Schadenbeispiele

Mögliche Angriffsarten von Cyberkriminellen auf Unternehmen und die Schäden, die sie verursachen.

Verantwortlich für den Inhalt: Perseus Technologies GmbH
Datum: 26.08.2022
Version 4.0
Vertraulichkeit: Intern + Kooperationspartner

perseus. technologies

Schadenbeispiele I

Es kann jeden treffen. Die Frage ist nicht ob, sondern wann!

1 **Stadtverwaltung**

Organisationschaos

Verzögerte Impftermine

2 **Handwerk**

Produktionsstillstand

Falscher Klick, zur falschen Zeit

3 **Gesundheitswesen**

Daten verschlüsselt

Ursache: Standard-Passwort

4 **Einzelhandel**

Denial-of Service-Angriff

Zurzeit nicht erreichbar

5 **Internetprovider**

Datenleck

Veröffentlichung von Kundendaten zu Erpressungszwecken

6 **Gaststättengewerbe**

Achtung: Phishing

Betrug via E-Mail

Beispiele anklickbar

Schadenbeispiele II

Es kann jeden treffen. Die Frage ist nicht ob, sondern wann!

7

Deutscher Mittelstand

Attacke im Homeoffice

Hacker nutzen Verwirrung aus

8

Cloud Server

Phishing for Passwords

Auch Cloud-Server sind „hackbar“

9

Microsoft Exchange Server

Zero-Day-Sicherheitslücke

Globales Problem

10

Logistik

Einstiegstor: Hardware

Komplette Neuinstallation der Hardware

11

Kanzlei

Analyse rettet Daten

Ransomware im zweiten Schritt

12

Produzierendes Gewerbe

Nicht zu entschlüsseln

Kampf gegen Ransomware „RYUK“

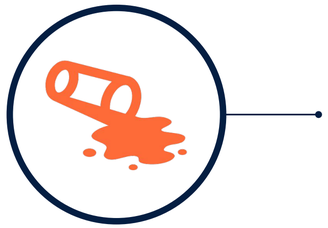
Beispiele anklickbar

Organisations chaos

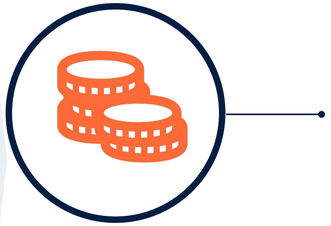
Verzögerte Impftermine

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebsunterbrechung
3. Drittschäden
4. Reputationsverlust

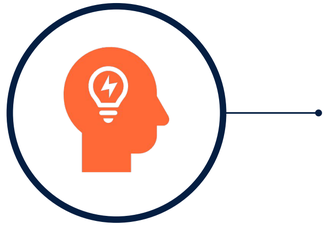


Durch einen schweren Hackerangriff wurde die **komplette Infrastruktur** einer Stadtverwaltung lahmgelegt. Ein **Verschlüsselungsvirus** hat **massive technische Schäden** und eine fatale **Betriebsunterbrechung** verursacht. **Verwaltungsdienste waren geschlossen,** die Mitarbeitenden nicht erreichbar, und auch das Bürgerbüro sowie Standesamt mussten vorübergehend schließen. Auch gegen das SARS-CoV-2 Virus sollte in der Folgewoche geimpft werden. Da aufgrund der technischen Störung nicht mehr auf Wartelisten und Terminvergaben zugegriffen werden konnte, stand die Stadtverwaltung vor einer massiven Herausforderung.



Ungefähre Schadenskosten

Kosten für Datenwiederherstellung	5.000 €
Kosten der Betriebsunterbrechung	2.500 €
Forensik Kosten	10.000 €
Kosten für Information der Kunden	2.000 €
Verwaltungskosten	4.500 €
Gesamt	**24.000 €**



Wie kann man dies verhindern?

