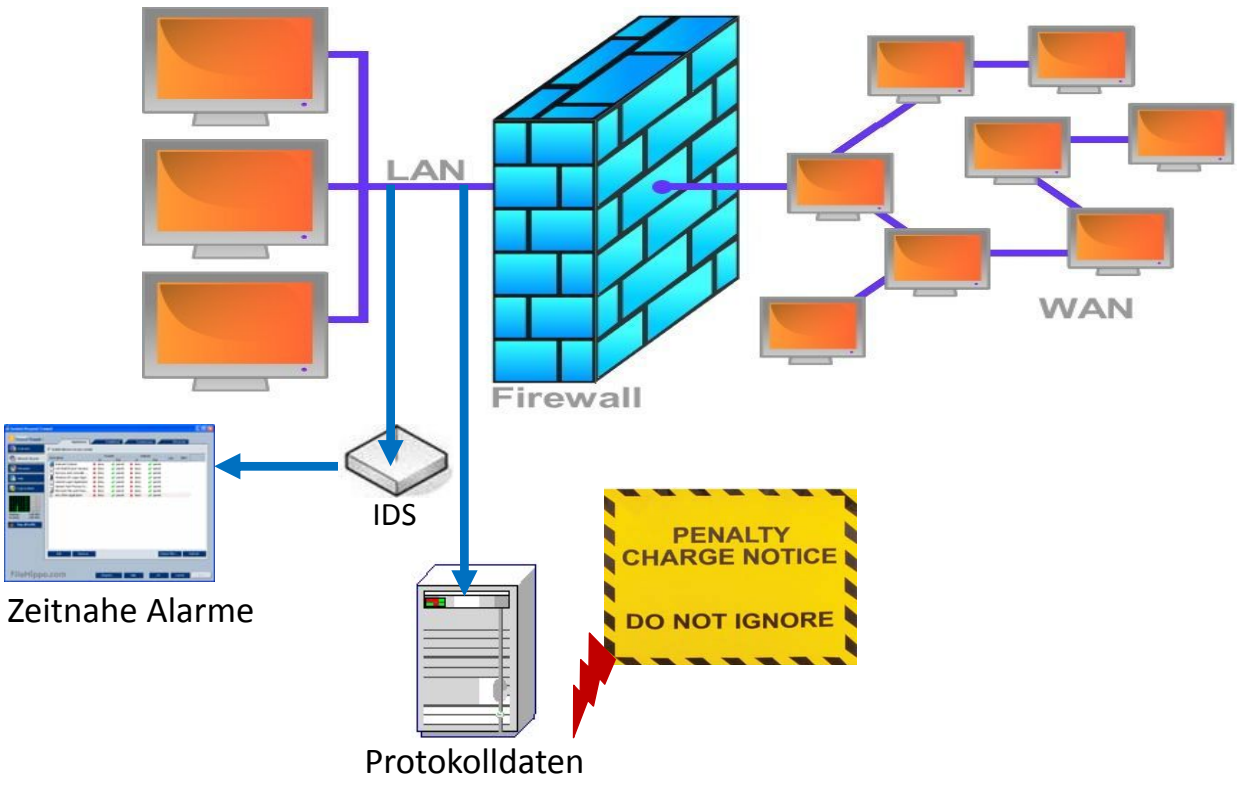
FIfF
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Fachhochschule Brandenburg
University of Applied Sciences

