



Cyber+
www.hdi.at/cyber



CYBER+
Das Plus für Ihre
IT-Sicherheit



Cyber+: Das Plus gegen Schäden durch Internet-Attacken

Trotz bester Abwehrmechanismen sind auch produzierende Industrieunternehmen nicht vor Risiken durch Cybercrime gefeit. Die finanziellen Folgen daraus sind schwer kalkulierbar. Neben der unternehmenseigenen IT-Sicherheit ist eine zusätzliche Absicherung gegen Schäden durch Internet-Attacken sinnvoll.

Zuverlässiger Schutz

Dieser ganzheitliche und überspartliche Versicherungsschutz deckt zum einen Eigenschäden durch Cybercrime. Zum anderen sichert er Drittschäden ab, für die Unternehmen gegenüber ihren Kunden, Dienstleistern oder sonstigen Dritten haften müssen. Zusätzlich kann auch den zivil- und strafrechtlichen Verantwortlichkeiten der Geschäftsleiter Rechnung getragen werden.

Das Wichtigste in Kürze:

- 1 Ganzheitlicher und überspartlicher Schutz**
Cyber+ ist ein ganzheitlicher und überspartlicher Versicherungsschutz gegen Schäden durch Internet-Attacken.
- 2 Eigenschäden und Drittschäden**
Cyber+ deckt sowohl Eigenschäden als auch Drittschäden ab, für die Unternehmen gegenüber Kunden, Dienstleistern oder sonstigen Dritten haften müssen..
- 3 Risikotechnische Analyse**
Versicherungsnehmer profitieren durch risikotechnische Analyse der IT-Sicherheit von der langjährigen Expertise, über die HDI im Bereich Informationstechnologie verfügt.
- 4 Modularer Aufbau, optionale Bausteine**
Durch modularen Aufbau können Unternehmen je nach Bedarf optionale Bausteine zu ihrer Cyber+-Polizze zusammenstellen, z. B. Rechtsschutz, Managerhaftpflicht und Industrie-Spionage.

Umfangreiche Deckung

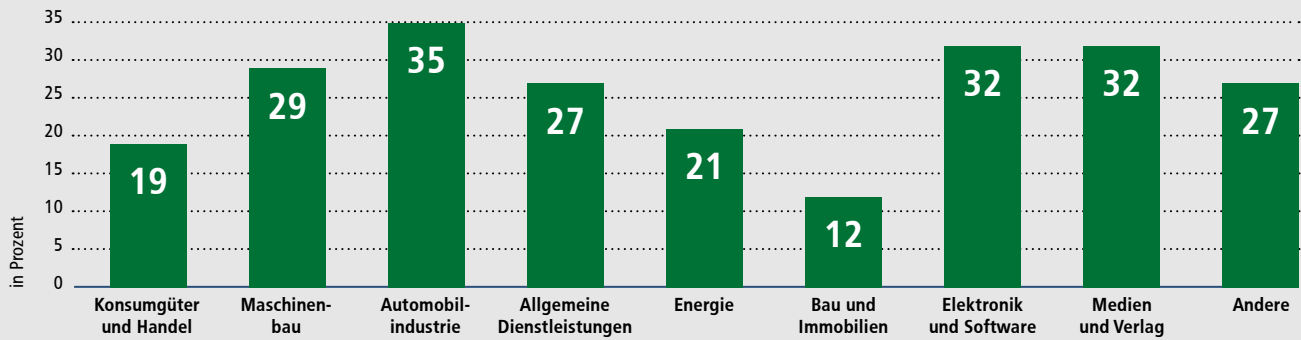
Zu den versicherbaren Schäden bzw. Kosten zählen unter anderem:

- > Beschädigung, Diebstahl oder unerlaubte Veröffentlichung von Daten sowie die Datenwiederherstellung
- > Betriebsunterbrechung in der Produktion
- > Krisenkommunikation und Benachrichtigung
- > Forensische Untersuchungen

Optional sind zudem unter anderem die folgenden Bausteine im Zusammenhang mit Cyber-Risiken versicherbar:

