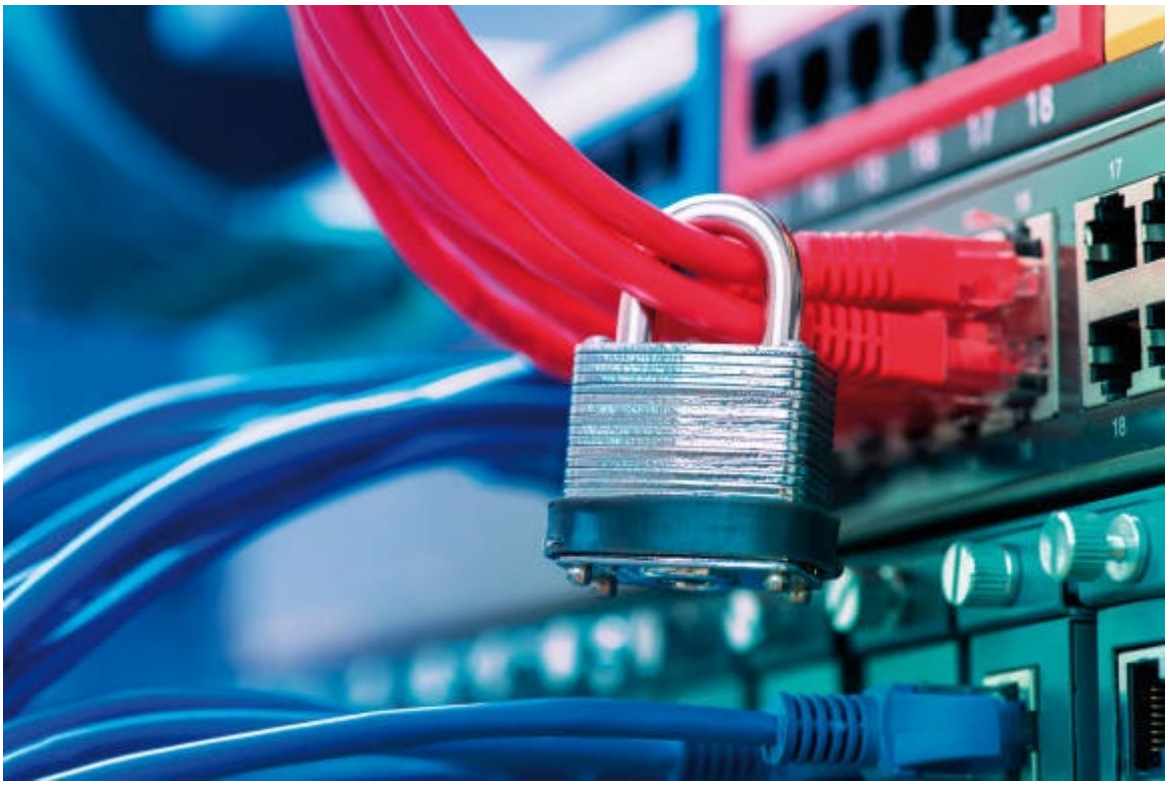
Gastbeitrag *19.04.2022, 07:30 Uhr*

… (Titel)

… (Lead)



… (Legende)
(Quelle: Shutterstock/asharkyu)

Die Entscheidung für die Digitalisierung ist ein entscheidender Wendepunkt für Unternehmen, insbesondere wenn diese mit einem Wechsel in die Cloud einhergeht. Die Vorteile sind nicht von der Hand zu weisen: mehr geschäftliche Agilität, höhere Flexibilität und deutlich mehr Effizienz. Doch die Cybersicherheit darf in diesem Zusammenhang nicht einfach als gegeben betrachtet werden.

Denn Anwendungen und Daten befinden sich jetzt nicht mehr länger «im» Unternehmen – also innerhalb des eigenen Netzwerks –, sondern können überall sein. Und auch die Mitarbeitenden selbst, die mit diesen Anwendungen und Daten arbeiten, sind heute nicht mehr nur im Büro anzutreffen. Durch die Pandemie beschleunigt, sind Home Office und Remote Working nicht nur mehr einer Minderheit vorbehalten; dieser Trend hat landauf, landab auch in Branchen Einzug gehalten, die sich das Anfang 2020 nicht hätten vorstellen können. Diese Entwicklung hat aber zur Folge, dass Mitarbeitende ohne die

Anwesenheit von Kollegen oder Vorgesetzten mit sensiblen Daten arbeiten und das Risiko für unbeabsichtigte und auch beabsichtigte Datenlecks steigt.

