Alle Sicherheit für uns im Norden.

PROVINZIAL
Die Versicherung der Sparkassen

# Schadenbeispiele zur Cyber-Versicherung

## Wir möchten Ihnen hiermit einen Überblick über konkrete Schaden-beispiele geben.

Im Schadenfall arbeitet die Provinzial eng mit führenden Dienstleistern im Bereich der Informations-sicherheit zusammen.




## Inhaltsverzeichnis


| | |
|---|---|
| Baubranche | 2 |
| KFZ-Dienstleistungsbetriebe | 3 |
| Hotels und Restaurants | 4-5 |
| Produzierendes Gewerbe | 6 |
| Handel | 7 |
| Heilwesen | 8 |
| Freiberufler | 9 |
| Dienstleister | 10 |




PROVINZIAL
Die Versicherung der Sparkassen

# Baubranche

- Ein Hoch- und Tiefbaubetrieb wird Opfer eines gezielten Hacker-Angriffs. Dabei werden dem Unternehmen sämtliche Baupläne und sonstige technische Unterlagen entwendet. Darunter fallen sensible Unterlagen (unter anderem für Gefängnisbau, Tresorräume, Sicherheitskonzepte, Schließanlagen und so weiter). Zudem geht eine Lösegeldforderung in Höhe von 120.000 EUR im Unternehmen ein. Auf diese Forderung wird nicht eingegangen.
- Die Polizei und die Provinzial werden umgehend vom Versicherungsnehmer informiert. Der beauftragte IT-Dienstleister führt IT-forensische Untersuchungen durch.
- Dabei wird festgestellt, dass die Täter wirklich im System waren. Die IT muss daher vom Netz getrennt, abgeschaltet und komplett aus dem Back-Up neu aufgebaut werden. Diese Maßnahmen dauern eine Woche.
- Die betroffenen Kunden werden informiert und das Unternehmen erhält Hilfe von spezialisierten Anwälten, die durch den Versicherer empfohlen wurden.
- Es werden Haftpflichtansprüche auf Grund erhöhter Sicherheitsmaßnahmen der Kunden gestellt.

## Entstandene Kosten

| | |
|---|---|
| Anwaltskosten | 10.000 EUR |
| IT-Dienstleister | 25.000 EUR |
| Betriebsunterbrechung / Einschränkung | 10.000 EUR |
| **Gesamt** | **45.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

