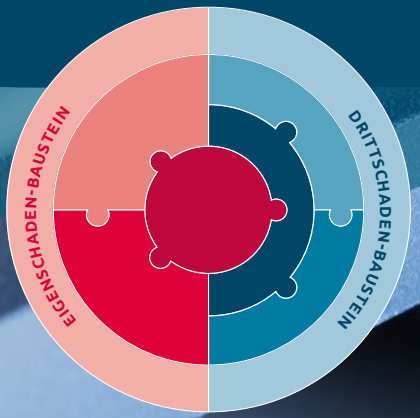
CYBERVERSICHERUNG

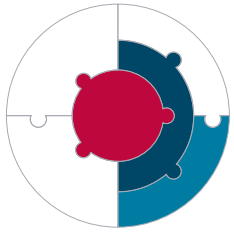
Cyberangriffe und ihre Kosten für Unternehmen



Alte Leipziger
ALH Gruppe

Zugang zu Kreditkartendaten gehackt.

EIGENSCHADEN
Forensik
Datenwiederherstellung
EC-/Kreditkarten-Monitoring Service
Kosten für Krisenkommunikation und PR-Maßnahmen
DRITTSCHADEN
E-Payment



Der Gast eines Hotels entdeckt auf seiner Kreditkartenabrechnung, dass es unmittelbar nach seinem Aufenthalt im Hotel zu einer offenbar betrügerischen Abbuchung auf seiner Kreditkarte gekommen ist. Er wendet sich an sein Kreditinstitut, welches die Karte sperrt und das Hotel über den Vorfall informiert. Das Hotel leitet daraufhin umgehend eine Untersuchung durch einen IT-Spezialisten ein. Dabei wird entdeckt, dass es sich um einen Cyberangriff handelt, bei dem Hacker die Firewall überwunden haben und so in das System eingedrungen sind. Mit einem schädlichen Skript, welches in den Code des Bezahlsystems eingeschleust wurde, konnten die Kriminellen eine Vielzahl an Kreditkartendaten während der Eingabe ausspähen. Diese Daten wurden dann für Online-Bestellvorgänge missbraucht.

Möglicher Fallverlauf:

- Der IT-Spezialist ist insgesamt zwei Tage mit forensischen Untersuchungen, der Ermittlung des Schadenhergangs und der Bereinigung des Systems beschäftigt. Die Firewall wird neu konfiguriert. **Kosten: 3.200 €.**

- Der genaue Zeitraum des Angriffs kann festgestellt werden. Alle Hotelgäste dieses Zeitraums werden über den Vorfall informiert. Einige der Hotelgäste wünschen ein Monitoring zur Überwachung und Prüfung ihrer Kreditkartendaten. **Kosten: 6.500 €.**

- Nach Bekanntwerden des Cyberangriffs wird das Hotel von der Kreditkarten-Abrechnungsfirma zu einer Vertragsstrafe verpflichtet, da sich herausstellt, dass die Firewall nicht korrekt konfiguriert war. Dieser Verstoß gegen die geltenden Datensicherheitsstandards wird mit einer **Strafe in Höhe von 13.000 €** belegt.

- Die Hotelbuchungen gehen in der Folgezeit zurück. Zur Wiedergewinnung des Vertrauens lässt sich das Hotelmanagement von einem Krisenmanager hinsichtlich erforderlicher PR-Maßnahmen beraten und leitet entsprechende Maßnahmen zur Kommunikation ein. **Kosten: 11.200 €.**

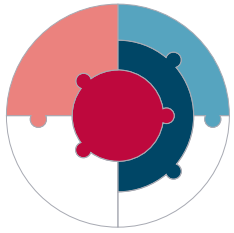
Die Leistungen und Services der Alte Leipziger in diesem Fall:

- **Erstattung der entstandenen Kosten in Höhe von 33.900 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Systembereinigung**

Trojaner-Angriff auf IT-Systeme ↓

Trojaner-Angriff auf IT-Systeme.

