Sicherheit

Gastbeitrag: Analyse muss sieben Ws beantworten: Wer hat was auf welchem Objekt wann von wo nach wo zu welchem Objekt geschickt?.

Security Corner: Mit Compliance Profiling dem Täter auf der Spur

Von Wolfgang Böhmer, CISSP, CISA, ISO27001, TU-Darmstadt

31. März 2008

Die Informationssicherheit muss sich heute vor allem mit dem Erfüllen von Compliance-Vorgaben und dem Eindämmen von internen Risiken beschäftigen. Gängige Security-Maßnahmen stoßen hier an ihre Grenzen. Zudem ist es enorm schwierig, internes Fehlverhalten und vor allem Angriffe aus der Flut von Logdaten herauszufiltern. Mit Methoden des Data Mining und erinnerungsbasierter Lernprozesse ließe sich dies zwar automatisieren – doch bisher sind nur wenige Continuous Audit Assessment Tools (CAAT) für Compliance Analysen auf dem Markt.

_Wolfgang Böhmer
Foto: Privat

Die Informationssicherheit hat sich in den letzten Jahren wellenartig entwickelt:

die erste Welle wurde durch rein technische Aspekte (IT-Sicherheit) geprägt;

die zweite Welle kennzeichnet die Anforderung an ein professionelles Management der Prozesse (Informationssicherheitsmanagementsystem);

die dritte Welle brachte Standardisierungen (Normen) mit sich;

die vierte Welle, in der wir uns im Moment befinden, wird bestimmt durch die Information Security Governance. Sie ist durch rechtliche, regulatorische und institutionelle Richtlinien und deren Einhaltung geprägt.

Diese Richtlinien resultieren aus einer neuen, durch Innentäter charakterisierten Bedrohungslage. Die klassische Perimeterabsicherung kam mit der ersten Entwicklungswelle und stellt heutzutage die gängige Praxis im Informationssicherheitsmanagement dar. Dabei ist das zugrunde liegende Bedrohungsmodell durch Angreifer charakterisiert, die von außerhalb gegen ein Unternehmen agieren und deren Merkmale und Verhaltensweisen durch eindeutige Muster geprägt sind.

Gängige technische Absicherungen und Technologien dieser Praxis sind etwa Firewalls, Proxies, Virenschutz, Mail-Scanning oder Intrusion Detection Systeme (IDS). Ziel dieser Absicherungen ist eine Reaktion in Echtzeit sicherzustellen, weshalb Sicherheitseinstellungen einzelner Systeme an Hand technischer Restriktionen erfolgen, die einem vorab definierten Regelwerk

(Policy) unterliegen.

Die Technologien der klassischen Perimeterabsicherung sind nicht für die neuen Bedrohungen durch Innentäter geeignet. Weder die gängigen Sicherheitsstandards (wie die ISO/IEC 27001:2005), noch das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) dressieren die neuen Bedrohungen.

Interne Bedrohungen sind im Vergleich zu externen oftmals wesentlich schwerer auszumachen. Protokollierte Prozesse (Logdaten) können nur schwer als sicherheitsgefährdend identifiziert werden, da sie oftmals von autorisierten Mitarbeitern ausgehen, die gegebenenfalls ungewollt auf einem falschem Pfad wandeln.

Die Indizien ähneln hierbei Puzzlestücken, die es zusammenzusetzen gilt. Darin liegt jedoch die Schwierigkeit. Oftmals – wie in einem echten Puzzle auch – sind sich mehrere Teile sehr ähnlich, was die Erkennung eines Fehlverhaltens und die Identifizierung eines Innentäters deutlich erschwert. Nur ein Einsetzen ins Puzzle zeigt, ob das einzelne Puzzlestück passgenau ist, so dass ein klares Täterprofil durch einen Profiler erstellt werden kann.

Inzwischen sind eine Reihe von gesetzlichen Vorschriften zum Schutz vor inneren Bedrohungen erlassen worden, allen voran der Sarbanes Oxley Act (SOX). Dieser verlangt den an der New Yorker Börse notierten Unternehmen geeignete interne Kontrollsysteme und ein Berichtswesen mit entsprechenden Reports ab.

