BVMW Unternehmerabend
Sicherheit im OnlineBanking

26.02.2024 in der
Raiffeisen-Volksbank Hermsdorfer Kreuz eG

29.02.2024 bei der
Thyotec IKS Service GmbH

Morgen kann kommen.
Wir machen den Weg frei.

Raiffeisen-Volksbank
Hermsdorfer Kreuz eG

Morgen kann kommen.
Wir machen den Weg frei.

OnlineBanking - Risiko Mensch

Maik Anders
Vorstandsmitglied
Raiffeisen-Volksbank Hermsdorfer Kreuz eG

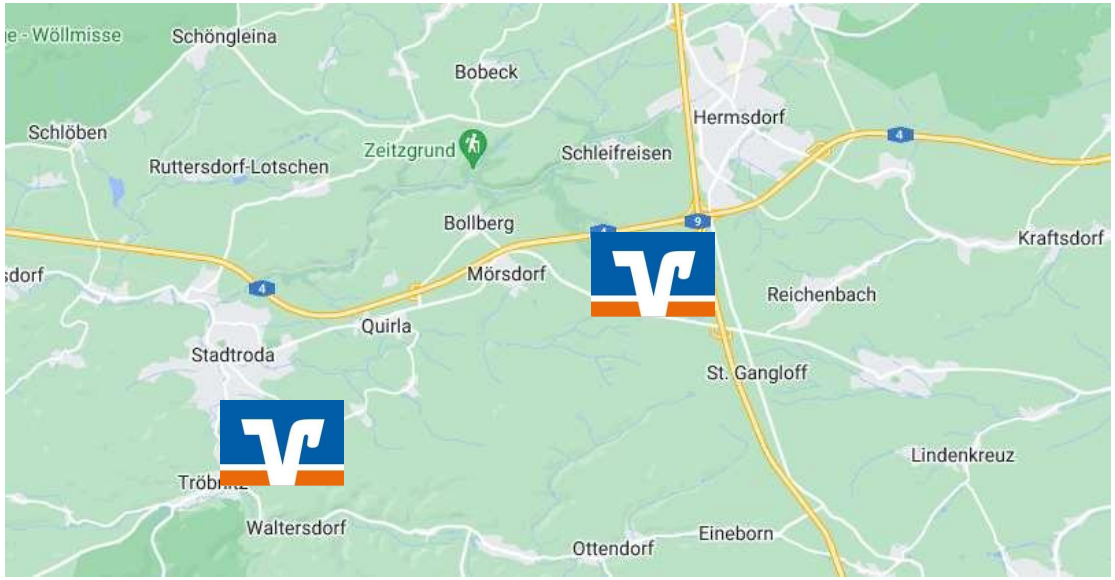
Raiffeisen-Volksbank
Hermsdorfer Kreuz eG

Morgen kann kommen.
Wir machen den Weg frei.

Verlässlicher Partner vor Ort

Regionalbank am Hermsdorfer Kreuz

- Standorte Stadtroda und Hermsdorf
- Einlagen- und Kreditgeschäft, Zahlungsverkehr
- Zusammenarbeit mit z. B. R+V Versicherung, VR-SmartFinanz
- OnlineBanking + App seit 2022 neu aufgesetzt + Beratungs-Tools



Raiffeisen-Volksbank Hermsdorfer Kreuz eG

Zum Aufwärmen …

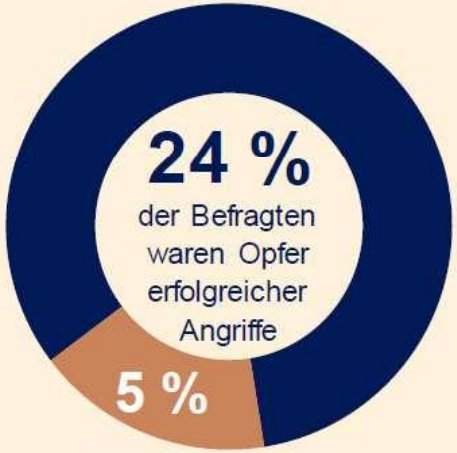
Sicheres OnlineBanking … Kleines Fundstück

Morgen kann kommen.
Wir machen den Weg frei.

Welches Risiko?