- Erstellen Sie Backups Ihrer Daten
- Achten Sie auf Aktualität und befolgen Sie die 3-2-1 Backup-Strategie
- Durch die Sicherheitskopien können Sie Ihre Daten nach der Verschlüsselung selbst wiederherstellen

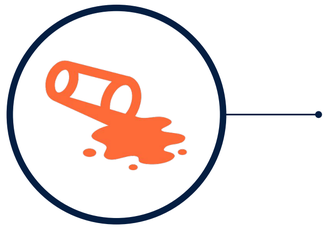
Produktions-stillstand

Falscher Klick zur falschen Zeit

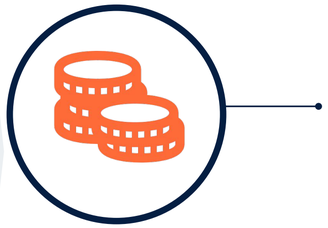
Folgen des Cybervorfalls:

1. Eigenschaden

2. Betriebsunterbrechung

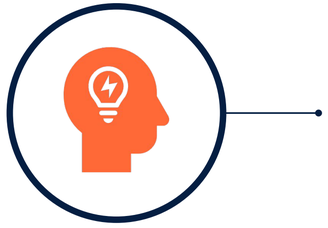


In einer Schreinerei standen **sämtliche Produktionsanlagen still**.
Ein Mitarbeiter hatte einen **Werbebanner** angeklickt, der mit einem **Schadprogramm** infiziert war. Da die installierte Version des Internetbrowsers veraltet war, wurde es automatisch heruntergeladen und **infizierte sämtliche Endgeräte im Unternehmen**: Computer, Mobiltelefone und computergestützte Fertigungsmaschinen. Produktionsdaten und Kundendaten waren nicht mehr zugänglich. Die vorhandenen Sicherheitskopien konnten erst nach über einem Tag installiert werden, da das Schadprogramm zunächst professionell entfernt werden musste.



Ungefähre Schadenskosten

Kosten für Datenwiederherstellung	6.000 €
Kosten der Betriebsunterbrechung	5.000 €
Forensik Kosten	7.000 €
Informationskosten des Ausfalls gegenüber Zulieferer und Abnehmer	1.000 €
Gesamt	**19.000 €**



Wie kann man dies verhindern?

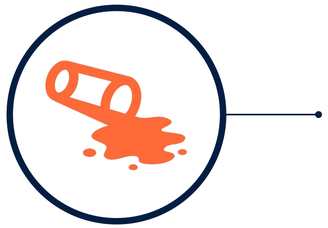
- Browser auf Aktualität prüfen und ggf. aktualisieren
- Sicherheitslücken identifizieren und schließen
- Mitarbeiter über Bedrohungen aus dem Internet schulen

Daten verschlüsselt

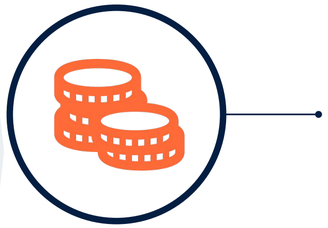
Ursache:
Standard-Passwort

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebsunterbrechung
3. Vertrauensverlust

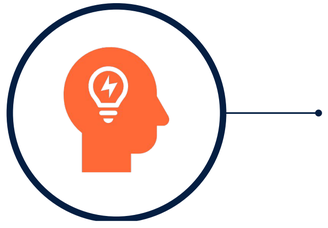


Angestellte einer Arztpraxis fuhren den Computer hoch und fanden ausschließlich **verschlüsselte Dateien** und eine Textnachricht darauf: **Zahlen Sie einen Bitcoin** (ca. 40.000 €), um wieder auf Ihre Daten zugreifen zu können. Die Ursache: Kriminelle hatten das **Passwort** (Praxis2004!) des Fernzugangs des Praxisservers **geknackt**. Mit einer Software wurden sämtliche Daten – Patientenakten, Kalendereinträge, Buchhaltung – verschlüsselt. Da auch der Dienstleister die Daten nicht entschlüsseln konnte, zahlte der Inhaber das Lösegeld. Von den Kriminellen hörten sie nie wieder. Mit Hilfe von **lückenhaften Sicherungskopien** wurde ein Teil der Daten wieder hergestellt. Die Praxis musste bis zur Wiederherstellung geschlossen bleiben.



Ungefähre Schadenskosten

Forensik Kosten	7.000 €
Kosten für Datenwiederherstellung	7.400 €
Kosten für die eigene Betriebsunterbrechung ab 24 Stunden	4.500 €
Lösegeldforderung	40.000 €
Gesamt	**58.900 €**



Wie kann man dies verhindern?

