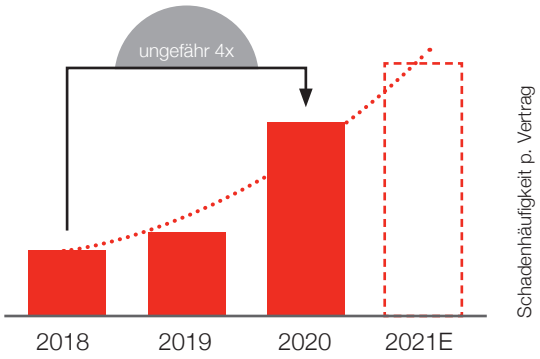
HISCOX
WISSEN VERSICHERT.

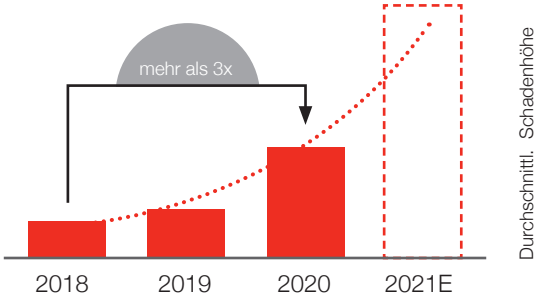
CYBER-VERSICHERUNG IM WANDEL
DIE SCHADENSITUATION DER CYBER-VERSICHERUNG SPITZT SICH WEITER ZU

Die Gefahrenlage in der Cyber-Welt hat sich innerhalb der letzten Jahre rasant zugespitzt. Fast täglich wird über Cyberangriffe auf bekannte Konzerne berichtet. Diese mediale Berichterstattung ist aber nur die Spitze des Eisbergs. Die Angreifer haben sich innerhalb kürzester Zeit so weit professionalisiert, dass nicht nur die Frequenz der Angriffe zugenommen hat, sondern vor allem auch deutlich kostenintensivere Schadenfälle entstehen. Dieser globale Trend erfordert auch in Deutschland und Österreich einen strukturellen Wandel. Damit Cyber-Schäden weiter versicherbar bleiben können, ist übergreifend ein höheres Beitragsvolumen unabdingbar.

Rasanter Anstieg von Schadenhäufigkeit und -höhe



- Die Schadenhäufigkeit war 2020 fast vier Mal so hoch wie in 2018.
- 2021 wird schätzungsweise beinahe jeder 10. Vertrag schadenbelastet sein.



- Die durchschnittliche Schadenhöhe hat sich 2020 im Vergleich zu 2018 mehr als verdreifacht.
- Einer der Hauptkostentreiber ist die zunehmende Komplexität bei der Datenwiederherstellung und der Wiederherstellung des IT-Systems aus dem Back-up.

Was hat sich fundamental verändert?

PROFESSIONALISIERUNG DER ANGREIFER

1. Übergang von nicht-zielgerichteten Massenphänomen zu manuell orchestrierten Attacken.

+

2. Neben der Verschlüsselung der Daten werden zunehmend auch Daten aus dem System geschleust, um den Forderungen der Angreifer maximalen Nachdruck zu verleihen.

=>

Investitionen in IT-Sicherheit sind keine optionale Maßnahme mehr, sondern zwingend erfoderlich, um einen professionellen Cyber-Versicherungsschutz zu erhalten.

HISCOX
WISSEN VERSICHERT.

SCHADENSZENARIEN

Exemplarischer Schadenfall:
Wie Hacker bei einem Mittelständler 3 Mio. Euro Schaden erzeugten

Ein exportstarker Mittelständler aus dem produzierenden Gewerbe mit 150 Mio. Euro Jahresumsatz nahm regelmäßig das Einpflegen von neuen Patches vor, um Sicherheitslücken zeitnah zu schließen. Dennoch gelang es Hackern, **durch eine offene Schwachstelle in das IT-System vorzudringen** und unbemerkt eine Hintertür einzubauen. Das ist ein Systemzugang unter Umgehung der normalen Zugriffssicherung. So konnten die Angreifer ein halbes Jahr lang das System auskundschaften und unbemerkt immer weitreichendere Adminrechte erschleichen. So gelang es den Cyber-Kriminellen, an einem Wochenende **das gesamte IT-System inklusive der Online-Back-ups zu verschlüsseln,** wodurch die gesamte Geschäftstätigkeit zunächst komplett lahmgelegt wurde. Das Unternehmen aktivierte umgehend seinen Geschäftsfortführungsplan und ging in den Notbetrieb.