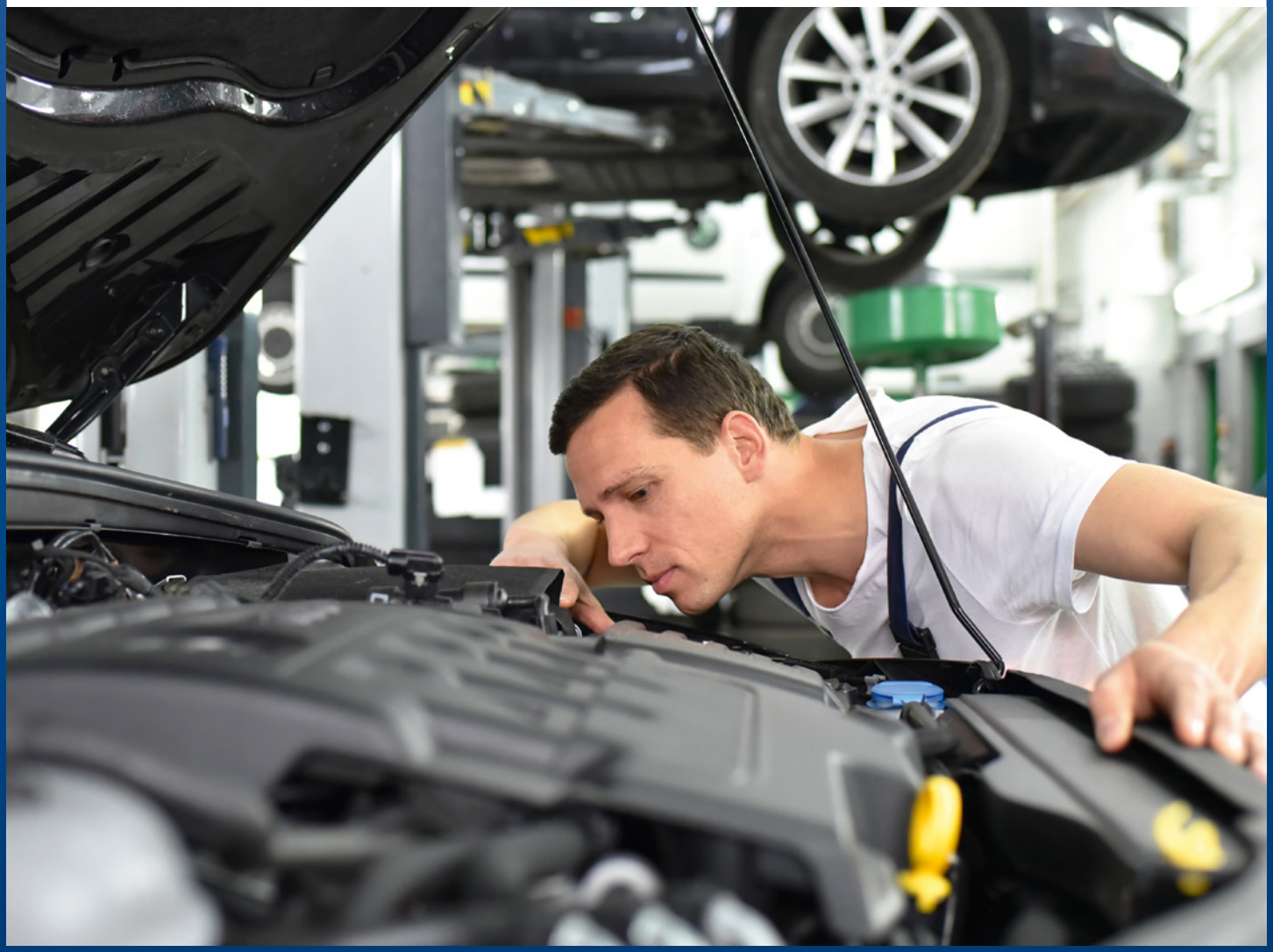
# KFZ-Dienstleistungsbetriebe

- Ein Autohaus mit einem Jahresumsatz von ca. 45 Mio. EUR ist von einem Hackerangriff betroffen. Über eine Bewerbungs-E-Mail ist ein Kryptotrojaner in das System gelangt. Die Verschlüsselung beginnt zeitversetzt, während nachts das Back-Up läuft.
- Die Verschlüsselung wird erst am nächsten Tag bemerkt. Da auch ein inkrementelles Tages-Back-Up (ein inkrementelles Backup enthält nur Daten, die sich seit der letzten Sicherung geändert haben) verschlüsselt ist, kann eine Datenwiederherstellung nicht durchgeführt werden.
- Der Versicherungsnehmer informiert die Polizei und die Provinzial. Die Provinzial schaltet seinen IT-Dienstleister ein. Dieser und der Vor-Ort-IT-Dienstleister arbeiten eng zusammen.
- Das System soll aus einem älteren Back-Up wiederhergestellt werden. Es kommt zu erheblichen Problemen, da dieser Vorgang im Vorfeld nie getestet wurde.
- Nach drei Tagen ist das System wieder einsatzbereit. Nach drei weiteren Tagen konnten über eine manuelle Nachpflege die wesentlichen Daten, die nicht gerettet werden konnten, nachgepflegt werden.
- Der Verkauf im Autohaus konnte drei Tage nicht stattfinden. Auch der Werkstattbetrieb stand für 3 Tage still.

### Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 30.000 EUR |
| Ertragsausfall / fortlaufende Kosten | 40.000 EUR |
| **Gesamt** | **70.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Hotels und Restaurants

- Ein großer Hotelbetrieb mit drei Hotels, an denen jeweils ein Restaurant angeschlossen ist, erleidet eine Cyber-Attacke. Die Hacker erreichen einen Zugriff auf das IT-System des Hotelbetriebs.
- Dabei werden sowohl die Kreditkartendaten des Hotel- und Gaststättenbereiches, als auch sämtliche Kundendaten über Hotelbuchungen entwendet. Der Angriff wird vom Unternehmen erst bemerkt, als die Täter sich melden. Sie drohen mit der Veröffentlichung der Daten beziehungsweise Verkauf im Darknet. Sie verlangen 50.000 EUR Lösegeld in Bitcoin (Kryptowährung). Das Lösegeld wird nicht gezahlt.
- Das Hotel schaltet umgehend die Polizei ein, informiert den eigenen IT-Dienstleister und setzt sich mit der Provinzial in Verbindung.
- Die IT-Forensiker des IT-Dienstleisters der Provinzial arbeiten eng mit dem Vor-Ort-IT-Dienstleister und der Polizei zusammen.
- Ziel der Forensik ist die Feststellung, ob es tatsächlich einen Angriff gab und es sich nicht nur um eine leere Drohung handelt. Es wird festgestellt, dass es sich um einen Hacker-Angriff handelt und die Täter noch im System sind. Daher muss sofort die Bezahlmöglichkeit mit Kreditkarte eingestellt werden. Dies führt direkt zu massiven Kundenbeschwerden, die zu einer schlechteren Bewertung im Internet führen.
- Daraufhin muss die Feststellung der Sicherheitslücken / des Einfallstores erfolgen. Zudem wird sorgfältig geprüft, auf welche Daten die Täter Zugriff hatten. Es erfolgt eine Beweissicherung verbunden mit Tipps zur Schließung der Lücken und Aussperrung der Täter. Der Vor-Ort-IT-Dienstleister schließt die Sicherheitslücken. Eine schlecht konfigurierte Firewall hatte den Zugriff auf bekannte Windows-Sicherheitslücken ermöglicht.
- Die von der Provinzial benannten Rechtsanwälte prüfen, inwieweit Benachrichtigungspflichten nach DSGVO bestehen (auf Grundlage der Ergebnisse der Forensiker). Anschließend erfolgt eine intensive Hilfestellung bei der Formulierung des Benachrichtigungsschreibens.
- Eine Benachrichtigung der betroffenen Personen wird durchgeführt. 85 Personen melden Schadenersatzansprüche an, da die Kreditkartendaten missbräuchlich genutzt wurden.
- Die IT des Hotelbetriebs ist durch die Unterstützung der IT-Dienstleister wieder betriebsbereit. Die Geschäftsleitung wird von einem PR-Coach für Öffentlichkeitsarbeit unterstützt.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 190.000 EUR |
| Betriebsunterbrechung / Einschränkung | 40.000 EUR |
| Rechtsanwälte | 80.000 EUR |
| PR-Beratung | 50.000 EUR |
| Haftpflichtschaden inkl. Abwehrkosten | 160.000 EUR |
| **Gesamt** | **520.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Hotels und Restaurants

- Ein Hotel mit 100 Betten ist von einem Hacker-Angriff betroffen.
- Die Hacker legen das IT-System des Hotels lahm. Dadurch sind keine Buchungsdaten und Zimmerbelegungen mehr vorhanden, zudem funktionieren die elektronischen Türsysteme (Schlüsselkarten) nicht mehr. Neben dem Drucken von Rechnungen ist auch das Bezahlen der Rechnungen nicht möglich. Das Hotel erhält massive Kundenbeschwerden.
- Das Unternehmen schaltet sofort die Polizei ein. Die Provinzial wird über den Hacker-Angriff informiert. Die Provinzial beauftragt unverzüglich den eigenen IT-Dienstleister, der mit der Polizei zusammenarbeitet.
- Es wird geprüft, ob zusätzlich noch Kundendaten entwendet wurden. Dieses ist nicht der Fall. Der IT-Dienstleister beginnt mit der Feststellung des Einfallstores. Danach werden die Täter ausgesperrt und das Hotel gewinnt die Kontrolle über das System zurück.
- Ein PR-Berater unterstützt den Versicherungsnehmer bei der Krisenbewältigung.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 120.000 EUR |
| Betriebsunterbrechung / Einschränkung | 20.000 EUR |
| PR-Beratung | 30.000 EUR |
| **Gesamt** | **170.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Produzierendes Gewerbe

