



Cyber. Versicherung. Experten.



SCHADENS- BEISPIELE

IN DER CYBERVERSICHERUNG



Der erfundene Notfall

Am Morgen des 19. September erhält die Sachbearbeiterin Angelika Fischer (Name geändert) den Anruf eines langjährigen Kunden. Dieser erklärte verzweifelt, dass Hacker das gesamte IT-System lahmgelegt hätten. Nun müssten alle wichtigen Dokumente rekonstruiert und wiederbeschafft werden. Aus diesem Grund bittet er um Zusendung des Schriftverkehrs zwischen den Unternehmen. Frau Fischer möchte unkompliziert helfen und versendet die Dokumente umgehend per E-Mail. Als sie zwei Wochen später bei dem Kunden anruft, um zu fragen, ob alles angekommen sei weiß dieser nichts von dem besagten Vorfall.



Konsequenzen

- Das erschütterte Kundenvertrauen führte zum Ende der Geschäftsbeziehung
- Es kam zu einer Schadensersatzklage

Deckung der Cyber-Versicherung

- Unterstützung bei der Kundenkommunikation
- Kosten für zu leistenden Schadensersatz

Schaden: 59.000 €



Infiziert durch die eigene Bank

Im November besuchte der Hotelier Thorsten Renneke (Name geändert) die Webseite seiner Hausbank, um Überweisungen durchzuführen. Wie die Bank später mitteilte, war in die Webseite allerdings über mehrere Stunden Schadsoftware eingebettet und unbemerkt aktiv. Diese durchsuchte die Systeme der Webseitenbesucher systematisch nach bekannten Sicherheitslücken.

Auf diesem Weg gelang es den Hackern, auf dem Rechner von Thorsten Renneke unbemerkt eine Spionagesoftware zu installieren und sensible Kundendaten abzugreifen.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Der Geschäftsbetrieb war für mehrere Tage erheblich gestört
- Alle betroffenen Kunden mussten über den Vorfall informiert werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für Umsatzausfall
- Kosten für die Kundenkommunikation
- Kosten für zu leistenden Schadensersatz

Schaden: 46.000 €



Der gehackte Onlineshop

Im März bestellte der Anlageberater Timo Becker (Name geändert) bei einem Online-Händler eine neue Kaffee-maschine für das Büro. Die Zahlung wurde über die Kreditkarte des Unternehmens geleistet.

Allerdings war die Webseite des Online-Shops manipuliert worden, um Kreditkartendaten abzugreifen. Die abgegriffenen Daten wurden für Einkäufe in den USA missbraucht.



Konsequenzen

- Aufgrund der Insolvenz des Online-Shops wurde der Schaden nicht erstattet

Deckung der Cyber-Versicherung

- Kosten für den Cyber-Betrug

Schaden: 9.000 €



Der schadhafte Link

Im September wurde ein Hamburger Makler Opfer von Cyberkriminellen. Als er morgens den Computer startet, sind alle Daten - sowohl auf seinem Computer als auch in den IT-Systemen des Unternehmens - verschlüsselt. Er erhält die Nachricht, dass gegen eine Zahlung von 16.000 Euro die Daten wiederhergestellt werden können. Der beauftragte IT-Experte stellt fest, dass der Makler auf den Link einer mit Schadsoftware infizierten Webseite geklickt hatte. Hierdurch wurde unbemerkt die Verschlüsselungssoftware installiert. Zudem wurden auch personenbezogene Daten ausgelesen.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Der Makler konnte 9 Tage nicht auf seine Daten zugreifen
- Über 100 betroffene Kunden mussten über den Vorfall informiert werden
- Mehr als 30 Kunden haben den Makler gewechselt

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für Betriebsunterbrechung
- Kosten für die Kundenkommunikation
- Kosten für zu leistenden Schadensersatz

Schaden: 31.000 €



Ein Virus in der Arztpraxis

Am Morgen des 13. Mai ließ sich auf den Rechnern einer Bonner Arztpraxis keine Datei mehr öffnen. In den Tagen zuvor hatte die Arztpraxis zahlreiche Bewerbungen für die ausgeschriebene Stelle als “Medizinische/r Fachangestellte/r” erhalten.

Eine Bewerbung enthielt einen als PDF angehängten Lebenslauf und eine Excel Tabelle. Beim Öffnen der Dokumente installierte sich unbemerkt eine Schadsoftware, die alle Daten verschlüsselte. Auch die Telefonanlage war von dem Angriff betroffen und Patienten konnten die Praxis nicht mehr erreichen.



