Fälle sicherer Nachweise
Fallen sicherer Nachweise

13.06.2012

Robert M. Albrecht, Matthias Renken

Erleben, was verbindet.

Agenda.

- Wer spricht hier?
- Was ist ein elektronischer Nachweis ?
- Praxisfallen
- Anforderungen an zukünftige Nachweisverfahren

Was ist ein elektronischer Nachweis?

- Log-Datei
  - Technische Informationen direkt aus dem IT-System
- EINE Log-Datei reicht nicht für alle Anwendungsfälle aus
  - Kombination aus mehreren Log-Dateien notwendig
  - Informationen sind doppelt
  - Informationen fehlen
  - Informationen sind nicht eindeutig
- Aggregierte Log-Dateien sind ein **Nachweis**
  - Die Aggregations-Vorschriften sind häufig spezifisch für einen Geschäftsfall

Bedeutung des Nachweises.

Ein elektronischer Nachweis muss viel mehr erfüllen als ein sicheres Logdatum.

- Nachweise werden im Telekommunikationsgeschäft an verschiedensten Stellen gefordert
- Bedienen unterschiedliche Geschäftsfälle
  - Abrechnung
  - Abstreitbarkeit
  - SLA Nachweis
- Erstrecken sich über unterschiedlichste Technologien
- Müssen vielfältig weiterverwendet werden können

➢ Wie funktioniert das in großem Maßstab?

Erleben, was verbindet.

Fall(e) 1.

Heterogene Infrastruktur.

- Nachweise sind über eine Kette von Systemen zu führen, die
  - unterschiedliche Betriebssysteme
  - nicht genormte Schnittstellen
  - verschiedene Protokolle, auch nicht-IP
  - verschiedene Zeichencodierungen
  - unterschiedliche Verfügbarkeiten

  verwenden.

Ein Nachweis ohne durchgängige Kette verursacht hohe Aufwände.

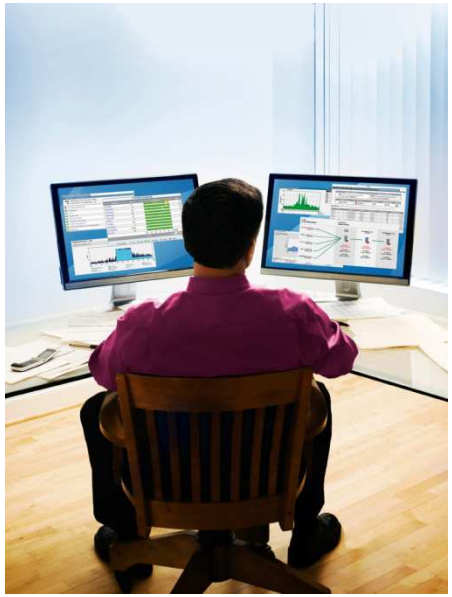
Referenzen Grundschutzkatalog: G 2.22 Fehlende Auswertung von Protokolldaten, G 2.44 Inkompatible aktive und passive Netzkomponenten, M 4.5 Protokollierung bei TK-Anlagen, M 4.106 Aktivieren der Systemprotokollierung, M 4.302 Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten

Erleben, was verbindet.

Fall(e) 2.

Mandantenfähige Logdateien.

- Das Syslog gehört dem System.
- Die Informationen sind nicht nach Benutzergruppen getrennt.
- Betriebsverfassung und Datenschutz fordern die Trennbarkeit der Informationen.



Standardlogs sind für mandantenfähige Systeme nicht verwendbar.

Referenzen Grundschutzkatalog: G 0.29 Verstoß gegen Gesetze oder Regelungen, G 2.61 Unberechtigte Sammlung personenbezogener Daten, M 2.1 Festlegung von Verantwortlichkeiten und Regelungen

Fall(e) 3.

Logdatensemantik.

- Die Inhalte von Log-Dateien auf unterschiedlichen Systemen sind nicht standardisiert:
  - Was bedeutet ein protokolliertes Logdatum?
    - Zeitpunkt an dem ein Ereignis auftritt ?
    - Zeitpunkt an dem das Ereignis protokolliert wurde ?
  - Welche Zeit ist gemeint ?
    - Zeitzone
    - Lokale Uhrzeit des Absenders ?
    - Lokale Uhrzeit des syslogd ?
  - Welche Bedeutung hat das Objekt einer MIB?