… (Zwischentitel)

Laut des aktuellen Ponemon-Reports zu den weltweiten Kosten von Insiderbedrohungen 2022 machen fahrlässig handelnde Insider den grössten Anteil (56 %) der Zwischenfälle aus – womit belegt ist, dass auch eine scheinbar harmlose Aktion zu ernsthaften Zwischenfällen führen kann. Die durchschnittlichen Kosten pro Zwischenfall liegen dabei laut Ponemon Institute bei 485 000 US-Dollar.

Was tun Unternehmen also, um vertrauliche oder sensible Daten zu schützen und den Benutzerzugriff sowie das Identitätsmanagement in der Cloud-Umgebung zu verwalten? Hier ein Blick auf einige der am häufigsten eingesetzten Massnahmen:

- 59 Prozent der Befragten gaben an, dass ihr Unternehmen Verschlüsselung, Tokenisierung oder andere kryptografische Tools zum Schutz von Daten in der Cloud einsetzt.
- 56 Prozent der Unternehmen verwenden einen Cloud Access Security Broker (CASB).
- 45 Prozent der Unternehmen haben getrennte Identitätsmanagement-Schnittstellen für die Cloud und die lokale Umgebung.
- 39 Prozent der Befragten gaben an, dass ihr Unternehmen eine einheitliche Identitätsverwaltungsschnittstelle für die Cloud und die lokale Umgebung verwendet.

… (Zwischentitel)

Ein Zwischenfall, der durch einen böswilligen Insider verursacht wurde, schlägt mit durchschnittlich 648 000 US-Dollar zu Buche. Und solche Vorfälle sind für etwas mehr als 25 Prozent aller Insiderbedrohungen verantwortlich. Gerade in Zeiten hoher Fluktuation, wie sie viele Branchen aktuell erleben, ist zu erwarten, dass dieses Risiko weiter zunimmt.

Neben fahrlässig und böswillig handelnden Mitarbeitern gibt es noch eine dritte Kategorie, nämlich wenn Cyberkriminelle Cloud-Konten übernehmen und damit im

technischen Sinn zu Insidern werden. Laut des zitierten Ponemon-Reports hat sich die Zahl der Vorfälle dieser Kategorie seit der letzten Erhebung im Jahr 2020 fast verdoppelt. Dem Bericht «The Cost of Cloud Compromise and Shadow IT» des Ponemon Institute zufolge, verlieren Unternehmen durch kompromittierte Cloud-Konten durchschnittlich jährlich 6,2 Millionen US-Dollar oder 3,5 Prozent ihres Gesamtumsatzes.

… (Zwischentitel)

Leider installieren viele Mitarbeiterinnen und Mitarbeiter neue Cloud-Anwendungen und -Services, ohne vorher die Zustimmung der IT-Abteilung eingeholt zu haben. Ein weiterer Faktor, der bei vielen Unternehmen zu einer schwachen Sicherheit im Bereich Cloud Computing beiträgt, ist das Fehlen klar definierter Rollen und Verantwortlichkeiten für den Schutz vertraulicher oder anderer sensibler Informationen in der Cloud. Weniger als die Hälfte, nämlich 44 Prozent, der Unternehmen haben diesen Prozess bereits implementiert, so die Ergebnisse der Studie des Ponemon Institute. Ausserdem gaben lediglich 39 Prozent der Befragten an, dass ihr Unternehmen vor der Bereitstellung von Cloud-Anwendungen eine sorgfältige Bewertung derer durchführt.

Besondere Vorsicht ist geboten, wenn OAuth ins Spiel kommt. OAuth ist ein Autorisierungsprotokoll, das einer Drittanbieteranwendung den begrenzten Zugriff auf einen Cloud-Dienst ermöglicht. Die Kontoinformationen oder Daten eines Anwenders können dabei von Drittanbieteranwendungen genutzt werden, ohne dass das Kennwort des Anwenders abgefragt wird. Leider dienen einige OAuth-Berechtigungsanfragen auch böswilligen Zwecken. Die Cyberangreifer können die OAuth-Zugriffsrechte zur Kompromittierung und Übernahme von Cloud-Konten nutzen. Solange der OAuth-Token gültig ist, haben die Angreifer zudem dauerhaften Zugriff auf das Konto und die Daten des Anwenders – selbst wenn der Anwender das Kennwort ändert oder die Zwei-Faktor-Authentifizierung (2FA) aktiviert hat.