- Ein Hersteller von Messsystemen erleidet einen Angriff durch Kryptotrojaner. Das Unternehmen stellt Thermometer für Kraftfahrzeuge und Maschinen her.
- Der Trojaner gerät über eine Bewerbungs-E-Mail in das System. Der Trojaner ist so programmiert, dass er mit seiner „Arbeit“ erst am Freitagabend beginnt. Er überwindet dabei (zum Beispiel wanna-cry) Netzsegmente und frisst sich durch alle Systeme. Am Montagmorgen funktioniert kein IT-System, keine Maschine, kein Telefon, kein E-Mail-System. Auch die Web-Site ist nicht mehr erreichbar.
- Die Erpresser melden sich mit einer Erpressermeldung auf den Bildschirmen und fordern 80.000 EUR in der Kryptowährung dash. Die geforderten 80.000 EUR werden nicht gezahlt.
- Da es sich um einen Automobilzulieferer mit „just in time“ Verträgen handelt, sind große Kundenverbindungen sofort in Gefahr. Zudem drohen hohe Schadenersatzforderungen wegen Produktionsstillstand in den Fabriken der Kunden.
- Die Polizei und die Provinzial werden unverzüglich informiert.
- Eine Entschlüsselung der Dateien ist nicht möglich. Die Datensicherungen funktionieren jedoch. Da die gesamten Systeme nicht mehr funktionieren, muss das gesamte Unternehmen IT-seitig wieder aufgebaut werden.
- Der IT-Dienstleister der Provinzial und der eigene IT-Dienstleister des Unternehmens arbeiten eng zusammen. Es vergehen jedoch 5 Tage bis alle Systeme wieder einwandfrei funktionieren.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 180.000 EUR |
| Betriebsunterbrechung / Einschränkung | 250.000 EUR |
| **Gesamt** | **430.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Handel

- Ein großer Fahrrad-Handel mit starker Online-Präsenz erleidet eine dDoS-Attacke. 80% des Umsatzes werden über die Homepage des Unternehmens generiert.
- Die Homepage der Firma wird für 3 Stunden gezielt mit Anfragen überlastet. Bis die Homepage wieder online ist, vergehen weitere 3 Stunden. Im Anschluss daran trifft eine Erpresserforderung in Höhe von 20.000 EUR in Bitcoin ein. Es wird damit gedroht, die Attacke täglich zu wiederholen. Auf die Erpresserforderung wird nicht eingegangen.
- Das Unternehmen informiert die Polizei und die Provinzial. Der IT-Dienstleister der Provinzial analysiert die Angriffsart und gibt Empfehlungen, wie die stattfindenden dDoS-Attacken in Zukunft verhindert werden können. Bis diese Empfehlungen jedoch umgesetzt werden können, vergehen weitere 5 Tage. Ein PR-Berater unterstützt den Versicherungsnehmer bei der Krisenbewältigung.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 40.000 EUR |
| Betriebsunterbrechung / Einschränkung | 50.000 EUR |
| PR-Beratung | 22.000 EUR |
| **Gesamt** | **112.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Heilwesen

- Eine Praxis für Allgemeinmedizin mit 2 Ärzten und 8 Angestellten erleidet einen Hacker-Angriff.
- Das unbedachte Öffnen eines E-Mail-Anhangs durch eine Sprechstundenhilfe aktiviert einen Trojaner, der im Anschluss eine Verbindung über den Rechner mit dem Hacker aufnimmt. Dies wird von den Ärzten und Angestellten nicht bemerkt. Der Hacker hat über Wochen Zugriff auf das gesamte Netz inklusive aller Patientendaten und E-Mails.
- Die Infiltrierung des Systems wird durch einen IT-Dienstleister entdeckt, der geplante System-änderungen vornehmen soll.
- Umgehend werden die Polizei und die Provinzial informiert. Der von der Provinzial beauftragte IT-Dienstleister arbeitet mit der Polizei zusammen.
- Es wird eine IT-Forensik durchgeführt. Zudem werden die Gesundheitsdaten sämtlicher Patienten exfiltriert.
- Die Provinzial unterstützt mit Nennung einer spezialisierten RA-Kanzlei und einem PR-Manager. Der Rechtsanwalt bereitet eine Meldung an die Datenschutzbehörde vor. Die gesetzliche Frist beträgt 72 Stunden. Zudem bereitet der Rechtsanwalt die Patienteninformation vor.
- Währenddessen findet der IT-Dienstleister der Provinzial den Trojaner und entfernt diesen und die geöffnete Remote-Verbindung. Dieser und der IT-Dienstleister der Arztpraxis härten das System durch verbesserte Firewall-Einstellungen.
- Über ein externes Call-Center wird eine Patienten-Hotline eingerichtet. 120 Patienten nehmen die Praxis auf Schadenersatz in Anspruch.
- Die Abwicklung der Schadenersatzansprüche ist komplex und zieht sich über ein Jahr hin.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 50.000 EUR |
| Rechtsanwalt | 35.000 EUR |
| Patientenbenachrichtigung | 12.000 EUR |
| Call-Center | 28.000 EUR |
| Schadenersatzzahlungen, gegnerische Anwälte, teilweise Anspruchsabwehr | 180.000 EUR |
| **Gesamt** | **305.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