Ohne Klärung der Semantik sind übergreifende Nachweise wertlos.

Referenzen Grundschutzkatalog: G 2.27 Fehlende oder unzureichende Dokumentation, M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation

Fall(e) 4.

Logdatensammlung ist ein rekursives Problem.

- Auch das Protokollieren von Protokollen muss nachgewiesen werden.
- Es fehlt ein Metamodell zur Protokollierung.
- Das Modell muss sich ins Governancemodell der Firma einpassen.
- Wie sieht der Prozess zur Logdatenerzeugung und Auswertung aus?

Protokollierungen müssen geregelt werden.

Referenzen Grundschutzkatalog: G 0.29 Verstoß gegen Gesetze oder Regelungen, G 2.1 Fehlende oder unzureichende Regelungen, M 2.1 Festlegung von Verantwortlichkeiten und Regelungen, M 2.64 Kontrolle der Protokolldateien

Fall(e) 5.

Rechtliche Fragen.

- Es gibt national und international unterschiedliche rechtliche Vorgaben für Logdatenerfassung. Daher muss mindestens geklärt sein:
  - In welchem Land und zu welchem Zweck erhebe ich Logdaten?
  - Dürfen die Daten die Landesgrenze verlassen?
  - Wer darf diese Daten sehen?
  - Wie lange dürfen Daten aufbewahrt werden?
- Transportierte Daten müssen anonymisierbar sein, ohne die Integrität zu verlieren

Vor einer Nachweisverwendung die rechtlichen Rahmenbedingungen klären.

Referenzen Grundschutzkatalog: G 0.29 Verstoß gegen Gesetze oder Regelungen, G 2.1 Fehlende oder unzureichende Regelungen, M 2.1 Festlegung von Verantwortlichkeiten und Regelungen

Fall(e) 6.
Architektur.

- Es gibt unterschiedliche architektonische Ansätze eine Protokollierung aufzubauen, wie z.B. zentral vs. dezentral.
- Die Authentifizierung an zentralen Instanzen ist häufig problematisch.
- Es gibt zu protokollierende Systeme, die in der Regel offline sind.

Die Architektur entscheidet über Erfolg der Nachweiskette.

Referenzen Grundschutzkatalog: G 2.44 Inkompatible aktive und passive Netzkomponenten, M 4.225 Einsatz eines Protokollierungsservers in einem Sicherheitsgateway, M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation

Fall(e) 7.
Metadaten.

- Sind die geloggten Informationen im Nachhinein überhaupt verwendbar?
- Sind zur Interpretation Kontextinformationen notwendig ?
  - Zu welcher Sitzung gehört das fehlerhafte HTTP-Paket ?
  - Wer hatte damals die IP-Adresse, von der der Angriff kam (DHCP) ?
  - Gibt es die Benutzerkennung noch oder wurde sie gelöscht ?
    - Oder noch schlimmer: Es gibt inzwischen einen neuen Benutzer oder Computer, der den gleichen Namen oder die gleiche UID hat.
    - Recycelte MAC-Adressen passiert heutzutage bei virtuellen Maschinen.

Metainformationen müssen abgestimmt und archiviert werden.

Referenzen Grundschutzkatalog: G 2.1 Fehlende oder unzureichende Regelungen, G 2.132 Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement,

Anforderungen an sicheren elektronischen Nachweis.

Wünschenswert ist eine durchgängige Nachweiskette.

- „State-of-the cryptographic art“
- Medienübergreifend
- Performant und massendatenfähig
- Von zentraler Stelle managebar
- Mandantenfähig
- Müssen Policies berücksichtigen
- Sollten auf einem Metamodell basieren

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

Robert Albrecht

Utbremer Str. 90
28217 Bremen
Tel.: +49 421 3799 712
eMail: robert-m.albrecht@t-systems.com

Dr. Matthias Renken

Utbremer Str. 90
28217 Bremen
Tel.: +49 421 3799 200
eMail: matthias.renken@t-systems.com

Erleben, was verbindet.