beazley

Cyber-Schadenregulierung

Anforderungen ans Schadenmanagement anhand eines Beispielfalls

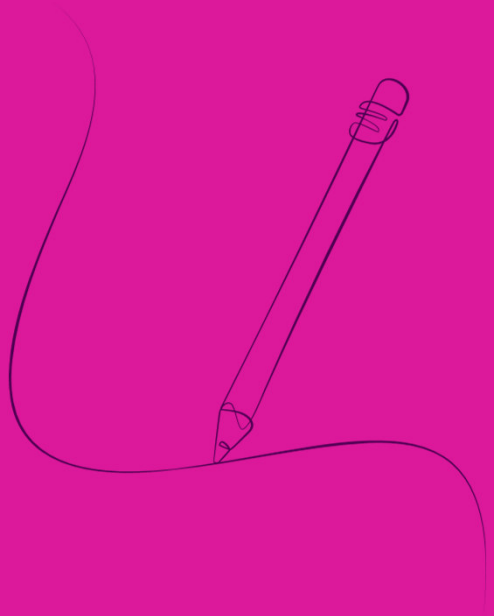
25.April 2024 Meike Drieß, Head of Claims DACH

Meike Drieß
Claims Manager DACH bei Beazley

- Leitet die Schadenabteilung der DACH-Region bei Beazley.
- Sitz in München.
- Verantwortet insbesondere Cyber- und Financial-Lines-Schäden, Schadenprozesse sowie alles andere rund um das Thema Schaden.
- Hat sich zuvor bei Hiscox S.A. und Allianz SE Reinsurance mit Schäden, Schadenthemen und Schadenprozessen beschäftigt.

beazley

Inhalt



beazley

01

Zahlen, Daten & Fakten

Hauptgründe für Cyberattacken

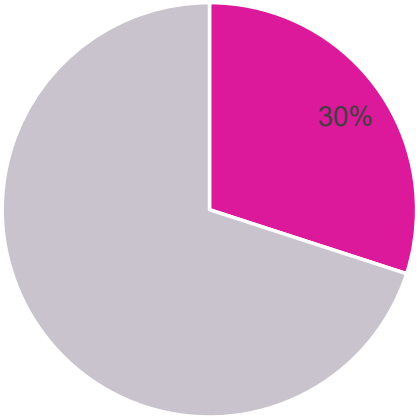
- Sorgloser Umgang mit IT-Sicherheit
- Unzureichend ausgebildete Mitarbeiter
- Mangelndes Risikoverständnis der Mitarbeiter
- Vermehrte Schwierigkeiten, die ersten Anzeichen von Verdachtsfällen zu erkennen
- Zunehmende Komplexität der eingesetzten Technologie

beazley

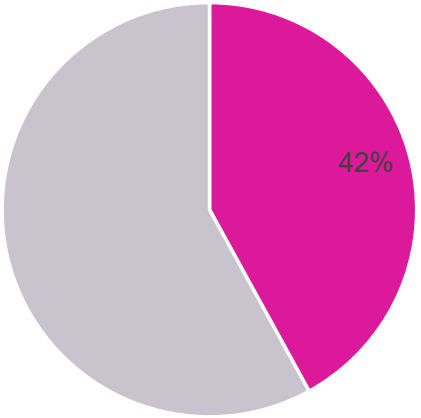
Quelle: KPMG AG Wirtschaftsprüfungsgesellschaft:
Studie e-Crime: Computerkriminalität in der deutschen Wirtschaft 2022

Wie vorbereitet sind Unternehmen

In Deutschland fühlen sich kleine und mittlere Unternehmen besonders verwundbar.



30 % aller Führungskräfte fühlen sich heute nicht auf die Bedrohung durch Cyberrisiken vorbereitet.

