IT - Service 7: Das Weg-Werf-System

Dipl.-Ing. Gerhard Röncke

„Im Webcast der EY Private Lounge, einer Plattform zum Erfahrungsaustausch für Führungskräfte mittelständischer und Familienunternehmen, sprachen die Unternehmer Thomas Pilz und Kim-Eva Wempe über ihre Erfahrungen und Handlungsstrategien beim kriminellen Shutdown ihrer jeweiligen IT. Beide wurden 2019 Opfer eines massiven Cyberangriffs, in beiden Fällen forderten die Hacker Lösegeld für die Rückgabe der Daten.

„Man ist vom Bildschirm verschwunden“, erinnert sich Thomas Pilz an die Sekunden der Schockstarre, in denen sich herausstellte: Die Daten seines Unternehmens für Automatisierungstechnik waren über alle 42 Landesgesellschaften komplett verschlüsselt. Nichts ging mehr. …

Bei Juwelier Wempe begann das Szenario ähnlich. „Unsere Niederlassung im Frankfurter Flughafen öffnet um 6.30 Uhr als erste. Der Geschäftsführer saß vor schwarzen Bildschirmen, zwei Stunden später stand fest, dass wir Opfer eines Hackerangriffs wurden. Es war kein Arbeiten mehr möglich.“

(https://www.ey.com/de_de/unlocking-ambitions-of-private-businesses-and-their-owners/was-zwei-familienunternehmen-aus-cyberattacken-gelernt-haben, 20 April 2021)

„Die besten Windows Antivirus-Programme …“

Fast jede IT-Zeitschrift veröffentlicht unter dieser Überschrift mehr weniger fundierte Tests über die gängigen Antivirus-Programme und zertifiziert sie mit den Labeln Top, Sehr Gut, Gut, Befriedigend, usw..

Nichtsdestotrotz werden regelmäßig selbst kompetente Firmen wie Apple, Microsoft, Oracle, u.a. von Hackern infiltriert und um Daten und Programme erleichtert.

Alles was schiefgehen kann, wird auch schiefgehen.“ (Murphy)

Daher unser Vorschlag: Kümmern wir uns mehr um die Schadens-Minimierung und verringern unser Vertrauen in die Versprechen der Antivirus-Entwickler.

Zusammen mit unseren Kunden haben wir folgendes Konzept entwickelt:

- Trennung des Computers in einen öffentlichen und einen privaten Bereich.
- Abwicklung des externen Datenverkehrs über einen **Schutz-Container**.
- Umsetzung des Internet-Containers als **Weg-Werf-System**.

Sobald der Schadcode mit seinem Erpressungsversuch startet und die Dateien der virtuellen Maschine verschlüsselt, können Sie diese abbrechen, **löschen und durch eine gespeicherte „saubere“ Maschine ersetzen.**

Welche Vorbedingungen müssen für eine sinnvolle Entsorgung erfüllt sein, damit der Schaden minimiert wir?

Gerne senden wir Ihnen dazu unsere **PDF-Datei** **Internet-Schutz-Container** zu.

Ing.-Büro Röncke

Hasenheide 61
29633 Munster

Telefon: 05192 – 98 71 12
Fax: 05192 – 98 71 25

info@simulation-online.de
www. simulation-online.de