Outsourcing oder Einbindung externer IT-Kräfte

Insider-Threat-Management: Wer macht was, wann, wo?

Die internationale Wirtschaft befindet sich noch immer im Übergang vom Zeitalter der IT-Industrialisierung hin zum Digitalisierungszeitalter. Getragen wird dieser Übergang durch den Einsatz und den Nutzen neuer Informationstechnologien im Geschäftskontext, welche auch zur schnellen Verdrängung etablierter Geschäftsmodelle und neuer Sicherheitsrisiken führen können.

Von Dennis Buroh, Consist Software Solutions GmbH

Der Wandel innerhalb der Wirtschaft durch innovative IT-Projekte ist mit einem enormen personellen Zeitaufwand verbunden und belastet die IT-Mitarbeiter der Firmen sehr stark. Die Lösung bieten hier die Zusammenarbeit mit externen IT-Dienstleistern und das Outsourcing von Regeltätigkeiten.

Allerdings verstecken sich in dieser Zusammenarbeit auch verschiedenste Sicherheitsaspekte, die durch regulatorische Anforderungen (Grundsätze ordnungsmäßiger Buchführung bei Auslagerung rechnungslegungsrelevanter Prozesse und Funktionen einschließlich Cloud-Computing, IDW RS FAIT 5, bankaufsichtliche Anforderungen an die IT, IT-Grundschutz etc.) oder durch die neuen Angriffsmöglichkeiten von außen erzeugt werden.

Fallstricke in der Zusammenarbeit

Im Fokus dieser Sicherheitsaspekte steht die Frage, „Wer hat wann mit welchen Mitteln was veranlasst beziehungsweise worauf zugegriffen?“. Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?“ Klare Verhaltensregeln, insbesondere im Umgang von Kollegen und Führungskräften untereinander, in Kombination mit geeigneten, internen Kontrollsystemen sind zusätzlich unabdingbar.

Sämtliche Maßnahmen sollten daher protokolliert und überwacht werden. Hierzu zählen beispielsweise Beantragungs-, Genehmigungs- und Überprüfungsverfahren für Berechtigungen. Betroffen sind sowohl IT-Infrastruktur als auch IT-Anwendungen. Von der Netzwerkkonfiguration über Server-, Storage- und Virtualisierungssysteme bis hin zu Datenbanken und Anwendungen erstreckt sich daher das Szenario. Auch die funktionale Trennung zwischen nicht zu vereinbarenden Tätigkeiten, beispielsweise der IT-Entwicklung und des IT-Betriebs, sollte dabei im Fokus stehen.

Jedoch greifen diese Sicherheitsversuche viel zu häufig ins Leere, da der Faktor Mensch zu wenig bedacht wird. Die beste und preiswerteste Sicherheitslösung bietet keinen Mehrwert, wenn sie von einem Mitarbeiter oder externen Dienstleister, der interne Rechte besitzt, umgangen werden kann.

Erweiterte Angriffsszenarien

Im Übrigen werden auch die Angriffsvarianten immer professioneller und die Angreifer wenden zunehmend Techniken an, die bisher nur aus Spionageangriffen bekannt waren. So attackierte beispielsweise die Lazarus-Gruppe weltweit Banken mit einer Malware, um gefälschte Überweisungen über das SWIFT-Netzwerk zu veranlassen. Die Carbanak-Gruppe wiederum kompromittierte Finanzinstitute und Geldautomaten, um ebenfalls Überweisungen zu fälschen. Beide Gruppen setzten Techniken ein, die über die bisher beobachteten Methoden normaler Malware hinausgingen. Das exakt auf ausgewählte Mitarbeiter zugeschnittene Social Engineering zählt hierzu ebenso wie das Lateral Movement, also das Ausbreiten im internen Netz, indem erbeutete Zugangsdaten verwendet und Nutzerrechte ausgeweitet werden.

Im Juni 2017 beobachtete das Bundesamt für Sicherheit in der Informationstechnik (BSI) professionelle Cyberangriffe via Spear-Phishing-Mails auf private E-Mail-Postfächer von Funktionsträgern der Wirtschaft. Ein Jahr zuvor registrierte das BSI bereits Spear-Phishing-Mail-Angriffe gegen Kunden der deutschen Webmail-Industrie wie gmx.de und web.de.

Neue Generation von Sicherheitslösungen

Als Antwort auf diese gestiegenen Sicherheitsaspekte und Angriffe via Social Engineering hat sich als Best Practise die Durchführung von Insider-Threats-Projekten, Penetrationstests und Log Management mit User Behaviour Analytics etabliert.