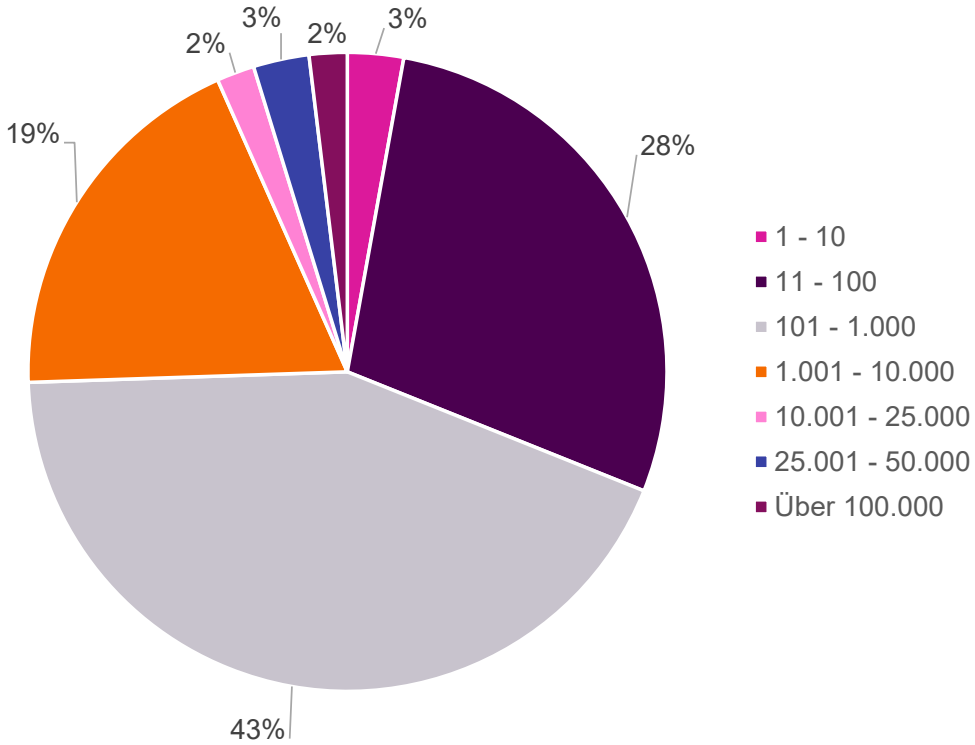


Bei kleineren Unternehmen mit einem Umsatz zwischen 250.000 und unter 1 Million sind es sogar 42 %.

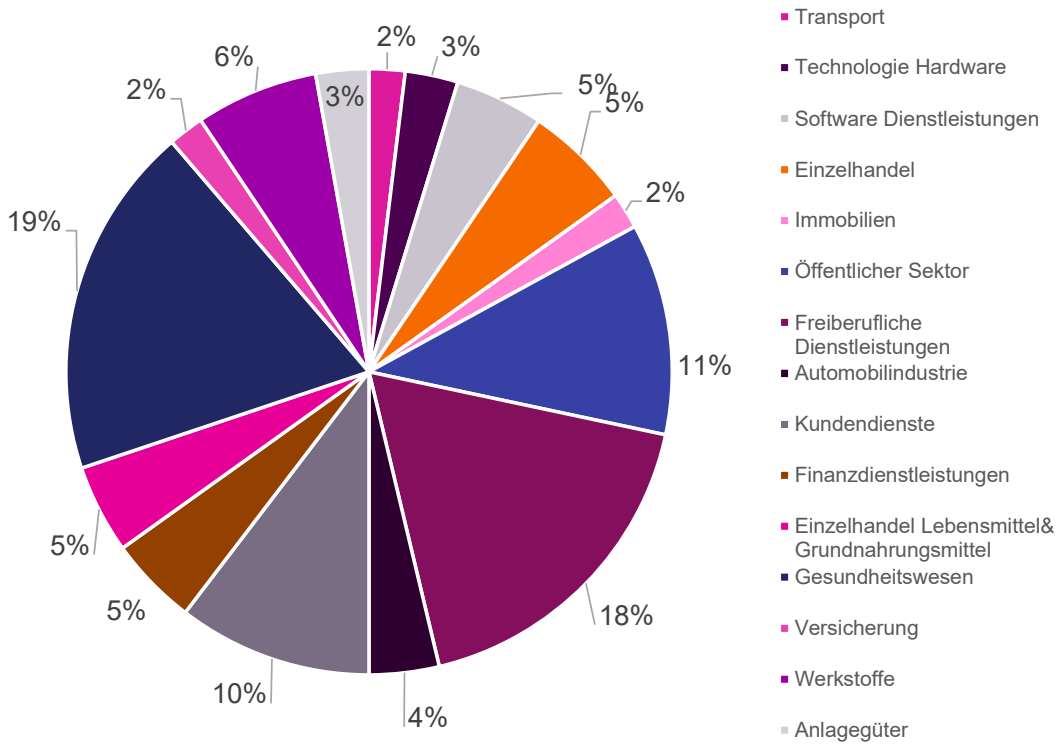
Quelle: Beazley risk resilience report 2023.

