GDV Gesamtverband der Versicherer

SYSTEMISCHE RISIKEN | CYBERSICHERHEIT

Cyberabwehr stärken, Stabilität sichern

Cyberschwächen als Stabilitätsrisiko

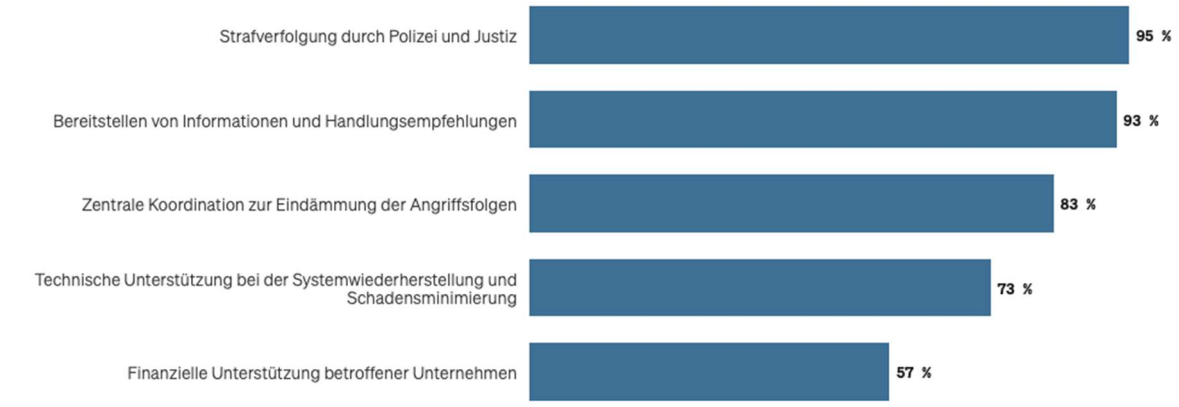
Angesichts der Bedrohungen durch kriminelle und staatliche Akteure sind die Cyberschwächen des Standortes Deutschland ein Risiko für Wachstum und Wohlstand. Zwei Drittel der Unternehmen sind so schlecht geschützt, dass sie nicht ohne Weiteres gegen Cyberrisken versicherbar sind. Stattdessen addieren sich die IT-Sicherheitslücken zu einer wirtschaftlichen Verwundbarkeit auf, die im Extremfall das Land destabilisieren kann.

Systemische Dimension: Die Gefahr einer Cyberpandemie

Cyberereignisse entfalten ihre Wirkung nicht isoliert. IT-Monokulturen, hochintegrierte Lieferketten und digitale Interdependenzen können im Fall einer Störung zu sektorübergreifenden Domino- und Kaskadeneffekten führen. Die Sorge vor einer solchen Cyberpandemie ist auch in der Wirtschaft weit verbreitet. Sie löst aktuell aber keine stärkeren Bemühungen bei der Prävention aus, sondern hohe Erwartungen an den Staat: Er soll im Katastrophenfall betroffenen Unternehmen sowohl technische als auch – ähnlich wie zuletzt während der Corona-Pandemie – finanzielle Hilfen zur Überbrückung der Krise zur Verfügung stellen.

Hohe Erwartungen an den Staat im Katastrophenfall

Was sollten staatliche Stellen im Fall einer Cyberkatastrophe auf jeden Fall leisten?



Quelle: Repräsentative Forsa-Befragung von 300 mittelständischen Unternehmen 2025; Mehrfachnennungen möglich

Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe

Die deutsche Wirtschaft muss widerstandsfähiger gegen Cyberrisiken werden. Entsprechende Lösungen zu entwickeln ist angesichts der drohenden volkswirtschaftlichen Schäden eine gesamtgesellschaftliche – und mithin auch öffentliche – Aufgabe. Der Staat muss mit einer Cyberpandemie rechnen und eine entsprechende Reaktion vorbereiten.

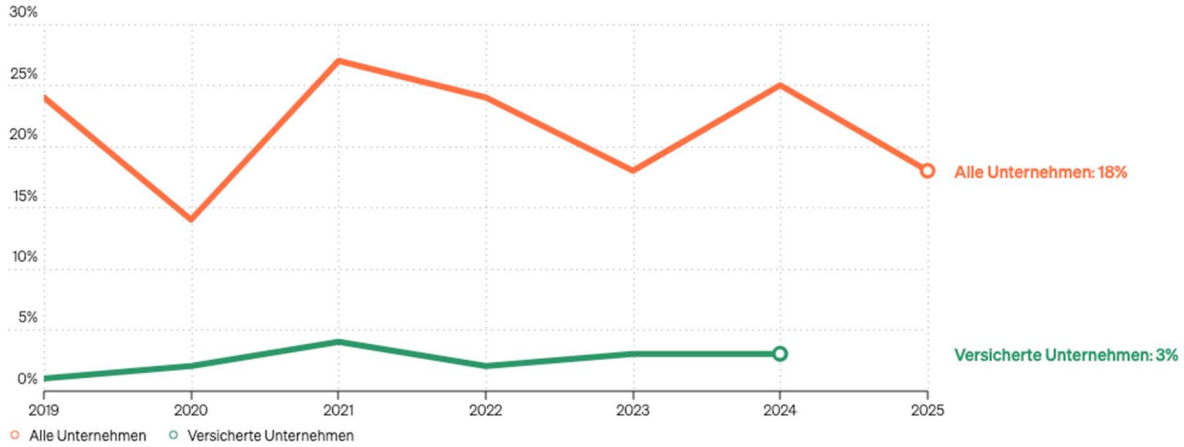
Leistungen und Potenziale der Versicherungswirtschaft

Cyberpolicen haben mit ihrer Kombination aus Prävention, Unterstützung im Ernstfall und finanziellem Risikotransfer das Potenzial volkswirtschaftlich stabilisierender Effekte.

