Cyber-Versicherungen

Effectively Managed Cyber Risk (EMCR)

www.hdi.global

RUNDUM-SCHUTZ GEGEN CYBER-RISIKEN

Bedarfsgerechte Versicherungslösungen und ganzheitlicher Service.

Digitalisierung erhöht Ausfallrisiken.

Die voranschreitende Digitalisierung und Vernetzung verändern massiv die Produktions- und Arbeitswelten in Wirtschaft und Industrie. So implementieren Unternehmen IT-Applikationen, erneuern IT-Komponenten und IT-Systeme, vernetzen diese und automatisieren administrative und Fertigungsprozesse. Im Zuge dieser dynamischen Entwicklungen steigt das potentielle Schadenausmaß von Cyber-Attacken, mit denen Mittelstand ebenso wie Großunternehmen täglich konfrontiert werden. Im Fokus steht der digitale Produktionsfaktor „Information", auf den Cyber-Kriminelle durch Spionage, Sabotage oder Diebstahl von Daten unmittelbar zugreifen wollen.

Täter setzen verstärkt Ransomware ein

Die Angriffsformen sind vielfältig. In jüngster Zeit ist der verstärkte Einsatz von Ransomware zu beobachten. Dabei setzen die Angreifer Schadsoftware ein, die IT-Systeme, Rechner oder Daten blockieren und geben diese erst gegen Zahlung eines Erpressungsgelds wieder frei. Auch sogenannte Zero-Day-Exploit-Attacken nehmen zu. Hier nutzen Täter bisher unbekannte Schwachstellen aus, bevor ein Sicherheitsupdate zur Verfügung steht, um diese Lücke zu schließen.

Digitale Wertschöpfung wird zum Schlüsselrisiko

Unternehmen sind durch derartige Cyber-Angriffe stark gefährdet. Denn das potenzielle Schadenausmaß beschränkt sich nicht allein auf die Wiederherstellung verlorener, gestohlener oder beschädigter Daten. Aufgrund der zunehmenden Vernetzung industrieller Prozesse steigt die Gefahr von Produktionsausfällen und eines kompletten Betriebsstillstands. Damit wird die Unterbrechung der digitalen Wertschöpfung zum Schlüsselrisiko der industriellen Fertigung.

Experten-Tipp

Auf den Ernstfall vorbereiten

Schadenfälle zeigen es: Sobald Hacker ins betriebliche IT-System eingedrungen sind, zählt jede Minute, um das Schadenausmaß noch begrenzen zu können. Für Unternehmen ist es daher ratsam, einen Notfallplan zu erstellen. Nur dann können Gegenmaßnahmen schnell umgesetzt werden, weil jeder Mitarbeiter weiß, was er tun muss. Zudem kann ein integriertes Krisenmanagement sofort aktiviert werden. Im Rahmen des Vier-Säulen-Konzepts EMCR (Effectively Managed Cyber Risk) können von Kunden individuell auch Angebote für präventive weitere Serviceangebote eingeholt werden. (Mehr dazu auf der nächsten Seite unter „4. Säule Prävention").

Risikobewusstsein schärfen

Angesichts dieser Gefahren besteht in Unternehmen großer Handlungsbedarf. Weder Softwarefehler oder technische Störungen noch Versäumnisse von Mitarbeitern lassen sich gänzlich ausschließen. Folglich reichen technische Schutzmaßnahmen allein nicht aus. Vielmehr müssen sie in einem unternehmensweiten, kontinuierlichen Risikomanagementprozess eingebunden sein, der auf vier Säulen basiert: Identifikation, Risikotransfer, Reaktion und Prävention. Mit dem Konzept „Effectively Managed Cyber Risk", kurz EMCR, bietet die HDI Global SE eine ganzheitliche Produktlösung, die als positiver Treiber dazu beitragen kann, das Risikobewusstsein hinsichtlich der digitalen Wertschöpfung im Unternehmen zu schärfen.