Schadenzahlen - Größe und Sektor der angegiffenen Firmen

Betroffene Unternehmen von Ransomware nach Mitarbeitanzahl



Betroffene Unternehmen von Ransomware je nach Branche Q1 2024



Quelle: Coveware QUARTERLY REPORT, Q1 2024

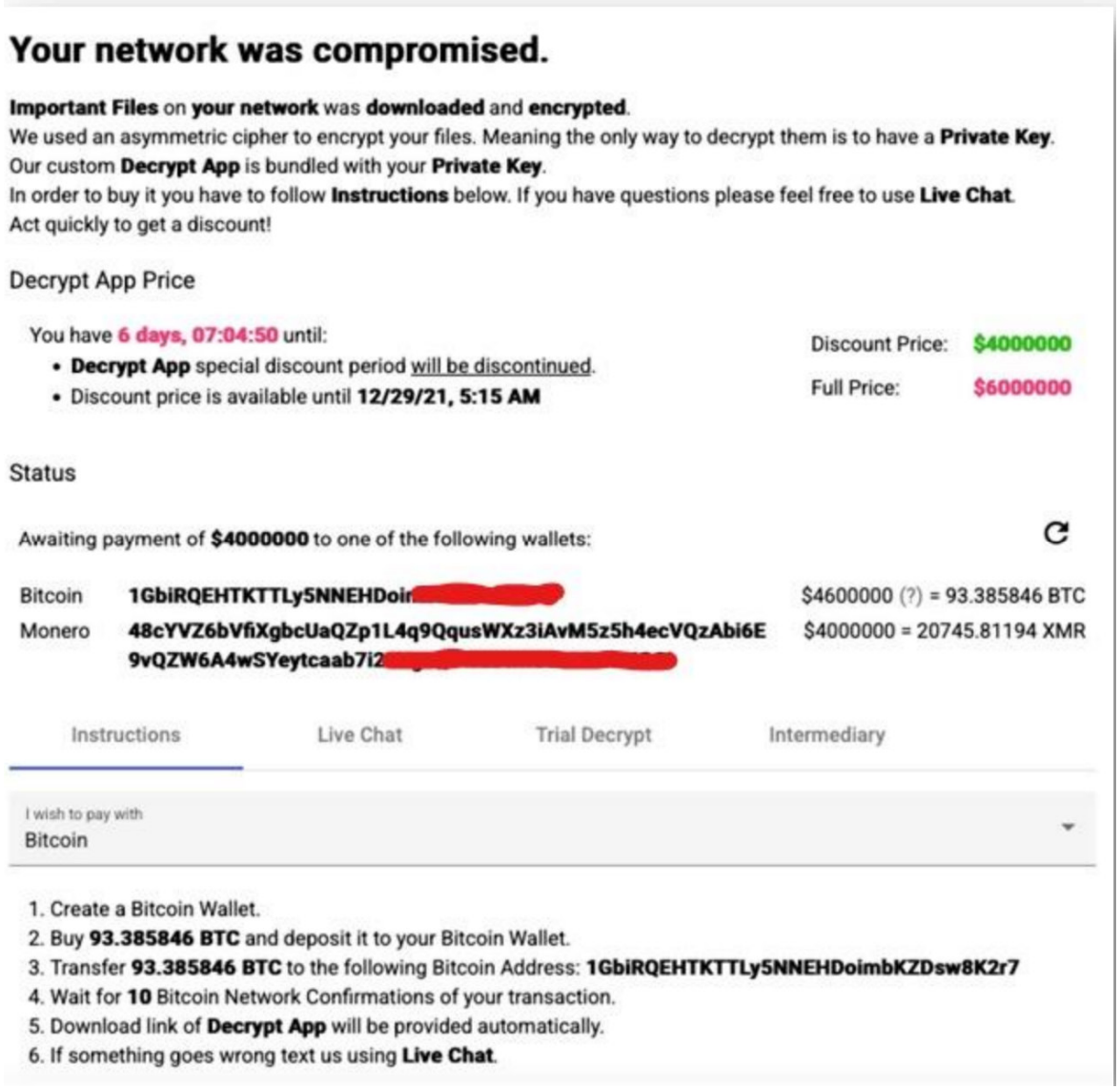
beazley

02

Schadenbeispiel Teil 1

Schadenbeispiel: Ransomware

- Als die Mitarbeiter am Morgen mit der Arbeit beginnen wollten, konnten sie sich nicht mehr einloggen.
- Alle Daten waren verschlüsselt und es wurde eine Ransom Note des Hackers gefunden.



Your network was compromised.

Important Files on **your network** was **downloaded** and **encrypted**.
We used an asymmetric cipher to encrypt your files. Meaning the only way to decrypt them is to have a **Private Key**.
Our custom **Decrypt App** is bundled with your **Private Key**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live Chat**.
Act quickly to get a discount!

Decrypt App Price

You have **6 days, 07:04:50** until:
- **Decrypt App** special discount period will be discontinued.
- Discount price is available until **12/29/21, 5:15 AM**

Discount Price: **$4000000**
Full Price: **$6000000**

Status

Awaiting payment of **$4000000** to one of the following wallets:

