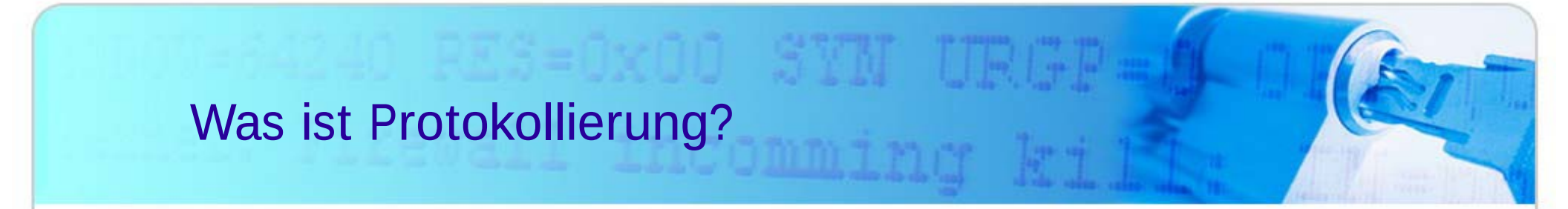
sec4you
Advanced IT-Audit Services Ges.m.b.H.

# Protokollierung

Initiative Informationssicherheit Austria, 20. November 2007

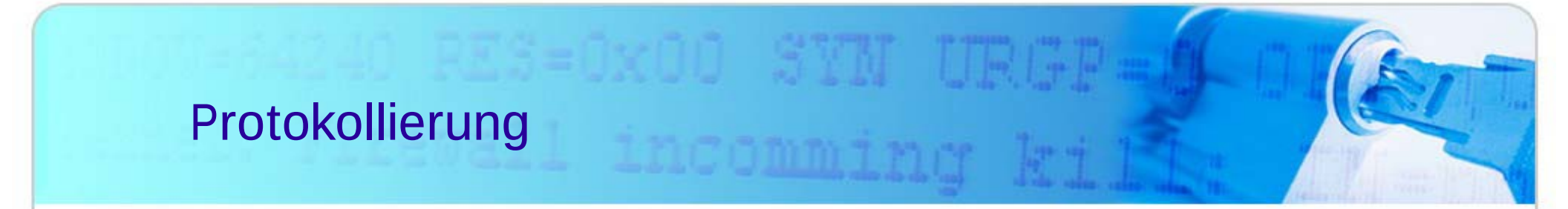
Ein Vortrag von Manfred Scholz CISA ®, CISM ®

# Was ist Protokollierung?



Manuelle oder automatisierte Aufzeichnung von Aktivitäten oder Ereignissen?

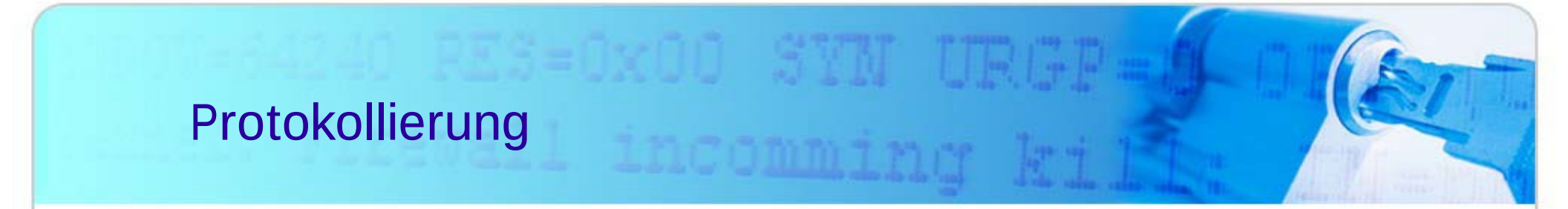
# Protokollierung



**Aspekte der Protokollierung**

- Zweck und notwendiger Umfang
- Technische Umsetzung
- Organisatorische Rahmenbedingungen
- Auswertung versus Kontrolle (Leistungskontrolle (?)
- Gesetzliche Anforderungen
- Beweiskraft vor Gericht
- Aufbewahrungsdauer