- Komplexe, lange und sichere Passwörter nutzen
- Passwörter nicht mehrfach oder für mehrere Anwendungen nutzen
- Mitarbeiter über Schutz der Zugangsdaten sensibilisieren

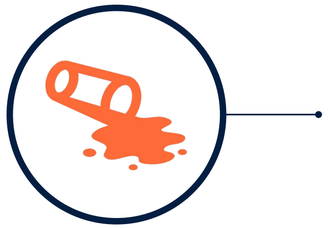
Denial-of Service-Angriff

Zurzeit nicht erreichbar

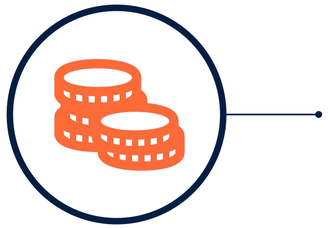
Folgen des Cybervorfalls:

1. Eigenschaden

2. Betriebsunterbrechung

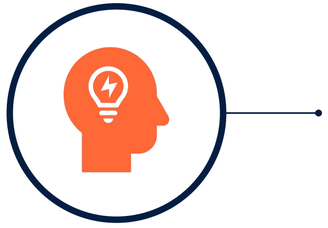


Eine Geschäftsführerin einer Boutique betreibt einen Online-Shop, in dem sie die Produkte ebenfalls verkauft. Genau in der Hochsaison war der Online-Auftritt plötzlich **tagelang nicht mehr zu erreichen**. Unter der Internetadresse tauchte lediglich eine Fehlermeldung auf. Die Ursache: Eine Masse an Anfragen **überlastete** den Online-Dienst – ein **Denial-of Service-Angriff (DDoS-Angriff)**. Kriminelle nutzten eine Sicherheitslücke aus, um den **Webserver zum Absturz** zu bringen. Dadurch war dieser nicht mehr verfügbar. Der externen IT-Dienstleister konnte zusammen mit dem Webhosting-Betreiber die Sicherheitslücke schließen. Nach etwa vier Tagen konnte der alltägliche Geschäftsbetrieb wieder aufgenommen werden.



Ungefähre Schadenskosten

IT-Team	15.000 €
Umsatzverlust durch die entgangenen Online-Bestellungen	9.000 €
Gesamt	**24.000 €**



Wie kann man dies verhindern?

IT-Sicherheitsprüfung zeigt u.a.:

- ob Server aktuell sind
- ob Schwachstellen der IT-Infrastruktur von außen sichtbar und angreifbar sind,

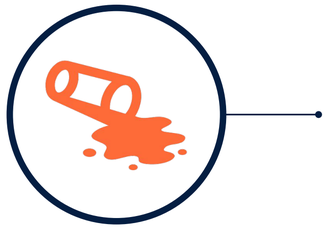
  und vieles mehr zur Sicherheitsproblemen.

Datenleck

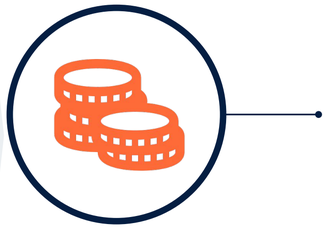
Kundendaten zu Erpressungszwecken veröffentlicht

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebs-unterbrechung
3. Drittschäden
4. Reputationsverlust

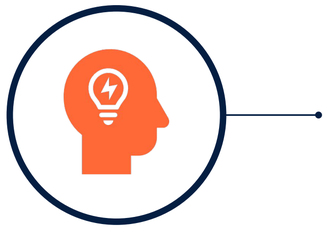


Ein Hackerangriff auf einen Internetprovider hatte zur Folge, dass **Kundendaten** von den Servern des Providers gestohlen wurden. Zielscheibe des Angriffs waren nicht operativ-technischen Systeme, sondern gezielt **Kunden- & Kommunikations-systeme.** Die gestohlenen Daten wurden auf der Website der Hacker veröffentlicht, um von dem Provider **Lösegeld zu fordern.** Nach einiger Zeit wurden diese Daten wieder offline genommen. Der Provider musste nun die kompromittierten Systeme bereinigen, den **Datenschutz- und Sicherheitsvorfall** an die zuständigen Behörden melden sowie die betroffenen Kunden über das Datenleck informieren.



