IT- & Datensicherheit in der Supply Chain

Die 7. Ausgabe des Hermes-Barometers präsentiert die Ergebnisse einer Telefonbefragung unter 200 Logistikentscheidern deutscher Unternehmen.

www.hermesworld.com/scs

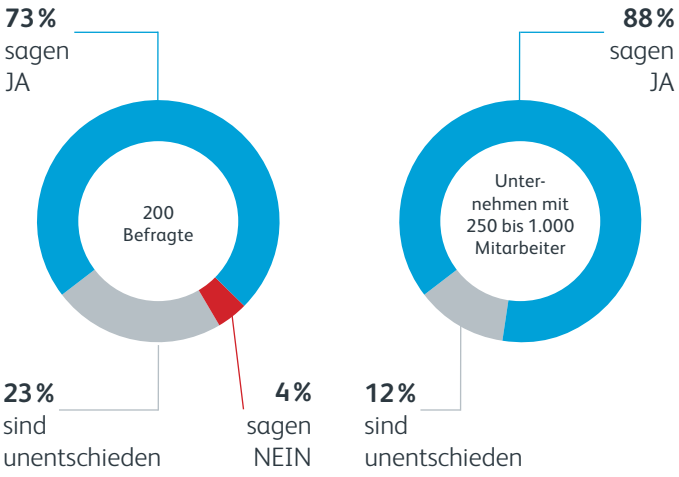
Hermes

IT- & Datensicherheit in der Supply Chain: Fast drei Viertel aller Logistikentscheider fühlen sich gut aufgestellt

IT-Sicherheitsvorfälle größte Bedrohung für die Lieferkette

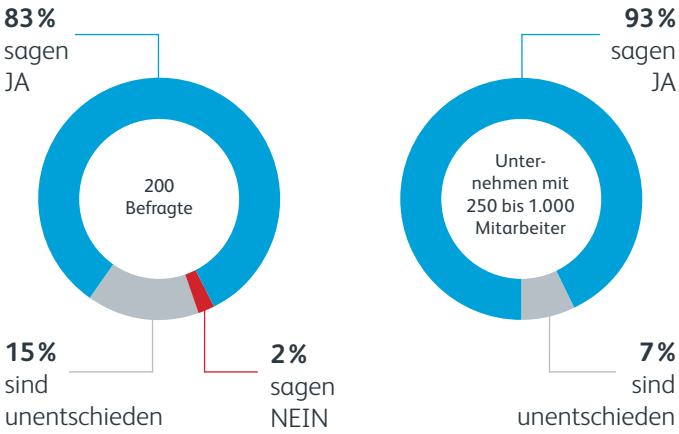
Die Logistikbranche gilt als Vorreiter im Hinblick auf die Digitalisierung und Vernetzung. Fast drei Viertel der befragten Logistikentscheider sind denn auch der Meinung, dass sie innerhalb ihres Unternehmens über das nötige Know-how verfügen, um Gefährdungen der IT-Systeme auf ein tragbares Maß zu beschränken. In großen Unternehmen mit 250 bis 1.000 Mitarbeitern stimmen sogar knapp 90 Prozent der Befragten dieser Aussage zu.

Verfügen Sie in Ihrem Unternehmen über das nötige Know-how, um Gefährdungen der IT-Systeme auf ein tragbares Maß zu beschränken?



Doch trotz dieser positiven Selbsteinschätzung sind sich die Unternehmen der mit der Vernetzung einhergehenden Risiken bewusst. Für 41 Prozent der Teilnehmer stellen Hackerangriffe, Computerviren und ähnliche IT-Sicherheitsvorfälle die größte Bedrohung für die eigene Lieferkette dar.
Große Unternehmen sehen sich um 3 Prozentpunkte weniger gefährdet, was mit der Nutzung zahlreicher Sicherheitstechnologien zu erklären ist. Mehr als jeder Neunte von ihnen ist jedoch der Meinung, dass künftig mehr investiert werden muss, um die Datensicherheit innerhalb der Supply Chain zu gewährleisten. Bei kleineren Unternehmen geht gut jeder Achte von einem erhöhten Investitionsbedarf aus.

