3 Supply-Chain-Attacken: Drittanbieter als Risiko für großflächige Datenschutzverstöße

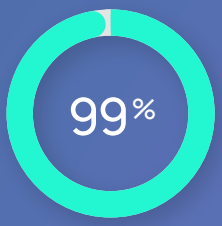
Drittanbieter sind aus dem Geschäftsbetrieb nicht mehr wegzudenken ...

Die Sicherheitsstrategie Ihrer Organisation ist immer nur so stark wie die Ihrer Drittanbieter. Laut unserer Umfrage zu den aktuellen Cybercrime-Trends **sind heute 99 Prozent der Organisationen in der DACH-Region bei der Bereitstellung ihres wichtigsten Angebots von Drittanbietern abhängig**. Doch diese Abhängigkeit hat ihren Preis. Jeder einzelne Anbieter bringt mehr Abhängigkeiten, Datenaustausch und Zugriffspunkte mit sich – alles potenzielle Eintrittstore für Cyberkriminelle. Anstatt in ihr Zielunternehmen direkt einzudringen, können Angreifende einen Umweg über einen weniger stark gesicherten Zulieferer nehmen und so lateral profitablere Opfer infiltrieren. Oder sie unterbrechen einen einzigen Service und treffen damit gleich mehrere Organisationen gleichzeitig.

Im vergangenen Jahr wurde deutlich, mit welcher Effizienz Cyberkriminelle Profit aus digitalen Lieferketten schlagen. Im Juli 2024 machten sich Angreifende schwere Sicherheitslücken in den Fortinet-Produkten FortiOS und FortiProxy zunutze.[1] Es gelang ihnen, Schutzmechanismen zu umgehen und sich unberechtigten Zugriff auf die betroffenen Systeme zu verschaffen. Nur einen Monat zuvor wurde CDK Global durch einen Ransomware-Angriff gezwungen, seine Systeme abzuschalten.[2] Dies hatte großflächige Geschäftsunterbrechungen und massive finanzielle Verluste bei über 15.000 US-Autohändlern zur Folge, die Dienste des Softwareanbieters nutzten.

... doch jeder weitere Partner vergrößert auch die Angriffsfläche

In den **komplexen und stark verknüpften Ökosystemen** vor allem der großen Unternehmen sind die Auswirkungen von Schwachstellen in der Lieferkette noch weitreichender. Große Organisationen sind nicht nur von **ihren eigenen Zulieferern abhängig, sondern wiederum auch von deren Zulieferern** – es entsteht ein großflächiges Netz an Schwachstellen, das auch als **Viertparteienrisiken** bezeichnet wird.[3] Da es für Organisationen kaum möglich ist, einen Überblick über sämtliche Verknüpfungen zu haben, können sie das Risiko ihrer Partnerschaften und das gesamte Ausmaß ihrer Angriffsfläche nur schwer einschätzen.



Prozent der Organisationen in der DACH-Region sind bei der Bereitstellung ihres wichtigsten Angebots von Drittanbietern abhängig.

1 **Golem (2024).** Kundendaten von Cybersecurity-Konzern abgeflossen.
2 **IT-Daily (2024).** Cyberangriff auf Software-Anbieter trifft tausende US-Autohändler.
3 **Dataminr (2024).** Third-party Vulnerabilities Put the Public Sector at Risk: What to Consider.