6 Schritte zu effektiver Datensicherheit

Datenschutz spielt in Unternehmen eine immer wichtigere Rolle. Bisher vertrauen viele auf das sogenannte Discovery-First-Modell. Bevor sich aber mit diesem Ansatz die Sicherheit verbessern läßt, sind aufwendige Analysen notwendig: Welche Daten sind an welchem Ort gespeichert? Wem gehören sie? Und wer kann darauf zugreifen? Darüber hinaus müssen Unternehmen Datenflüsse sowie Lebenszyklen abbilden und auch bestimmen, welche Vorschriften für sie gelten. Das kostet wertvolle Zeit und Ressourcen. Eine Alternative bietet die werteorientierte Datensicherheit.

Eine Studie von Bitkom aus dem Jahr 2022 zeigt, daß Cyberkriminelle weiterhin die digitalen Daten Dritter ins Ziel nehmen. 68 % der betroffenen Unternehmen geben an, daß Kommunikationsdaten wie E-Mails entwendet wurden. Jedes vierte Unternehmen meldet den Verlust kritischer Business-Informationen wie Marktanalysen (28 %) oder Daten von Mitarbeitern (25 %). Doch wie können Unternehmen ihr Sicherheitsrisiko minimieren?

Sechs Prinzipien der werteorientierten Datensicherheit: Grundsätzlich sollten sich Unternehmen auf praktische Kontrollen zur Behebung von Datenschwachstellen und Bedrohungen konzentrieren:

1. Produkte definieren: Eine erste Vorgehensweise läßt sich aus der industriellen Produktion lernen. Dort führten lange Planungsprozesse und übermäßige Lagerhaltung zu ineffizienten Prozessen. Um diesen Problemen entgegenzuwirken, entstanden neue Methoden – beispielsweise die agile Fertigung oder der Lean-Construction-Ansatz. Beide definieren bereits zu Beginn ihr Produkt und ermitteln, wie es geliefert wird. Dadurch läßt sich die Wertschöpfungskette optimieren. Ein ähnliches Vorgehen empfiehlt sich bei der Datensicherheit. Dort ist der Datenschutz das Produkt. Doch diese technischen Maßnahmen allein reichen nicht. Auch der Mensch sollte mit einbezogen und nicht nur als Sicherheitslücke gesehen werden. Er kann als zusätzlicher Abwehrschirm gegen Cyberangriffe helfen.

2. Effiziente Entdeckung: Die Kenntnis über den Speicherort bestimmter Daten ist zwar wichtig, sollte aber nicht im Mittelpunkt stehen. Stattdessen empfehlen sich am Anfang eher umfassende Kontrollen von offensichtlichen Sicherheitsrisiken. Dazu gehören Wechseldatenträger und Übertragungen auf persönliche Cloud-Speicher oder E-Mail-Konten. Aber auch die automatische Bereinigung öffentlicher Ordner oder die Quarantäne stark veralteter Daten sollte beachtet werden. Idealerweise liegt der Fokus stets auf Aufgaben, die den Betrieb nicht stören.

3. Zuerst Dienste aufbauen: Erfolgreiche Kontrollen sollten mit den Unternehmenszielen vereinbar sein – etwa in Bezug auf Benutzerfreundlichkeit und Kommunikation, aber auch Prozesse für Ausnahmen sollten nicht vergessen werden. Es empfiehlt sich, Mitarbeiter so früh wie möglich über Risiken oder wichtige Maßnahmen zu informieren. Hierfür eignen sich z B. Pop-up-Fenster mit einem Hinweis zur sicheren Zusammenarbeit. Auch lassen sich Metriken einbinden, um Führungskräften eine bessere Übersicht zum Nutzerverhalten ihrer Mitarbeiter zu liefern.

4. Automatisierte Abläufe: Effektive Sicherheitsdienste nutzen Informationen aus der Datenerkennung oder -klassifizierung, um die Ergebnisse zu operationalisieren. Beispielsweise könnte das System mithilfe eines DLP-Dienstes bei Uploads auf persönliche Webmails warnen. Auch eine vollständige Sperrung anstelle einer einfachen Warnung läßt sich bei Bedarf auslösen.

5. Metriken bewußt einsetzen: Mithilfe genauer Analysen lassen sich Sicherheitskontrollen verbessern und Dienste bewerten. Wichtig sind dabei intern ausgerichtete Metriken. Sie zeigen etwa, wie lange der Dienst für eine typische Kontrolle braucht. Zusätzlich gibt es externe Metriken, mit denen sich der grundsätzliche Erfolg erkennen lässt – beispielsweise die Menge gelöschter Altdaten oder die Anzahl blockierter Uploads. Außerdem lassen sich mit einigen extern ausgerichteten Parametern die Schwächen des Dienstes identifizieren. So zeigt die Reaktionszeit bei der Eskalation an, ob etwa eine Neuverteilung von Verantwortlichkeiten notwendig ist.

6. Insider-Risikomanagement: Es wird immer wichtiger, interne Sicherheitsrisiken zu minimieren. Derzeit reagieren Unternehmen oftmals erst, nachdem eine Schwachstelle erkannt wurde. Doch ein solches Vorgehen hat Schwierigkeiten bei großen, komplexen und hybriden Betriebsumgebungen. Das sogenannte Insider Risk Management (IRM) nutzt hingegen einen ganzheitlichen Ansatz. Es versucht grundsätzlich zu verstehen, warum gegen bestimmte Richtlinien verstoßen wird. Aus den Ergebnissen dieser Untersuchungen lassen sich dann die Sicherheitskontrollen und die Kompetenz der Mitarbeiter verbessern. Schulungen helfen außerdem bei der Mitarbeiterbindung und -zufriedenheit. Im Kern des IRM geht es also um Menschen, Prozesse und deren Interaktion. Je besser diese Maßnahmen greifen und akzeptiert werden, desto eher kann auch in weitere Technologien investiert werden, um die Transparenz zu erhöhen und sie in bestehende Prozesse zu integrieren.

Noch Fragen?
www.kudelskisecurity.com/de