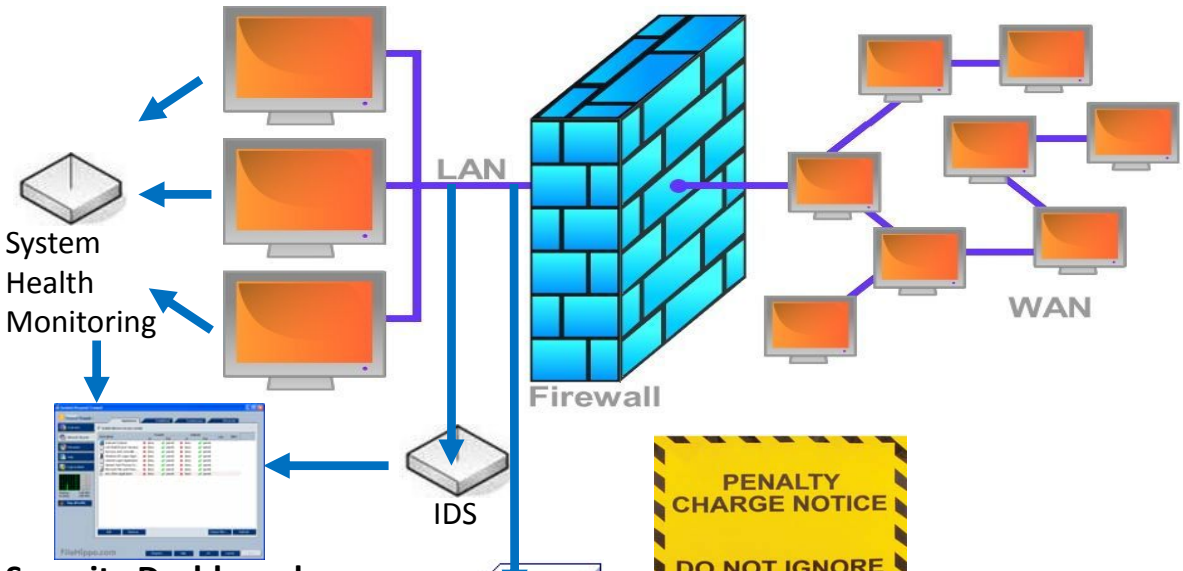
Ute Bernhardt, Ingo Ruhmann

IT-Sicherheitsgesetz und die Praxis

IT-Sicherheitswerkzeuge im Alltag – gestern und heute



IT-Sicherheitswerkzeuge im Alltag – heute und morgen

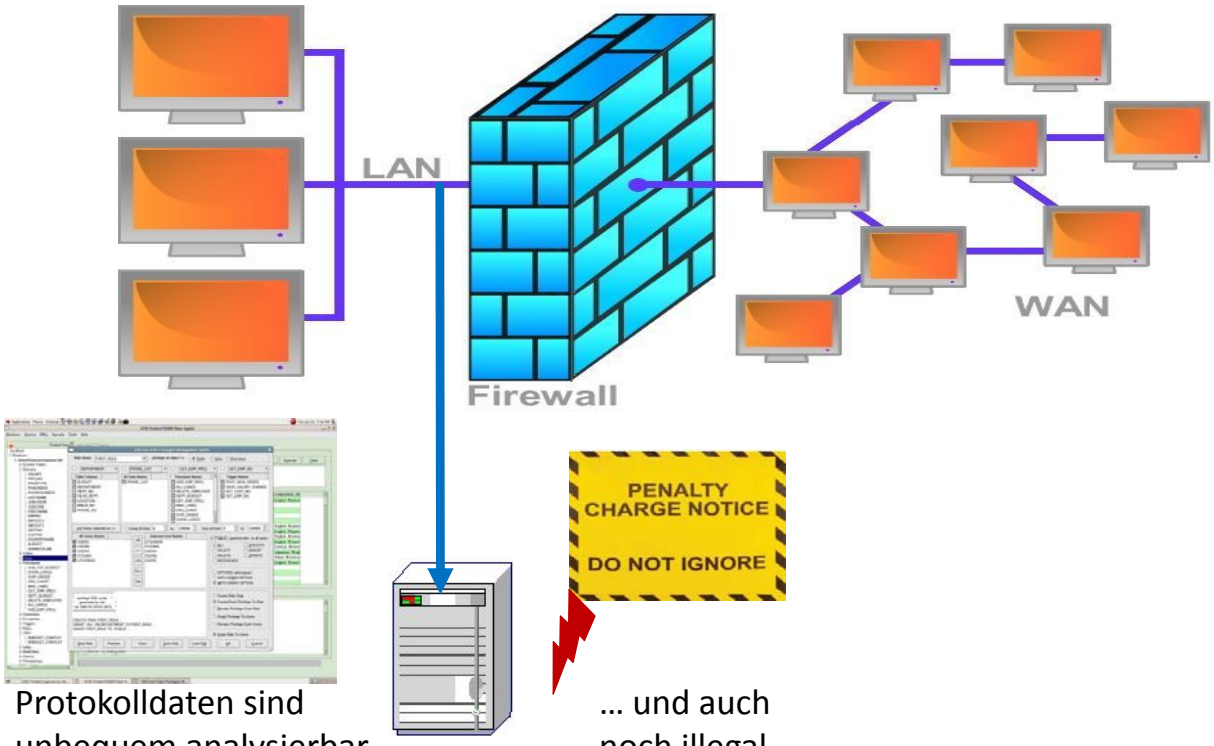


Security Dashboard:
Verbesserte Anomalie-Detektion für zeitnahe Alarme

Zur Verfolgung konkreter Angreifer

Protokolldaten

IT-Sicherheitswerkzeuge im Alltag: Protokolldaten



Protokolldaten sind unbequem analysierbar…

… und auch noch illegal

Mögliche Lösung im BSI-Gesetz?