EIGENSCHADEN
Forensik
Datenwiederherstellung
Kosten für Krisenkommunikation und PR-Maßnahmen
Betriebsunterbrechung
DRITTSCHADEN
Haftpflicht
Datenschutz
Datenschutzrechtsverletzung
Benachrichtigungskosten



Cyberkriminelle attackieren die IT-Systeme einer radiologischen Arztpraxis. Unbemerkt kopieren sie sich Patientendaten, einschließlich digitaler Röntgenbilder mitsamt Diagnosen und Behandlungsmethoden. Kurze Zeit später wendet sich ein Patient an den Radiologen und berichtet, dass MRT-Bilder, die eindeutig dem Patienten und der Praxis zugeordnet werden können, in den sozialen Netzwerken aufgetaucht seien.

Möglicher Fallverlauf:

- Der Arzt beauftragt daraufhin eine IT-Security-Firma, welche unmittelbar mit der forensischen Untersuchung beginnt. Dabei wird die Schwachstelle, die den Tätern Zugriff auf die Daten erlaubte, identifiziert und der Datenabfluss von 100 Patientendatensätzen festgestellt. Die Systeme werden bereinigt und die Schwachstelle behoben, um weitere Datendiebstähle zu verhindern. **Kosten: 7.000 €.**

Zugang zu Kreditkarten gehackt ↑

- Der Arzt ist nun verpflichtet, die Datenschutzbehörden und seine Patienten über den Verlust der sensiblen Daten zu informieren. Er holt sich Hilfe bei einem Rechtsanwalt für IT- und Datenschutzrecht, um sicher zu gehen, dass er seinen Pflichten vollständig nachkommt. **Kosten: 5.500 €.**

- In der Zeit, bis die Systeme bereinigt sind und die Schwachstelle geschlossen ist, bleibt die Arztpraxis geschlossen. Die Abrechnung mit den Krankenkassen kann währenddessen nicht erfolgen. Insgesamt fällt die Praxis für eine Dauer von 4 Tagen aus. **Kosten: 6.000 €.**

- Die Patienten, die von der unrechtmäßigen Veröffentlichung ihrer Gesundheitsdaten betroffenen sind, beauftragen nun Spezialisten mit der Löschung ihrer Daten. Zudem verlangen sie vom Arzt Schadenersatz nach Art. 82 DSGVO. **Kosten: 30.000 €.**

- Viele Patienten wenden sich von der radiologischen Praxis ab, nachdem die lokale Presse über den Datendiebstahl berichtet. Damit sein Patientenstamm nicht noch weiter schrumpft und um seine öffentliche Reputation wieder herzustellen, schaltet der Arzt einen Krisenmanagementberater ein. **Kosten: 2.800 €.**

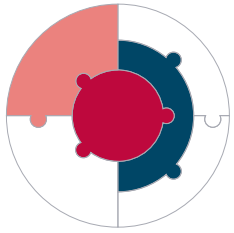
Die Leistungen und Services der Alte Leipziger in diesem Fall:

- **Erstattung der entstandenen Kosten in Höhe von 51.300 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Systembereinigung**
- **Vermittlung eines spezialisierten Anwalts**

Hackerangriff mit Ransomware ↓

Hackerangriff mit Ransomware.

EIGENSCHADEN
Forensik
Datenwiederherstellung
Abwehr Erpressung
Kosten für Krisenkommunikation und PR-Maßnahmen
Betriebsunterbrechung
DRITTSCHADEN
Vertragliche Schadensersatzansprüche



Ein mittelständischer Metallbearbeitungsbetrieb wird Opfer eines Hackerangriffs. Alle Rechner sowie die vernetzten Produktionssysteme sind ohne Funktion. Auf den Bildschirmen der Steuerungsrechner erscheint lediglich eine Lösegeldforderung. Die Erpresser wollen die gesperrten Rechner erst wieder gegen eine Zahlung von 50.000 € freigeben.