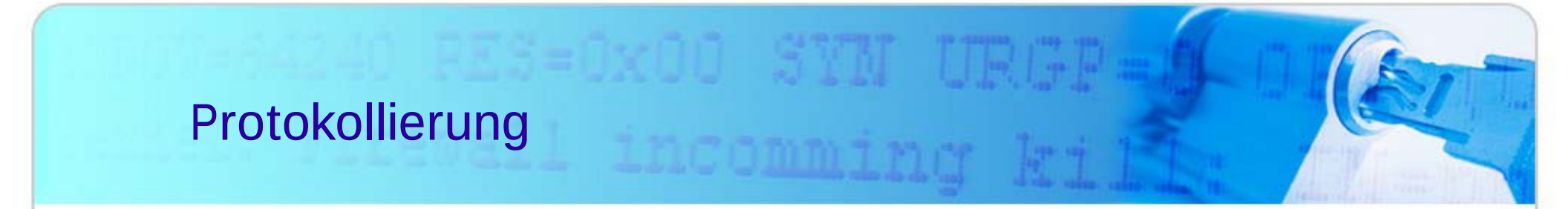
# Protokollierung



**Protokolle sollen die folgenden Fragen beantworten**

- Wer ?
- Was ?
- Wo ?
- Wann ?
- (Warum)

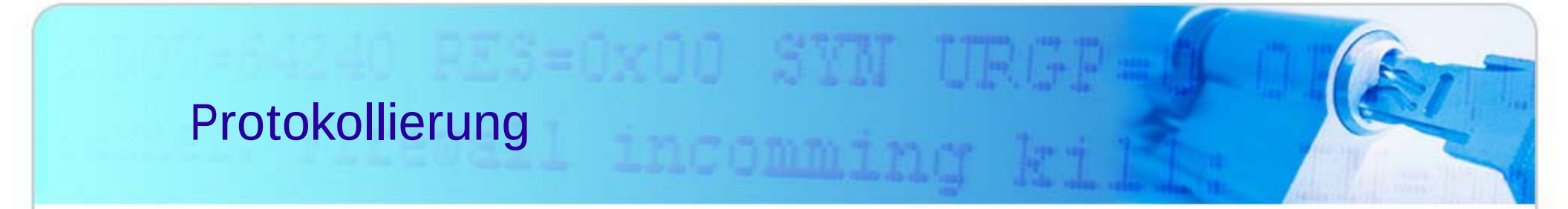
# Protokollierung



**Was kann protokolliert werden?**

- Vergabe von Berechtigungen
- Änderung an Systemen
- Zugriff/ Eingabe/ Änderung oder Löschung von Daten
- Aufruf von Programmen
- Datenübermittlung
- Internet- und Emailnutzung
- Zutritte zu Räumlichkeiten
- Manuelle Tätigkeiten (Kontrolle des täglichen Backups)
- Änderungen in der Protokollierung
- Entscheidungen (?)
- Etc.

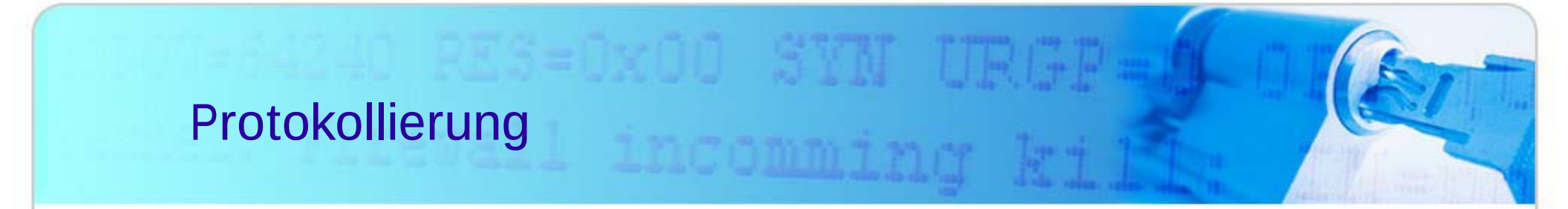
# Protokollierung



**Motivation**

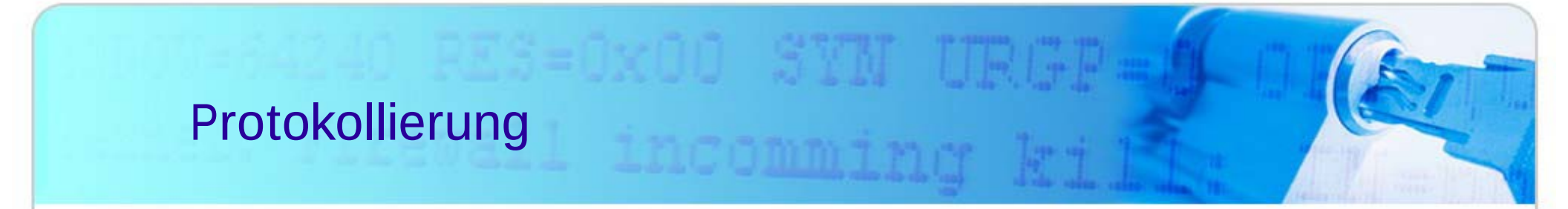
- Fehlersuche
- Nachvollziehbarkeit gewährleisten
- Möglichkeit der nachträglichen Kontrolle
- Erkennen von Unregelmäßigkeiten (Betrug)
- Erkennen von Sicherheitszwischenfällen (Incidents)
- Erfüllung rechtlicher Anforderungen (Compliance)
- Etc.

