Umfassendes und dennoch datenschutzgerechtes Sicherheitsinformations- & Vorfallmanagement

(Privacy Respecting Security Information & Event Management)

SEALEDFREEZE BY UNISCON GMBH

Ausgangslage: SIEM und Datenschutz in Organisationen

Je mehr die Betriebsprozesse von der IT abhängen, umso wichtiger ist für Unternehmen ein funktionierendes Sicherheitsinformations- & Vorfallmanagement (security information and event management, SIEM).

Beispiel: Analyse bei Hackerangriffen

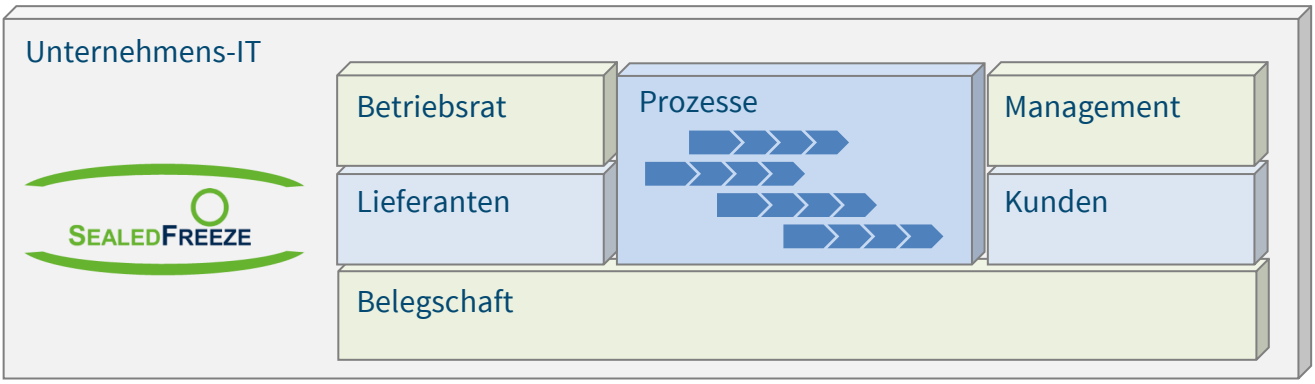
Hackerangriffe werden oft erst nach Tagen, Wochen oder gar mehreren Monaten entdeckt. Nun möchte das Unternehmen wissen:

- Wo ist der Einbruch passiert?
- Welcher Schaden ist vermutlich angerichtet worden?
- Wo waren die Angreifer überall?
- Etc.

Für eine erfolgversprechende forensische Analyse benötigt man eigentlich Daten zu allen Nutzeraktivitäten über mehrere Monate hinweg, sogenannte Metadaten.

Die Erhebung großer Mengen dieser Daten und Speicherung über lange Zeiträume wird jedoch oft wegen Datenschutzbedenken nicht im wünschenswerten Umfang durchgeführt – Stichwort „Gefahr der Mitarbeiterüberwachung".

Mitarbeiter und Betriebsräte haben Bedenken wegen möglichem Missbrauch. Andererseits sind alle Beteiligten jedoch auch an hoher IT-Sicherheit interessiert, denn nur so sind Unternehmenserfolg und Arbeitsplätze geschützt. Die aktuell vorherrschende Datensparsamkeit ist somit ein Hindernis.



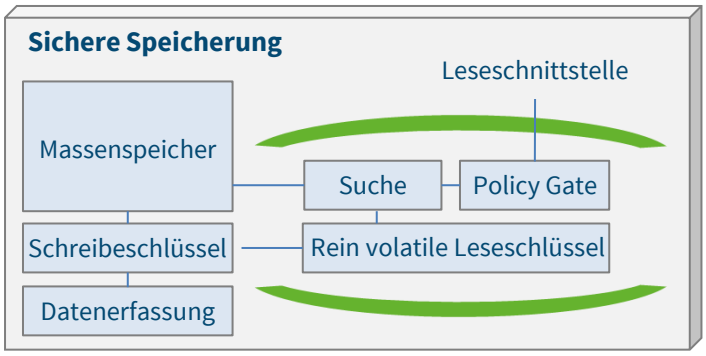
Sealed Computing als Game-Changer

Die zunächst widersprüchlich erscheinenden Ziele der Sicherheit und des Datenschutzes können nun dank eines technologischen Durchbruchs in Übereinstimmung gebracht werden.