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

   Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können.

Einschaltung des Datenschutz-Beauftragten bei Durchführung des Verfahrens

Warum verbinden wir nicht die Grundrechte

- Fernmeldegeheimnis nach Art. 10 GG
- Datenschutz-„Grundrecht auf informationelle Selbstbestimmung“
- IT-Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“

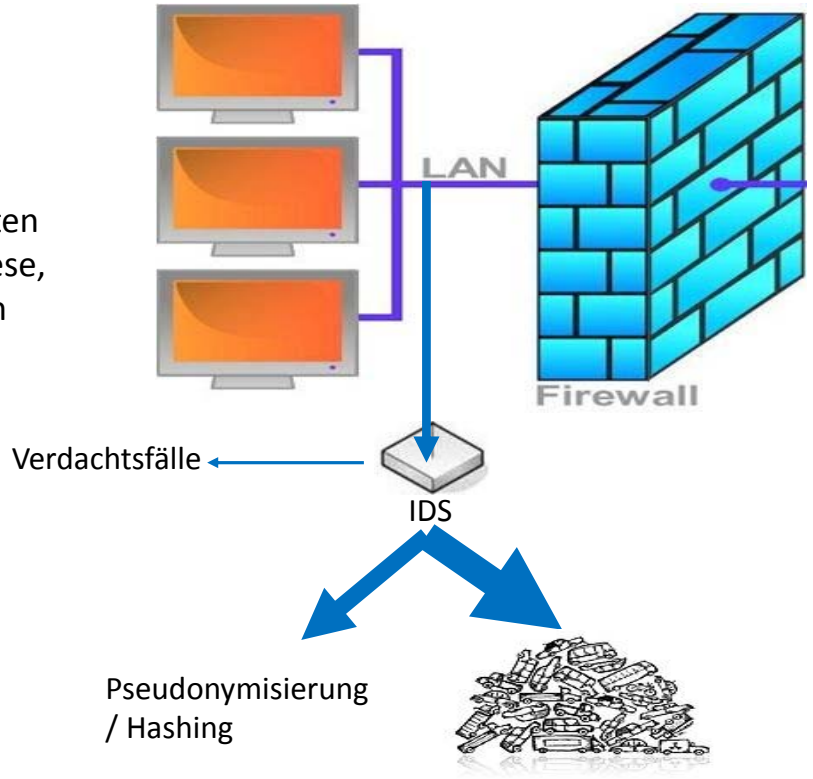
mit dem praktischen Nutzen

- Suchraum verringern: Daten auf begründete Verdachtsfälle reduzieren
- Mensch und Maschine suchen nach bekannten Mustern: Bessere Anomalie-Analysewerkzeuge könnten Verdachtsfälle präziser liefern
- Pseudonymisierung nutzen

und wenden das auf Telekommunikation und Telemedien gleichermaßen an?

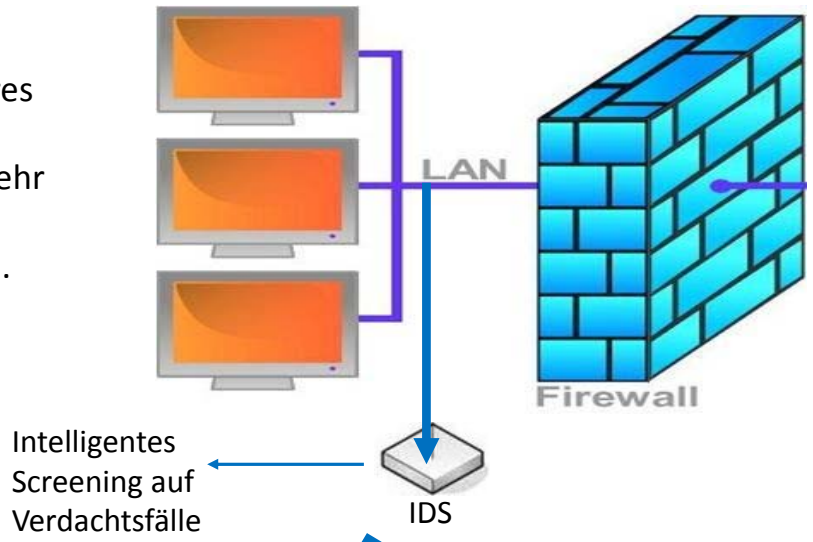
1. Schritt: Vorsortieren

Ein Intrusion Detection System grenzt laufende Verkehrsdaten auf Verdachtsfälle ein und verwirft den Rest der Daten bzw. pseudonymisiert diese, etwa durch ein Verkürzen der IP-Adressen oder ein Hashing der IP-Daten.