Bitcoin	**1GbiRQEHTKTTLy5NNEHDoi** [redacted]	$4600000 (?) = 93.385846 BTC
Monero	**48cYVZ6bVfiXgbcUaQZp1L4q9QqusWXz3iAvM5z5h4ecVQzAbi6E**	$4000000 = 20745.81194 XMR
	9vQZW6A4wSYeytcaab7i2 [redacted]	

Instructions | Live Chat | Trial Decrypt | Intermediary

I wish to pay with
Bitcoin

1. Create a Bitcoin Wallet.
2. Buy **93.385846 BTC** and deposit it to your Bitcoin Wallet.
3. Transfer **93.385846 BTC** to the following Bitcoin Address: **1GbiRQEHTKTTLy5NNEHDoimbKZDsw8K2r7**
4. Wait for **10** Bitcoin Network Confirmations of your transaction.
5. Download link of **Decrypt App** will be provided automatically.
6. If something goes wrong text us using **Live Chat**.

beazley

Psychologisch gesehen setzen uns Krisen akut unter Stress, da wir das Gefühl haben, die Kontrolle über die innere oder äußere Situation verloren zu haben.

Die Krise beginnt

01

SCHOCK

Am Anfang der Krise macht sich inneres Chaos breit, einige Menschen fühlen sich wie gelähmt, verleugnen sogar die Realität – und somit auch den Krisenzustand.

Die Krise beginnt

Es folgen aufbrechende, chaotische Emotionen und Gefühle von Angst, Hilflosigkeit, Bedrohung und Kontrollverlust machen sich breit.