Möglicher Fallverlauf:

- Die beauftragten IT-Spezialisten stellen fest, dass die Systeme des Betriebs mit einem Verschlüsselungs-Trojaner attackiert wurden. Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt das Unternehmen kein Lösegeld. Die IT-Spezialisten arbeiten mehrere Tage daran, den Trojaner von sämtlichen Systemen zu entfernen. Anschließend werden die Systeme neu aufgesetzt und die lokalisierte Schwachstelle wird behoben. Alle Daten aus den Backups werden wiederhergestellt. **Kosten: 11.000 €.**

Trojaner-Angriff auf IT-Systeme ↑

- Bis zur Wiederinstandsetzung der Systeme stehen die Produktion und die Fertigung still. Die Verwaltung kann ebenfalls nicht arbeiten. Insgesamt dauert die Betriebsunterbrechung fünf Tage. **Kosten: 24.000 €.**

- Ein wichtiger Kunde wartet vergebens auf eine vertraglich zugesicherte Lieferung von speziellen Metallzuschnitten. Durch die Verzögerung entsteht bei ihm ein finanzieller Schaden, für dessen Ausgleich er den Metallbearbeitungsbetrieb in Anspruch nimmt. **Kosten: 13.000 €.**

- Da sich nun einige Kunden vom Unternehmen abwenden, scheint der gute Ruf des Unternehmens Schaden zu nehmen. Daher lässt sich die Geschäftsführung des Betriebs von einem Krisenmanager beraten. Daraufhin werden Maßnahmen zur Krisenkommunikation veranlasst. **Kosten: 33.000 €.**

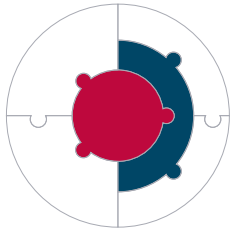
Die Leistungen und Services der Alte Leipziger in diesem Fall:

- **Erstattung der entstandenen Kosten in Höhe von 81.000 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik, Abwehr der Erpressung und der Bedrohungslage, Systembereinigung**
- **Prüfung der Haftpflichtfrage**

Schadsoftware heruntergeladen ↓

Schadsoftware heruntergeladen.

EIGENSCHADEN
Forensik
Datenwiederherstellung
DRITTSCHADEN
Haftpflicht



Die Angestellte eines Architekturbüros erhält eine E-Mail von einem unbekannten Absender. Bedenkenlos öffnet sie die Mail, da im Büro täglich viel E-Mail-Verkehr mit unbekannten Absendern herrscht. Der Absender verweist als Beleg für die Korrespondenz auf ein Word-Dokument im Anhang, welches die Angestellte daraufhin öffnet. Am nächsten Tag beschwert sich ein Geschäftspartner des Architekturbüros darüber, dass die Angestellte ihm eine mit einem Virus infizierte Datei zugeschickt habe, die seinen Rechner infiziert habe. Das Architekturbüro unterbindet sofort die E-Mail-Kommunikation und beauftragt eine IT-Sicherheitsfirma mit der Untersuchung. Die forensischen Untersuchungen zeigen, dass die eingegangene E-Mail vom unbekannten Absender tatsächlich

Hackerangriff mit Ransomware ↑

die Ursache war. Nach dem Öffnen des Anhangs hatte der PC unbemerkt im Hintergrund eine Datei mit Schadcode heruntergeladen und so die Malware ins Unternehmensnetzwerk eingeschleust. Diese wurde dann unwissend per E-Mail an den Geschäftspartner weitergegeben; weitere Kontakte des Unternehmens waren glücklicherweise nicht betroffen.

Möglicher Fallverlauf:

- Die Malware wird entfernt, das System neu aufgesetzt und die Backups werden aufgespielt. **Kosten: 4.300 €.**

- Der Geschäftspartner verlangt den finanziellen Ausgleich für die Beseitigung das Schaden, der bei ihm entstanden ist.
  Kosten: 6.500 €.

Die Leistungen und Services der Alte Leipziger in diesem Fall:

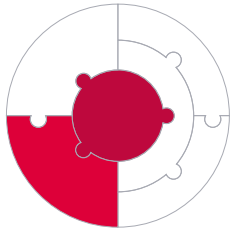
- **Erstattung der entstandenen Kosten in Höhe von 10.800 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Systembereinigung**
- **Prüfung der Haftpflichtfrage**

Schaden durch CEO-Fraud ↓

Schadsoftware heruntergeladen ↑

Schaden durch CEO-Fraud.