Konsequenzen

- Die Arztpraxis war für 4 Tage geschlossen
- Alle Computer mussten bereinigt und neu aufgesetzt werden
- Vertrauliche Patientendaten gingen verloren Schadenersatzforderungen der infizierten Webseitenbesucher

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für den Mehraufwand der Mitarbeiter
- Kosten für den Umsatzausfall

Schaden: 69.000 €



Der betrogene Handwerker

Als der Installateur- und Heizungsbaumeister Fabian Koch (Name geändert) die Kontoauszüge des Firmenkontos prüft, fällt ihm eine Überweisung über 13.000 Euro auf ein ausländisches Konto auf. Diese kann er keinem Buchungsvorgang zuordnen. Auf Nachfrage erfährt er, dass sein Buchhalter vor kurzem eine E-Mail der Hausbank erhalten hatte. In der Mail wurde er aufgefordert, seine Kontoumsätze und Kontodaten zu überprüfen. Der Buchhalter kam der Aufforderung nach und wurde auf eine Phishing-Seite geleitet. Dort gab er wie gewohnt die Zugangsdaten ein.



Konsequenzen

- Das Konto wurde vorsorglich gesperrt, um alle Umsätze der letzten Monate detailliert zu überprüfen
- Der Zahlungsverkehr war 7 Tage erheblich gestört
- Der Schaden musste selbst getragen werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für den Mehraufwand der Mitarbeiter
- Kosten des Cyber-Betrugs

Schaden: 13.000 €



Die Quittung kommt zum Schluss

Im März erfuhr der Besitzer eines beliebten Restaurants in Ostdeutschland, dass die Kreditkartendaten von mehr als 450 Kunden gestohlen wurden. Einer der Mitarbeiter hatte auf einen schadhaften Link in einer E-Mail geklickt. Dadurch konnten Hacker das computergestützte Kassensystem infiltrieren und über einen Zeitraum von mehr als zwei Jahren die Kreditkartendaten abgreifen. Die Daten wurden anschließend für Einkäufe in den USA missbraucht.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Alle betroffenen Kunden mussten über den Vorfall informiert werden
- Visa hat das Restaurant in Regress genommen

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für die Kundenkommunikation
- Kosten für den Umsatzausfall

Schaden: 1.200.000 €



Ausgeschlossen in den eigenen vier Wänden

Im Oktober 2016 funktionierte plötzlich das elektronische Schließsystem eines bayrischen Landgasthofes nicht mehr. Der Juniorchef hatte über Facebook unbemerkt eine Schadsoftware heruntergeladen. Einer seiner Kontakte wurde gezielt gehackt und über sein Facebook Konto ein Bild verschickt. Als der Juniorchef das Bild öffnete, installierte sich ein Schadprogramm und infizierte über das lokale Netzwerk auch den Hauptrechner des Hotels, über den das elektronische Schließsystem gesteuert wird. Die Hacker konnten über einen Fernzugriff die Schließanlage manipulieren und forderten ein Lösegeld im fünfstelligen Bereich.



Konsequenzen

- Die Kunden konnten ihre Zimmer für mehrere Stunden nicht betreten
- Erheblicher Imageverlust
- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für den Mehraufwand der Mitarbeiter
- Unterstützung bei der Kundenkommunikation
- Kosten für zu leistenden Schadensersatz

Schaden: 47.000 €



Der falsche Facebook-Freund

Der Personalberater Michael Wilde (Name geändert) nutzt seinen Laptop sowohl für berufliche als auch für private Zwecke. Dies wurde ihm im letzten August zum Verhängnis. Er erhielt über Facebook eine private Nachricht von einem Bekannten, die einen Link zu einem Video enthielt. Als Michael Wilde auf den Link klickte, installierte sich eine Schadsoftware, mit der private Informationen, Passwörter, E-Mail-Konten und Browser-Verläufe ausspioniert wurden. Zudem wurde der schädliche Link in seinem Namen automatisch an seine E-Mail-Kontakte weitergeleitet.