Die Krise beginnt

Die Stecker werden gezogen, die Verbindung zum Internet wird getrennt.

Der eigene externe IT-Dienstleister wird herangezogen.

Sensemaking:

Wenn die äußere Welt nicht mehr mit der inneren Welt in Übereinstimmung zu bringen ist, dann muss man eine neue Möglichkeit finden, die Welt wieder rational zu erklären.

Schuldgefühle ….

Habe ich was falsch gemacht?

Wie konnte das passieren?

Wo ist der Fehler?

Habe ich die Warnzeichen übersehen?

… und Druck!

beazley

Schuldgefühle ….

Habe ich was falsch gemacht?

Wie konnte das passieren?

Wo ist der Fehler?

Habe ich die Warnzeichen übersehen?

… und Druck!

beazley

Und so werden Logs gelöscht und die IT-Umgebung wieder aufgebaut.

beazley

Die Krise entwickelt sich

Nun beginnt der Ausweg aus der Krise. Gleichzeitig beginnt die Suche nach Lösungen, mit denen man die Krisensituation bewältigen kann.

Beazley Services wird eingeschaltet

- Alle Beteiligten arbeiten in engem Austausch.
- Beazley vermittelt den Kontakt zu einem Team von technischen Experten, die sofort mit dem externen IT-Dienstleister des VN zusammenarbeiteten.
- Anwälte für Datenrecht/GDPR werden hinzugezogen, um innerhalb von 72 Stunden eine Meldung an die Behörden zu versenden.

beazley

Schadenbeispiel: Sofortmaßnahmen

- Der Wiederherstellungsprozess dauerte 4 Tage.
- Die Beteiligten waren zuversichtlich, dass die wichtigsten Systeme wieder in Betrieb sind.
- In der Zwischenzeit kam es zu einer Betriebsunterbrechung.
- Es blieb unmöglich, den Weg des Angriffs herauszufinden und die Lücke zu schließen.

beazley

03

Schadenbeispiel Teil 2

Pierre: hello? what is happened to us?
11/26/2020, 9:01:46 PM

Support: Your network and all of your data were encrypted by our team. Besides the encryption process we've downloaded about 1.5TB of your internal documents and files that will be published in case our negotiations fail.
11/26/2020, 9:11:43 PM

Support: The recovery price is $9500000 (550 BTC). This initial offer is based on the details about your revenue and internal financial documents we currently have access to. If you want to

Schadenbeispiel: Double Extortion

- Zugangswege wurde erneut genutzt, auf den ersten Angriff folgte ein Zweiter.
- Alles, was wiederhergestellt war, wurde erneut zerstört.
- Der Angreifer drohen nun mit der Veröffentlichung sensibler Kundendaten, falls das geforderte Lösegeld von 550 BTC (damals ca. 9,5 Mio. €) nicht gezahlt wird.

beazley

„Wenn Druck aufgebaut wird, werden Fehler gemacht. Sie müssen verstehen, wie es zu dem Angriff gekommen ist - nicht nur, damit Sie Ihr Sicherheitsniveau in Zukunft verbessern können, sondern auch, um sicherzustellen, dass die Angreifer nicht mehr im Netzwerk sind."

Quelle: Andrada Fiscutean, Panik, Wut, Schuldgefühle: Die emotionalen Phasen eines Cyberangriffs - CSO (csoonline.com).

Die Krise entwickelt sich

Nun beginnt der Ausweg aus der Krise. Gleichzeitig beginnt die Suche nach Lösungen, mit denen man die Krisensituation bewältigen kann.

Die Krise entwickelt sich

Nun beginnt der Ausweg aus der Krise. Gleichzeitig beginnt die Suche nach Lösungen, mit denen man die Krisensituation bewältigen kann.

Am Ende konnte ein Lösegeld von 1,2 Mio. Euro ausgehandelt werden.

