

CYBER-SCHADENMELDUNG EXALI

Um Ihre Schadenmeldung optimal bearbeiten zu können, bitten wir Sie möglichst vollständige Angaben zum Schadenfall zu machen. Bitte beantworten Sie dazu alle in Ihrem Fall zutreffenden Fragen auf den folgenden Seiten und schicken Sie diese schnellstmöglich an die Kundenbetreuung von exali (E-Mail: schaden@exali.de).

Vielleicht ist es Ihr erster Cyber-Schadenfall, daher möchten wir Ihnen nachfolgend ein paar hilfreiche Informationen geben, wie Sie sich im Schadenfall richtig verhalten:

Wählen Sie unbedingt die **24-Stunden Notfall-Nummer** bei Cyberschäden: **0800 6275350**.
Bei der Cyber-Notfall-Hotline nehmen sich Cyber-Experten Ihrem Notfall an und leiten alle notwendige Maßnahmen ein.

- Bewahren Sie Ruhe und führen Sie zuerst eine Bewertung des Vorfalls durch, um einen technischen Defekt auszuschließen. Deutet beispielsweise alles auf einen Hackerangriff, gilt es Folgendes zu klären: Woher kam der Angreifer? Wie ist er in die Systeme gelangt? Welche Systeme sind von dem Angriff betroffen? Wurden Daten entwendet und wenn ja, in welchem Umfang?
- Prüfen Sie, ob der Cyber- Dateneigenschaden einer behördlichen Meldepflicht unterliegt.
- Greifen Sie nur mit Bedacht in die Systeme ein. Ein Neustart der Systeme kann bspw. die Ursachenforschung erschweren. Die Systeme sollten nur nach Rücksprache mit einem Experten abgeschaltet werden.
- Halten Sie genau fest, was sich wann ereignet hat, welche Maßnahmen Sie getroffen haben und wer Zugriff zu möglichen Beweismitteln hatte. Notieren Sie sich, wer ab dem Zeitpunkt des Angriffs an den kompromittierten Systemen Änderungen vorgenommen hat und welcher Art diese waren. Diese Informationen sind für die Aufarbeitung des Vorfalls wichtig.
- Sichern Sie alle möglichen Beweise des Cyber- Dateneigenschadens. Dazu gehören die System-Protokolle, Logfiles, Datenträger, Notizen und eventuell Fotos von Bildschirminhalten. Dies erleichtert eine IT-forensische Untersuchung.
- Versuchen Sie so schnell wie möglich, den Schaden einzudämmen. Prüfen Sie, inwiefern eine Beendigung aller unautorisierten Zugriffe und Verbindungen zum betroffenen System notwendig ist.
- Leiten Sie uns die Sachverhaltsbeschreibung Ihres Cyber-Dateneigenschadens mit dieser Schadenmeldung weiter.
- Informieren Sie alle relevanten Fachabteilungen Ihres Unternehmens nach dem Need-to-Know-Prinzip über den Vorfall und das weitere Vorgehen. Prüfen Sie, ob externe Stakeholder und die Öffentlichkeit zusätzlich informiert werden müssen.
- Sollten sich nach dieser Schadenmeldung weitere wichtige Informationen ergeben, leiten Sie diese bitte an uns oder die Schadenregulierungsstelle weiter (sofern vorhanden mit Angabe der Schadennummer).

Bitte beachten Sie zudem:

- Sie als Versicherungsnehmer sind zur Einhaltung der in Punkt I. des Bedingungswerkes aufgeführten Obliegenheiten verpflichtet.
- Bei einer Schadenersatzzahlung durch den Versicherer wird die ggf. vertraglich vereinbarte Selbstbeteiligung in Abzug gebracht.
- Der Schriftverkehr mit exali oder dem Versicherer über das Vorgehen bei der Schadenfallbearbeitung, insbesondere Einschätzungen und Vorgaben zum weiteren Vorgehen, ist vertraulich zu behandeln.

Sollten Sie weitere Fragen haben, helfen Ihnen unsere Kundenbetreuer gerne weiter **0 821 / 80 99 46 - 0**.

Mit freundlichen Grüßen,



Tino Wiedemann
Teamleiter Kundenbetreuung

ANGABEN ZUM VERSICHERUNGSNEHMER

Vertragsnummer/Police

Name/Firma

Straße/Nr.

PLZ/Ort

Telefon

E-Mail

Ansprechpartner

Betrifft der Schaden eine Tochterfirma?