EIGENSCHADEN
Forensik
Datenwiederherstellung
CEO-Fraud



Der Buchhalter eines Möbelhauses bekommt eine E-Mail vom Geschäftsführer, in der er beauftragt wird, 25.000 € an die angegebene Bankverbindung zu überweisen. Da die Überweisung laut Auftrag möglichst schnell erfolgen soll, überweist der Buchhalter den Betrag umgehend. Der Fehler fällt erst drei Tage später im Rahmen eines Mitarbeitergesprächs auf. Daraufhin beauftragt der Geschäftsführer einen IT-Spezialisten mit der Prüfung dieses Vorfalls. Die forensische Untersuchung zeigt auf, dass der Buchhalter Opfer eines klassischen „Fake President"-Angriffs geworden ist. Mit der vorher gehackten, tatsächlichen E-Mail-Adresse des Geschäftsführers wurde die Buchhaltung angewiesen, den Geldbetrag zu überweisen. Es stellt sich heraus, dass die Cyberkriminellen das IT-System des Möbelhauses über einen Monat lang ausspioniert haben. Mithilfe der erlangten Informationen über Termine des Geschäftsführers und über die Art der Kommunikation innerhalb des Unternehmens, konnte die Betrugs-E-Mail glaubhaft gestaltet und der Betrug erfolgreich durchgeführt werden.

Möglicher Fallverlauf:

- Der IT-Spezialist untersucht über zwei Tage die Systeme, bereinigt sie und setzt sie neu auf. **Kosten: 3.400 €.**
- Der überwiesene Geldbetrag kann nicht mehr nachverfolgt werden und ist verloren. **Kosten: 25.000 €.**

Die Leistungen und Services der Alte Leipziger in diesem Fall:

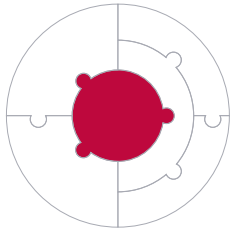
- **Erstattung der entstandenen Kosten in Höhe von 28.400 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Systembereinigung**

Innentäter im Unternehmen ↓

Schaden durch CEO-Fraud ↑

Innentäter im Unternehmen.

EIGENSCHADEN
Forensik
Datenwiederherstellung



Da in einem Sachverständigenbüro sein Kollege anstelle von ihm befördert wurde, fühlt sich ein Mitarbeiter übergangen. Er möchte es daraufhin seinem Arbeitgeber heimzahlen und löscht unter Verwendung seiner Zugangsrechte einige elektronische Ordner mit wichtigen Daten vorsätzlich. Als der Geschäftsführer von einem seiner Angestellten auf die verschwundenen Dateien aufmerksam gemacht wird, beauftragt er einen IT-Spezialisten.

Möglicher Fallverlauf:

- Der IT-Spezialist untersucht den Vorfall und ermittelt schnell den Mitarbeiter als Quelle der Datenlöschung. **Kosten: 1.200 €.**

- Die verloren geglaubten Daten konnten durch das vorhandene Backup (Datensicherung) wieder eingespielt werden. **Kosten: 1.500 €.**

Die Leistungen und Services der Alte Leipziger in diesem Fall:

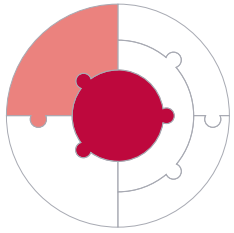
- **Erstattung der entstandenen Kosten in Höhe von 2.700 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Datenwiederherstellung**

DDoS-Angriff auf Online-Shop ↓

Innentäter im Unternehmen ↑

DDoS-Angriff auf Online-Shop.

EIGENSCHADEN
Forensik
Sicherheitsverbesserungen nach einem Angriff
Betriebsunterbrechung



Ein Spielwarengeschäft betreibt auch einen kleinen Online-Shop auf seiner Website. Eines Tages meldet sich ein Kunde per Telefon und berichtet, dass der Online-Shop nicht funktioniere. Eine Überprüfung durch einen IT-Spezialisten ergibt, dass der Online-Shop durch einen DDoS-Angriff lahmgelegt wurde. Der Angreifer hat dabei zur Ressourcenüberlastung den Webserver des Spielwarengeschäfts mit einer Vielzahl von HTTP-Requests überschwemmt. Schließlich brach dann der Server unter der Last an Anfragen zusammen.