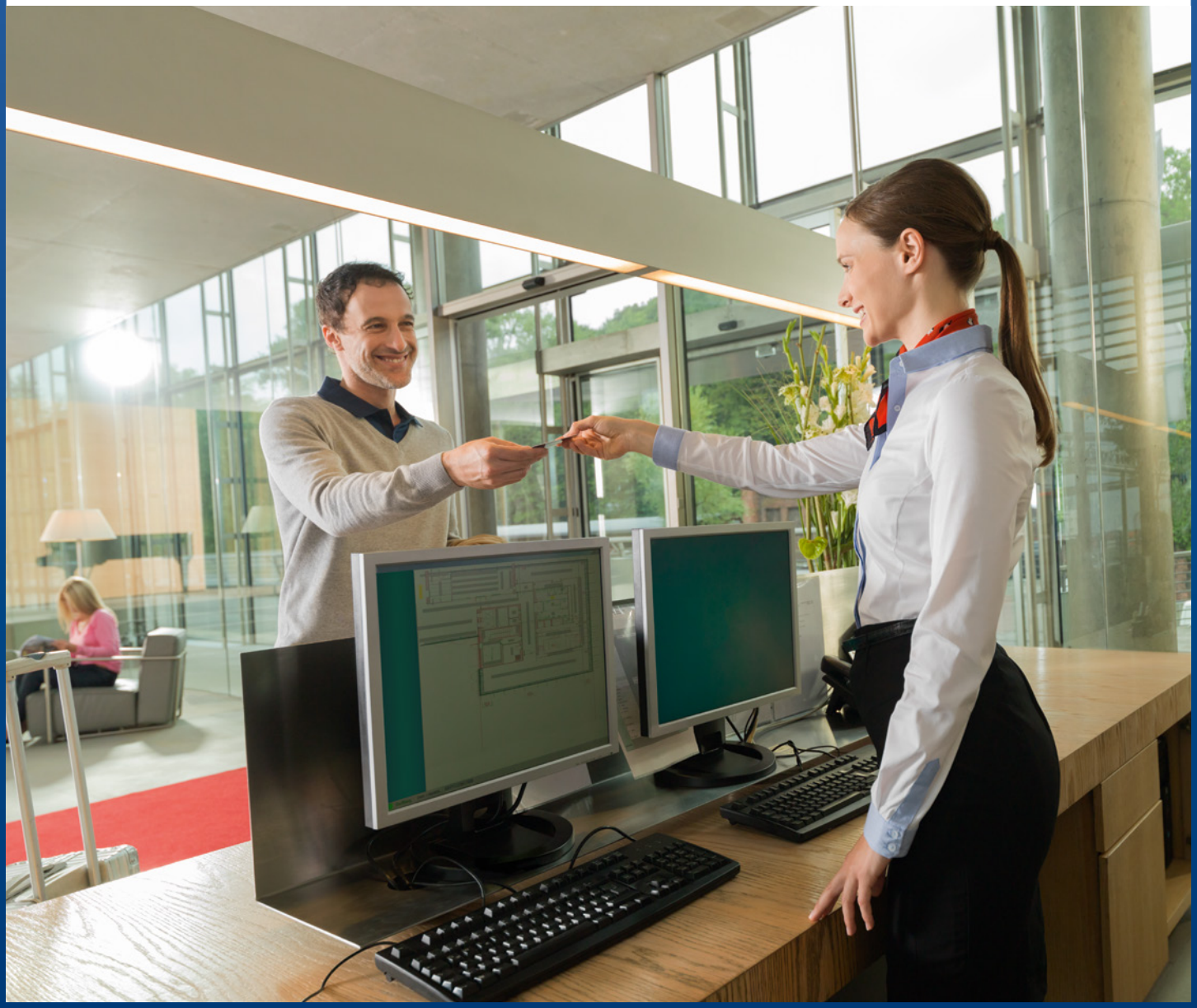
# Freiberufler

- Eine Steuerberater-Kanzlei beschäftigt 5 Berufsträger und 12 Mitarbeiter.
- Durch eine Bewerbungs-E-Mail gelangt der Krypto-trojaner gand.crab in das IT-System der Kanzlei. Dadurch werden über Nacht alle Dateien verschlüsselt.
- Sämtliche Rechner der Kanzlei sind auf Grund des Trojaners nicht mehr nutzbar. Zudem ist auch der Zugang zur DATEV eG (Softwarehaus und IT-Dienstleister unter anderem für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte) nicht mehr möglich. Auch die Homepage der Firma ist nicht mehr erreichbar. Lediglich die Telefone funktionieren noch.
- Der Schaden wird der Provinzial gemeldet.
- Der IT-Dienstleister der Provinzial unterstützt den IT-Dienstleister der Kanzlei bei der Wiederherstellung der Systeme aus den Back-Ups. Zudem spürt der IT-Dienstleister Schadprogramme auf und entfernt diese.
- Die Steuerberatungs-Kanzlei war 3 Tage nicht in der Lage zu arbeiten.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 35.000 EUR |
| Betriebsunterbrechung / Einschränkung | 15.000 EUR |
| **Gesamt** | **50.000 EUR** |

zurück zur Titelseite



PROVINZIAL
Die Versicherung der Sparkassen

# Dienstleister

- Ein Unternehmensberater beschäftigt 5 Mitarbeiter. Ein Mitarbeiter hat auf der lokalen Festplatte seines Laptops vertrauliche Daten von aktuellen und vergangenen Projekten. Seinen Laptop hat er nur durch ein schwaches