Ja

Nein

Firmenname

Straße/Nr.

PLZ/Ort

1. VORVERSICHERUNG

Hatten Sie früher eine Cyber-Versicherung?

Ja

Nein

Wenn JA,

von:

bis:

Bei welcher Gesellschaft?

2. FRAGEN ZUR SCHADENSURSACHE

Welche Art von Schaden liegt vor?

Cyber-Eigenschaden

Cyber-Drittsschaden

Welche Schadensursache liegt vor?

Cyber-Eigenschaden - Hackerangriff

Cyber-Eigenschaden - Hackereinbruch

Cyber-Forderung/-Erpressung

Cyber-Schaden bei Dritten (Cyber-Haftpflicht)

Cyber-Vertrauensschaden (Betrug, Diebstahl)

Cyber-Zahlungsmittel (Kreditkartendiebstahl)

Was ist ursächlich für den Schadenfall?

Verschlüsselung von Daten

Schadsoftware (z.B. Viren, Trojaner, Verschlüsselung)

Hacker-Einbruch

Erpressung durch Dritte

Denial of Service (DDoS)

Straftat durch eigenen Mitarbeiter

Täuschung durch Dritte mit Zahlungsvorgang

Wer ist für den Schaden verantwortlich?

Ein Dritter (z.B. Hacker, Krimineller)

Ein Mitarbeiter

Ein Repräsentant (leitender Angestellter, Organ)

3. ALLGEMEINE FRAGEN ZUM SCHADENFALL

Wie hoch ist der Schaden infolge des Angriffs bzw. Zugriffs?

€

Benötigen Sie externe Unterstützung?

Ja

Nein

Welche IT-Systeme sind von dem Angriff bzw. Zugriff betroffen?

Haben Sie im Zusammenhang mit dem Cyber-Schaden bereits Leistungen beauftragt oder irgendeine Zahlung

veranlasst?

Ja

Nein

Falls JA, an wen?

Interner IT-Dienstleister

Externer IT-Dienstleister

Rechtsanwalt

Sonstige:

Bitte nennen Sie noch, sofern bekannt, den Betrag:

€

Haben Sie Maßnahmen zur Schadensbehebung eingeleitet?

Ja

Nein

Falls ja: Welche Maßnahmen wurden bislang durchgeführt?

Krisenmanagement-Maßnahmen

Systemwiederherstellung

IT-Datenforensik (intern)

Reparatur

Erstberatung (intern)

IT-Datenforensik (extern)

Erstberatung (extern)

Wer betreut Ihre IT-Systeme?

extern

intern

Wenn extern, nennen Sie uns bitte den Ansprechpartner und die Daten Ihres externen Supports:

Firma

Ansprechpartner

Telefon

E-Mail

Bitte reichen Sie uns alle Vertragsbedingungen (AGB und den schriftlichen Vertrag) ein.

Sind nachfolgende Daten durch den Angriff betroffen oder offengelegt worden?

- Personenbezogene Daten
- Kreditkartendaten
- Betriebs- und Geschäftsgeheimnisse
- Ausschließlich eigene Daten

Falls ja: Wie viele Daten sind betroffen?

Besteht eine gesetzliche Melde- /Anzeigepflicht? **Ja** **Nein**

Falls ja: Welche weiteren Verstöße werden Ihnen vorgeworfen?

- Datenschutzbestimmungen
- Geheimhaltungspflichten
- Namens- und Persönlichkeitsrechte
- Wettbewerbs- oder Markenrecht

4. FRAGEN ZU VORKEHRUNGEN UND SICHERHEITSMABNAHMEN

Existieren schriftliche Arbeitsanweisungen zu folgenden Themen in Ihrem Unternehmen?

- Sicherer Umgang mit und Verarbeitung von personenbezogenen Daten
- Sicherer Umgang mit mobilen Geräten (Laptops, Tablets, Smartphones)
- Sichere Passwörter

Über welchen Virenschutz verfügen Sie (Produkt und Hersteller)?

Haben Sie einen IT-Sicherheitsbeauftragten bestellt? **Ja** **Nein**

Falls ja: Wie ist der IT-Sicherheitsbeauftragte tätig? **extern** **intern**

Besteht für nachfolgende Reaktionsvorfälle eine Reaktionsplan im Unternehmen?

- Unbefugter Eingriff oder Angriff Dritter auf IT-Systeme
- Infektion der IT-Systeme mit Schadsoftware, Viren, Trojaner
- Cyber-Erpressung

Welche technischen IT-Sicherheitssysteme verwenden Sie?