Die Reports beruhen unter anderem auf Aufzeichnungsdaten (Logdaten), die das korrekte Verhalten beziehungsweise Fehlverhalten von Nutzern und Anwendern belegen sollen. Die Logdaten unterscheiden sich von denen, die für die klassische Perimeterabsicherung gesammelt werden. Die Fragestellung hinsichtlich der Auswertung dieser Logdaten ist auch eine völlig andere. Eine Echtzeitfähigkeit, wie sie bei der klassischen Perimeterabsicherung zum Beispiel bei einem IDS-System zwingend erforderlich ist, spielt keine Rolle. Relevant hierbei ist die Zugriffsoption auf historische Daten.

Im Falle einer Compliance-Analyse, die Teil eines Reports sein kann, werden konkrete Fragestellungen formuliert, die sich als die sieben Ws (W7) bezeichnen lassen: Wer hat was auf welchem Objekt wann von wo nach wo zu

welchem Objekt geschickt. Mit dieser W7-Fragestellung, die auch als Inferenz-Analyse bezeichnet wird, ist eine Schlussfolgerung zwischen potenziellen Tätern und unerlaubten Handlungen in einem Unternehmen möglich.

In diesem Zusammenhang gewinnt das Identity Management nebst ausreichenden und granularen Policies eine besondere Bedeutung. Denn, wenn nicht jeder Mitarbeiter eine zentral verwaltete und überprüfbare Zugriffsberechtigung hat, lässt sich im Nachhinein ein mutmaßlicher Datenmissbrauch nicht eindeutig einer Person zuordnen.

So naheliegend und einsichtig diese W7-Fragestellung ist – umso anspruchsvoller ist es, diese mittels Methoden der Informatik abzubilden und zu automatisieren; sprich ein geeignetes Computerprogramm zu entwerfen. Als eine für diesen Zweck geeignete Methode hat sich das fallbasierte Schließen (Case Based Reasoning, CBR) aus dem Gebiet des Data Mining herauskristallisiert.

Hierbei werden keine Regeln abgleitet, sondern aus einer Sammlung von Fällen (Cases), in den frühere Erfahrungen gespeichert sind, ein erinnerungsbasierter Lernprozess entworfen. Der Lernprozess basiert auf Analogien, im Unterschied zum Lernen durch Induktion und Deduktion. Die Art und Weise wie Fälle repräsentiert werden hängt vom Zweck und Nutzen der Fälle ab.

CBR wird in einem Zyklus von vier Schritten eingesetzt (Selektieren, Wiederverwendung, Überprüfung und Aufnahme). Dabei sind die Fälle keine einfache Auflistung von Merkmalen, sondern dienen bestimmten Zwecken. Im Fall der Compliance-Analyse dient das CBR mit Hilfe der W7-Fragenstellung dem Auffinden von Abweichungen (Fehlverhalten) gegenüber rechtlichen, regulatorischen und institutionellen Vorgaben.

Um auf einem realen Datenbestand eine Compliance-Analyse durchführen zu können, werden vorab eine Reihe unerwünschter Fälle im Zusammenhang mit dem Identitiy Management und den Polices definiert (Trainingsdaten). Beispiel: Wenn eine Person zu ungewöhnlichen Zeiten regelwidrig Datenbestände in einem SAP-System ändert, so stellt dies eventuell einen Datenmissbrauch dar.

Um die unerwünschten Fälle allgemeingültig zu gestalten, wird ein

Ähnlichkeitsmaß definiert, das in der Lage ist, dieselbe Handlung unter anderen Randbedingungen (Zeit, Objekt) ebenfalls zu erkennen. Werden in einem Unternehmen geeignete Daten (Logdaten) aufgezeichnet, so kann mit diesem Verfahren eine Spur (Datenspur) durch die Systeme, Datenbestände und Datenbank nachvollzogen werden, auch wenn diese bereits vor geraumer Zeit entstanden ist. Allerdings schlägt dies System zur Compliance-Analyse nur dann Alarm, wenn Abweichungen zu dem normalen Nutzerverhalten erkennbar sind und eine Toleranzschwelle überschritten wird.

So zukunftsweisend diese kontinuierlichen Überwachungen für Compliance-Analysen sind, umso bedauerlicher ist es, das nur wenige Tools existieren, die in der Lage sind derartiges zu leisten. Hier sind die Softwarehersteller gefordert ihre Security Management Systeme, um die benötigten CAAT zu erweitern.

Die Security-Corner erscheint regelmäßig auf der Homepage der Computer Zeitung in Zusammenarbeit mit (ISC)². In der Kolumne geben IT-Sicherheitsexperten (Certified Information Systems Security Professional, CISSP) Tipps aus der Praxis und kommentieren aktuelle Entwicklungen.

Meinungen bitte an: securitycorner@konradin.de