Passwort gesichert. Die Festplatten sind zwar verschlüsselt, nach Eingabe des Laptop-Passworts jedoch für jedermann zugänglich. Zudem kann der Rechner mittels VPN-Zugang auf den zentralen Server zugreifen. Das VPN-Passwort ist identisch mit dem Laptop-Passwort.
- Der Laptop des Mitarbeiters wird entwendet. Über einen Passwort-Cracker wird das Passwort geknackt. Der Hacker gelangt an die sensiblen Daten und erpresst den Unternehmensberater.
- Der Unternehmensberater schaltet die Polizei und die Provinzial ein. Die Polizei rät vom Zahlen des Lösegelds ab.
- Daraufhin verschafft sich der Täter über den VPN-Zugang zusätzlich Zugriff auf den Server. Er löscht alle Dateien inklusive Back-Ups. Dies ist problemlos möglich, da es keine Nutzerverwaltung gibt und alle Mitarbeiter des Unternehmensberaters Admin-Rechte besitzen.
- Der IT-Dienstleister der Provinzial schafft es, über die lokalen Daten der anderen Laptops und mittels einer Spezialsoftware gelöschte Dateien zu rekonstruieren und 80 % der Daten wiederherzustellen. Die restlichen Daten sind endgültig verloren.

## Entstandene Kosten

| | |
|---|---|
| IT-Dienstleister | 25.000 EUR |
| Benachrichtigungskosten | 9.000 EUR |
| Ertragsausfall | 15.000 EUR |
| Rechtsanwalt | 6.000 EUR |
| **Gesamt** | **55.000 EUR** |

zurück zur Titelseite



3.01.253.0.0012.0 9.2021 | Provinzial Nord Brandkasse AG, Postanschrift: 24097 Kiel, www.provinzial.de