# Protokollierung



Systemüberwachung versus Verfahrensüberwachung!

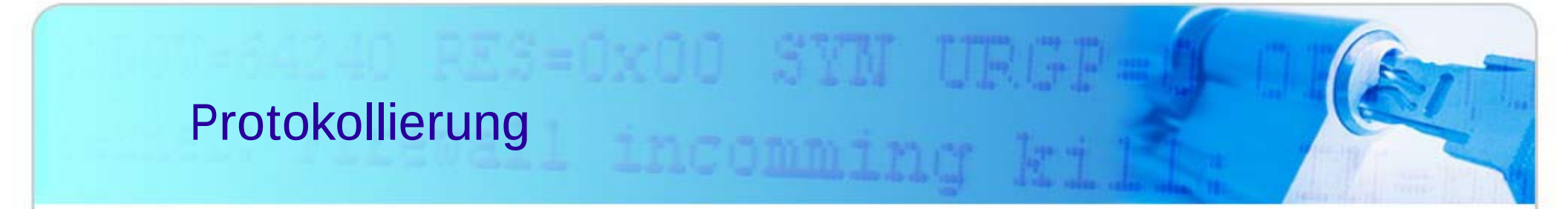
# Protokollierung



**Systemüberwachung (Administration)**

- Monitoring der Basisfunktionen eines Systems
- Modifikation von Systemparametern
- Benutzerverwaltung
- Berechtigungsvergabe
- Datensicherungsaufzeichnungen