Uniscon ist der Pionier im Bereich versiegelter Datenverarbeitung (Sealed Computing) und hat die „Sealed Freeze“ genannte Technologie für umfassende, dennoch hochsichere und außerdem datenschutzgerechte Speicherung und Verwaltung von sensiblen Daten entwickelt.

Beispiele für typische Anwendungsszenarien von Sealed Freeze:

- Aufklärung und Schwachstellenanalyse bei Hacker-Angriffen
- Umfassende Nachweismöglichkeiten der Ende-zu-Ende-Compliance
- Interner Schutz vor und Aufklärung von Industriespionage durch untreue Mitarbeiter



Datenverarbeitung ohne Personenbezug

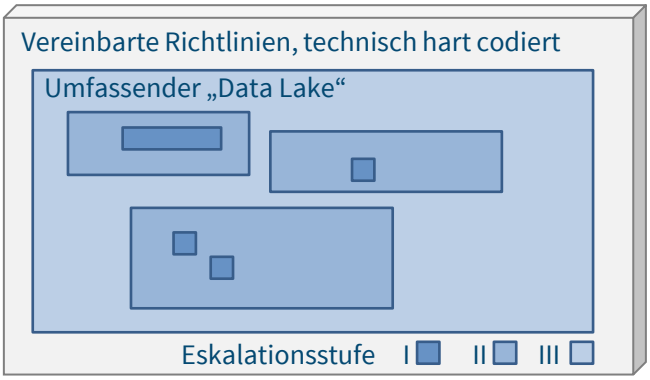
Versiegelte Datenverarbeitung, d.h., „Sealed Computing“, ist eine neue, patentierte Basistechnologie, die verschlüsselnde Verfahren um sichere Verarbeitung ergänzt. Im Rechenzentrum, zu dem die Daten verschlüsselt gelangen und wo diese verschlüsselt gespeichert werden, müssen die Daten dennoch unverschlüsselt verarbeitet werden. Die sogenannte Versiegelung bewirkt durch harte technische Maßnahmen, dass die Daten rein technisch und nicht nur organisatorisch vor dem Zugriff durch Administratoren geschützt sind:

Eine technische Kapselung, technische Versiegelung, verhindert, dass weder der Betreiber des Rechenzentrums noch die Administratoren auf die Daten während der Verarbeitung zugreifen können. Durch diese technische Eigenschaft lebt der Personenbezug in dieser Infrastruktur bei den verarbeiteten Daten gar nicht auf. Diese Innovation eröffnet ein Reihe von neuen Möglichkeiten:

- Mehr Daten können rechtskonform länger gespeichert werden als herkömmlich erlaubt ist
- Daten anderer Art können rechtskonform gespeichert werden als herkömmlich erlaubt ist

Lesen nur gemäß technisch hart kodierter Richtlinien

Die Richtlinien, bei Vorliegen einer juristischen Rechtfertigung Lesezugriffe auf Teile der Daten gestatten, sind technisch hart kodiert und nicht rückwirkend änderbar. Damit ist eine Umgehung der Regeln ausgeschlossen. Die Einhaltung der gesetzlich vorgeschriebenen oder mit dem Betriebsrat vereinbarten Richtlinien ist auf diese Weise technisch sichergestellt. Beispiele für Regeln sind:



- Höchstspeicherdauern
- 4-Augen-Prinzip Betriebsrat & Management
- Mengenkontingente, maximale Datenflüsse
- Eskalationsstufen je nach Datenart
  - z.B. höchste Stufe nur mit Notar

Vollsuche

Die Suche in den gespeicherten Daten kann in dem gesamten „Data Lake“ erfolgen und bei Bedarf auch sehr leistungsfähig gestaltet sein.

Kontakt:
Uniscon GmbH – The Web Privacy Company
Agnes-Pockels-Bogen 1, 80992 München

www.uniscon.de | contact@uniscon.de
Telefon: 089 / 4161 5988 100