Lieferantenhaftung: Cyber-Security als USP
Der sicherste Lieferant macht zukünftig das Rennen

Geschrieben von Joshua Bucheli, Talent Community Manager bei cyberunity, in Zusammenarbeit mit Tolga Ergin, Cyber-Security-Spezialist in den Bereichen, Digital- und Mobility-Solutions bei der Mercedes-Benz Mobility AG, und Peter Kosel, Gründer von cyberunity

Vor einigen Monaten wurde das US-Softwareunternehmen Kaseya Opfer eines Ransomware-Angriffs im Wert von 70 Millionen Dollar. Wenn man alle direkten und indirekten Kunden von Kaseya-Produkten mit einbezieht, wurden durch diesen einzigen Angriff mehr als 1.500 Unternehmen weltweit kompromittiert und sogar Hunderte von schwedischen Supermärkte gezwungen, ihren Betrieb einzustellen, da ihre Kassen nicht mehr funktionierten.

Die Unternehmen erkennen zunehmend, dass Awareness ein grosser Bestandteil der Cybersicherheit ist. Aber dieses Bewusstsein ist oft nach innen gerichtet und befasst sich mit den Schwachstellen, die innerhalb eines Unternehmens entstehen. Dabei werden oft die indirekten Bedrohungen übersehen, die mit Geschäftsbeziehungen zu Dritten verbunden sind. Jeder weiss, dass es riskant ist, am Ausbau der Sicherheit zu sparen. Weniger häufig wird darüber gesprochen, welche Auswirkungen die Cybersicherheitsreife eines Unternehmens auf diejenigen hat, mit denen es in der Aussenwelt in Kontakt steht.

Die Wirtschaft findet nicht in einem Vakuum statt. Es ist von Natur aus ein interaktives Unterfangen. In den meisten Fällen handelt es sich um eine Kette der Zusammenarbeit zwischen Auftraggebern, Kunden, Lieferanten, Verkäufern, Auftragnehmern, Originalgeräte-herstellern (OEMs), Händlern, externen Dienstleistern und vielen anderen. Während die

Unternehmen immer mehr darauf achten, wie sicher ihre eigenen Prozesse sind, vernachlässigen sie oft noch, wie sicher die Prozesse ihrer Geschäftspartner sind.

Tolga Ergin, Cyber-Security-Spezialist in den Bereichen, Digital- und Mobility-Solutions bei der Mercedes-Benz Mobility AG, weist jedoch darauf hin, dass Lieferanten diese Achillesferse mit etwas Geschick in ein wertvolles USP verwandeln können, mit dem sie stabilere, sichere und nachhaltige Geschäftsbeziehungen zu ihren Kunden aufbauen können.

Versorgungssicherheit: ein Schwachpunkt in der Cyber-Rüstung

Wie bei jeder sprichwörtlichen Kette ist auch die digitale Versorgungskette nur so stark (oder sicher) wie ihr schwächstes Glied. Dieses schwache Glied zeigt sich zunehmend in Lieferanten, die Zugang zu Kundendaten haben. Gerade wenn die Sicherheitsprotokolle eines Lieferanten nicht denen des Kunden entsprechen besteht erhöhte Gefahr von Sicherheitslücken.

Cyberkriminelle haben es auf Daten abgesehen. Es ist ihnen egal, woher diese Daten kommen. Wenn sie über einen Anbieter mit weniger robusten Sicherheitsprotokollen leichter auf die Daten eines Unternehmens zugreifen können, dann tun sie das. Wenn dieser Anbieter zufällig Zugang zu den Daten mehrerer Kunden gleichzeitig hat, wie im Fall von Kaseya, so ist das ein gefundenes Fressen für die Übeltäter.

Laut ENISA, der EU-Agentur für Cybersicherheit, haben Cyberkriminelle erkannt, dass viele Unternehmen nicht mehr die leichten Beuteziele sind, die sie einst waren. Also nehmen sie stattdessen ihre Opfer zunehmend indirekt ins Visier, indem sie die immer noch oft übersehenen und hochgradig skalierbaren Schwachstellen in digitalen Lieferketten ausnutzen. 2021 beruhen über 60 % aller Cyberangriffe auf dem Vertrauen, das die Kunden in ihre Lieferanten setzen, wobei sogar 66 % den Code der Lieferanten ausnutzen, um an die Daten des eigentlich anvisierten Opfers zu gelangen.