Konsequenzen

- Der Computer musste durch einen IT-Spezialisten bereinigt und neu aufgesetzt werden
- Über 250 betroffene Kunden mussten über den Vorfall informiert werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation

Schaden: 36.000 €



Die teure Geschäftsreise

Am 05. April infizierte sich der selbstständige Unternehmensberater Jörg Husemann (Name geändert) in einem Café mit einer Schadsoftware. Diese verschlüsselte in wenigen Sekunden sein gesamtes Computersystem. Der beauftragte IT-Spezialist erklärte Jörg Husemann später, dass sich wahrscheinlich Hacker in das WLAN-Netzwerk des Cafés eingewählt hatten. Im Netzwerk suchten diese gezielt nach Geräten mit veralteter Software. Ein nicht vorhandenes Software- update wurde dem Unternehmensberater zum Verhängnis.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Seit der letzten Datensicherung erstellte Dokumente konnten nicht wiederhergestellt werden
- Der Computer konnte für 2 Tage nicht genutzt werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für den Mehraufwand der Mitarbeiter
- Kosten für den Umsatzausfall

Schaden: 7.000 €



Das unsichere Hotel WLAN

Immer wieder versuchen Hacker über die WLAN-Netze von Hotels vertrauliche Daten auszuspähen.

Opfer eines solchen Angriffs wurde auch ein Anwalt aus Köln. Die Cyberkriminellen verleiteten das Opfer dazu, ein Update für eine Standardsoftware herunterzuladen und zu installieren. Dabei infizierte sich der Jurist mit einem Virus. Die Hacker erhielten Zugriff auf gespeicherte Passwörter, Klientendaten und das Bankkonto.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Alle betroffenen Klienten mussten über den Vorfall informiert werden
- Von dem Bankkonto wurden mehrere tausend Euro abgebucht

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für des Cyber-Betrugs

Schaden: 76.000 €



Das vergiftete Werbegeschenk

Im Dezember wird der Steuerberater Michael Figge (Name geändert) von einem Geschäftspartner informiert, dass im Zuge einer Werbeaktion möglicherweise USB- Sticks mit Schadsoftware verteilt wurden.

Da Michael Figge den USB Stick bereits verwendet hatte, wandte er sich an einen IT-Spezialisten. Dieser stellte fest, dass die IT-Systeme mit einem Virus infiziert waren. Mit Hilfe des Virus hatten Cyberkriminelle direkten Zugriff auf die gesamten Kundendaten.



Konsequenzen

- Alle Computer mussten bereinigt und neu aufgesetzt werden
- Der Steuerberater konnte 6 Tage nicht auf seine Systeme zugreifen
- Über 120 betroffene Klienten mussten über den Vorfall informiert werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für den Umsatzausfall

Schaden: 98.000 €



Der gestohlene Laptop

Am 12. Juni wurde dem Geschäftsführer einer Münchner Beteiligungsgesellschaft auf einer Geschäftsreise der Laptop gestohlen.

Er meldete den Diebstahl umgehend der Bundespolizei. Da der Laptop direkten Zugang zum Firmennetzwerk ermöglicht, empfahl der aufnehmende Beamte einen IT Spezialisten einzuschalten. Bei der Sicherung des Netzwerks stellte der beauftragte IT-Dienstleister fest, dass von dem gestohlenen Laptop bereits auf sensible Firmendaten zugegriffen wurde.



Konsequenzen

- Der Laptop konnte nicht wiederbeschafft werden
- Die IT-Systeme mussten abgesichert werden und waren für 3 Tage nicht nutzbar
- Über 70 Geschäftspartner mussten über den Vorfall informiert werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für Umsatzausfall
- Kosten für die Kundenkommunikation

Schaden: 96.000 €



Kein Anschluss unter dieser Webseite

Im Mai attackierten Hacker Onlineshops mit einer großen Zahl an Anfragen, bis die jeweiligen Server und IT-Systeme unter der Last zusammen brachen.

Opfer wurde unter anderem ein Händler für Telekommunikationsanlagen und -geräte, der seine Produkte auch über seinen eigenen Webshop vertreibt. Die Täter forderten ein Schutzgeld in 5-stelliger Höhe, ansonsten würden sie den Webshop weiterhin attackieren. Auf Anraten der Behörden weigerte sich der Betreiber zu zahlen.