Möglicher Fallverlauf:

- Der IT-Experte benötigt zwei Tage für die forensische Untersuchung und die Wiederherstellung des Online-Shops. Zudem wird die Firewall mit einem Filter versehen, der künftige DDoS-Attacken unterbindet. **Kosten: 4.000 €.**

- Für Kunden war der Online-Shop fünf Tage nicht ereichbar. Die so ausgebliebenen Bestellungen verursachten einen **Ertragsausfall von 1.800 €.**

Die Leistungen und Services der Alte Leipziger in diesem Fall:

- **Erstattung der entstandenen Kosten und des Ertragsausfalls in Höhe von insgesamt 5.800 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik und Datenwiederherstellung**

Betrug durch Phishing Mail ↓

Betrug durch Phishing Mail.

EIGENSCHADEN
Forensik
Cyberdiebstahl

Ein Physiotherapeut erhält eine E-Mail von seiner Hausbank. Darin wird mitgeteilt, dass das Online-Banking auf ein neues System umgestellt wird und dafür alle Kunden ihre Kontodaten verifizieren müssen. Über einen entsprechenden Link in der E-Mail sollen die Kunden die Verifizierung vornehmen. Der Physiotherapeut klickt auf den Link und wird direkt auf die Website seiner Hausbank geleitet, wo er per Eingabe seiner Kontodaten und seiner PIN den Verifizierungsvorgang abschließt. Nach einiger Zeit meldet sich ein Handwerker in der Praxis und erinnert ihn an die noch offene Rechnung für die Renovierung eines Behandlungszimmers.
Der Physiotherapeut ist sich jedoch sicher, dass er die Rechnung bereits per Überweisung beglichen hat. Da die Bank auf seine Rückfrage hin keine entsprechende Zahlung feststellen kann, vermutet er einen Betrug. Deshalb beauftragt er einen IT-Experten mit der Untersuchung. Es stellt sich heraus, dass der Physiotherapeut auf eine täuschend echt wirkende Phishing-Mail hereingefallen ist. Der Link in der E-Mail führte dann nicht wie angenommen auf die Website der Hausbank, sondern auf eine Nachbildung, auf welcher Kriminelle dann alle notwendigen Kontodaten von seinem Opfer erbeuten und seine Überweisungen manipulieren konnten.

Möglicher Fallverlauf:

- Der IT-Experte benötigt einen Tag für die forensische Untersuchung und die Bereinigung des Systems. **Kosten: 1.200 €.**
- Insgesamt wurden drei Überweisungen des Physiotherapeuten betrügerisch umgeleitet und müssen nun ordnungsgemäß nachgeholt werden. **Kosten: 18.500 €.**

Die Leistungen und Services der Alte Leipziger in diesem Fall:

- **Erstattung der entstandenen Kosten in Höhe von 19.700 €**
- **Notfall-Hotline mit IT-Spezialisten für telefonische Erstberatung und Schadenfeststellung**
- **Stellung eines IT-Dienstleisters für Forensik**

Haben wir Sie überzeugt?
Die Risiken aus dem Netz sind vielfältig und nicht für alle Firmen gleichermaßen relevant. Mit der Cyberversicherung der Alte Leipziger können Sie sich individuell gegen die Folgen eines Cyberangriffs absichern.

- Mit der **Eigenschadendeckung** versichern Sie Kosten, die Ihnen durch einen Cyberschaden entstehen. Die Grundabsicherung ist erweiterbar um die Zusatzmodule Betriebsunterbrechung und CEO-Fraud.
- Die **Drittschadenabsicherung** ist optional und deckt die Kosten, die Sie Dritten durch einen Cyberschaden zufügen, quasi die Haftpflichtversicherung. Erweiterbar ist dies um die Zusatzmodule Datenschutz und E-Payment.

Cyberkriminalität bedroht alle Unternehmen.
Gerne beraten wir Sie zu Ihrer individuellen Absicherung.
Nehmen Sie Kontakt mit uns auf.

Folgen Sie uns

Alte Leipziger
Versicherung AG
Alte Leipziger-Platz 1
61440 Oberursel
sach@alte-leipziger.de
www.alte-leipziger.de
www.alh-newsroom.de

fhs 080.02 – 06.2022