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.ch).

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: **0 800 80 33 56.**
Bei der Cyber-Notfall-Hotline nehmen sich Cyber-Experten Ihrem Notfall an und leiten alle notwendige Massnahmen ein.

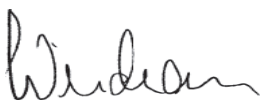
- Bewahren Sie Ruhe und führen Sie zuerst eine Bewertung des Vorfalls durch, um einen technischen Defekt auszuschliessen. Deutet beispielsweise alles auf einen Hackerangriff, gilt es Folgendes zu klären: Woher kam der Angreifer? Wie ist er in die Systeme gelangt? Welche Systeme sind von dem Angriff betroffen? 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 Beweis-mitteln hatte. Notieren Sie sich, wer ab dem Zeitpunkt des Angriffs an den kompromittierten Systemen Änderungen vorgenom-men 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 **+49 (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-Drittschaden

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 Repräsentant (leitender Angestellter, Organ)
- ☐ Ein Mitarbeiter

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
- ☐ Reparatur
- ☐ Erstberatung (extern)
- ☐ Systemwiederherstellung
- ☐ Erstberatung (intern)
- ☐ IT-Datenforensik (intern)
- ☐ IT-Datenforensik (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
- ☐ Betriebs- und Geschäftsgeheimnisse
- ☐ Kreditkartendaten
- ☐ 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
- ☐ Namens- und Persönlichkeitsrechte
- ☐ Geheimhaltungspflichten
- ☐ Wettbewerbs- oder Markenrecht

4. FRAGEN ZU VORKEHRUNGEN UND SICHERHEITSMASSNAHMEN

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
- ☐ Software-Firewall
- ☐ Viren-Scanner

- ☐ mit automatischen Updates
- ☐ mit automatischen Updates
- ☐ mit automatischen Updates
- ☐ Standard-Virensscanner über Betriebssystem
- ☐ Lizenzierter Virenscanner von Drittanbietern

- ☐ Hersteller:
- ☐ Hersteller:
- ☐ Hersteller:

Führen Sie manuelle **Updates** der vorgenannten IT-Sicherheitssysteme durch? Ja ☐ Nein ☐

Falls ja: in welchem Turnus erfolgt dies?

☐ Täglich ☐ Monatlich
☐ Wöchentlich ☐ Sonstiges:

Führen Sie regelmässig **Back-ups** (Datenkopien) und **Systemüberprüfungen** für Ihre Daten und Programme durch? Ja ☐ Nein ☐

Falls ja: in welchem Turnus führen Sie diese Massnahmen durch?

☐ Täglich ☐ Monatlich
☐ Wöchentlich ☐ Sonstiges:

Speichermedium:

☐ Festplatte ☐ Bandsicherung
☐ Weiterer Server ☐ Sonstiges:

Wann wurde das letzte Back-up bzw. die letzte Massnahme durchgeführt (Datum)?

5. SPEZIFISCHE FRAGEN ZUM SCHADENUMFANG

5.1 Cyber-Betriebsunterbrechung

Wie lange dauerte der Betriebsausfall / die Betriebsunterbrechung oder -beeinträchtigung?

5.2 Cyber-Erpressung

Liegt eine Erpressung (unter Androhung eines Angriffs) vor? Ja ☐ Nein ☐

Falls ja: Wer wurde getäuscht?

☐ Repräsentant (leitender Angestellter, Organ) ☐ Mitarbeiter des Unternehmens

Haben Sie eine Zahlung an den Erpresser veranlasst? Ja ☐ Nein ☐

Falls ja: In welcher Höhe? €

Falls ja: Wer hat die vermögensmindernde Handlung vorgenommen?

☐ Repräsentant (leitender Angestellter, Organ) ☐ Mitarbeiter des Unternehmens

---

5.3 Cyber-Vertrauensschaden

Hat einer Ihrer Mitarbeiter bei seiner Berufsausübung eine Straftat begangen? Ja ☐ Nein ☐

Falls ja: Welche?

5.4 Cyber-Zahlungsmittel

Steht der Cyber-Angriff im Zusammenhang mit Kreditkartenverarbeitungs-oder Zahlungsprozessen? Ja ☐ Nein ☐

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

exali AG
Aufsichtsratsvorsitzender:
Dirk Czaya
Vorstand: Ralph Günther (Vorsitz),
Alexander Schmid

Sitz der Gesellschaft:
Franz-Kobinger-Straße 9
86157 Augsburg, Deutschland
Amtsgericht Augsburg,
HRB 34272

Finanzamt Augsburg
Steuernummer: 103/120/20667
Die exali AG ist in der Schweiz als gebundener
Versicherungsvermittler tätig.
Registrierungsnummer D-7I7T-3ORVX-36