Cyberschäden:
So hilft HDI.

HDI

Firmen und Freie Berufe ▪ Cyberversicherung

Wenn in der digitalen Welt reale Sicherheit wichtig ist.

HDI hilft.

Marketing-Unterlage

www.hdi.de/cyberversicherung

Tipps bei häufig auftretenden Cyberangriffen.

Mit professioneller Schadsoftware ist es für Angreifer ein Leichtes, um an vertrauliche Daten zu kommen, die Abläufe zu stören oder gar den Geschäftserfolg zu sabotieren. Die folgenden drei Tipps aus der Praxis zeigen Ihnen, wie Sie mit häufig auftretenden Cyberangriffen umgehen.

Malware

Sie vermuten, dass Malware Ihren Rechner beschädigt hat, beispielsweise durch das Öffnen eines unbekannten E-Mail-Anhangs:

- Deaktivieren Sie das aktuell verbundene Netzwerkgerät, indem Sie das Netzwerkkabel ziehen (bei WLAN in den Flugmodus wechseln).
- Schalten Sie den Computer nicht aus.

Ransomware-Angriff

Bei einem Ransomware-Angriff versucht ein Dritter mit Schadsoftware, die Ihren Computer sperrt oder Ihre Daten verschlüsselt, Geld für das Entsperren bzw. Entschlüsseln zu erpressen.

- Zahlen Sie die Lösegeldforderung nicht.
- Notieren Sie die Dateiendung der verschlüsselten Dateien und machen Sie einen Screenshot des Erpressungsscreens.
- Deaktivieren Sie das aktuell verbundene Netzwerkgerät (Netzwerkkabel ziehen; bei WLAN in den Flugmodus wechseln).
- Schalten Sie den Computer nicht aus.

DoS(Denial of Service)- oder DDoS(Distributed Denial of Service)-Angriff

Ein Angreifer versucht, eine bestimmte Applikation, wie zum Beispiel den Webauftritt des Unternehmens, gezielt zu überlasten. Der Angriff kann in Form einer Störung auftreten oder die angegriffene Applikation komplett lahmlegen.

- Beschaffen Sie sich von Ihrem IT-Experten Firewall-Logs mit den Aufzeichnungen des eingehenden (böswilligen) Traffics.
- Kontaktieren Sie Ihren Internetdienstanbieter (ISP) mit der Bitte, den Verursacher des böswilligen Traffics zu blockieren. Unser IT-Sicherheitsdienstleister SEC Consult unterstützt Sie gern.

Grundsätzlich gilt: Erstellen Sie eine regelmäßige Datensicherung und lagern diese an physisch getrennten Orten zu Ihren normalen Systemen. So können Sie im Notfall Ihre Daten wiederherstellen.

Kurze Schadenbeispiele aus der Praxis.

1 Durch einen gezielten Angriff auf Ihre Onlinepräsenz wird der Server vollständig manipuliert und zum Versenden von Spam-Mails missbraucht. Verschiedene Kunden beschweren sich über die unseriösen Mails und drohen mit Klage. In diesem Fall muss die Ursache schnell geklärt und das System bereinigt werden. Eine PR-Agentur steuert die Entschuldigung bzw. Rechtfertigung gegenüber den Kunden. Die Kosten dafür übernimmt HDI.

2 Durch die gezielte Übernahme eines E-Mail-Servers ist es einem Angreifer gelungen, einen sogenannten Fake President, auch CEO-Fraud-Angriff genannt, durchzuführen. Auf diese Art und Weise gibt sich der Angreifer mit einer gefälschten E-Mail-Adresse als CEO des Unternehmens aus und beauftragt einen Mitarbeiter, eine Überweisung auf sein Konto vorzunehmen. HDI übernimmt die Kosten für die Analyse der Vorgehensweise, das Schließen der Lücke im E-Mail-Server sowie die forensische Aufbereitung, die vor Gericht verwendbar ist.

3 Ein Fernwartungszugang war unzureichend abgesichert. Dadurch wurde Ihr Server zum Crypto Mining missbraucht. Der Angreifer veränderte das Administratorpasswort, wodurch Ihr IT-Dienstleister nicht mehr auf das System, die Firmenpräsenz oder die E-Mail-Accounts zugreifen kann. HDI übernimmt die Kosten für das Aussperren des Angreifers, die Beseitigung der Crypto-Mining-Software sowie die Absicherung des Fernwartungszugangs.