Trotz all ihrer Vorteile schaffen Cloud-basierte Anwendungen und Dienste also neue Risiken, die es abzuwägen und einzudämmen gilt. Für moderne Unternehmen, die mit einer hybrid tätigen Belegschaft arbeiten, kann es ein schwieriger Balanceakt sein, diese neuen Risiken zu bewältigen, ohne die vielen Vorteile einer Cloud-Migration aufs Spiel zu setzen.

Wenn es für fahrlässige, kompromittierte und böswillige Anwender nur einen universellen Sicherheitsansatz gibt, hat das häufig folgende Konsequenz: Fahrlässige Anwender sind frustriert, weil sie blockiert werden, während böswillige Anwender und externe Angreifer die Kontrollen schlicht umgehen.

Die Cloud-Sicherheit sollte mit der Absicherung genehmigter Anwendungen – wie Microsoft 365 und Google G Suite – beginnen, doch dort nicht enden. Um umfassende Sicherheit zu gewährleisten, sind deutlich mehr Transparenz und Kontrolle darüber erforderlich, wie Mitarbeiter auf Anwendungen und sensible Daten in der Cloud zugreifen, sie nutzen und teilen.

… TITEL FÜR KASTEN

Fahrlässige Anwender machen ohne böse Absicht einen Fehler oder suchen bei der Wahrnehmung ihrer Aufgaben nach einem einfacheren Weg. Zusätzlich zum Blockieren riskanter Aktivitäten bietet moderne DLP (Data Loss Prevention) für diese Anwender Coachings an, damit sie ihr Verhalten verstehen und ändern und dennoch produktiv bleiben.

Kompromittierte Anwender sind Opfer eines externen Cyberangreifers, der die Kontrolle über ihre Konten übernimmt und diese missbräuchlich verwendet. Modernes DLP nutzt risikobezogene Kontrollen, um nach Anzeichen für eine Kompromittierung zu suchen, zusätzliche Sicherheitskontrollen anzuwenden und bei Bedarf riskante Aktivitäten zu blockieren.

Böswillige Anwender exfiltrieren vorsätzlich Daten zu ihrem persönlichen Vorteil. Basierend auf Risikofaktoren wie Kündigungen oder unübliche Aktivitäten in Verbindung mit vertraulichen Dateien, ist es mit moderner DLP möglich, bestimmte Anwender enger zu überwachen, strengere Zugriffskontrollen anzuwenden und schädliche Aktionen proaktiv zu blockieren.

… (Zwischentitel)

Die heutigen Angriffe zielen auf Menschen, nicht auf Technologie. Unternehmen können sich nicht mehr allein auf den Perimeterschutz konzentrieren (der die Insiderbedrohung ohnehin nie wirksam abwehren konnte). Stattdessen müssen sie einen modernen,

personenzentrierten Sicherheitsansatz für die Cloud und gegen Datenverlust (Data Loss Prevention, DLP) verfolgen.

Eine solche Lösung, die den Menschen in den Mittelpunkt stellt, berücksichtigt, wer am häufigsten angegriffen wird, wer anfällig für Angriffe ist und wer privilegierten Zugriff auf sensible Unternehmensdaten hat. Dieses Mass an Transparenz und Kontrolle ermöglicht es Unternehmen, Bedrohungen abzuwehren, Informationen zu schützen und rechtliche Vorschriften einzuhalten.

Um ein Unternehmen in der Cloud umfassend zu schützen, müssen sich Sicherheitsteams mit Bedrohungsschutz, Datensicherheit und App-Governance befassen. Ferner sind Investitionen in Technologien, internes Fachwissen und Benutzerschulungen/Awareness-Trainings erforderlich, welche die Mitarbeiter in den Mittelpunkt der Strategie stellen und den Bogen zur Sicherheit schlagen.