Jedes vierte Unternehmen bereits betroffen

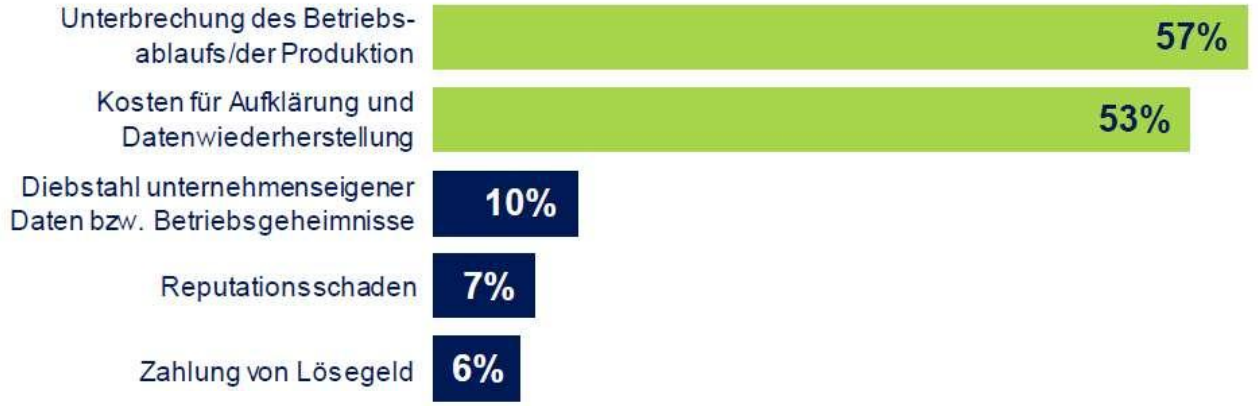
Wurde Ihr Unternehmen durch Cyberangriffe geschädigt?



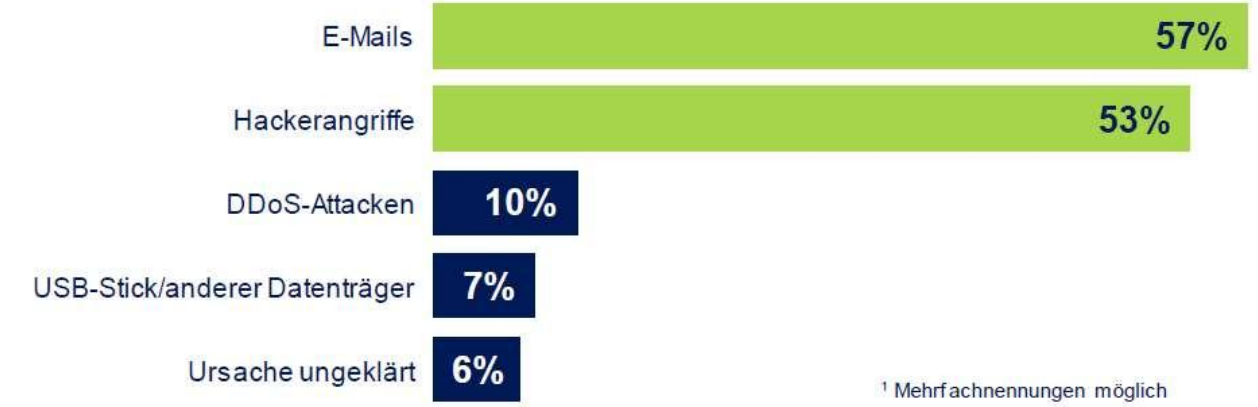
Quelle: Forsa-Umfrage „Cyberrisiken im Mittelstand"

Es gibt keine 100% Sicherheit!

Welche Schäden sind im Unternehmen durch den Cyberangriff entstanden?



Erfolgreiche Cyberangriffe erfolgten durch …[1]



[1] Mehrfachnennungen möglich

Morgen kann kommen.
Wir machen den Weg frei.

Passender technischer Zugang

- ohne Software
  - **FinTS - PIN/TAN Verfahren** - Browser / Banking-App
    - TAN erzeugen mit App SecureGo Plus (Smartphone)
    - TAN erzeugen mit TAN-Generator (+ Bankkarte)

- mit Software (VR-Networld-Software oder Profi cash)
  - **FinTS – Signatur (alt HBCI)** Stick/Kartenlesegerät+Karte
  - **EBICS – Signatur** Massenzahlungsverkehr

Morgen kann kommen.
Wir machen den Weg frei.

