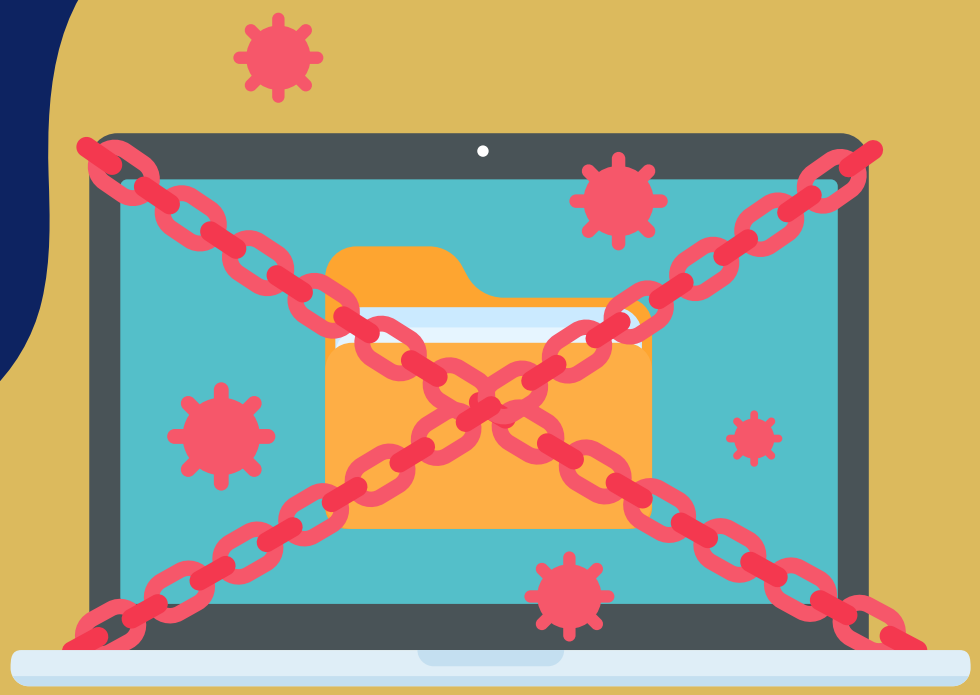

Jedes 2. Ransomware-Opfer zahlt Lösegeldforderung!

Und viele zahlen Lösegeld
in 7-stelliger Höhe...

Die Anzahl der Erpressungstrojaner war noch nie so hoch!

- 2 von 3 Befragten in Deutschland gaben an, einen Ransomware Angriff im vergangenen Jahr gehabt zu haben.

- ca. 42% der Ransomware-Opfer in Deutschland zahlen Lösegeld.

- Durchschnittlich lagen die Kosten einen Ransomware Angriffs i.H.v. **1,64 Mio.€** bei den befragten deutschen Unternehmen.

- Durchschnittlich zahlten deutsche Unternehmen **250.000€** Lösegeld.

Quelle: Sophos Whitepaper ‘The State of Ransomware 2022", April 2022

Nur 64 % der Unternehmen, die Lösegeld zahlten bekamen ihre Daten zurück!

Quelle: Sophos Whitepaper “The State of Ransomware 2022", April 2022

100 % IT-Sicherheit wird es wohl nie geben!

Wie stellen Unternehmen nun am Sinnvollsten sicher, dass der Geschäftsbetrieb nach einem (Ransomware-) Angriff möglichst schnell wieder aufgenommen werden kann?

→ **Stichwort: Systemwiederherstellung nach Totalausfall**

Was ist die beste Backup Strategie?

Entwicklung eines detaillierten Backup & Recovery Plans!

Hört sich leichter an als es ist bei der Komplexität heutiger Cybersecurity Infrastrukturen.

Hybride Systeme

Multicloud Systeme

IoT

Edge Computing

Folgende Punkte sollten bei der Entwicklung einer Backup & Recovery beachtet werden:

- Kategorisierung von unternehmenskritischen Anwendungen nach Wichtigkeit Dienste mit höchster Priorität sollten nach 15min wieder laufen.

- Kennzahlen bzgl. Datenverlusten & Ausfallzeiten wie z.B. RTO (Response Time Objective) und RPO (Response Point Objective) sollten definiert und ein konkreter Maßnahmenplan zur Erreichung der Ziele aufgestellt werden.

- Flexibilität & Anpassungsfähigkeit der Strategien sollten berücksichtigt werden.

- **CDP** (Continuous Data Protection)
- Es gibt CDP Lösungen, die Backup, Disaster Recovery und Cloud-Mobilität zusammenführen.

zu aller letzt heißt es:

Testen, testen, testen,

um Funktionalität der Abläufe auch nach neuen Konfigurationen im System gewährleisten und Ausfallzeiten prognostizieren zu können!!!