

CYBERSicher

Transferstelle.
Cybersicherheit.
Mittelstand.



IT-Sicherheit
IN DER WIRTSCHAFT

Auf Angriffe richtig reagieren

Mit Unterstützung durch die Transferstelle Cybersicherheit

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Digitalisierung ganz konkret

- <https://www.shz.de/lokales/eckernfoerde/artikel/instagram-hit-laurin-bock-aus-eckernfoerde-gibt-zimmermann-tipps-45245281>
- <https://www.instagram.com/derholzbock.official/>

Digitalisierung als IT-Sicherheitsproblem

- Mit jeder neuen Technologie, die wir nutzen, werden wir angreifbarer
 - <https://www.washingtonpost.com/world/2020/12/17/dutch-trump-twitter-password-hack/>

Prävention

... soll Schäden vermeiden

Mittelstand-Digital
Zentrum
Chemnitz

Unternehmensdaten schützen – 10 Goldene Regeln

ROLAND HALLAU

Mittelstand-Digital
Zentrum
Chemnitz

Praxisbeispiel

Stellen im Unternehmensnetzwerk

Mittelstand-Digital
Zentrum
Chemnitz

Nachgelesen

Sicherheit in Unternehmen: für den Basisschutz

Mittelstand-Digital
Zentrum
Chemnitz

Praxisbeispiel

Stellenanalyse Unternehmensnetzwerken

Mittelstand-Digital
Zentrum
Chemnitz

Nachgelesen

Bild Mensch - 10 Regeln

Mittelstand-Digital
Zentrum
Chemnitz

Check

IT-Sicherheitsrisiko Mensch

Die Mehrheit der Sicherheitsvorfälle geht auf das Fehlverhalten von Mitarbeitern zurück. Sind Ihre Mitarbeiter auf digitale Angriffe vorbereitet und ausreichend zum Thema IT-Sicherheit informiert?

Sicherheitsleitlinie, die von Ihren Mitarbeitern unterstützt wird? Ja Nein

Essenden Sicherheitsleitlinie können Sie festhalten, wie Mitarbeiter Ihren Daten umgehen sollen. Darin können Sie begründen, welche Regeln warum untersagt sind und somit IT-Sicherheit ins Bewusstsein rufen.

Zentrale Anlaufstelle für Mitarbeiter, denen etwas passiert? Ja Nein

Sprechpartner ist wichtig. So wissen Mitarbeiter an wen sie sich wenden wenn sie beispielsweise Opfer eines Hackerangriffs wurden oder vermuten. Damit verringern Sie Risiken und begrenzen den Schaden.

Regeln für den Umgang mit USB-Sticks festgelegt? Ja Nein

Die Mitarbeiter insbesondere über den Umgang mit externen oder nicht firmeneigenen USB-Sticks auf. Diese können Schadsoftware enthalten, welche Firmendaten und sensible Daten ausspionieren. Nutzen Sie zum Testen separaten Rechner, der nicht am Firmennetz angeschlossen ist.

Regeln für den Umgang mit Cloud-Diensten? Ja Nein

Passwort beinhaltet laut BSI mind. 8 Zeichen, Buchstaben, Zahlen, Sonderzeichen und Kleinschreibung. Außerdem sollten Sie es nie wiederverwenden und in regelmäßigen Abständen ändern. Ganz wichtig: Angerstatt für alle einsehbarer Klebezettel am Bildschirm!

Mittelstand-Digital
Zentrum
Chemnitz

Risiko-Check: Sicherheit einfach

gemäß der neuen DIN SPEC 27076

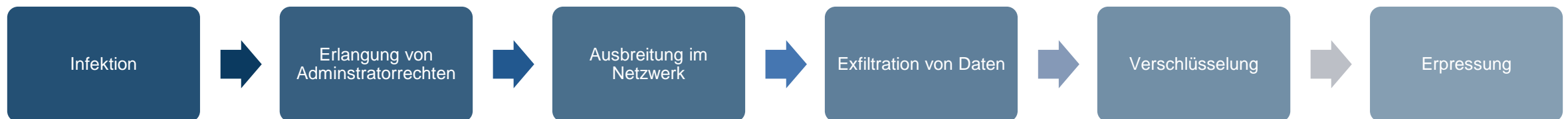
Und trotzdem ...

- Sophos Ransomware-Report 2023:
 - 66 % der befragten Unternehmen waren im letzten Jahr von Ransomware betroffen
 - Durchschnittliche Lösegeldforderung: 1,54 Millionen USD
 - Durchschnittliche Bereinigungskosten: 1,82 Millionen USD

Sophos Ransomware-Report 2023 abrufbar unter:
<https://www.sophos.com/de-de/content/state-of-ransomware>

Ransomware – was passiert da?