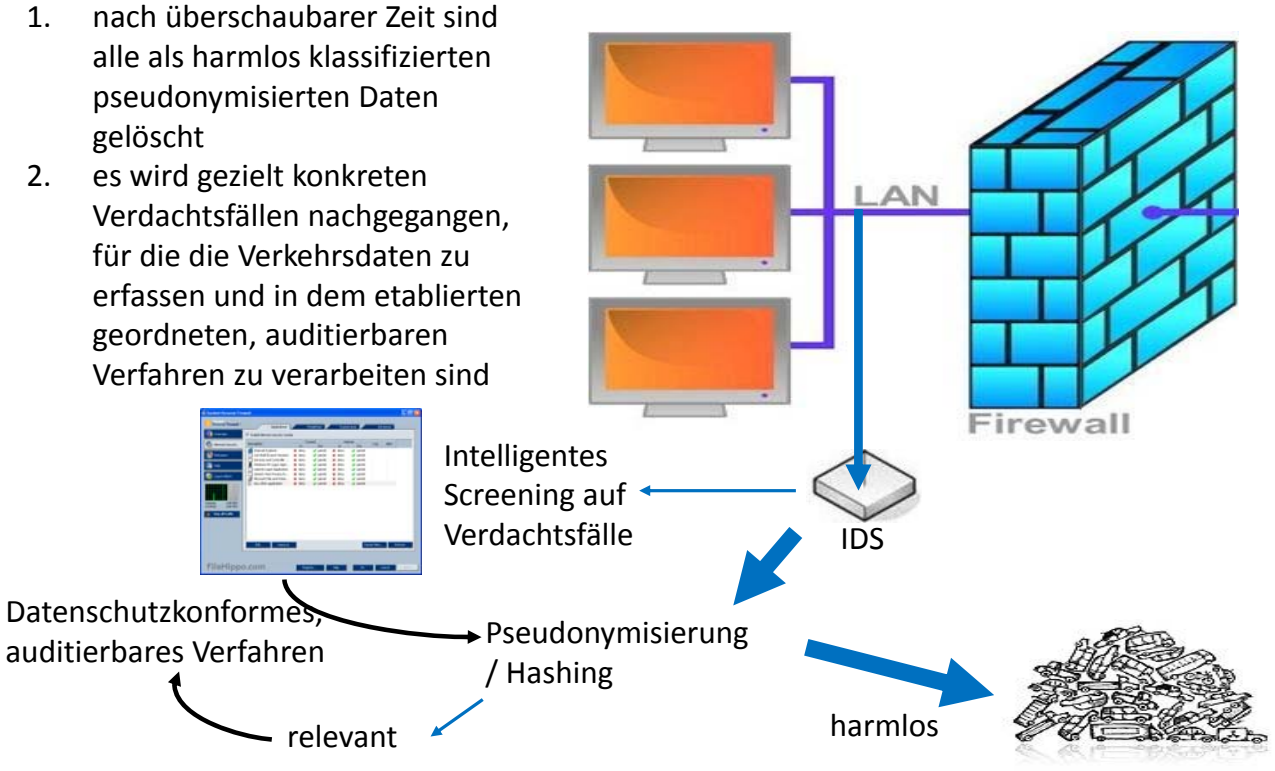
2. Schritt: Verdachtsfall

Im Verdachtsfall ist unmittelbar ein auditierbares IT-Sicherheitsverfahren zur Gefahrenanalyse und -abwehr auf den Daten des Verdachtsfalls anzuwenden.



3. Ergebnis: Weniger Daten, fokussierte Suche nach Anomalien

1. nach überschaubarer Zeit sind alle als harmlos klassifizierten pseudonymisierten Daten gelöscht
2. es wird gezielt konkreten Verdachtsfällen nachgegangen, für die die Verkehrsdaten zu erfassen und in dem etablierten geordneten, auditierbaren Verfahren zu verarbeiten sind



Antwort aus der Praxis

IT-Sicherheit in Deutschland lässt sich grundrechtskonform für alle realisieren

- Mit verfügbarer Technik (noch besser: Weiterentwicklungen)
- mit weniger Aufwand als nach dem BSIG
- mit der inhärenten Option, Anomaliedaten verstärkt auszutauschen
- weg von der „Handarbeit“, hin zu intelligenten Unterstützungssystemen

Jedes Verfahren wird noch besser durch laufende Optimierung in der Praxis – wenn wir damit einmal anfangen.