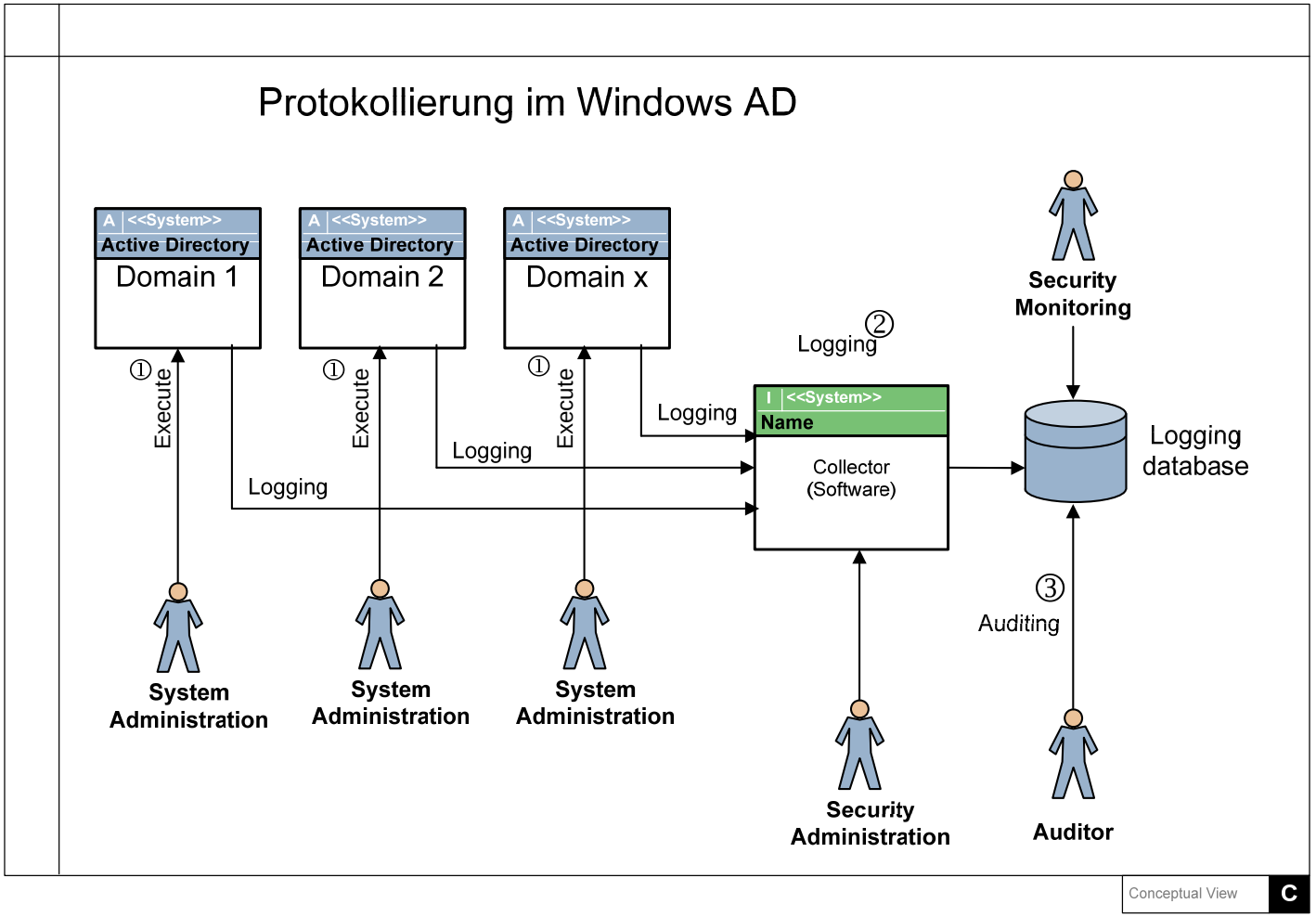
# Protokollierung



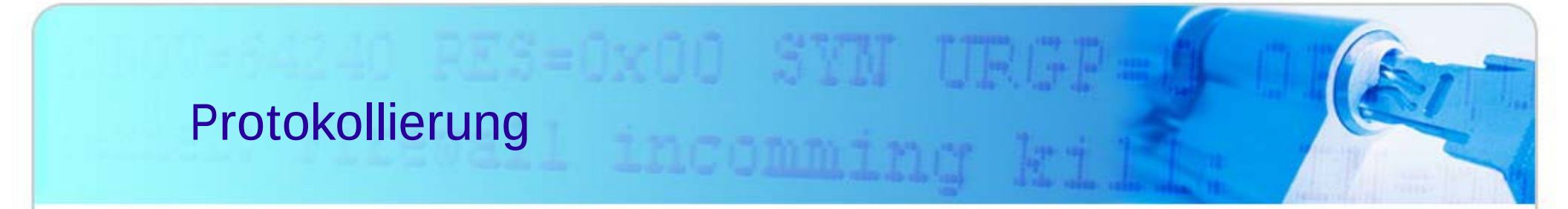
**Verfahrensüberwachung (Nutzung)**

- Monitoring der Nutzung von bereitgestellten Ressourcen
- Verarbeitung von Daten
- Zugriff/ Eingabe/ Änderung oder Löschung von Daten
- Datenübermittlung

# Beispiel aus der Praxis



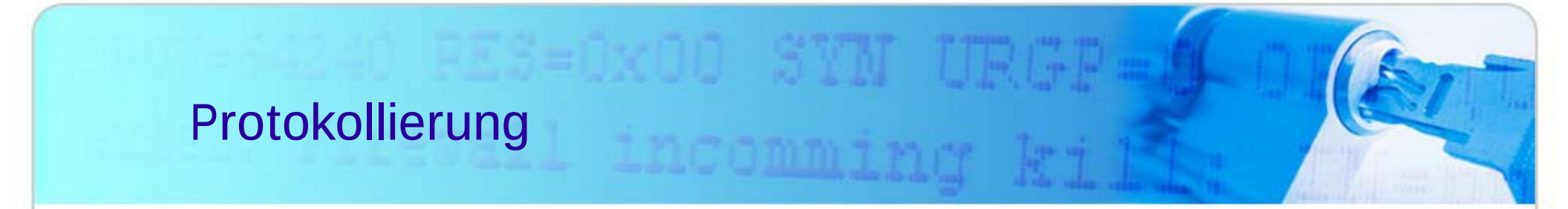
# Protokollierung



**Empfehlungen für die Umsetzung**

- Personalisierte Benutzerkennungen sicherstellen
- Übergreifendes Protokollierungskonzept erstellen
- Zweck der jeweiligen Protokollierungsmaßnahmen festlegen
- Regelungen für die Nutzung von Protokollen festlegen (Auswertungen)
- Gesetzliche Rahmenbedingungen berücksichtigen (Leistungskontrolle)
- Aufbewahrungsdauer festlegen
- Evt. eine notwendige Archivierung berücksichtigen
- Organisatorische Voraussetzungen festlegen und einfordern
- Funktionentrennung berücksichtigen (Beweiskraft !)

# Protokollierung



Offene Fragen?

Tel.: +43 2262 728 57
Manfred.Scholz@sec4you.com