Abbildung 1: Anstieg Cyberkriminalität gesamt und Anteile Computerbetrug sowie Ausspähen/Abfangen von Daten daran. Bild: Polizeiliche Kriminalstatistik des BKA

Im besonderen Fokus dieser neuen Generation von Sicherheitsmechanismen stehen der Mitarbeiter und der externe Dienstleister beziehungsweise Provider, der im Unternehmen interne Rechte eines Mitarbeiters besitzt. Aufgrund der meist ausgelagerten administrativen Tätigkeiten handelt es sich hierbei zum Teil sogar um hoch privilegierte Administrationsrechte, die auch zur Verschleierung von Aktivitäten verwendet werden könnten. Inzwischen achtet auch der Gesetzgeber immer mehr auf diese weitreichenden Eingriffsmöglichkeiten und fordert von den Unternehmen technisch-organisatorische Maßnahmen, damit Vorgaben aus Berechtigungskonzepten nicht umgangen werden können (z. B. BaFin und BSI).

Mehr als 58 Prozent der US-amerikanischen Firmen betreiben aus diesem Grunde bereits eine Anwenderprotokollierung und führen Penetrationstest durch, wie aus einer aktuellen Cybercrime-Umfrage aus den USA hervorgeht. In Deutschland ist diese Anzahl wesentlich geringer, da häufig die Bedenken betreffend Datenschutz und Mitarbeiterrechten fälschlicherweise sehr hoch und zum Teil negativ behaftet sind.

Sind die Bedenken bei einem klassischen Penetrationstest mit den drei Test-Modulen „Social-Engineering-Angriff“, „Interne Sicherheit“ und „Externe Sicherheit“ in Deutschland noch sehr gering, sind sie bei einer Insider-Threat-Lösung mit „Data Loss Prevention“ (DLP), „User Access Management“ (UAM) und „User Behavoir Analytics“ (UBA) bereits wesentlich höher. Gleichwohl dient ein Insider-Threat-System sowohl dem Datenschutz als auch der Datensicherheit und baut auf den gewonnenen Erkenntnissen aus einem Penetrationstest auf. Es bewahrt somit vor finanziellen Schäden durch entwendetes geistiges Eigentum und schützt vor dem Imageverlust, der durch eine solche Datenpanne verursacht werden kann. Gleichzeitig schließt es die gefundenen Sicherheitslücken aus einem Penetrationstest.

Die Einführung eines Insider-Threat-Systems bietet noch wesentliche weitere Sicherheitsvorteile und wird angesichts der gestiegenen Bedrohungslage in Deutschland immer wichtiger. In seiner letzten Erhebung aus 2016 verzeichnete das Bundeskriminalamt 80,5 Prozent mehr Straftaten im Bereich der Cyberkriminalität gegenüber dem Vorjahr (vgl. Abbildung 1).

Technische Lösungen nur in der Verknüpfung erfolgreich

Aktuelle Zahlen der International Data Group (IDG) aus den USA zeigen jedoch, dass die alleinige Einrichtung eines Insider-Threat-Systems und Durchführung eines Penetrationstests nicht zum Erfolg führen ohne ein adäquates User Behaviour Analytics. Denn es geht nicht nur um den böswillig handelnden Mitarbeiter oder externen Dienstleister im Unternehmen, sondern auch um solche, die nicht umsichtig, zum Teil fahrlässig handeln. Beispielsweise der Mitarbeiter, der am Wochenende noch zuhause arbeiten möchte und zu diesem Zweck die erforderlichen Daten an seine private E-Mail-Adresse versendet oder auf einen USB-Stick kopiert.

Die protokollierten Tätigkeiten des Mitarbeiters müssen daher immer im gesamten Arbeitskontext betrachtet werden. Diesen Kontext erreicht man in der Tiefe durch die Verknüpfung des Insider-Threat-Systems mit einem umfassenden Log-Management. Experten, die mit beiden Sicherheitssystemen vertraut sind, können durch diese Verknüpfung schnelle Erfolge und Mehrwerte für das Unternehmen erzielen. Sicherheitsvorfälle wie jüngst beim Unternehmen Tesla können so verhindert werden. Bei diesem Vorfall hatte ein Mitarbeiter von Tesla interne Firmengeheimnisse entwendet und der Produktentwicklung durch falsche Eingaben schweren Schaden zugefügt.

IT-Sicherheit als Innovationsgarant

Es wird somit zwingend empfohlen, eine firmenweite Lösung aufzubauen, bei der die neuen Sicherheitsmechanismen eng miteinander verzahnt sind und sich gegenseitig ergänzen. Hierbei sollte man sich nicht zu viel Zeit lassen, schließlich muss durch die allumfassende Digitalisierung das Sicherheitssystem immer wieder neu und in hohem Tempo an die dynamischen Rahmenbedingungen angepasst werden. Nur eine direkte enge und angemessene Verzahnung der Sicherheitssysteme gewährleistet, dass die großen Digitalisierungsprojekte zu einem Gewinn und nicht zu einem Data Leak mit Imageverlust werden. Denn Cybersicherheit ist keine Innovationsbremse, sondern ein Innovationsgarant, wie es auch das BSI in seinem letzten Lagebericht beschrieben hat. ■