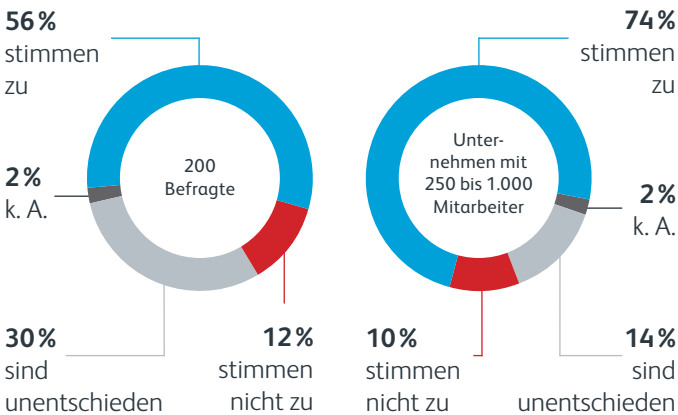
Müssen Unternehmen in Zukunft deutlich mehr investieren, um die IT- und Datensicherheit innerhalb der Supply Chain zu gewährleisten?



Lieferkette als Risikokette

Lieferketten verfügen zunehmend über eine unternehmensübergreifende Informationsarchitektur, wie zum Beispiel Supply-Chain-Management-Systeme oder ERP-Clouds. In dieser Kooperation sieht die Mehrheit der Befragten ein Risiko. 56 Prozent der Logistikentscheider gehen davon aus, dass sie zunehmend von Informationssicherheitsvorfällen ihrer Kunden, Partner oder Zulieferer betroffen sein werden.
In größeren Unternehmen, deren Vernetzung häufig weiter vorangeschritten ist, gehen sogar 74 Prozent der Befragten von einem erhöhten Risiko aus. Diese Einschätzung wird auch dadurch genährt, dass nur gut ein Drittel der Unternehmen über umfassende Informationen zu den IT-Sicherheitssystemen ihrer Partner verfügt.

Da die Lieferkette auch eine Risikokette darstellt, werden Unternehmen zunehmend von Informationssicherheitsvorfällen ihrer Kunden, Partner oder Zulieferer betroffen sein.

