Sicherheit in der Lieferkette

Wie sicher sind Supply-Chains noch?

Im Zuge der Cloudifizierung von Lieferketten häufen sich potenzielle Schwachstellen – das Cyber-Risiko steigt. Die Gründe dafür sind vielfältig, ebenso wie die Möglichkeiten, die Gefahren zu reduzieren.

Michael Moser, DSAG-Fachvorstand Produktion & Supply-Chain-Management

Supply-Chain-Management (SCM)-Software ist von ihrer Architektur her so konzipiert, dass Unternehmen über sie miteinander kommunizieren und Planungsdaten, Spezifikationsdokumente, Bestandsinformationen etc. austauschen. Klassischerweise laufen SCM-Lösungen On-Premise und sprechen im Zweifelsfall nicht einmal mit dem Internet. Inzwischen aber werden solche Prozesse zwischen Unternehmen und ihren Zulieferunternehmen mehr und mehr in Cloud-Lösungen bzw. hybride Landschaften verlagert. Das Risiko, dass Kriminelle über die dabei verwendeten Schnittstellen Angriffe gegen die Supply-Chain starten können, steigt dadurch. Wer System A von Lieferant B knackt, hat schnell auch Zugriff auf System C vom Kunden D.

Lieferketten werden also anfälliger – und dies, obgleich sie angesichts der weltweiten Krisenlage ohnehin bereits instabil sind. Gegen die neuen Gefahren im Zuge der Cloudifizierung müssen sie folglich abgesichert werden. Das funktioniert beispielsweise über die Härtung von Schnittstellen via Web-Application-Firewall.

Risiko-Management oft nur unzureichend definiert

Die neuen, hybriden Prozesse müssen darüber hinaus ausreichend überwacht und gemanaged werden. In vielen Unternehmen aber ist das Risiko-Management innerhalb der Supply-Chain nur unzureichend definiert.

Arbeitskreis Security & Vulnerability Management

Der Arbeitskreis Security & Vulnerability Management mit seinen über **2.100 Mitgliedspersonen** beschäftigt sich generell mit Fragestellungen der **technischen und organisatorischen Sicherheit**, vermehrt jedoch auch mit den neuen **Herausforderungen durch die Digitalisierung und IoT**.

dsagnet.de/go/security

Gibt es jemanden, der dafür zuständig ist, dass alle Lieferanten ISO 27001-zertifiziert sind? Der festlegt, dass nur mit solchen Lieferanten Geschäfte gemacht werden, die eben dieses Sicherheitsniveau nachweisen können? Wer ist beim Zulieferer, Zwischenhändler oder Kund:innen dafür verantwortlich, dass über die reine Zertifizierung hinaus jemand deren Einhaltung überwacht und entsprechende interne Prozesse aufsetzt (Internal Control System)?

Das Grundproblem bei der Verletzbarkeit von Supply-Chains ist ihnen inhärent – es ist eben gerade die Vernetzung zwischen verschiedenen IT-Systemen, über die ein permanenter Datenaustausch stattfindet. Wird dann nur ein Glied der Kette angegriffen, ist der Weg für Cyber-Kriminelle auf die Systeme des Partners nicht weit – eine Gefahr, die mit der Verlagerung in hybride Landschaften noch zugenommen hat.

Ökosystem in Sicherheitsstrategie einbeziehen

Deshalb kann es nicht damit getan sein, sich nur um den Schutz der eigenen IT-Infrastruk-

tur zu kümmern. Vielmehr müssen Unternehmen auch ihre Umwelt – d. h. die Partner innerhalb der Supply-Chain – in ihre Security-Strategie einbeziehen. Zum Beispiel in der Art und Weise, dass man die verkaufenden Unternehmen zu bestimmten Maßnahmen verpflichtet: Audits, ISO-Zertifizierungen, Einfordern von Sicherheitszertifizierungen oder die Einhaltung dezidierter Vertragsvereinbarungen. Allerdings werden solche Maßnahmen bislang nur selten umgesetzt – bis es zu einem Zwischenfall kommt.

Je intensiver man in der Cloud oder hybrid unterwegs ist, umso mehr ist man darauf angewiesen, dass der Hosting-Partner, der die Cloud-Lösung zur Verfügung stellt, das Thema Sicherheit im Blickfeld hat. Dies wird bei jedem professionellen Dienstleister natürlich der Fall sein. Nur muss man genau klären, wer für welchen Part zuständig ist und wer im Falle eines Angriffs haftet.

Beim Hosting ist Differenzierung gefragt

Keinesfalls ist es so, dass Verantwortung für Software und Betrieb allein beim Cloud-Provider liegen. Es kommt vielmehr auf die Ausgestaltung der Service-Level-Agreements (SLA) an. Wenn es hart auf hart kommt, sind in der Regel CIO/CISO bzw. letzten Endes der/die CEO des Kundenunternehmens haftbar. Vor allem muss man sich darüber im Klaren sein: Der Hoster sichert zwar seine Infrastruktur, aber nicht die Software, die darauf läuft. Es macht also einen Unterschied, was man unter „cloudbasiert" im Einzelnen versteht: „Infrastructure-as-a-Service" (IaaS), „Platform-as-a-Service" (PaaS) oder „Software-as-a-Service" (SaaS)?

In der Private Cloud findet sich oft ein Mix aus IaaS mit bestimmten Managed Services ontop. In puncto Sicherheit und Haftung gilt es deshalb auseinanderzuhalten: Der Hoster verantwortet Infrastruktur und operatives System, die Software-Anwendungen hingegen wird er nicht anfassen und darin Einstellungen vornehmen, denn dies würde einen expliziten Eingriff in die Geschäftsprozesse der Kundenunternehmen bedeuten. Es kann dementsprechend von Vorteil sein, SCM-Lösungen – von SAP oder anderen Herstellern – an einen Cloud-Provider auszulagern. Die Sicherheitslage betreffend, muss dafür aber vorab detailliert geregelt werden, wer für welche Komponenten zuständig und verantwortlich ist.

Hybride Szenarien als Ausweg

Bei Distributed-Denial-of-Service (DDoS)-Attacken auf die Cloud-Software ist man fein raus – was bleibt, ist der geschäftliche Schaden. Diesen ersetzt dem Unternehmen auch der Cloud-Provider nicht. Was ist zudem bei einem Angriff auf den Internet-Anschluss oder die Standleitung, die im eigenen Verantwortungsbereich liegen?

Hier könnte ein hybrides Szenario ein Ausweg sein, bei dem die eigene Produktion und Supply-Chain in Teilen autark funktionieren. Beispiel Manufacturing-Cloud: Die für den Produktionsprozess erforderlichen Funktionen laufen On-Premise, alle weiteren Szenarien (für Prognosen, Analysen etc.), die nicht dem laufenden Betrieb, sondern eher der Weiterentwicklung und Optimierung dienen, werden aus der Cloud bezogen. Dann kann die Produktion auch bei DDoS-Angriffen, oder wenn die Cloud-Software ausfällt, ungehindert weiterlaufen. ■

„Je intensiver man in der Cloud oder hybrid unterwegs ist, umso mehr ist man darauf angewiesen, dass der Hosting-Partner, der die Cloud-Lösung zur Verfügung stellt, das Thema Sicherheit im Blickfeld hat."

Michael Moser, DSAG-Fachvorstand Produktion & Supply-Chain-Management