4 Ein Firmennetzwerk ist mit Malware infiziert. Sensible Daten wurden dadurch verschlüsselt und an die Angreifer geschickt. Zusätzlich wurden durch die Software Keylogger installiert, mit denen sich eingetippte Passwörter abfangen lassen. Um diese Probleme zu lösen, müssen die Sicherheitslücken erkannt und geschlossen werden, die Ausbreitung der Malware im Netzwerk überprüft und die befallenen Systeme isoliert werden. Der Angreifer wird ausgesperrt, die Passwörter der betroffenen Accounts geändert. Die Kosten für diese Maßnahmen trägt HDI.

Die HDI Cyberversicherung unterstützt im Schadenfall aktiv und bietet von Beginn an kompetente Unterstützung durch einen IT-Sicherheitsdienstleister – und das in den ersten 90 Minuten ohne Anrechnung auf den Selbstbehalt.

Was ist bei einem Cyberangriff zu tun?

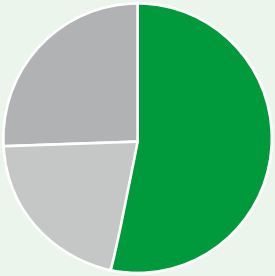
Trojaner, Viren, Schadsoftware – Cyberattacken gefährden den Geschäftserfolg. Abläufe werden gestört, sensible Daten gehen verloren oder geraten in die falschen Hände. Die Folge: Das Vertrauen Ihrer Kunden ist erschüttert, es kommt zur Klage – ein Albtraum sowohl für klein- als auch für mittelständische Unternehmen, Kanzleien und Arztpraxen. Die hohen Kosten, die Cyberangriffe nach sich ziehen, aber auch die verschärfende Datenschutz-Grundverordnung (DSGVO) erfordern einen starken und verlässlichen Partner an Ihrer Seite und einen Ad-hoc-Krisenplan für den Fall der Fälle.

Im Fall der Fälle unterstützen wir Sie selbstverständlich bei der Auswahl:

- des IT-Sicherheitsdienstleisters
- eines geeigneten Rechtsanwalts mit der Expertise IT-Sicherheit und Datenschutz
- einer geeigneten PR-Agentur
- eines Dienstleisters zur Überwachung von Kreditkarten
- von Fachleuten zur Datenrettung und Schadeneindämmung

Cybercrime – es kann fast jeden treffen

Anteil der deutschen Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren.



53 % betroffen

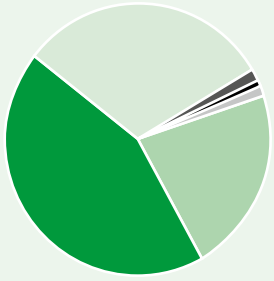
26 % vermutlich betroffen

21 % nicht betroffen

ca. 55 Mio. Euro Schaden pro Jahr

Cybercrime – Entwicklung der Bedrohungslage

Wie hat sich die Bedrohungslage durch Cyberangriffe in den letzten 12 Monaten aus Ihrer Sicht geändert?



43,5 % erhöht

30,8 % gleich geblieben

22,5 % stark erhöht

1,8 % verringert

1,3 % weiß nicht, k. A.

0,3 % stark verringert

Quelle: Wirtschaftsschutz in der digitalen Welt, Bitkom, Juli 2017

1 Schadenbeispiel: Bewerbung im digitalen Zeitalter.

Onlinebewerbungen sind heutzutage gang und gäbe. Dies birgt viele Vorteile, aber auch neue Risiken.

Was ist passiert?
Sie erhalten die E-Mail eines Bewerbers. In den Anhängen ist ein Trojaner in Form einer Erpressungssoftware enthalten, der nach dem Öffnen den Zugang zu den eigenen Daten versperrt.

Die Erpresser fordern eine Zahlung in der Online-Währung „Bitcoin", damit Sie wieder Zugriff auf Ihre Daten erhalten. Durch die Sperrung sind die Abläufe blockiert, eine eigene IT-Abteilung ist nicht vorhanden. Die Hilfe eines IT-Spezialisten ist gefragt.