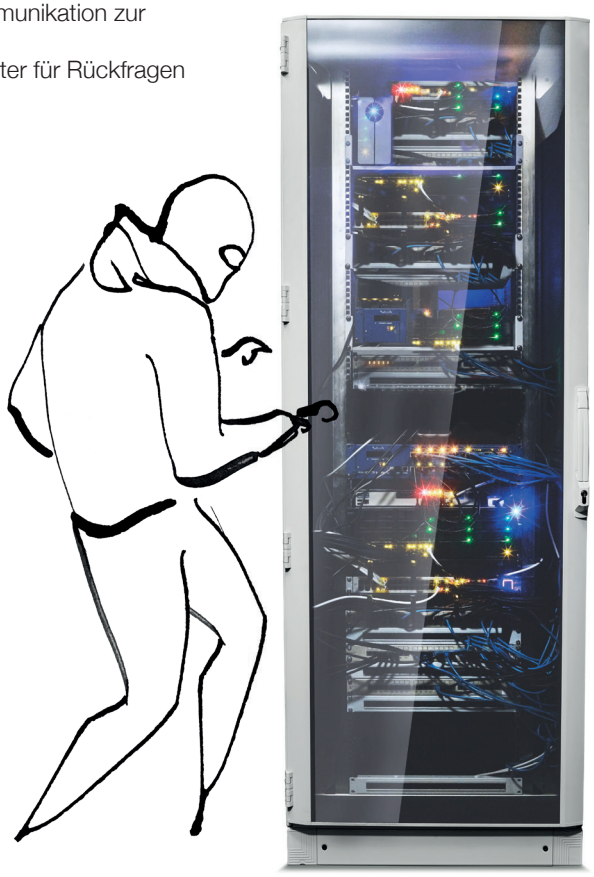
Glücklicherweise gab es eine **funktionstüchtige Offline-Datensicherung.** Durch die lange Zeit der unbemerkten Kompromittierung des IT-Systems konnte dieser allerdings nicht mehr vertraut werden. Daher wurde in Abstimmung mit Hiscox beschlossen, mit Hilfe von Experten im Parallelbetrieb ein komplett neues und integres IT-System aufzubauen. In den ersten Tagen nach dem Angriff waren die Einschränkungen und Verluste am größten. Insgesamt dauerte es mehrere Wochen, bis das neue IT-System komplett stand und es keine Einschränkungen mehr gab. Zusätzlich musste dem Verdacht nachgegangen werden, dass von den Hackern unberechtigt Daten Dritter eingesehen wurden und es so zu einer Vertraulichkeitsverletzung gekommen ist. Im Rahmen der Informationspflichten wurde eine Meldung bei der zuständigen Datenschutzbehörde vorgenommen und alle Betroffenen informiert.

Fazit: 3.000.000 Euro Gesamtschadenaufwand, davon:

- 650.000 Euro für Krisenmanagement, IT-Forensik, Wiederherstellung
- 550.000 Euro für den Aufbau eines Parallelsystems
- 1.700.000 Euro für den Ertragsausfallschaden
- 30.000 Euro für den Datenschutz-Anwalt und das behördliche Meldeverfahren
- 30.000 Euro für PR-Beratung – umfangreiche Krisenkommunikation zur Vermeidung eines Reputationsverlusts
- 40.000 Euro für die Information der Kunden inkl. Call Center für Rückfragen

Video aus unserer Praxis: „Nur noch der Lichtschalter ließ sich bedienen“ – so legten Hacker ein Unternehmen komplett lahm

Cyber-Kriminelle legten durch Schadsoftware das komplette IT- und Telefonsystem des mittelständischen Unternehmens Schäfer Trennwandsysteme GmbH lahm. Erfahren Sie im Video alles zur Attacke, zum Weg aus der Krise und warum es für Unternehmen aller Größen und Branchen so entscheidend ist, eine gute Cyberversicherung zu haben: hiscox.de/cyber-attacke-video



Hiscox
Arnulfstraße 31, 80636 München
T +49 89 54 58 01 100 **F** +49 89 54 58 01 199
E hiscox.info@hiscox.de **W** **hiscox.de**