Ungefähre Schadenskosten

Forensik-Kosten	20.000 €
Schließung der Sicherheitslücke	4.000 €
Kosten für Information der Kunden	3.000 €
Lösegeldzahlung	30.000 €
Gesamt	**57.000 €**



Wie kann man dies verhindern?

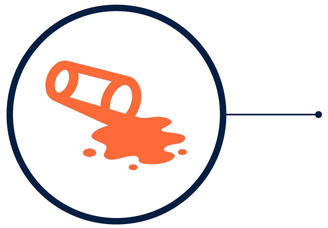
- Aktuelle Betriebssysteme
- Regelmäßige IT-Sicherheitsprüfungen
- Schulung der Mitarbeitenden

Achtung: Phishing

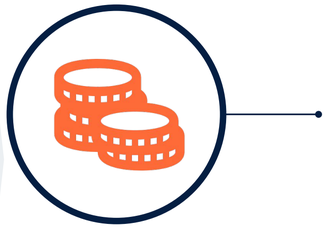
Betrug via E-Mail

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebsunterbrechung
3. Drittschäden
4. Reputationsverlust

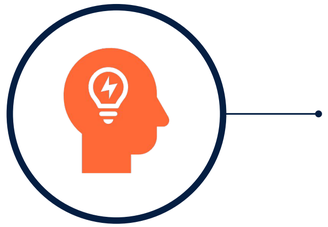


Ein Mitarbeiter öffnete eine als **Rechnung getarnte Betrugs-E-Mail**. Der Anhang war mit einem **Trojaner** infiziert, dadurch konnten sich **Kriminelle Zugang zur Datenbank** der Restaurantkette verschaffen. Wurde der Online-Bestellservice genutzt, konnten die Kriminellen die **eingegebenen Zahlungsdaten der Kunden kopieren**. In der Datenbank waren etwa 2.000 Kundendaten enthalten. Mehr als **400 Kreditkarten-informationen** wurden zweckentfremdet. Als Folge der Datenschutzverletzung machten die Kreditkartenunternehmen vertraglich vereinbarte Strafen geltend.



Ungefähre Schadenskosten

Forensik-Kosten	15.000 €
Entfernung des Schadprogramms	9.000 €
Kosten für Information der Kunden	10.000 €
Forderungen der Kreditkartenunternehmen	32.000 €
Umsatzverlust durch entgangene Online-Reservierungen	15.000 €
Rechtsanwaltskosten	46.500 €
Gesamt	**127.500 €**



Wie kann man dies verhindern?

Mitarbeiter erkennt Betrugsversuch:

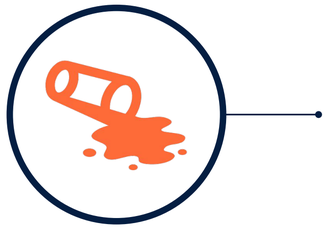
- öffnet Verdächtige E-Mails nicht
- klickt nicht auf die enthaltenen Links in der E-Mail und / oder
- öffnet den Anhang nicht

Attacke im Homeoffice

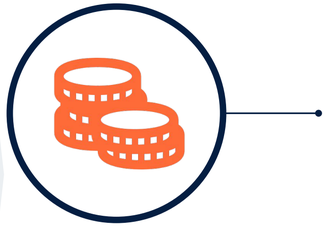
Hacker nutzen Verwirrung aus

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebsunterbrechung
3. Betriebsausfall

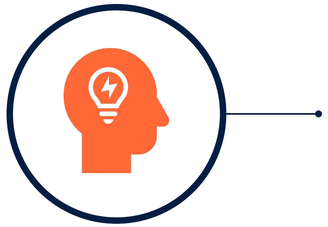


Deutschland während der Corona-Pandemie. Wie unzählige andere Unternehmen, musste auch dieser **Mittelständler seine komplette Belegschaft ins Homeoffice schicken** – darunter auch die gesamte IT-Abteilung. Eine ungewohnte Situation für das Unternehmen. Cyberkriminelle nutzten dies schamlos aus und **platzierten einen Verschlüsselungstrojaner im System mit dem Ziel alle Daten unzugänglich** zu machen. Alle Systeme mussten heruntergefahren werden.
Mehrere Werke und Niederlassungen waren von dem Stillstand betroffen. Mit Kunden konnte kaum kommuniziert werden.



