



GDV

Gesamtverband
der Versicherer

FAKTENBLATT CYBERKRIMINALITÄT

Cyber Risiken im Großhandel



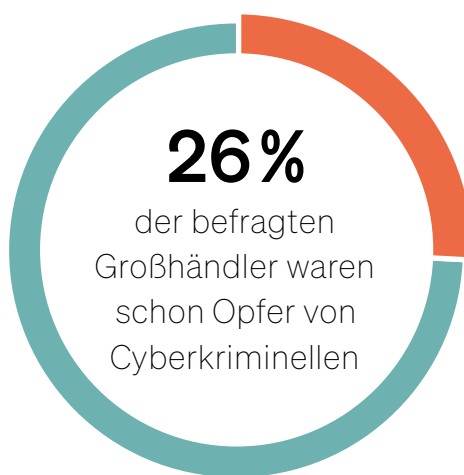
Hohe Risiken, viele Sicherheitslücken

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

In einer Forsa-Umfrage gab jeder vierte Großhändler (26%) an, bereits Opfer erfolgreicher Cyberattacken gewesen zu sein. Trotz dieser starken Betroffenheit ihrer Branche gehen aber nur 40% der von Forsa befragten Großhändler von einem hohen Risiko für ihr eigenes Unternehmen aus. Ein Grund dafür: 72% der Entscheider meinen, sie täten bereits genug zum Schutz gegen Cyberkriminalität. Doch diese Selbsteinschätzung hält der Realität nicht stand: Insgesamt erfüllen nur 24% der Unternehmen die wichtigsten Basis-Anforderungen an die IT-Sicherheit, alle anderen haben eine oder gleich mehrere Schutzlücken:

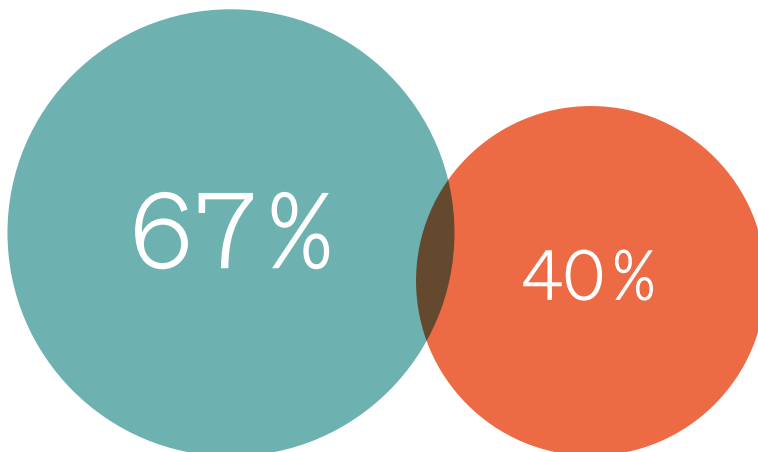
- **11%** spielen Sicherheitsupdates nicht automatisch ein;
- **21%** lassen auch einfachste Passwörter wie „1234“ oder „Passwort“ zu;
- **28%** bewahren ihre Sicherheitskopien so auf, dass sie bei einem Hackerangriff verschlüsselt oder gelöscht werden könnten.

Großhandel häufig von Cyberkriminalität betroffen



Viele Großhändler unterschätzen das eigene Risiko

halten das Risiko **für den deutschen Großhandel** für hoch



halten das Risiko **für das eigene Unternehmen** für hoch

Nicht funktionierende IT legt die meisten Großhändler lahm

Der Betrieb wäre...

sehr oder eher stark **eingeschränkt**

wenig oder **nicht eingeschränkt**

82 %

18 %

Gleichzeitig sind viele Unternehmen nur unzureichend auf einen erfolgreichen Angriff vorbereitet: 25% der befragten Großhändler schulen ihre Mitarbeiter nicht im Umgang mit den Gefahren aus dem Netz, 44% Prozent haben für den Ernstfall weder ein Notfallkonzept noch eine Vereinbarung mit ihrem IT-Dienstleister. Angesichts der hohen Abhängigkeit von funktionierenden IT-Systemen – 82 Prozent der Großhändler wären nach eigenen Angaben ohne funktionierende IT stark eingeschränkt – ist dieser sorglose Umgang mit den Risiken geradezu fahrlässig.