Konsequenzen

- Über mehrere Wochen wurde der Shop immer wieder attackiert
- Schadenersatzforderungen der infizierten Webseitenbesucher
- Die Internetseite war für 7 Tage nicht erreichbar

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für den Umsatzausfall

Schaden: 123.000 €



Diese Seite wurde möglicherweise gehackt

Im Juli wurde ein Unternehmen aus Baden- Württemberg von einem Kunden darüber informiert, dass bei Google für die Website des Unternehmens die Meldung “Diese Seite wurde möglicherweise gehackt” erscheine.

Hackern war es gelungen, die Webseite mit Schadsoftware zu infiltrieren. Diese Software durchsuchte die Systeme der Webseiten- besucher systematisch nach Sicherheitslücken und infizierte zahlreiche Computer.



Konsequenzen

- Verschlechtertes Google Ranking und Imageverlust
- Schadenersatzforderungen der infizierten Webseitenbesucher
- Die Internetseite war für 7 Tage nicht erreichbar

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für den Umsatzausfall

Schaden: 133.000 €



Der gut gemeinte Rat

Aufgrund eines Anwenderfehlers funktionierte im Frühjahr das Warenwirtschaftssystem eines Baustoffhandels nicht mehr. Aus diesem Grund konnten Bestellungen nur noch manuell bearbeitet werden, wodurch nur ein Bruchteil der üblichen Bestellmengen verarbeitet wurde.



Konsequenzen

- Das Warenwirtschaftssystem musste durch einen IT-Spezialisten wiederhergestellt werden
- Der Baustoffhandel war 4 Tage nur eingeschränkt arbeitsfähig
- Es kam zu hohen Umsatzeinbußen

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation
- Kosten für den Mehraufwand der Mitarbeiter
- Kosten für den Umsatzausfall

Schaden: 15.000 €



Die unsichere Kundendatenbank

Im letzten März wurde der Hotelier Jochen Schumann (Name geändert) Opfer von Cyberkriminellen. Zwei Jahre zuvor hatte er sich eine elektronische Kundendatenbank und einen Server zur zentralen Datenspeicherung angeschafft. Allerdings war die Server- und Datenbanksoftware nicht auf dem neuesten Stand und hatte Sicherheitslücken. Hacker suchten im Internet gezielt nach solchen unzureichend gesicherten Systemen, da diese leicht mit Schadsoftware infiziert werden können. Den Hackern gelang es auf diese Weise hunderte Kundendatensätze, Kreditkartendaten und Rechnungen abzugreifen.



Konsequenzen

- Alle betroffenen Kundendaten mussten bereinigt und neu aufgesetzt werden
- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Unterstützung bei der Kundenkommunikation

Schaden: 56.000 €



Der falsche IT-Spezialist

Im August war der Internetanschluss der Unternehmerin Saskia Grünberg (Name geändert) plötzlich gestört. Daraufhin erhielt sie einen Anruf von ihrem vorgeblichen Internetprovider. Zur Behebung des Fehlers sollte Frau Kiesewetter ihm einen temporären Zugriff auf das Netzwerk ermöglichen. Unter Anleitung des IT-Spezialisten richtete die Unternehmerin den Fernzugriff ein. Allerdings war der Anrufer ein Cyber-krimineller, der den Internetanschluss vorsätzlich gestört hatte. Durch den Fernzugriff wurde eine Schadsoftware installiert, die alle Daten verschlüsselte.



Konsequenzen

- Die IT-Systeme mussten bereinigt und neu aufgesetzt werden
- Die Unternehmerin konnte 14 Tage nicht auf ihre Systeme zugreifen
- Wichtige Daten konnten nicht wiederhergestellt werden

Deckung der Cyber-Versicherung

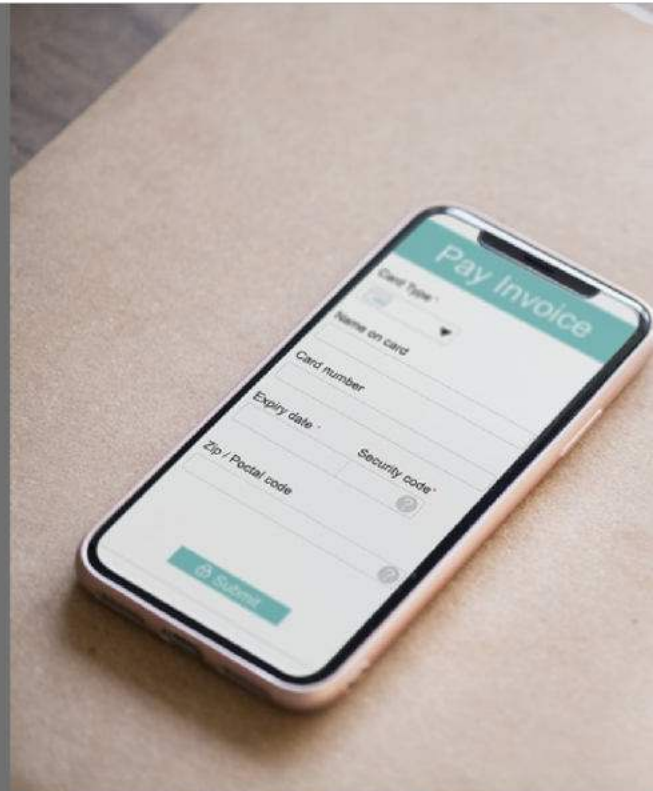
- Kosten für IT-Spezialisten
- Kosten für den Cyber-Betrug