Der enge Rahmen, den viele Unternehmen für ihre Cybersicherheit noch immer vorgeben, trifft den Kern des Problems. Wie Tolga feststellt, «ist die Bedeutung ganzheitlicher Ansätze für die Cybersicherheit derzeit stark unterbelichtet, insbesondere in KMUs. Solche Sicherheitsüberlegungen sollten eigentlich in der Verantwortung der Geschäftsführung und des Managements liegen, aber in der Praxis ist das selten der Fall.»

Stattdessen wird die Cybersicherheit oft bruchstückhaft und reaktionär angegangen und weitgehend den einzelnen Sicherheitsspezialisten innerhalb eines Unternehmens überlassen. Dies führt unweigerlich zu unvorhergesehenen Schwachstellen – Risse in der digitalen Rüstung eines Unternehmens – die nicht nur das Unternehmen selbst, sondern auch seine Kunden und sogar die Endnutzer gefährden.

Die Lösung für diese Problematik? - Mehr Dialog über die Notwendigkeit der Sicherheit von Drittparteien, sagt Tolga:

«Die Unternehmen werden Ressourcen für die Bekämpfung der Bedrohungen bereitstellen müssen, welche Drittparteien verursachen. Schwachstellen im Zusammenhang mit Phishing-Angriffen, Identitäts- und Zugriffsmanagementprotokollen und Social-Engineering- Bedrohungen müssen zur Priorität werden. Dazu ist es unerlässlich, dass sowohl die Lieferanten als auch ihre Kunden damit beginnen, die Risiken zu bewerten, die durch ihre Interaktionen entstehen. Eine offene Kommunikation über diese zusätzlichen Einfallstore und die Art und Weise, wie sie geschlossen werden können, ist von entscheidender Bedeutung. Wenn mehr über die gegenseitigen Sicherheitsrisiken gesprochen wird, die sich aus den Beziehungen zwischen Kunden und Lieferanten ergeben, kann dies den nötigen Druck von aussen erzeugen, damit die Unternehmen eine breitere Perspektive einnehmen.»

Preis, Qualität *und* Sicherheit

IT-Sicherheit wird oft als eine Frage der ‘Sicherheit zum Selbstzweck’ betrachtet - der Ermittlung und Schliessung von Wahrnehmungslücken. Aber Sicherheit kann viel mehr sein als eine Last, die Unternehmen pflichtbewusst tragen. Zunehmend erkennen einige Unternehmen, dass Sicherheit auch ein vermarktungsfähiges und potenziell lukratives Alleinstellungsmerkmal sein kann.

Wie wäre es, wenn sowohl Lieferanten als auch ihre Kunden eine Unternehmenskultur schaffen würden, in der Sicherheit als Wettbewerbsvorteil erkannt und genutzt wird, anstatt sie nur zu ihrem eigenen Schutz einzusetzen? Ein transparenter Ansatz für die Cybersicherheit auf der Lieferantenseite macht nicht nur alles sicherer, sondern eröffnet den Unternehmen auch die Möglichkeit, sich von der Konkurrenz abzuheben.

Herkömmlich sind Qualität und Preis die beiden wichtigsten Kriterien für Unternehmen bei der Entscheidung, mit wem sie Geschäfte machen wollen. Da das Bewusstsein der Unternehmen für die Bedrohungen der digitalen Welt wächst, wird die Sicherheit zunehmend zum dritten Faktor in dieser Gleichung.

«In einer Welt, in der die Cybersicherheit und die Integrale Unternehmenssicherheit (IUS) immer mehr an Bedeutung gewinnen, werden die Kunden letztlich den sichersten Lieferanten wählen. Die Unternehmen werden zwangsläufig eher dazu neigen, Geschäfte mit Partnern zu machen, deren Prozesse und Sicherheitskultur ihren eigenen entsprechen oder diese übertreffen», sagt Tolga.