- Hardware-Firewall mit automatischen Updates Hersteller:
- Software-Firewall mit automatischen Updates Hersteller:
- Viren-Scanner mit automatischen Updates Hersteller:
- Standard-Virensscanner über Betriebssystem
- Lizenzierter Virensscanner von Drittanbietern

5.5 Cyber-Haftpflichtschaden:

Kam es zu einem Haftpflichtschaden bei einem Dritten? **Ja** **Nein**

Falls ja: Worin liegt der Schaden?

Falls ja: Wie hoch, in etwa, ist der bei dem Dritten entstandene Schaden? €

Angaben zum Geschädigten/Anspruchsteller

Name/Firma

Straße/Nr.

PLZ/Ort

Telefon

E-Mail

Ansprechpartner

Rechtlicher Vertreter

In welchem Verhältnis stehen Sie zum Geschädigten?

Kunde

Mandant

Geschäftspartner

Auftraggeber

Sonstiges

6. BANKVERBINDUNG ZUR REGULIERUNG

Soll bei einer Regulierung auf das uns bekannte Konto überwiesen werden? **Ja** **Nein**

Kontoinhaber

Kreditinstitut (Name)

IBAN

Ist der Versicherungsnehmer zum Vorsteuerabzug berechtigt? **Ja** **Nein**

Ich bestätige hiermit, dass ich den Gesamtschadenbetrag an den Anspruchsteller beziehungsweise dessen rechtlichen Vertreter überweise (nur bei Cyber-Haftpflichtschaden bei Dritten angeben).

Ich bestätige hiermit die Richtigkeit der oben getätigten Angaben.

Ort, Datum

Unterschrift

Mitteilung nach § 28 Abs. 4 VVG über die Folgen bei Verletzungen von Obliegenheiten nach dem Versicherungsfall

Sehr geehrte Kundin, sehr geehrter Kunde,
wenn der Versicherungsfall eingetreten ist, brauchen wir Ihre Mithilfe.

Auskunfts- und Aufklärungsobliegenheiten

Aufgrund der mit Ihnen getroffenen vertraglichen Vereinbarungen können wir von Ihnen nach Eintritt des Versicherungsfalls verlangen, dass Sie uns jede Auskunft erteilen, die zur Feststellung des Versicherungsfalls oder des Umfangs unserer Leistungspflicht erforderlich ist (Auskunftsobliegenheit), und uns die sachgerechte Prüfung unserer Leistungspflicht insoweit ermöglichen, als Sie uns alle Angaben machen, die zur Aufklärung des Tatbestands dienlich sind (Aufklärungsobliegenheit). Wir können ebenfalls verlangen, dass Sie uns Belege zur Verfügung stellen, soweit es Ihnen zugemutet werden kann.

Leistungsfreiheit

Machen Sie entgegen der vertraglichen Vereinbarungen vorsätzlich keine oder nicht wahrheitsgemäße Angaben oder stellen Sie uns vorsätzlich die verlangten Belege nicht zur Verfügung, verlieren Sie Ihren Anspruch auf die Versicherungsleistung. Verstoßen Sie grob fahrlässig gegen diese Obliegenheiten, verlieren Sie Ihren Anspruch zwar nicht vollständig, aber wir können unsere Leistung im Verhältnis zur Schwere Ihres Verschuldens kürzen. Eine Kürzung erfolgt nicht, wenn Sie nachweisen, dass Sie die Obliegenheit nicht grob fahrlässig verletzt haben.

Trotz Verletzung Ihrer Obliegenheiten zur Auskunft, zur Aufklärung oder zur Beschaffung von Belegen bleiben wir jedoch insoweit zur Leistung verpflichtet, als Sie nachweisen, dass die vorsätzliche oder grob fahrlässige Obliegenheitsverletzung weder für die Feststellung des Versicherungsfalls noch für die Feststellung oder den Umfang unserer Leistungspflicht ursächlich war. Verletzen Sie die Obliegenheit zur Auskunft, zur Aufklärung oder zur Beschaffung von Belegen arglistig, werden wir in jedem Fall von unserer Verpflichtung zur Leistung frei.

Hinweis :

Wenn das Recht auf die vertragliche Leistung nicht Ihnen, sondern einem Dritten zusteht, ist auch dieser zur Auskunft, zur Aufklärung und zur Beschaffung von Belegen verpflichtet.