Schaden: 63.000 €



Echte Rechnung - Falsches Konto

Am Morgen des 27. August ruft die Unternehmerin Simone Winkler (Name geändert) bei einem Ihrer langjährigen Kunden an, um sich zu informieren, warum auch die zweite Mahnung nicht gezahlt wurde. Der Kunde teilte ihr mit, dass der Rechnungsbetrag auf das angegebene Konto überwiesen wurde. Allerdings war dies nicht das Konto von Simone Winkler. Ein beauftragter IT-Spezialist stellte später fest, dass der E-Mailserver manipuliert worden war. Von Ihrem Sekretär erfährt Simone Winkler, dass vor einigen Wochen das IT-Unternehmen anrief, welches den Mailserver eingerichtet hatte. Es gäbe ein neues Sicherheitsupdate, dass umgehend installiert werden müsse. Der Sekretär nahm die Installation unter Anleitung des Anrufers vor. Anstatt der Installation eines Sicherheitsupdates wurde allerdings der Mailserver manipuliert.



Konsequenzen

- Das erschütterte Kundenvertrauen führte zum Ende der Geschäftsbeziehung
- Es kam zu einer Schadensersatzklage

Deckung der Cyber-Versicherung

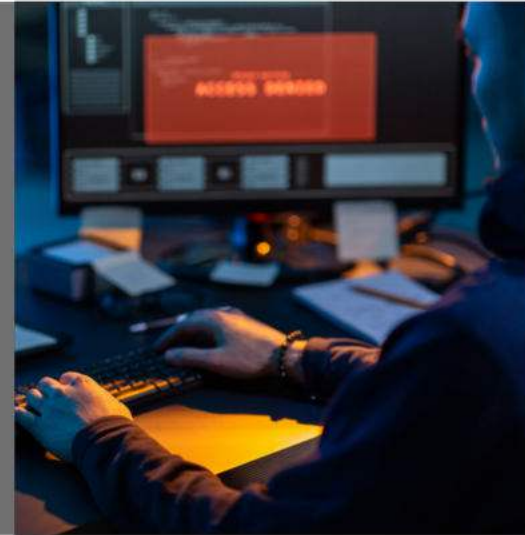
- Unterstützung bei der Kundenkommunikation
- Kosten für zu leistenden Schadensersatz

Schaden: 112.000 €



Sicherheitsrisiko: Veraltete Software

Im letzten Dezember wurde ein mittelständischer Handwerksbetrieb aus Nordrhein-Westfalen Opfer von Cyberkriminellen. Durch fehlende Software-Updates war der Betrieb für die Hacker ein leichtes Ziel. Die Cyberkriminellen hatten zunächst eine Software installiert, mit der sie aus der Ferne auf die Unternehmensserver zugreifen konnten. Nachdem sie Zugang zu den IT-Systemen hatten, verschlüsselten sie den zentralen Datenbankserver. In der Folge konnte keiner der Mitarbeiter mehr auf Auftrags-, Kunden- oder Rechnungsdaten zugreifen.



Konsequenzen

- Datenbankserver musste durch einen externen IT-Spezialisten neu aufgesetzt werden
- Nicht gesicherte Daten gingen verloren
- Der Handwerksbetrieb war eine Woche nur eingeschränkt arbeitsfähig

Deckung der Cyber-Versicherung

- Kosten für IT-Spezialisten
- Kosten für den Mehraufwand der Mitarbeiter
- Kosten für den Umsatzausfall

Schaden: 31.000 €