Zukunftsorientierte Lieferanten sind daher gut beraten, ein Gefühl der Partnerschaft und des Vertrauens zu fördern, indem sie ihre Kunden in die Planung ihrer Sicherheitsstrategien einbeziehen.

«Sicherheit ist ein Erfolgsfaktor, mit dem sich Unternehmen von der Konkurrenz abheben können. Je mehr sie sich dessen bewusst werden, desto wichtiger werden Fragen wie 'Was brauchen Sie von unserer Seite als Ihr Lieferant/Kunde in Bezug auf die Sicherheit? ’», betont Tolga.

Den Silberstreif nutzen: “Security Inside” als geschäftsförderndes USP nutzen

"Das ist keine Hexerei, und mit den richtigen Menschen am Ruder ist es durchaus machbar", sagt Tolga.

Die Unternehmen brauchen sowohl Führungskräfte als auch Mitarbeitende, die den Wert und die Bedeutung der interaktiven Sicherheit erkennen und schätzen. Nur dann werden sie in der Lage sein, diese Einstellung in ihren Unternehmen proaktiv zu fördern und voranzutreiben.

Ein gutes Hilfsmittel, mit dem KMU und ihre Mitarbeitenden beginnen können, sich einen Ruf für die Sicherheit auf der Lieferantenseite zu erarbeiten, ist das BSI, das mit seinen zahlreichen Publikationen Unternehmen, beim Etablieren robuster IT-Schutzverfahren, unterstützt. Der ICS-Sicherheits-Kompendium-Test und das IT-Grundschutz-Kompendium sind hier beispielhaft zu nennen.

Alternativ können OT-Hersteller auch den dedizierten OT-Sicherheitsdemonstrator und die Kurse des ICBC oder das internationale Sicherheitszentrum für ICT und OT von VINCI Energies in Anspruch nehmen.

Eine weitere Möglichkeit, die es zu erkunden gilt, ist die Cybersicherheitsversicherung. Letztlich lassen sich Sicherheitsverletzungen nicht ganz vermeiden, und die Kunden werden sich viel sicherer fühlen, wenn sie ihre Daten einem Unternehmen anvertrauen, das sie nicht nur schützt, sondern auch angemessen versichert. Neben dem finanziellen Schutz, erfordert eine solche Versicherung häufig auch eine Prüfung der internen Sicherheit eines Unternehmens, was zu einer zusätzlichen Sensibilisierung beiträgt. Namhafte Versicherer haben beispielsweise kürzlich ihre Haftpflichtversicherung für Sicherheit und Datenschutz erweitert und bieten sogar einen Präventionsdienst an, der Endnutzer und Kunden bei der sicheren Nutzung digitaler Produkte unterstützt.

Angebotsseitige Security Awareness Spezialisten: Gefragte Fähigkeiten und Ausbildungen

Tolga betont: «Die Mitarbeitenden sind das wertvollste Gut eines Unternehmens, nicht das schwächste Glied, wie oft behauptet wird, und sie sollten entsprechend befähigt werden.» Wenn Unternehmen ihre Sicherheit zu einem Alleinstellungsmerkmal machen wollen, brauchen sie engagierte Spezialisten auf der Lieferantenseite, die eine ausgereifte Cybersicherheits-Kultur aufbauen und weiterentwickeln können.

Was die formale Ausbildung betrifft, so sind Interessenten, die eine Karriere in diesem Bereich anstreben, gut beraten, mit grundlegenden Cybersicherheitszertifizierungen wie dem BSI IT-Grundschutz Kurs zu beginnen. Von dort aus können sie ihre Fähigkeiten mit Hilfe von Schulungen wie dem CISSP von ISC2 ausbauen, um sich von anderen Kandidaten abzuheben.

Unternehmen sollten nach Personen Ausschau halten, die Industriestandards im Bereich der Cybersicherheit auf der Lieferantenseite auf ihre speziellen Bedürfnisse zuschneiden können. Diese Personen sollten sowohl die internationalen als auch die lokalen rechtlichen und regulatorischen Grundlagen im Bereich der IT-Sicherheit und des Datenschutzes kennen, wie z. B. die EU-DSGVO, das NIST-Cybersecurity-Framework und das Schweizer DSG.