- Ein Ransomware-Angriff dient der Erpressung von Lösegeld.
- Daten der Opfer werden heruntergeladen und anschließend verschlüsselt.
- Auf die Erstinfektion mit einer Schadsoftware folgt der eigentliche Angriff:



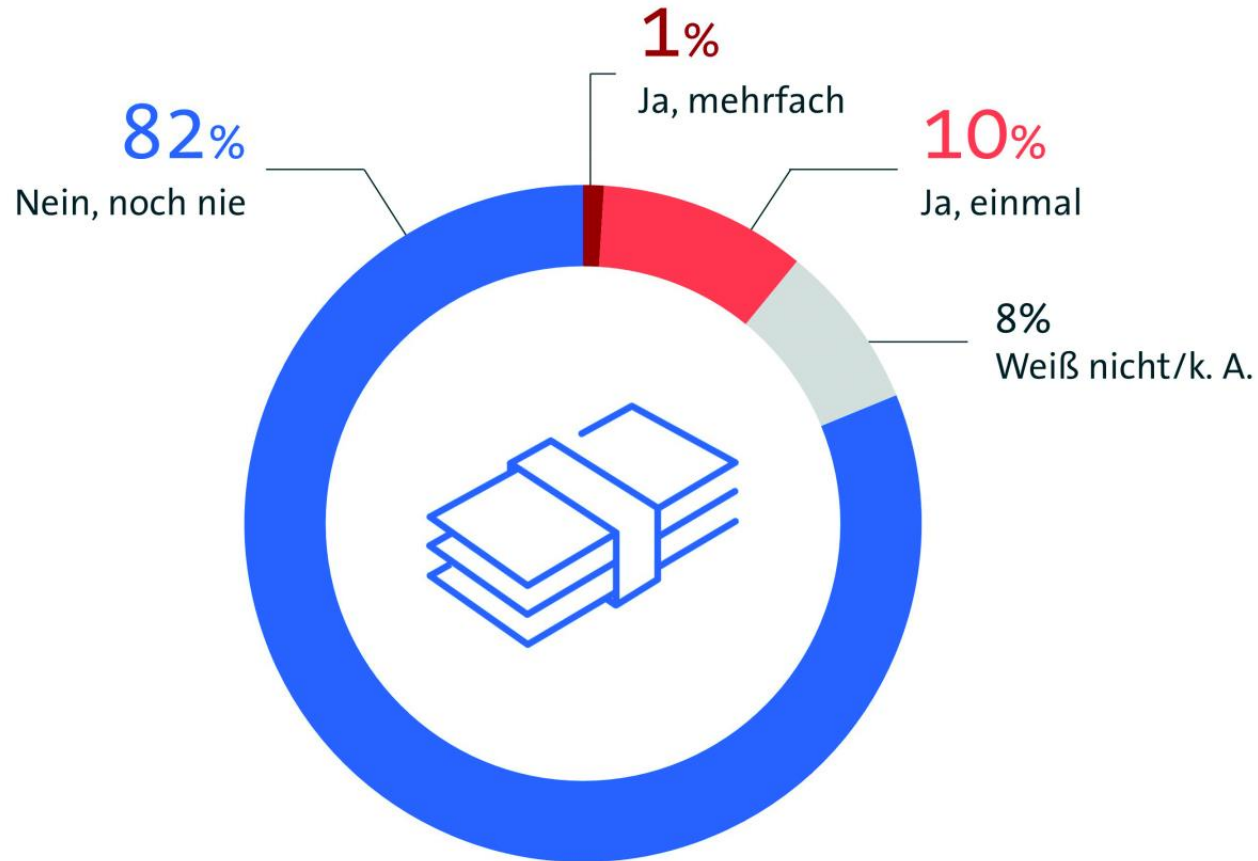
Umfrage

- Denken Sie, Sie würden zahlen?
 - Ja
 - Es kommt darauf an
 - Nein



Ransomware: Jedes neunte Opfer bezahlt Lösegeld

Haben Sie bei dem Ransomware-Angriff Lösegeld bezahlt?



Geschäftsbetrieb beeinträchtigt

Bei 4 von 10 Ransomware-Opfern (44 Prozent) kam es durch den Angriff zu Beeinträchtigungen im Geschäftsbetrieb. Im Durchschnitt dauerten diese rund 3 Tage.

Aber was kann man bei einem Vorfall tun?

Eine Lanze für Prävention

Eine gute Vorbereitung hilft auch bei einem Vorfall, Schäden zu begrenzen

- Kritische IT-Infrastruktur identifizieren – ohne welche IT geht es gar nicht?
- Sensibilisierte Mitarbeitende können große Schäden zumindest begrenzen!
- Erstellen Sie einen Notfallplan – schon eine Kontaktliste ist im Notfall eine große Hilfe!
- Fertigen Sie Datensicherungen an – Backups nach der 3-2-1-Regel sind krisensicher!

- Auf der Webseite der Transferstelle Cybersicherheit steht Informationsmaterial bereit

Das Wichtigste!

- Das Wichtigste beim IT-Sicherheitsvorfall: Holen Sie sich qualifizierte Unterstützung.
- Die Transferstelle entwickelt dazu zwei Werkzeuge:
 - Ein Werkzeug zur Selbsteinschätzung „Habe ich einen akuten IT-Sicherheitsvorfall“ hilft, die eigene Situation besser einzuschätzen.
 - Eine Plattform verweist auf bundesweite und regionale Unterstützungsangebote und vermittelt auf Wunsch eine passgenaue Dienstleistung zur Bewältigung des Vorfalls.

Assistent zur Selbsteinschätzung

Konzeptgrafiken

Plattform für Unterstützungsleistungen

Konzeptgrafiken

Plattform für Unterstützungsleistungen

Konzeptgrafiken

VIELEN DANK

Dr. Dirk Achenbach

dirk.achenbach@transferstelle-cybersicherheit.de