- > Rechtsschutz
- > Managerhaftpflicht
- > Cyber-Bedrohung
- > Industrie-Spionage (Verletzung von Betriebsgeheimnissen)
- > Vertrauensschäden durch Dritte / Fehlverhalten von Mitarbeitern

War Ihr Unternehmen in den vergangenen zwei Jahren von e-Crime-Handlungen betroffen? (nach Branchen)



Quelle: KPMG AG, e-Crime-Studie 2012

Beispiele für mögliche Cyber-Szenarien:

Hacker erbeuten Kreditkartendaten

Ein mittelständisches Unternehmen, welches seit einigen Jahren erfolgreich auf Online-Shopping gesetzt hat, wird seit einigen Monaten unbemerkt gehackt. Erst nachdem ein Kreditkartenunternehmen auf unautorisierte Buchungen bei einer Vielzahl von Kunden aufmerksam macht, beginnt die Suche des Unternehmens nach der IT-Sicherheitslücke.

Obwohl dem Vorfall höchste Priorität eingeräumt wird, kann die Ursache erst nach einigen Wochen gefunden und behoben werden. Zwischenzeitlich ist der Vorfall von der lokalen Presse öffentlich gemacht worden, woraufhin behördliche Ermittlungen veranlasst werden.

Während dieser Zeit brechen die Umsätze des Unternehmens stark ein. Wochen später ist der Sachverhalt Gegenstand der Generalversammlung und veranlasst einige Gesellschafter dazu, nach der Verantwortlichkeit der Unternehmensleitung für diesen Fall und für die IT-Sicherheit im Allgemeinen zu fragen.

Produktion steht still

Die Firma S. ist in einem hoch spezialisierten Segment tätig und steht kurz vor der Markteinführung eines allseits erwarteten Produkt-Updates. Als Weltmarktführer genießt das Unternehmen große öffentliche Wahrnehmung – die nicht immer nur gut gemeint ist.

Mitten in der Produktion bei Vollauslastung bleiben die Maschinen plötzlich stehen. Erst nach einiger Zeit und Hinzuziehung von externen IT-Spezialisten kann die Produktion wieder aufgenommen werden. Ursache für den Stillstand war ein gezielter Angriff auf die Steuerungssoftware der Produktionsanlage.

Neben der verspäteten Markteinführung ist u. a. ein wesentlicher Umsatzausfall durch die Betriebsunterbrechung und hohe Aufwendungen für die Wiederinbetriebnahme zu verzeichnen.

Hoher Schutz plus flexible Erweiterung

Einzelne Risiken aus dem Cyberbereich wurden bisher eher auf individueller Basis ausschnittsweise versichert. Mit Cyber+ bietet HDI Industrie-Unternehmen eine Versicherungslösung aus einem Guss.

Ein großer Vorteil der Cyberversicherung von HDI ist ihr modularer Aufbau. Das heißt, Unternehmen können je nach Bedarf optionale Bausteine zu ihrer Cyber+-Police zusammenstellen. Daneben werden wichtige Zusatzleistungen standardmäßig geboten, welche das Risk- bzw. Krisenmanagement sinnvoll ergänzen.

Risikodialog auf Augenhöhe plus mehr IT-Sicherheit

HDI Industrie unterstützt seine Kunden auch aktiv bei der risikotechnischen Analyse der IT-Sicherheit. Diese erfolgt mittels einer Selbstauskunft des Kunden, mit welcher mögliche Cyber-Risiken identifiziert werden können.

Gleichzeitig dient diese Analyse der Bewertung der IT-Sicherheit. In speziellen Fällen kann ergänzend ein Vertiefungsgespräch sinnvoll sein. Auf diesem Weg profitieren Versicherungsnehmer von der langjährigen Expertise von HDI im Bereich Informationstechnologie.

Zu Cybercrime zählen:

- > Computerbetrug
- > Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- > Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung
- > Datenveränderung/Computersabotage
- > Ausspähen, Abfangen von Daten einschließlich Vorbereitungs-handlungen

Quelle: BKA Deutschland, Cybercrime Bundeslagebild 2012

Wir sind für Sie da.
HDI Service-Center +43 (0) 509 05 - 0
Mo - Fr 7.30 - 17.00 Uhr
office@hdi.at