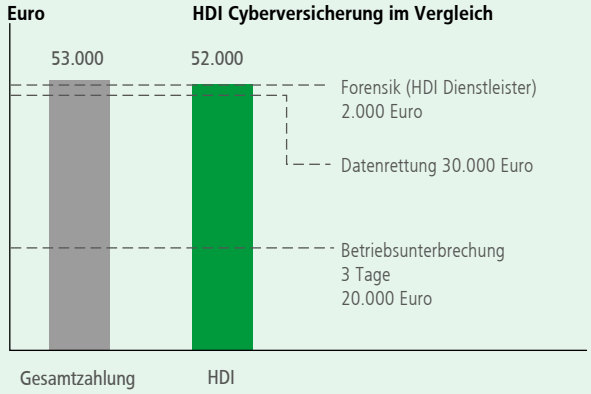
Einsatz des IT-Sicherheitsdienstleisters
HDI kann Sie in dieser Situation unterstützen. Über eine Cyberschaden-Hotline können Sie direkt mit unserem qualifizierten Cyber-Dienstleister verbunden werden. Dieser Spezialist schaltet sich sofort per Fernwartung auf den betroffenen Rechner und beginnt mit der Forensik. Zunächst werden erste akute Maßnahmen besprochen und durchgeführt. So kann der Schaden schnellstmöglich eingedämmt werden. Im Anschluss erfolgt die Koordination mit weiteren Dienstleistern.

Je nach Größe des Betriebs kann die benötigte Hilfe im Einzelfall variieren. Die jeweils notwendigen Kosten sind im Versicherungsschutz enthalten.

Ergebnis

Die Entschlüsselung und die Betriebsunterbrechung konnten zeitnah behoben und der Angriff mithilfe des Dienstleisters erfolgreich abgewehrt werden.

Leistung und ungefähre Kosten



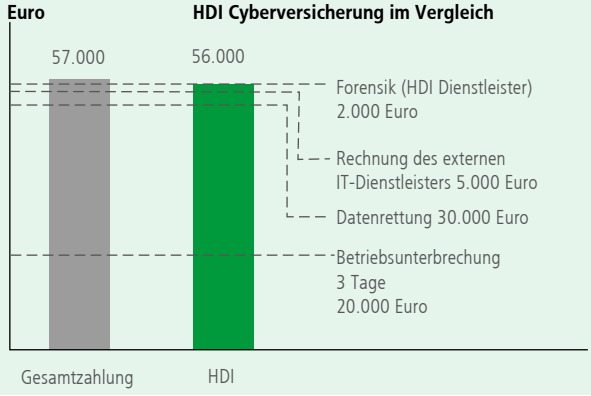
2 Schadenbeispiel: Cyberangriff durch Schadsoftware.

Sie verfügen über einen beruflich genutzten Pool von ca. 30 Rechnern, auf denen Antivirenprogramme installiert sind. Trotzdem werden Sie Opfer eines Cyberangriffs.

Was ist passiert?
Das eingesetzte Antivirenprogramm blockiert einen Virus und meldet diesen Fall. Die Geschäftsführung geht davon aus, dass mit einer Schadsoftware angegriffen wurde, und schaltet den eigenen IT-Dienstleister ein. Da es sich jedoch nicht um einen IT-Forensiker handelt, wird die Malware nicht identifiziert. Den Geschädigten wird lediglich empfohlen, die Backups einzuspielen. Der Dienstleister stellt eine Rechnung über 5.000 Euro für diesen Fall aus – die Sicherheitslücke wurde allerdings nicht behoben. Innerhalb kürzester Zeit wird die Agentur erneut angegriffen, in diesem Fall mit einem Trojaner. Durch die Verknüpfung sämtlicher Computer verbreitet sich der Trojaner im gesamten Serverbereich und damit auf allen 30 Rechnern. Der Betrieb ist insgesamt unterbrochen und nicht mehr handlungsfähig.

Vermittlung eines IT-Sicherheitsdienstleisters durch HDI
Wenn Sie wünschen, vermitteln wir Ihnen direkt einen Cyber-Dienstleister, der sich per Fernwartung auf den betroffenen Rechner schaltet und mit der Forensik beginnt. Nach Rücksprache mit uns vereinbart der Dienstleister mit Ihnen alle weiteren Schritte. Für eine zukünftige Schadenprävention ist

Leistung und ungefähre Kosten



es notwendig, dass die Ursache für den Angriff gefunden und beseitigt wird. Anderenfalls müssen Sie immer wieder mit einem Angriff rechnen.