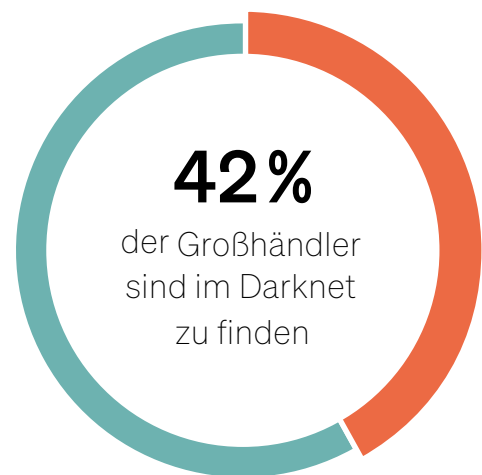
Viele Informationen von Großhandelsunternehmen im Darknet

Wie einfach es Hacker vielfach gemacht wird, zeigt auch eine Darknet-Recherche nach Daten von 500 zufällig ausgewählten Großhändlern. Die damit beauftragte PPI AG fand mit ihrem Cyberrisikobewertungstool Cysmo Daten von 209 dieser Unternehmen (42%) 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 15 Prozent der untersuchten Großhändler 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

42% der Großhändler sind im Darknet zu finden – in vielen Fällen mit E-Mail/Passwort-Kombinationen



Tickende Zeitbomben

Anteil der Großhändler, die Software einsetzen, für die es keine Sicherheitsupdates mehr gibt



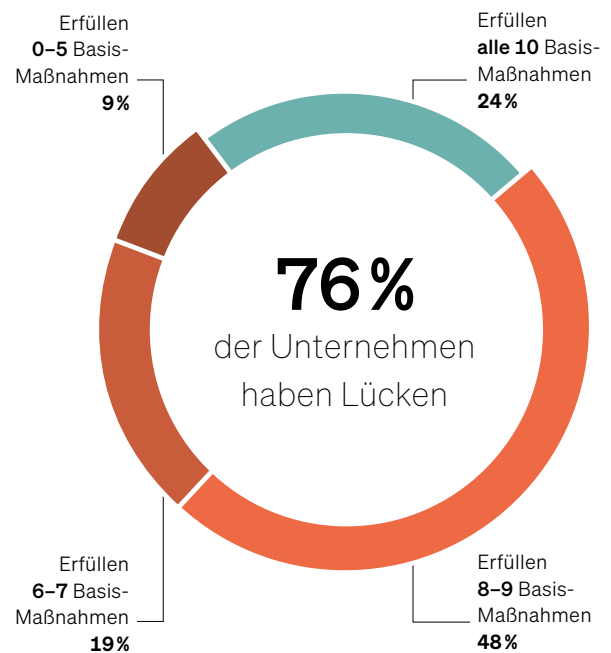
Wie gut ist die IT-Sicherheit Ihres Unternehmens? Machen Sie den Check!

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 24 Prozent bestehen den Sicherheitscheck und erfüllen alle zehn Basis-Maßnahmen¹ – 76 Prozent haben hingegen eine oder mehrere Sicherheitslücken.

¹ Die zehn Basis-Schutzmaßnahmen entsprechen grundlegenden 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
SICHER**

Eine Initiative der Versicherer

Für die Initiative Cybersicher hat Forsa die für Internetsicherheit zuständigen Mitarbeiter von 100 kleinen und mittleren Großhandelsunternehmen befragt. Die PPI AG hat mit ihrem Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 500 mittelständischen Großhändlern 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.



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

Publikationsassistentz
Roman Rossberg

Disclaimer
Dieses Faktenblatt stellt eine allgemeine, unverbindliche Information dar. Die Inhalte wurden mit der erforderlichen Sorgfalt erstellt. Gleichwohl besteht keine Gewährleistung auf Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der darin enthaltenen Angaben oder Einschätzungen. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.