imprivata® | Ponemon INSTITUTE

Cybersicherheits-Risiko durch komplexe Lieferketten

PONEMON Bericht 2025 | Deutschland

01 Einführung

Unternehmen agieren heutzutage in komplexen Lieferketten, um effektiv und erfolgreich zu sein. Dazu zählen u.a. Lieferanten, Zulieferer, Subunternehmer, Dienstleister und andere Partner. Oft sind gerade diese sogenannten Drittanbieter die Verursacher von Cyber-Vorfällen. Tatsächlich berichteten 51 Prozent der Befragten von Organisationen in Deutschland, dass sie in den letzten zwölf Monaten einen Datenverlust oder einen Angriff erlebt haben, der aus einem Drittanbieter-Zugriff resultierte. Das sind mehr als im globalen Durchschnitt von 47 Prozent.

Das Ponemon Institute befragte in Deutschland 573 IT-Profis aus den Branchen Gesundheitswesen, öffentliche Verwaltung, Finanzdienstleistungen, Fertigung und anderen. Zu den wichtigsten Erkenntnissen der Studie gehören: .

- Die durch Drittanbieter-Zugriff verursachte Gefahr für die IT-Sicherheit ist erheblich und dauerhaft.
- Organisationen bemühen sich, das Risiko zu minimieren, was jedoch nur teilweise gelingt. Zu oft fehlen Budget, Ressourcen und zentrale Kontrolle oder Verantwortlichkeiten.
- Organisationen müssen ihre Strategien zur Absicherung von Drittanbieter-Zugriffen optimieren und ausbauen.

Dieser Kurzbericht konzentriert sich auf die wichtigsten Erkenntnisse aus Deutschland, mit zusätzlichen Daten zur Verbreitung von Zugriffsrisiken durch Drittanbieter. Um mehr über den globalen Kontext und weitere Erkenntnisse zu erfahren, lesen Sie den vollständigen Bericht **„The state of third-party access in cybesecurity“**.

02 Wichtige Erkenntnisse: Häufigkeit der Bedrohungen durch Drittanbieter -Zugriffe in Deutschland

Das Risiko durch Zugriffe von Drittanbietern ist groß und Angriffe können erhebliche geschäftliche, finanzielle und betriebliche Auswirkungen haben. Die Bedrohung wird auf dem aktuellen hohen Niveau verbleiben – oder sich sogar verschlimmern – und Organisationen ist bewusst, dass sie sich mit den Gefahren durch den Zugriff von Drittanbietern beschäftigen müssen.

51% der befragten Organisationen in Deutschland haben in den letzten 12 Monaten einen Datenverlust oder Cyber-Angriff erlebt, der durch den Zugriff eines Drittanbieters ausgelöst wurde.

34% sagten, der Angriff oder Datenverlust sei auf zu umfassende und weitreichende Zugriffsrechte des Lieferanten zurückzuführen.

26% konnten die Ursache für den Cyber-Angriff oder Datenverlust nicht herausfinden, vermutlich aufgrund mangelnder Nachvollziehbarkeit der Attacke.

Häufigste Folgen von Datenverlusten

Verlust sensibler Informationen **(55%)**

Beendigung der Beziehung zum Drittanbieter **(55%)**

Bußgelder und Geldstrafen **(47%)**

68%

der Befragten befürchten, dass Datenverluste, die durch Drittanbieter verursacht werden, in den nächsten 12 bis 24 Monaten gleichbleiben oder zunehmen werden.

47%

der Befragten geben an, dass sich der Fernzugriff durch Drittanbieter zu ihrem größten Risiko entwickelt.

95.000€ Durchschnittliche Kosten für die Wiederherstellung des Zugriffs nach einem Datenverlust in Deutschland

03 Mehr zum Thema Risiken durch Drittanbieter-Zugriffe

Deutsche Organisationen haben bei der Minimierung des Risikos durch Drittanbieter-Zugriffe einen schweren Stand. Mehr als die Hälfte der Organisationen haben in den vergangenen zwölf Monaten einen Drittanbieter-Zugriff-bezogenen Angriff oder Datenverlust gemeldet und 68 Prozent gehen davon aus, dass solche Angriffe gleichbleiben oder zunehmen. Damit ist die Notwendigkeit einer besseren Sicherheitsstrategie für Drittanbieter-Zugriffe offensichtlich. Mit angemessener Priorisierung und Finanzierung können Organisationen ihre Strategie zur Abwehr des Risikos durch Zugriffe von Drittanbietern verbessern.

Laden Sie den Bericht „*The state of third-party access in cybesecurity*“ herunter, um umfassende Informationen über die weltweiten Bedrohungen durch Drittanbieter-Zugriffe zu erhalten. Erfahren Sie, wie Organisationen versuchen, sie zu bekämpfen, warum sie Schwierigkeiten haben und welche Strategien für mehr Zugriffssicherheit eingesetzt werden.

Jetzt herunterladen