Ungefähre Schadenskosten

Forensik-Kosten	7.000 €
Netzwerk Wiederherstellung	3.000 €
Kosten der Betriebsunterbrechung	4.000 €
Kosten Betriebsausfall	15.000 €
Kosten für Information der Kunden	1.000 €
Gesamt	**30.000 €**



Wie kann man dies verhindern?

Sensibilisierung der Mitarbeitenden im Homeoffice

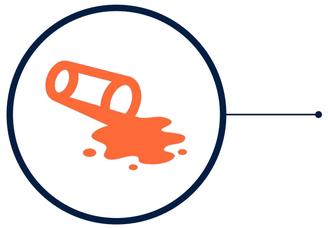
- Ausreichende Aufklärung über Gefahren im Homeoffice
- Klar formulierte Anweisungen für Mitarbeitende im Homeoffice
- Klar formulierter & transparenter Notfallplan

Phishing for Passwords

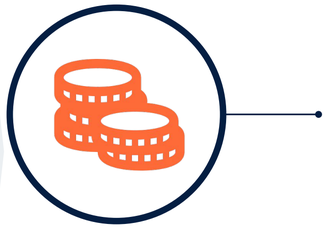
Auch Cloud-Server sind „hackbar“

Folgen des Cybervorfalls:

1. Eigenschaden
2. Vertragsstrafen
3. Imageschaden

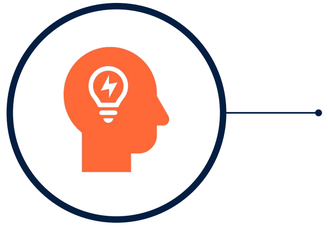


Um die Zusammenarbeit innerhalb eines Online-Unternehmens zu optimieren, wurden alle **Unternehmensdaten in einer Cloud gespeichert**. Ein Mitarbeiter dieses Unternehmens erhielt eine E-Mail des Cloud-Anbieters mit der Aufforderung seine **Login-Informationen aus Sicherheitsgründen** zu aktualisieren. Der Mitarbeiter kam dieser Aufforderung sofort nach und klickte auf den angegebenen Link. Dieser führte auf eine **gefälschte Internetseite**. Anstelle seine Zugangsinformationen zu aktualisieren, teilte der Mitarbeiter seine Login-Daten mit Cyberkriminellen, die nun **freien Zugang auf die Unternehmensdaten** in der Cloud hatten und über diese frei verfügen und Lösegeld fordern konnten.



Ungefähre Schadenskosten

Lösegeldforderung	20.000 €
Kosten für Information der Kunden	1.000 €
Kosten für Vertragsstrafen, Rechtsberatung oder Klage	50.000 €
Kosten für Drittschäden	5.000 €
Gesamt	**76.000 €**



Wie kann man dies verhindern?

Zwei- oder Multi-Faktor-Authentifizierung

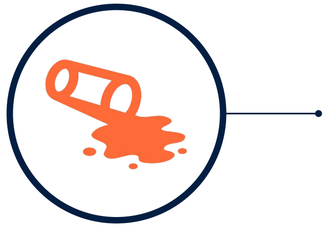
- Bietet eine zusätzliche Sicherheitsebene
- Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (bspw. Passwort + Pin-Eingabe)

Zero-Day-Sicherheitslücke

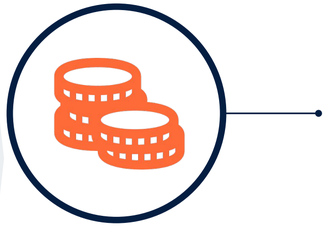
Globales Problem

Folgen des Cybervorfalls:

1. Eigenschaden
2. Betriebsunterbrechung
3. Imageschaden

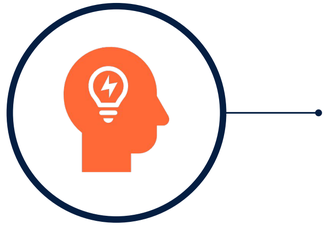


Im März 2021 wurde bekannt, dass mehrere Sicherheitslücken, darunter auch vier **Zero-Day-Sicherheitslücken** in **Microsoft Exchange Servern** existierten. Auch ein Medienunternehmen aus Nordrhein-Westfalen war von diesem Sicherheitsvorfall betroffen. Cyberkriminelle konnten über eine der Schwachstellen einen **Webshell im System des Unternehmens einschleusen** und somit Befehle aus der Ferne auf dem betroffenen System ausführen. Dadurch hätten die Angreifer potentiellen Zugriff auf sämtliche Dateien des Exchange Servers – und somit auf E-Mail-Postfächer und Adressbücher. Es bestand außerdem die Befürchtung, dass es zu **Infektionen mit bösartigem Code oder nachgelagerten Cyberangriffen** kommen könnte.



Ungefähre Schadenskosten

Forensik-Kosten	7.500 €
Rechtsberatung im Zuge der Meldung an die Datenschutzbehörde	1.500 €
Kosten für Information der Kunden	2.000 €
Gesamt	**11.000 €**



Wie kann man dies verhindern?

Software-Hygiene

- Installieren Sie Software-Aktualisierungen immer unverzüglich
- Stellen Sie sicher, dass Mitarbeitende einen Ansprechpartner zur Installation für Updates haben

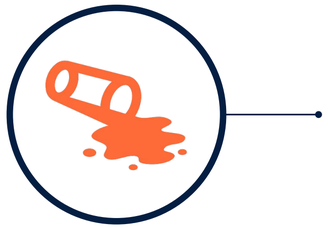
Einstiegstor: Hardware

Komplette Neuinstallation der Hardware

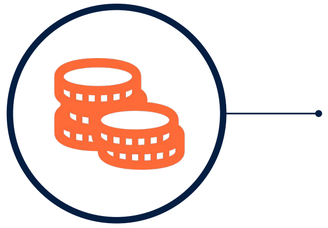
Folgen des Cybervorfalls:

1. Eigenschaden

2. Betriebsunterbrechung

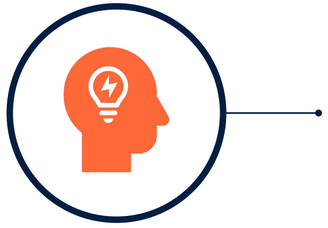


Bei einem Transportunternehmen wurde ein **System zur Entlastung der Rechenkapazitäten** von Servern angegriffen. Hacker hatten im Vorfeld **kritische Sicherheitslücken innerhalb dieser Technologie** enttarnt, welche es ermöglichen IT-Systeme **komplett zu kompromittieren**. Die Informationen zur Ausnutzung der kritischen Lücke wurden veröffentlicht. Dies hat eine **systematische Suche nach verwundbaren Systemen** in Gang gesetzt, darunter auch das Transportunternehmen. Zu diesem Zeitpunkt gab es noch keine Software-Updates für das System, wodurch ein erhöhtes Angriffsrisiko bestand. Im Zuge der Schadenbekämpfung musste die komplette Hardware neuinstalliert und die Zugangsdaten aller Personen aktualisiert werden.



Ungefähre Schadenskosten

Forensik-Kosten	7.500 €
Installation der Hardware	2.500 €
Gesamt	**10.000 €**



Wie kann man dies verhindern?

- Starke Firewall zu Schutz der Daten, Systeme und Netzwerke. Viele Schadprogramme und mögliche unautorisierte Zugriffsversuche können hier bereits erkannt, gestoppt oder zumindest teilweise geblockt werden.