Neben Juristen sind auch Fachleute aus dem Bereich der Lieferkette ideal, z. B. Beschaffungsspezialisten oder Techniker mit fundierten Kenntnissen in Governance und Compliance. Besonders wertvoll sind auch Risikomanagement-Experten, die einen ganzheitlichen Sicherheitsansatz verfolgen, potenzielle Risiken klassifizieren und Methoden wie Datenschutzfolgenabschätzungen (DSFA) anwenden können. Letztendlich sind es Pragmatismus und das 'Big-Picture'-Denken, die den Unterschied ausmachen, und nicht eine reaktive, ad-hoc-Haltung bei der Eindämmung von Vorfällen.

Persönlichkeit – über technisches Know-How hinaus:

Cybersecurity-Spezialisten auf der Lieferantenseite brauchen mehr als nur technische Fähigkeiten. Sie müssen nicht nur proaktiv Risiken und Chancen erkennen, sondern auch in der Lage sein, der Geschäftsleitung effektiv die nächsten Schritte zu unterbreiten, die im besten Interesse des Unternehmens liegen. In dieser Hinsicht ist die Fähigkeit, effektiv zu kommunizieren und komplexe Themen aus einer umfassenden Perspektive zu betrachten – um zu sehen, wie die technologische, rechtliche und geschäftliche Welt miteinander verknüpft sind – absolut entscheidend.

Auch Beharrlichkeit ist wichtig. Das Thema Cybersicherheit rückt zwar immer mehr in das Blickfeld der Unternehmer, doch wird ihr oft noch nicht die Priorität eingeräumt, die sie verdient. Fachleute, die mit einer ablehnenden Haltung gegenüber der Cybersicherheit umgehen und die Geschäftsleitung davon überzeugen können, dass es die Investition wert ist, werden von höchster Bedeutung sein.

Letztlich runden Hartnäckigkeit und ein natürliches Talent für die überzeugende Darstellung von Ideen das Profil eines idealen Kandidaten ab. Die Unternehmen müssen sich erst noch mit den Bedrohungen auseinandersetzen, die ihre digitalen Lieferketten mit sich bringen, und sie brauchen möglicherweise Hilfe, um den versteckten USP zu erkennen, der sich daraus ergibt. Die Fähigkeit, sowohl die Notwendigkeit der Cybersicherheit auf der Lieferantenseite als auch die damit verbundenen Chancen für den guten Ruf beharrlich zu vermitteln, wird ein wichtiges Instrument im Arsenal der künftigen Cybersecurity-Spezialisten sein.

Die Digitalisierung der Lieferketten von Unternehmen ist unausweichlich. Versicherungs-unternehmen, denen die sensiblen persönlichen Daten von Millionen von Menschen anvertraut werden, verlagern diese Informationen in die Cloud. Die Automobil- und Flottenmanagementbranche, in der es nicht nur um Daten, sondern um Menschenleben geht, verlässt sich zunehmend auf digitale Systeme, um ihre Produkte zu koordinieren und zu automatisieren. OEMs verknüpfen ihre Schalttafeln mit dem IoT.

Die Risiken für Unternehmen und die Öffentlichkeit sind alles andere als trivial, fasst Peter Kosel, Gründer der cyberunity AG zusammen. Cybersicherheit ist kein Kinderspiel, und das Beste, was wir hoffen können ist, dass die richtigen Persönlichkeiten in Erscheinung treten und wir diese frühzeitig kennenlernen - auch hier geht es darum, die entscheidende Nasenlänge voraus zu sein, um im Wettbewerb bestehen zu können. Wer heute erst anfängt, nach seinen Leistungsträgern zu suchen, die er morgen bzw. übermorgen für sich gewinnen möchte ist zu spät dran. Es sind Individuen gefragt, die dabei helfen, robuste Standardarbeitsanweisungen für die Interaktion zwischen Lieferanten und Kunden zu entwickeln und umzusetzen. Fachleute die in der Lage sind, das Bewusstsein der Branche für die verheerenden Risiken und die potenziell lukrativen Alleinstellungsmerkmale zu schärfen, die die digitalen Lieferketten heute mit sich bringen. Diese Persönlichkeiten stehen nicht an der nächsten Strassenecke und warten darauf, einen Job zu finden.