Regelung in der Firma?

- Wer hat alles Zugriff auf Passwörter/Hardware?
  - keine Weitergabe der Zugangsdaten
  - Aufbewahrung der Passwörter

- PC-Nutzer = den hinterlegten Bankvollmachten?
  - Idealerweise keine Abweichung
  - Jeder Nutzer eigenen Zugang

Morgen kann kommen.
Wir machen den Weg frei.

Mails/Webseiten mit Risiken

Mails:

- Per Mail Datenabfragen oder auch Geldanweisungen vom Chef?
  - Absender manipuliert? = Phishing
- „Link“ in Ordnung? Beispiel:
  - https://hermsdorfer-kreuz.de/-link2/**18748check.org**/h8
  - Trojanisches Pferd …z.B. Animierter Osterhase klicken

Ergebnis:

- Unbemerkt Passwörter und Daten ausspähen
- Zugriff aufs OnlineBanking
- Betriebsdaten werden gestohlen/gesperrt

Morgen kann kommen.
Wir machen den Weg frei.

Beispiele aus meinem Umfeld

- Zusatz-Überweisung Amazon
- Anruf von der „Bank“, sitzt im Auto, Auftragsfreigabe Gesichtsscan
- „Kunde“ ruft bei der Bank an … Firma Überweisung ?
- Zugangsdaten … Hacker ist schon im OnlineBanking … 1.Schritt
- Identitätsdiebstahl – Aufbewahrungsort der Zugangsdaten
- Anruf bei mir am 31.01. – Automatische Ansage…

Morgen kann kommen.
Wir machen den Weg frei.

Lösungsansätze

Vorbeugend …

- Viren- und Firewall-Programm (+Erkennung von Verhaltensmustern)
- Professionelle IT-Partner + Notfallordner (in Papierform)
- Aktion Test-Mail an MA - MA sensibilisieren
- Backup – mehrere zeitversetzt, getrennt vom System
- Separater abgehärteter Browser fürs OnlineBanking
- Cyberversicherung der R+V Versicherung

Morgen kann kommen.
Wir machen den Weg frei.

Lösungsansätze

Wenn es passiert ist …

- Netzwerk-Kabel ziehen, Wlan aus >> PC anlassen
- Viren- und Firewall-Programm ausführen
- Notfallordner in Papierform mit Ansprechp. + Anweisungen
- Technische Unterstützung und Anzeige Polizei
- **schnell** auf die Bank zugehen … Zahlung stoppen
- Schadenregulierung mit der R+V Versicherung

Morgen kann kommen.
Wir machen den Weg frei.

Links

kurzes Video zu den Umgang mit Links

→https://wiki.secuso.org/videos/nophish/Phishing-Links-2020-Deutsch-005_recode.mp4

Download - abgehärteter Browser - nur fürs OnlineBanking - (ggf. weitere Onlinebanking-Webseiten anderer Banken zufügen/erlauben)

→https://www.vrbank.de/banking-service/sicherheit/banking-browser-protect.html#parsys_linkbox

Sind Sie betroffen? Hier finden Sie es heraus.

Der Service „Havel Been Pwned?“ (Pwnedwird gesprochen wie „poned“) hat über 6 Milliarden Datensätze

aus mehr als 300 Datenlecke gesammelt. Wenn Sie überprüfen wollen, ob auch Ihre Mail-Adresse darunter ist,

geben Sie diese einfach in der entsprechenden Suchmaske ein, das Ergebnis wird sofort angezeigt.

→https://haveibeenpwned.com/

Das Hasso-Platter-Institut bietet den „HPI Identity LeakChecker“ an. Sie können anhand Ihrer E-Mail-Adresse prüfen,

ob die Adresse in Verbindung mit anderen persönlichen Daten wie Geburtsdatum oder Adresse im Internet offengelegt wurde

und missbraucht werden könnte. Anders als bei „Havel BeenPwned?“ erhalten Sie das Ergebnis per Mail.

→https://sec.hpi.de/ilc/

Vielen Dank für Ihre Aufmerksamkeit

Gemeinsam erfolgreich bleiben.

„Was einer allein nicht schafft,

das schaffen viele.“