Das Vier-Säulen-Modell EMCR (Effectively Managed Cyber Risk) der HDI Global SE:			
Identifikation **Risk Assessment Services**	**Ganzheitliche, zielgruppen-spezifische Produkt-lösungen** **Cyber+ und Cyber+ Smart**	**Reaktion** **Cyber Incident Response & Claims Hand-ling**	**Prävention** **Weitere Service-angebote, z. B. Workshops zum Krisen-management, Penetrations-tests oder Mitarbeiter-schulungen**

1. Säule: Identifikation
Risk Assessment Services

Die HDI Cyber-Risikoingenieure unterstützen Sie dabei, den Reifegrad Ihrer IT- und Informationssicherheit festzustellen. Ergänzend zum Ergebnis erhalten Sie konkrete Empfehlungen, mit welchen Aktivitäten der Reifegrad angehoben werden kann. Besonders vorteilhaft für Sie:

- Der individuelle Reifegrad wird nicht nur auf Basis von technischen Schutzmaßnahmen ermittelt. Die HDI Cyber-Risikoingenieure betrachten hierfür auch die organisatorischen Abläufe und damit verbundene Richtlinien im Rahmen Ihrer Sicherheitsorganisaton.
- Unsere Risk Assessment Services orientieren sich an den Methoden internationaler Standards, wie zum Beispiel ISO 27001 oder BSI Grundschutz.
- Durch eine Betriebsunterbrechungs- und Lieferketten-analyse werden relevante IT-Prozesse identifiziert und betriebliche Folgekosten einer IT-Störung aufgrund eines Cyber-Angriffs ermittelt. Risiko-Ingenieure von HDI Risk Consulting unterstützen bei Bedarf diesen Prozess.

2. Säule: Ganzheitliche, zielgruppenspezifische Produktlösungen
Cyber+ und Cyber+ Smart

Bedarfsgerecht können Unternehmen ihre finanziellen Risiken durch die HDI Versicherungsprodukte Cyber+ und Cyber+ Smart absichern, da der Deckungsschutz auf die jeweiligen Anforderungen zugeschnitten ist: Beide Lösungen sichern Eigenschäden ab, die zum Beispiel durch eine Betriebsunterbrechung nach einem Cyber-Angriff entstehen. Auch Drittschäden sind abgedeckt, für die betroffene Betriebe von ihren Kunden und Geschäftspartnern in Anspruch genommen werden. Im Ergebnis sind Unternehmen gegen vielfältige Formen sogenannter Informationssicherheitsverletzungen gewappnet. Konkret geht es dabei um Fälle, wenn beispielsweise personenbezogene Daten entwendet, Betriebsgeheimnisse Dritter verletzt oder das firmeneigene Netzwerk attackiert werden.

3. Säule: Reaktion
Cyber Incident Response & Claims Handling

Bei HDI sind Cyber-Schadenexperten im Einsatz, die praktische Erfahrung mit Groß- und Frequenzschäden haben.

Gleichzeitig kooperiert HDI mit professionellen Dienstleistern, wie zum Beispiel Forensikern und Fachanwälten. Sie erhalten so in jeder Phase eines Cyber-Vorfalls bestmögliche Unterstützung, insbesondere auf diesen Feldern:

- Wiederherstellung von Daten und Software
- Information von Betroffenen aufgrund von Datenschutz-anforderungen (DSGVO)
- PR-Beratung zum Schutz der Reputation

4. Säule: Prävention
Weitere Serviceangebote

Cyber-Kriminelle verschaffen sich Zugriff auf sensible Informationen und gefährden die digitale Wertschöpfung hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Das essenzielle Ziel der dauerhaften Informationssicherheit lässt sich daher nur durch stetige Prävention erreichen. Hierfür haben professionelle Kooperationspartner mehrere Service-angebote entwickelt, für die Kunden individuell Angebote einholen können.

- Vor-Ort-Onboarding von Dienstleistern
- Workshops zu ISO-Zertifizierungen, Krisenmanagement und Notfallplanung bei Cyber-Vorfällen, Compliance und Best Practices
- Externe Schwachstellenanalysen
- Technisches Assessment geschäftskritischer Systeme wie SAP
- Penetrationstests durch Simulation von Cyber-Angriffen
- Mitarbeiterschulungen und andere Maßnahmen zur Prävention

		Jahresumsatz	Selbsbehalte (SB)	Versicherungsumfang
Cyber+	anpassbar	▪ ab 5 Mio. Euro	▪ Monetäre SB abhängig von Umsatz und Limit ▪ 12 Stunden SB bei BU (Integralfranchise)	▪ max. 25 Mio. Euro ▪ Haftzeit 180 Tage bei BU
Cyber+ Smart	standardisiert	▪ 5 Mio. bis 50 Mio. Euro	▪ Mindest-SB 2.500 Euro ▪ 12 Stunden SB bei BU (Integralfranchise)	▪ max. 1 Mio. Euro ▪ Haftzeit 180 Tage bei BU

Bedarfsgerechte Produktlösungen für den Mittelstand und Großunternehmen (2. Säule)

HDI Global SE
HDI-Platz 1
30659 Hannover
cyber@hdi.global
www.hdi.global

404-FL017 201909