GDV Gesamtverband der Versicherer

FAKTENBLATT CYBERKRIMINALITÄT

Cyberrisiken im Transportsektor

Hohe Risiken, viele Sicherheitslücken

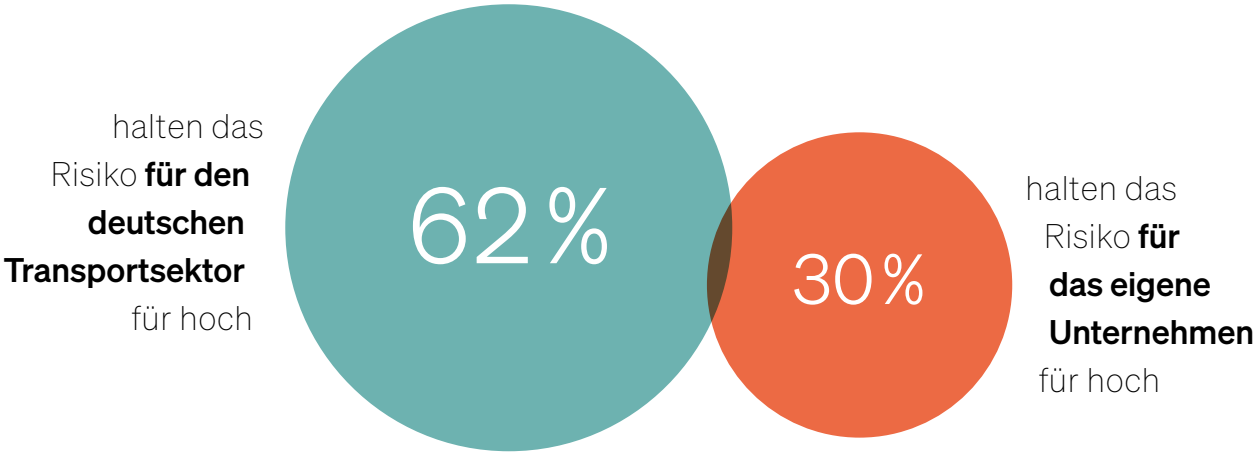
Mittelständische Transport- und Logistikunternehmen sind häufig Ziel von Cyberkriminellen, aber auf diese Angriffe nicht ausreichend vorbereitet: Die IT-Sicherheit vieler Transport- und Logistikunternehmen zeigt **gefährliche Lücken**, wie Analysen im Auftrag der deutschen Versicherer zeigen.

In einer Forsa-Umfrage gab jedes sechste Transport- und Logistikunternehmen (18 %) an, bereits Opfer erfolgreicher Cyberattacken gewesen zu sein. Trotz dieser starken Betroffenheit ihrer Branche gehen aber nur 30 % der von Forsa befragten Entscheider von einem hohen Risiko für ihr eigenes Unternehmen aus. Ein Grund dafür: Vier von fünf (79 %) meinen, sie täten bereits genug zum Schutz gegen Cyberkriminalität. Doch diese Selbsteinschätzung hält der Realität nicht stand: Insgesamt erfüllen nur 38 % der Transport- und Logistikunternehmen die wichtigsten Basis-Anforderungen an die IT-Sicherheit, alle anderen haben eine oder gleich mehrere Schutzlücken:

- → **13 %** lassen auch einfachste Passwörter wie „1234“ oder „Passwort“ zu;
- → ebenfalls **13 %** sichern ihre Daten seltener als wöchentlich;
- → **22 %** bewahren ihre Sicherheitskopien so auf, dass sie bei einem Hackerangriff verschlüsselt oder gelöscht werden könnten.

Transportsektor häufig von Cyberkriminalität betroffen

Viele Transport- und Logistikunternehmen unterschätzen das eigene Risiko



Nicht funktionierende IT legt die meisten Transport- und Logistikunternehmen lahm

Der Betrieb wäre…

sehr oder eher stark **eingeschränkt** — wenig oder **nicht eingeschränkt**

Gleichzeitig sind viele Unternehmen nur unzureichend auf einen erfolgreichen Angriff vorbereitet: 34% der befragten Transport- und Logistikunternehmen schulen ihre Mitarbeiter nicht im Umgang mit den Gefahren aus dem Netz, 43 % haben für den Ernstfall weder ein Notfallkonzept noch eine Vereinbarung mit ihrem IT-Dienstleister. Angesichts der hohen Abhängigkeit von funktionierenden IT-Systemen – 71 % der Unternehmen wären nach eigenen Angaben ohne funktionierende IT stark eingeschränkt – ist dieser sorglose Umgang mit den Risiken geradezu fahrlässig.

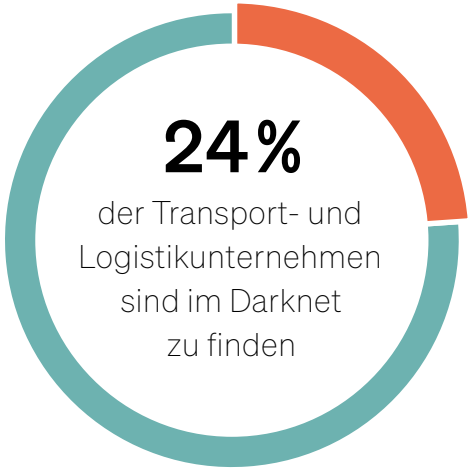
Viele Informationen von Transport- und Logistikunternehmen im Darknet

Wie einfach es Hacker vielfach gemacht wird, zeigt auch eine Darknet-Recherche nach Daten von 500 zufällig ausgewählten Unternehmen des Transportsektors. Die damit beauftragte PPI AG fand mit ihrem Cyberrisikobewertungstool Cysmo Daten von 118 dieser Unternehmen (24 %) im Darknet – oft berufliche E-Mail-Adressen samt dazugehöriger Passwörter, die Angestellte auch für private Zwecke genutzt hatten. Weil viele Menschen immer die gleichen oder sehr ähnliche Passwörter nutzen, können gerade solche E-Mail-/Passwort-Kombinationen von Cyberkriminellen leicht ausgenutzt werden. Unternehmen sollten für die Nutzung beruflicher Mail-Adressen daher klare Regeln aufstellen und die Mitarbeiter entsprechend schulen.

