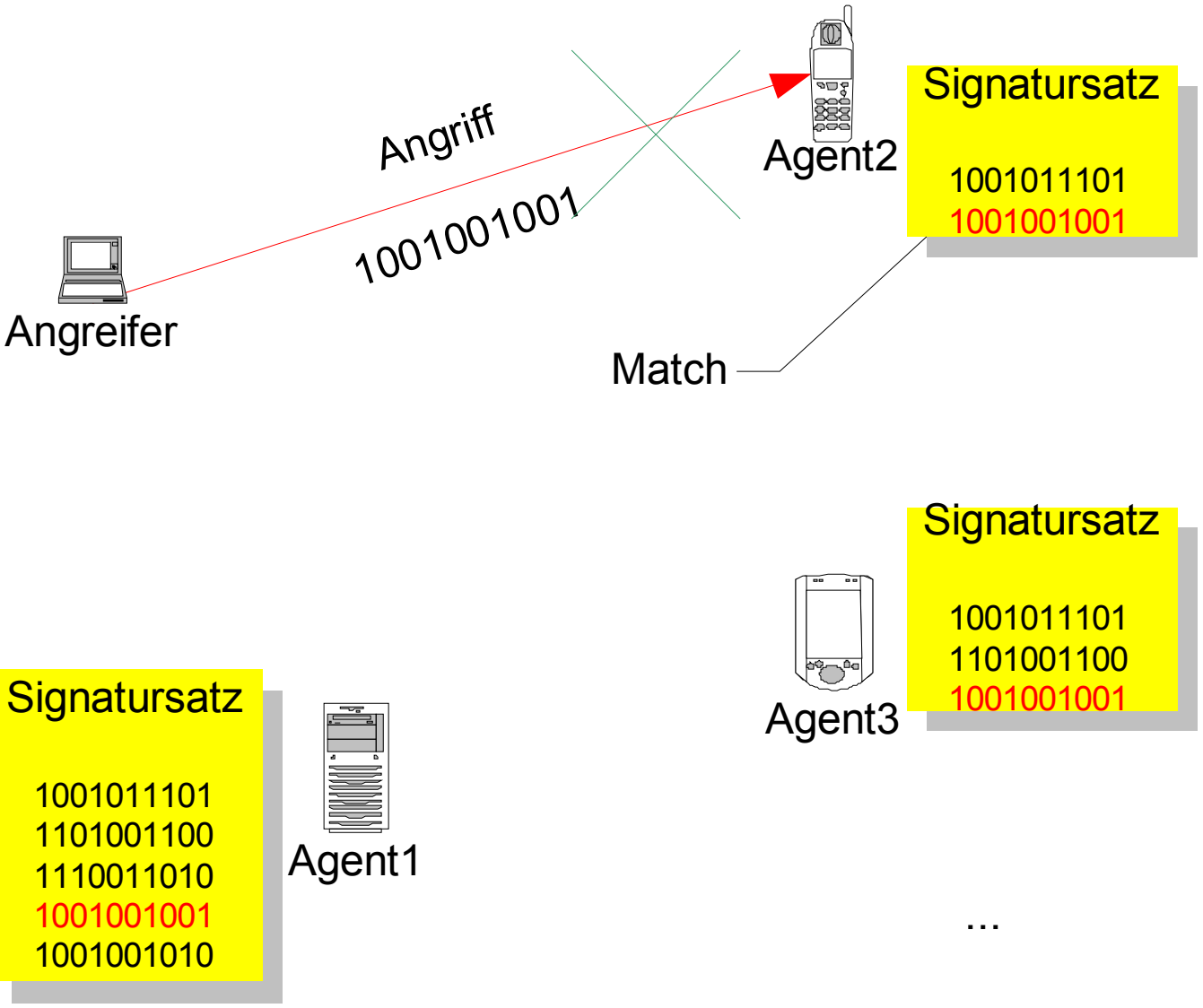
Verwendung unterschiedlicher Signatursätze in Abhängigkeit von den verfügbaren Ressourcen:



Angriffserkennung

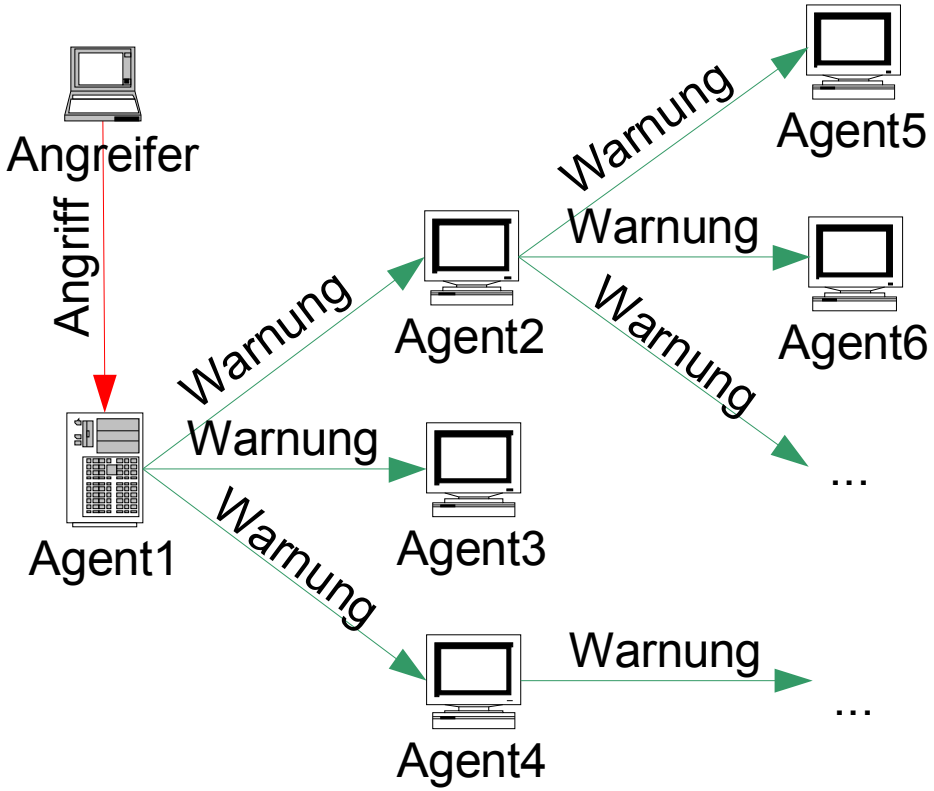


Angriffserkennung



Angriffserkennung

Wellenartige „Immunisierung“ der Systeme:

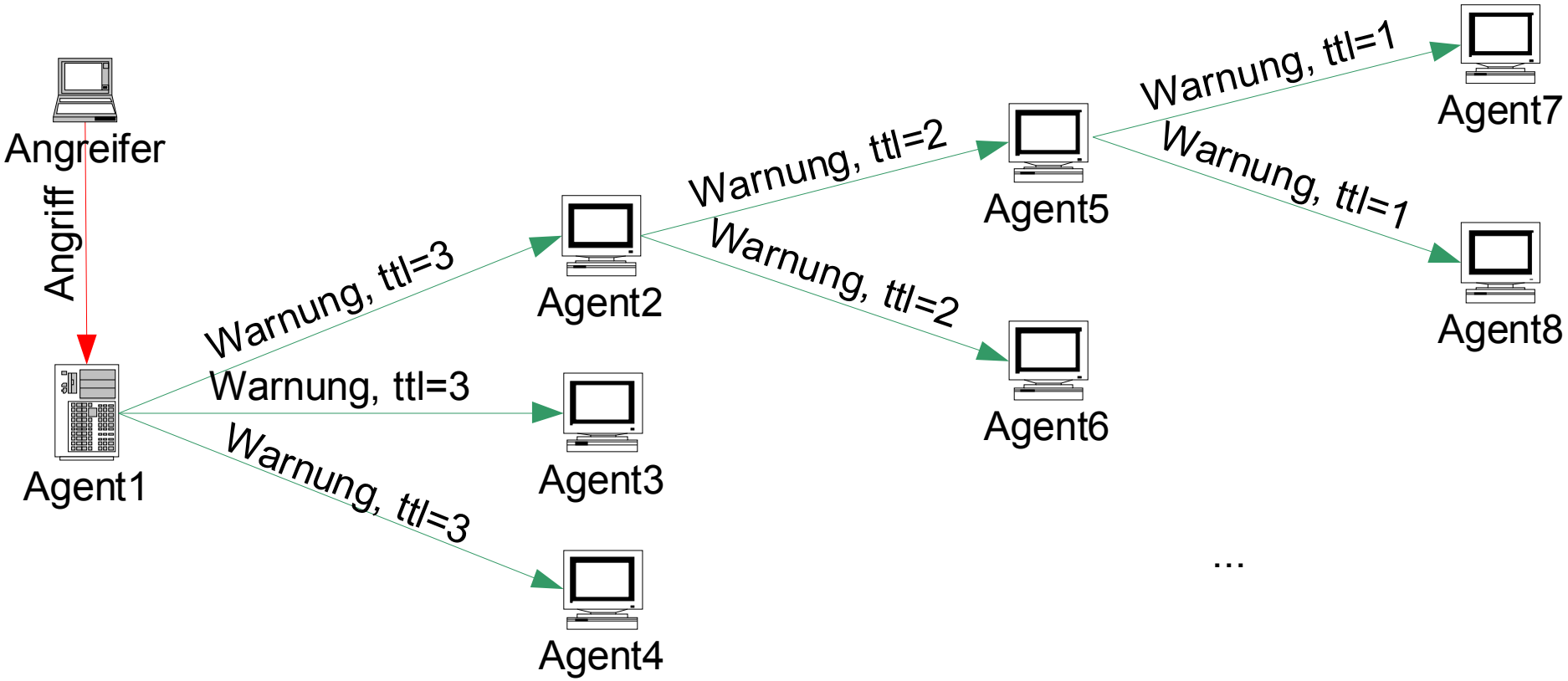


Nachteile:

- Verschwenderischer Umgang mit Ressourcen
- möglicher DoS

Vertrauensnetz

Lösungsansatz: die Warnmeldung wird nach dem Erreichen einer bestimmten Anzahl von Weiterleitungen verworfen.





Fragen und Antworten



Themenübersicht

Definition des Agentenbegriffs

Anwendungsgebiete für Agenten

Angriffserkennung

- Nachteile des klassischen Modells
- Agentenbasierter Schutz

Zusammenfassung

Vielen Dank für Ihre Aufmerksamkeit