Mehr Datensicherheit bei Internet-Geschäften

Mit ihrer Offensive im Cyberspace winken den Unternehmen nicht nur bessere Geschäfte. Je weiter sie sich mit ihrem Business ins Internet vorwagen, desto mehr laufen sie volles Risiko, Opfer von Cyberkriminellen jeglicher Couleur zu werden. Ihre Daten könnten ausgespäht, manipuliert oder sabotiert werden. Das heißt für die Unternehmen im Umkehrschluss: Wenn sie nicht ihr Geschäft, ja ihre geschäftliche Existenz, aufs Spiel setzen wollen, müssen sie ihre Offensive im Internet durch mehr Datensicherheit flankieren. Ganz vorne an steht dabei eine hieb- und stichfeste Zugriffskontrolle. Sie sollte alle wichtigen Funktionen für Data-Governance einschließen.

Das geschäftliche Engagement der Unternehmen im Internet stellt veränderte Anforderungen an die Planung ihrer Zugriffskontroll- und Data-Governance-Lösung. Daten wandern nicht nur von Verarbeitungs- zu Verarbeitungsinstanz und Speicherort zu Speicherort. Daten, aus strukturierten Anwendungen entnommen, werden auf dem Weg von Anwendung zu Anwendung und Datentopf zu Datentopf oftmals auch zu unstrukturierten Daten. Nicht strukturiert, kann auf diese Anwendungen und ihre Daten kaum Zugriffskontrolle ausgeübt werden. Dieses Manko trifft die Unternehmen bei ihrem geschäftlichen Engagement im Internet um so mehr, zumal, unabhängig davon, wo die Anwendungen und Daten residieren, die Zugriffe bis auf Datenebene kontrolliert werden müssen.

Die Herausforderung für die Planer besteht einerseits darin, den Fluss der geschäftskritischen Daten en detail nachzuvollziehen, andererseits den unstrukturierten Daten die Struktur und das Format der jeweiligen Anwendung zu verleihen. Zuvor ist es die Aufgabe der Fachabteilungen, für ihren Verantwortungsbereich zu klären, welche Daten für das Geschäft und für Data-Governance kritisch sind und welche nicht. Mit Blick auf Data-Governance sollte außerdem analysiert werden, wer wo entlang der digitalen Geschäftsprozesse für die Rechtevergabe und für die Kontrolle der erteilten Zugriffsrechte zuständig ist. Die Recherche und Strukturierung der Daten muss mit gleicher Gründlichkeit nicht nur innerhalb des eigenen Unternehmens, sondern auch bei den Geschäftspartnern und Service-Providern, die an den digitalen Prozessen mitwirken, durchgeführt werden. Danach kann ein Datenzugriffsmodell erstellt werden. Es sollte die organisatorische Konstellation, die digitalen Prozesse sowie die daran beteiligten IT-Ressourcen und Personen widerspiegeln. Dieses Datenzugriffsmodell ist wiederum notwendig, um angelehnt an der Sicherheitsstrategie des Unternehmens für die Zugriffskontrolle und für Data-Governance alle erforderlichen Regeln und Rollen sowie Auswertungen festzulegen.

Das Gesamtkonzept aus Regeln, Rollen und Auswertungen sollte anschließend dem jeweiligen Fachverantwortlichen zur Prüfung vorgelegt werden. Sie kennen für ihren Bereich die Sicherheits- und Data-Governance-Auflagen, einschließlich der Compliance-Vorschriften, am besten. Demzufolge können sie auch für ihren Verantwortungsbereich am besten die Folgen quantifizieren, wenn Regeln und Rollen nicht angemessen befolgt beziehungsweise umgesetzt werden. Damit sollten es auch die Fachverantwortlichen sein, die für die Genehmigung und Erteilung der Rollen mit den Zugriffsrechten verantwortlich zeichnen.

Anhand der vorgegebenen Regeln kann immer wieder geprüft werden, inwieweit sich die Fachverantwortlichen und ihre Mitarbeiter tatsächlich an die Vorgaben und Vorschriften gehalten haben. Zudem wird mittels des Regeleinsatzes an der Konsole sofort transparent, wenn sich entlang digitaler Geschäftsprozesse Sicherheits- und/oder Data-Governance-Lücken auftun. Last but not least dienen die sicherheitsstrategiekonformen Regeln dazu, um für Data-Governance, einschließlich Compliance, alle notwendigen Audits und Reports zu bestimmen. Kommt es zu Regelverstößen in jeglicher Form, wird an der zentralen Konsole automatisch ein Alarm ausgelöst.

Erst nach dieser gründlichen Vorarbeit sind die Voraussetzungen für eine granulare Zugriffskontrolle geschaffen, um daran für Data-Governance gezielt mit Funktionen wie Alarming, Auditing und Reporting anzudocken. Für eine angemessene technische Umsetzung kristallisiert sich im Markt ein neues Werkzeugset heraus. Es vereint beides, tiefgehende Zugriffskontrolle bis auf Datenebene und alle für Data-Governance wichtigen Funktionen, in einem System. Sogar forensische Auswertungen räumt die neue Tool-Generation ein. Auch diese Form der Auswertungen ist für die Unternehmen extrem wichtig. Sie können die daraus gewonnen Erkenntnisse immer wieder nutzen, um die herausgebildeten Regeln, Rollen und Kontrollen über die Zeit zu verfeinern, also zu verbessern.

Allerdings bietet der Markt bisher nur wenige Toolsets, die komplett aufgestellt sind sowie sich verhältnismäßig einfach in der Implementierung, als eingänglich in der Bedienung und kostensparend im Betrieb erweisen. Zu diesen Ausnahmen gehören die Toolsets von Dell („Dell One Identity Manager“) oder White Box Security („WhiteOps“). Angesichts dieser Ausgangssituation sollten die Unternehmen die Offerten ob ihrer funktionalen und praktischen Fähigkeiten genau prüfen oder prüfen lassen und auf Referenzen bestehen. Erprobte Lösungen bringen es mittlerweile auf immerhin mehr als einhundert Installationen, dies sowohl in größeren als auch in kleineren Unternehmen.

Norbert Drecker,
Geschäftsführer des Sicherheitsspezialisten Twinsec E-Mail: Norbert.Drecker@twinsec.de