Einsatz weiterer IT-Dienstleister
Für die Bereinigung des Rechners und das Einspielen der vorhandenen Back-ups spricht sich unser Dienstleister mit Ihnen ab. Je nach Wunsch auch mit Ihrem IT-Dienstleister. Sollten Ihre kompletten IT-Systeme betroffen sein, ist eine Betriebsunterbrechung von mehreren Tagen nicht auszuschließen.

Fazit

Beauftragen Sie bei dem Verdacht eines Cyberangriffs sofort einen Spezialisten, der Sie nicht nur kurzfristig von Ihrem Problem befreit, sondern auch die Ursache für den Angriff lokalisiert und behebt. In diesem Schadenfall sind zusätzlich die externen IT-Dienstleisterkosten angefallen.

3 Schadenbeispiel: verlorener USB-Stick/ verlorenes Diensthandy/-laptop.

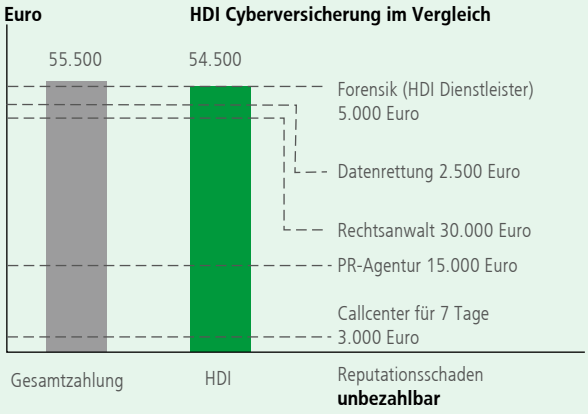
Einer Ihrer Mitarbeiter verliert auf einer Dienstreise einen USB-Stick, ein Diensthandy oder ein Dienstlaptop. Auf dem verlorenen Gerät befinden sich sensible Daten, es handelt sich somit um einen möglichen Verstoß gegen die EU-Datenschutz-Grundverordnung.

Was ist passiert?
Die Kundendaten sind in falsche Hände geraten, die Erpresser drohen nun, die Daten zu veröffentlichen. Neben einem Reputationsschaden drohen enorme Schadenersatzforderungen der Betroffenen. Zudem können erhebliche Geldbußen nach der EU-Datenschutz-Grundverordnung (DSGVO) anfallen. Auch ohne eine Erpressung durch Dritte sind Sie nach den Bestimmungen der DSGVO in der Verantwortung. Je nach Einzelfall muss geprüft werden, ob eine Benachrichtigungspflicht gegenüber den Klienten und/oder den Behörden besteht.

Unterstützung durch HDI
Stellen Betroffene Schadenersatzforderungen, übernimmt HDI die Kosten für die Haftungsprüfung. Darüber hinaus vermitteln wir Ihnen für den Eigenschaden einen Rechtsanwalt, der im Bereich IT-Recht und Datenschutz spezialisiert ist. Der Anwalt bespricht mit Ihnen die weiteren Schritte und veranlasst die notwendigen Maßnahmen. Insbesondere erhalten Sie Unterstützung im Umgang mit den Behörden, um Ihren Melde- und Informationspflichten nach der EU-Datenschutz-Grundverordnung nachzukommen.

Darüber hinaus übernehmen wir die notwendigen Kosten für eine PR-Agentur, die Ihnen bei einem drohenden Reputationsschaden zur Seite steht. Ebenfalls abgedeckt sind – sofern erforderlich – die Kosten für ein externes Callcenter, das die zahlreichen Kundenanfragen beantwortet.

Leistung und ungefähre Kosten



7003001133-201802

Ihre Zukunft in besten Händen.
HDI steht für umfassende Versicherungs- und Vorsorgelösungen, abgestimmt auf die Bedürfnisse unserer Kunden aus mittelständischen Unternehmen, den Freien Berufen und Privathaushalten. Was uns auszeichnet, sind zukunftsorientierte, effiziente Produktkonzepte mit einem guten Preis-Leistungs-Verhältnis sowie ein exzellenter Service.

HDI Versicherung AG
HDI-Platz 1
30659 Hannover
www.hdi.de/cyberversicherung