Noch wichtiger ist stets aktuelle Software. Sicherheitsupdates sollten so schnell wie möglich, am besten automatisiert eingespielt werden – denn veraltete Software mit bekannten Sicherheitslücken sind tickende Zeitbomben. Trotzdem waren 13 % der untersuchten Transport- und Logistikunternehmen mit Systemen im Internet erreichbar, die teilweise schon lange keine Sicherheitsupdates mehr erhalten. Für diese Unternehmen ist das Risiko eines erfolgreichen Cyberangriffs extrem hoch – und wächst täglich weiter.

Sensible Daten im Darknet

24 % der Transport- und Logistikunternehmen sind im Darknet zu finden – in vielen Fällen mit E-Mail/Passwort-Kombinationen



Tickende Zeitbomben

Anteil der Transport- und Logistikunternehmen, die Software einsetzen, für die es keine Sicherheitsupdates mehr gibt

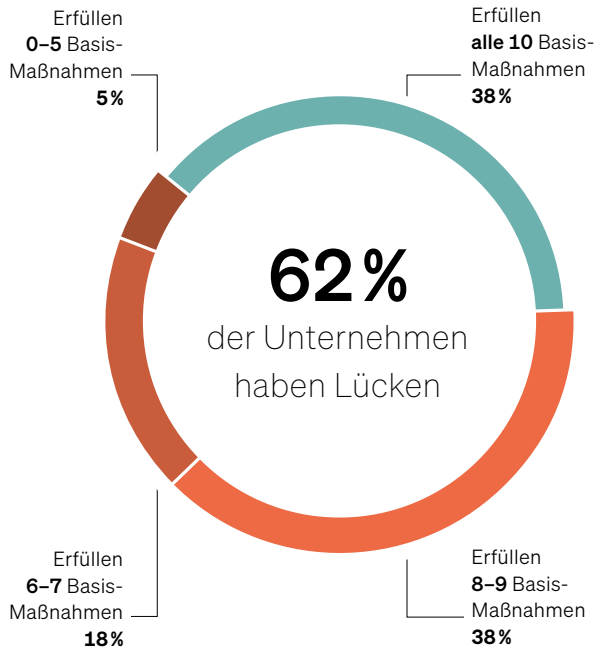
Wie gut ist die IT-Sicherheit Ihres Unternehmens? Machen Sie den Check!

Absolute Sicherheit im Netz gibt es nicht. Doch Widerstand gegen Cyberkriminelle ist möglich. Wer die Gefahren realistisch einschätzt und bei seiner IT-Sicherheit die wichtigsten Grundlagen beachtet, ist gegen viele Angriffe wirksam geschützt und kann die wirtschaftlichen Folgen eines erfolgreichen Angriffs eindämmen. Der kostenlose Cyber-Sicherheitscheck des GDV unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können.

Die Forsa-Umfrage des GDV hat gezeigt: An vielen Stellen klaffen Lücken in der IT-Sicherheit. Nur 38 Prozent bestehen den Sicherheitscheck und erfüllen alle zehn Basis-Maßnahmen[1] – 62 Prozent haben hingegen eine oder mehrere Sicherheitslücken.

[1] Die zehn Basis-Schutzmaßnahmen entsprechen grundliegenden Obliegenheiten der GDV-Musterbedingungen für eine Cyberversicherung. Hier geht es unter anderem um Passwörter und Zugänge, Schutz vor Schadsoftware, Datensicherungen und Sicherheitsupdates. Die konkreten Basis-Schutzmaßnahmen finden Sie unter www.gdv.de/cybercheck.

Nur eine Minderheit erfüllt den Basisschutz des GDV-Cybersicherheitschecks vollständig



CYBER S!CHER
Eine Initiative der Versicherer

Für die Initiative Cybersicher hat Forsa die für Internetsicherheit zuständigen Mitarbeiter von 100 kleinen und mittleren Transport- und Logistikunternehmen befragt. Die PPI AG hat mit ihrem Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 500 mittelständischen Unternehmen des Transportsektors passiv getestet und dabei alle öffentlich einsehbaren Informationen aus Sicht eines potentiellen Angreifers erfasst und bewertet. Die Forsa-Interviews fanden im Herbst 2022, die Cysmo-Analyse im Januar 2023 statt.

GDV

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e.V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel. 030 2020–5000, Fax 030 2020–6000
www.gdv.de, berlin@gdv.de

Verantwortlich
Daniela Werner
Tel. 030 2020–5950, E-Mail: d.werner@gdv.de

Redaktion
Dr. Christian Siemens
Tel. 030 2020–5945, E-Mail: c.siemens@gdv.de

Publikationsassistenz
Roman Rossberg