



© Pilz

Thomas Pilz
Geschäftsführender Gesellschafter
Pilz GmbH & Co. KG in Ostfildern

Falsch verstandenes Heldentum spielt Cyberangreifern in die Daten

Wenn Monitoringsysteme verdächtige Aktivitäten registrieren, ist es oft schon zu spät. Hacker sind findig. Und schnell in den Systemen einer Industrieorganisation. Oft und in der Regel sind dann sofort weltweit sämtliche Server- und Kommunikationssysteme durch diesen Angriff betroffen. Dazu nutzen die Täter etwa sogenannte Verschlüsselungstrojaner, also Ransomware, die umfassend attackiert und einen Teil an oder gar alle Daten verschlüsselt. Eine virale Ausbreitung ist Ziel der Angreifer. Bekannt ist dieses Angriffsmuster unter dem Namen Bitpaymer. Das alleinige Ziel: Lösegeld erpressen.

Was tun in einer solchen Lage? Held sein und den Kampf allein aufnehmen? Das tun viele Unternehmen, sie scheuen den Weg der Anzeige, noch mehr die Öffentlichkeit. Das Image des Unangreifbaren führt. Das ist aber falsch verstandenes Heldentum: Unverzüglich die Behörden verständigen, unverzüglich an die Öffentlichkeit gehen, das muss der Weg sein!

Weil: Cyberkriminalität braucht technisch versierte, speziell hierfür ausgebildete Experten für die Bekämpfung, braucht schnellen Zugriff auf verunreinigte IT-Infrastrukturen. Ansonsten lässt sich kaum Beweismaterial sichern. Das spielt Hackern

in die Karten, sprich Daten: Sie agieren – weil sie nicht zur Rechenschaft gezogen werden können, wo der Beweis fehlt – im Sinne des Wortes ungestraft weiter. Und Lösegeldforderungen zu trotzen, ist der richtige Schritt. Dies verhindert, dass Angreifer ein noch tieferes Wissen über ihre Opfer erlangen können, die IT-Infrastruktur eingeschlossen. Ganz abgesehen davon, dass eine Zahlung nicht Garant dafür ist, verschlüsselte Daten wiederzubekommen.

Die seit 2019 laufende, aktuelle Angriffswelle macht deutlich, dass Cyberkriminalität immer mehr zur ernststen Bedrohung für Wohlstand und Frieden in Deutschland wird. Umfragen des VDMA zeigen, dass bereits mehr als ein Drittel der vom Verband befragten Mitglieder von Produktionsausfällen berichten. Kapitalschäden verzeichnen bereits die Hälfte der befragten Unternehmen. Es liegt also an uns allen, dass diese Form der organisierten Kriminalität eingedämmt wird und wir – Unternehmen, Verbände, Behörden und Politik – noch stärker zusammenarbeiten, um unsere IT-Strukturen wo auch immer zu schützen. Heldentum richtig verstanden. Nur so kann Cyber-Kriminalität die Geschäftsgrundlage genommen werden.