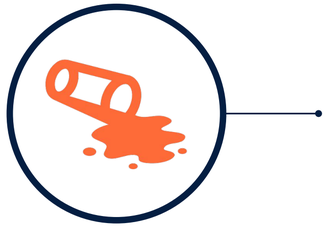
Analyse rettet Daten

Ransomware im zweiten Schritt

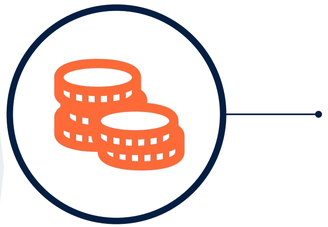
Folgen des Cybervorfalls:

1. Eigenschaden

2. Betriebsunterbrechung

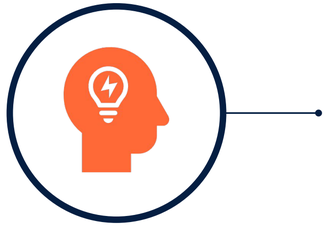


Mitarbeitende einer Anwaltskanzlei erhielten verschiedene E-Mails eines ehemaligen Kunden. Der ersten Mail war eine Zip-Datei beigefügt, die mit einem Passwort verschlüsselt war. Das **Entpacken der Zip-Datei** und das **Öffnen der darin befindlichen Word-Dateien** führte zu einer **Infektion** der IT. Die Notfallhilfe eines externen IT-Dienstleisters schien im ersten Moment das Problem zu beheben, doch schon bald traten die gleichen Fehler erneut auf. Infolgedessen wurden ein IT-Forensiker hinzugezogen, der ein Programm feststellte, das **kontinuierlich weiteren Schadcode** nachlud. Obwohl den Angreifern dies nur bedingt gelang, wurde zumindest ein weiteres System mit einer Ransomware infiziert.



Ungefähre Schadenskosten

Arbeit IT-Dienstleister	2.000 €
Forensik-Kosten	5.500 €
Wiedereinspielen der Daten	5.000 €
Betriebsausfall	2.700 €
Gesamt	**15.200 €**



Wie kann man dies verhindern?

- Konsultieren Sie einen Cyberforensiker im Cybernotfall
- Erstellen Sie Backups Ihrer Daten
- Achten Sie auf Aktualität und befolgen Sie die 3-2-1 Backup-Strategie

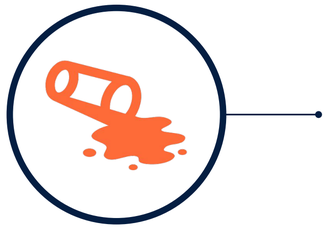
Nicht zu entschlüsseln

Kampf gegen Ransomware „RYUK“

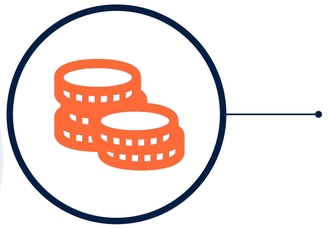
Folgen des Cybervorfalls:

1. Eigenschaden

2. Betriebsunterbrechung

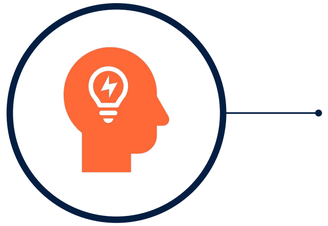


Ein Unternehmen für Alarmanlagen wurde Opfer eines **Ransomware-Angriffs**. Durch die Verwendung eines **kompromittierten Administrations-Accounts** war es dem Hacker möglich sich schnell durch das Netzwerk zu bewegen. Automatisch drang der Angreifer in verschiedene Systeme vor und konnte **Benutzernamen und Passwörter weiterer Accounts auslesen**. Kurz nach der ursprünglichen Infektion, verschlüsselte die **Ransomware „RYUK“** eines der betroffenen Systeme. Zu dem damaligen Zeitpunkt gab es kein öffentliches Entschlüsselungstool gegen diese Ransomware. Da der Angreifer über **Domain-Admin-Berechtigungen** verfügte, galt die **komplette Domain** als kompromittiert.



Ungefähre Schadenskosten

Forensik-Kosten	15.000 €
Wiedereinspielen der Daten	2.000 €
Betriebsunterbrechung	3.000 €
Gesamt	**20.000 €**



Wie kann man dies verhindern?

- Komplexe, lange und sichere Passwörter nutzen
- Passwörter nicht mehrfach oder für mehrere Anwendungen nutzen
- Mitarbeitende über Schutz der Zugangsdaten sensibilisieren