Schadenbeispiel: Versicherungsleistung

Letztlich sind folgende Posten angefallen und von Beazley bezahlt worden:

- Anwälte für Datenschutz
- Ransomware-Verhandler
- IT-Forensik
- PR-Berater
- Betriebsunterbrechung
- Lösegeld
- Datenwiderherstellungskosten

beazley

Outlook

01 SCHOCK

02 REAKTION

03 BEARBEITUNG

04 NEUORIENTIERUNG

In der letzten Phase der Krisenbewältigung richten wir uns neu aus.

Outlook

In der letzten Phase der Krisenbewältigung richten wir uns neu aus – uns selbst, aber auch in Bezug auf unsere Umwelt.

Nach der Krise ist vor der Krise!
Krisen schaffen Resilienz!

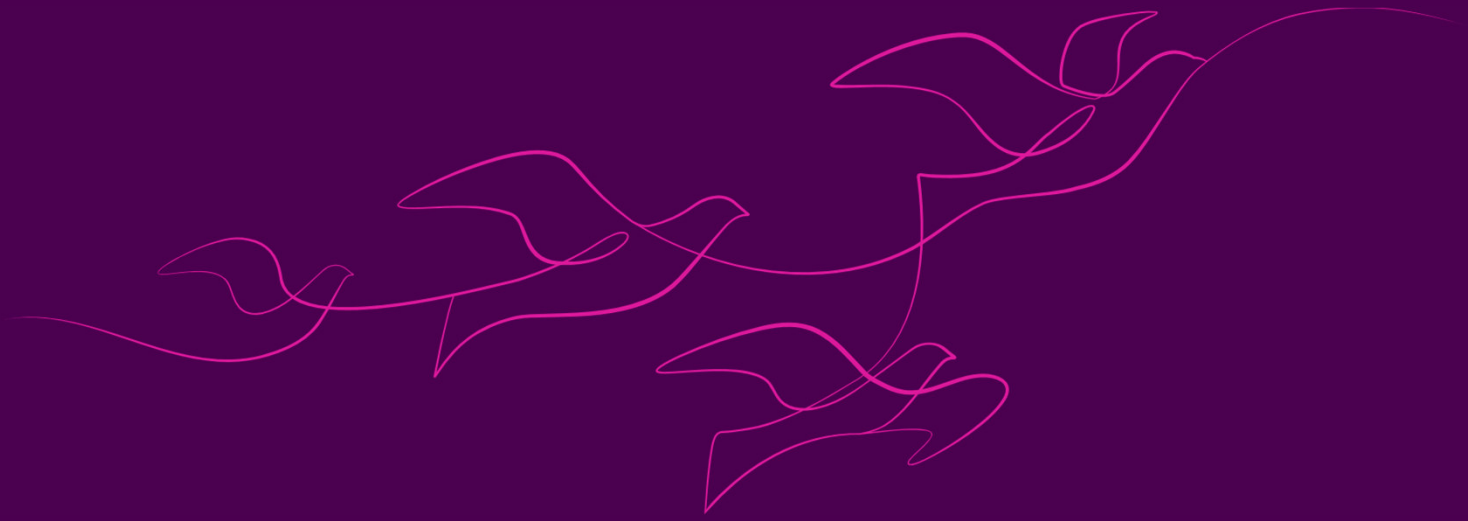
Präventionsparadoxon nach Geoffrey Rose

Mit der Prävention ist es nicht so einfach. Denn wenn sie erfolgreich ist, verlieren wir Menschen das Gefühl für die Gefahren.

Wenn Security-Maßnahmen wirken und dadurch weniger Angriffe passieren entsteht der Eindruck, dass die Maßnahmen nicht notwendig gewesen wären. Es ist ja nichts oder nur sehr wenig passiert.

Niemand kann genau sagen, was passiert wäre, wenn es keine Maßnahmen gegeben hätte.

beazley



Vielen Dank.

Follow us