Prävention: Klare Sicherheitsanforderungen und Schulungsangebote heben das Sicherheitsniveau der versicherten Unternehmen und senken die Wahrscheinlichkeit erfolgreicher Angriffe: Während in Umfragen rund 20 Prozent der Unternehmen angeben, Opfer von Cyberattacken geworden zu sein, waren unter den versicherten Unternehmen in den vergangenen Jahren jeweils nur drei Prozent betroffen.

Hohe Betroffenheit in der Breite – aber Prävention wirkt

Versicherte Unternehmen werden nur selten zum Opfer eines Cyberangriffs



Quelle: Forsa für GDV 2019-2025; GDV-Geschäftsstatistik Cyberrisikoversicherung 2019-2024

Hilfe im Ernstfall: Cyberversicherungen stellen schnelle und professionelle Assistance-Leistungen bereit. Spezialisierte IT-Experten unterstützen unmittelbar bei der Eindämmung des Angriffs und der Wiederherstellung der Systeme. Gerade für kleine und mittlere Unternehmen, denen entsprechende interne Ressourcen ebenso wie Beziehungen zu spezialisierten Dienstleistern häufig fehlen, sind diese Leistungen entscheidend.

Risikotransfer: Lassen sich trotz Prävention und schneller Reaktion Betriebsunterbrechungen, Wiederherstellungskosten oder Haftungsansprüche nicht vermeiden, so wirken diese dank des finanziellen Risikotransfers nicht existenzbedrohend.

Mangelnde Prävention und systemische Risiken bremsen die Marktentwicklung

Aktuell sind nur rund fünf Prozent der deutschen Unternehmen gegen Cyberangriffe versichert. Die hohen gesamtwirtschaftlichen Potenziale der Cyberversicherung bleiben aus den beiden oben beschriebenen Gründen bisher ungenutzt:

- Zahlreiche Unternehmen erfüllen die Sicherheitsanforderungen für den Abschluss einer Cyberversicherung nicht.
- Die Gefahr einer Cyberpandemie bremst das Marktwachstum, da die schwer kalkulierbaren Kaskadeneffekte zahlreiche Versicherte gleichzeitig treffen und die Kapitalreserven der Versicherer besonders exponieren könnten.

Lösungsansätze

Handlungsfeld: Mehr Befugnisse für das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte eine stärkere Rolle im aktiven Wirtschaftsschutz gegen Cyberrisiken übernehmen. Hierzu sollte gesetzlich:

- die Kernaufgabe des BSI auf den informationstechnischen Schutz der gesamten Wirtschaft ausgeweitet werden;
- die Befugnis des BSI zur aktiven Detektion von Schwachstellen und Schadsoftware im Sinne eines Präventionssystems erweitert werden;
- der Zersplitterung der Behördenlandschaft entgegengewirkt werden, indem das BSI stärkere Kompetenzen als nationaler Systemverantwortlicher für Cybersicherheit erhält. Hierzu sollten klar definierte Prozesse zur Erstellung gesamtwirtschaftlicher Lagebilder und Koordinierung landesübergreifender Normungsprojekte geschaffen werden.

Handlungsfeld: Lagebilder und Frühwarnsysteme

Die bei den Cyberversicherern einlaufenden Schadensmeldungen können die tatsächliche Schadensrealität in der Wirtschaft besonders rasch und realitätsnah abbilden. Zusammen mit einer qualitativen Auswertung des Schadensgeschehens durch die öffentliche Hand und zentralen Playern der IT-Wirtschaft könnten diese Informationen die Grundlage für ein aussagekräftiges Gesamtbild in Echtzeit schaffen.

Zur Verbesserung der Datenlage fordert der GDV daher eine Plattform zum gemeinsamen Datenaustausch zwischen Staat, Wirtschaft und Versicherungswirtschaft. Auf dieser Basis sollten Daten zu Angriffswellen, neuen Schwachstellen oder eskalierenden Schadenslagen in Echtzeit ausgetauscht und somit frühzeitig erkannt werden.

Handlungsfeld: Gemeinsame Vorbereitung auf die Krise

Die Cyberpandemie bewältigt sich nicht von allein. Staat, Wirtschaft und Versicherungswirtschaft müssen bereits vor dem Ernstfall klären, wie gemeinsam auf Krisen zu reagieren ist. Notwendig ist ein gemeinsames Verständnis aller Stakeholder, wie und auf welche gemeinsamen Responsekapazitäten (z.B. IT-Forensiker, Wiederherstellungsmanager) zugegriffen wird. Zudem sollten gemeinsame Tabletop-Übungen und Simulationen des Pandemiefalls sicherstellen, dass die verfügbaren Ressourcen im Sinne einer Triage dort prioritär eingesetzt werden, wo sie gesamtgesellschaftlich den größten Nutzen stiften.

Fazit

Cyberrisiken sind eine gesamtwirtschaftliche Herausforderung mit erheblicher Bedeutung für Wohlstand und Stabilität. Die Cyberversicherungswirtschaft bringt konkrete Leistungen, Daten und Strukturen ein, die staatliche Cybersicherheitsstrategien sinnvoll ergänzen. Ziel muss es sein, diese Potenziale konsequent zu nutzen, die Resilienz des Wirtschaftsstandorts Deutschland zu stärken und staatliche Krisenreaktionsfähigkeit vorausschauend zu stärken.