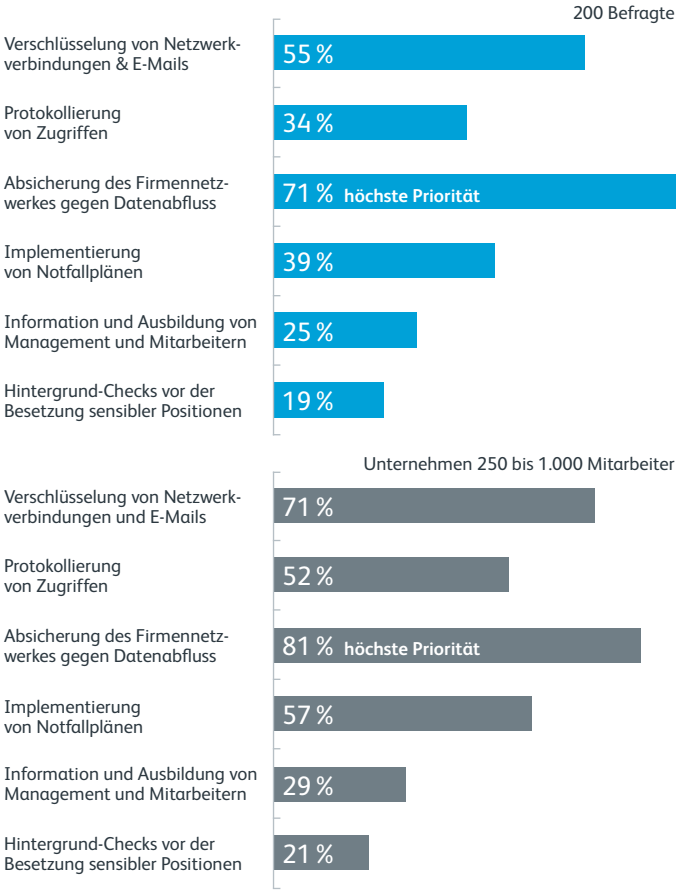


Cyberangriffen aktiv vorbeugen

Um Sicherheitsvorfällen vorzubeugen, gibt es verschiedene Ansätze: 71 Prozent der Befragten sind der Meinung, dass die Absicherung des Firmennetzwerkes gegen Datenabfluss eine hohe Priorität habe. Gefolgt von der Verschlüsselung von Netzwerkverbindungen und E-Mails (55 Prozent), der Implementierung von Notfallplänen (39 Prozent) sowie der Protokollierung von Zugriffen (34 Prozent). Der Weiterbildung von Management und Mitarbeitern sowie Hintergrund-Checks vor der Besetzung sensibler Positionen messen lediglich 25 bzw. 19 Prozent der Logistikentscheider eine hohe Bedeutung bei.

Auffällig ist, dass die Logistikentscheider größerer Unternehmen die Bedeutung dieser Maßnahmen ausnahmslos höher einstufen als die kleinerer Unternehmen. Besonders drastisch ist diese Abweichung bei der Protokollierung von Zugriffen sowie der Implementierung von Notfallplänen. Dies mag daran liegen, dass sich diese Technologien in größeren Unternehmen bereits bewähren konnten.

Welchen der nachfolgend genannten Technologien und Maßnahmen messen Sie eine sehr hohe Priorität bei der IT- und Datensicherheit zu? (Basis: 200 Befragte)



Besonders gefährdete Unternehmensbereiche

Aktuell berichten 19 Prozent der befragten Logistikentscheider, dass ihre Lieferkette in der Vergangenheit durch Cyberangriffe gestört oder sogar unterbrochen wurde. Die IT-gestützte Lagerhaltung, die Produktion und der Online-Handel werden von der breiten Mehrheit der Teilnehmer (knapp 70 Prozent) als weniger bedrohte Unternehmensbereiche eingestuft. Gut die Hälfte aller Befragten schätzt hingegen die Kunden- und Mitarbeiterdaten sowie den automatischen Datenaustausch zwischen Lieferanten und Partnern als besonders gefährdet ein. Dies lässt sich sowohl mit der Zunahme von Hackerangriffen auf diese Unternehmensbereiche erklären als auch mit dem Ausbau des Datenaustauschs auf diesen Gebieten. Die implementierten IT-Sicherheitskonzepte müssen sich in diesen Bereichen erst bewähren.

Fazit

Die Unternehmen sind sich der Probleme und Risiken, die mit einer erhöhten Transparenz der Lieferkette einhergehen, bewusst. Auch in Zukunft erwartet die Mehrheit der Entscheider eine Zunahme der Gefährdung durch den unternehmensübergreifenden Datenaustausch. Mehr als jeder siebte Befragte sieht sich dieser Herausforderung jedoch gewachsen und vertraut auf die bereits implementierten Sicherheitsmechanismen. Gerade die größeren Unternehmen scheinen bereits verschiedene Technologien erfolgreich zu nutzen und positive Erfahrungen beispielsweise mit der Protokollierung von Netzwerkzugriffen zu haben. Trotzdem spricht sich die überragende Mehrheit der Logistikentscheider für weitere Investitionen in die Datensicherheit aus, um auch für die weiteren Schritte zur Logistik 4.0 bestmöglich aufgestellt zu sein.

Das komplette Hermes-Barometer sowie mehr Informationen zum Thema Logistik 4.0 und Supply Chain Management finden sich im Hermes Supply Chain Blog unter *www.hermes-supply-chain-blog.com.*

KONTAKT

Hermes Germany GmbH
Essener Straße 89
22419 Hamburg
E-Mail: Info-Supplychainsolutions@hermesworld.com