

IT-Gefahren, die Sie kennen sollten

# Ransomware

*Ransomware ist eine bösartige Software, die Daten auf dem betroffenen Gerät verschlüsselt und den Benutzer dazu auffordert, ein Lösegeld zu zahlen, um wieder Zugriff auf die Daten zu erhalten. Die Verschlüsselung ist oft so stark, dass eine Entschlüsselung ohne den speziellen Schlüssel des Angreifers nahezu unmöglich ist.*

## ZIEL / SCHADEN

Ransomware zielt darauf ab, einen finanziellen Gewinn zu erzielen, indem sie den Zugriff auf die Daten eines Benutzers blockiert und ein Lösegeld für deren Freigabe verlangt. Die Schäden können erheblich sein, einschliesslich des Verlusts wichtiger Daten und finanzieller Verluste.

## INFEKTIONSWEG

Ransomware kann über verschiedene Methoden verbreitet werden, darunter Spam-E-Mails, infizierte Software-Downloads oder Exploit-Kits, die Sicherheitslücken ausnutzen.

## BEFREIUNG MÖGLICH?

In einigen Fällen können Entschlüsselungstools helfen, aber der sicherste Weg ist das Wiederherstellen der Daten aus einem Backup.

## ABWEHR

Halten Sie Ihr Betriebssystem und Ihre Software stets auf dem neuesten Stand, um Sicherheitslücken zu schliessen. Verwenden Sie eine zuverlässige Sicherheitssoftware und führen Sie regelmässige Backups Ihrer wichtigen Dateien durch.

## ANGRIFF - WAS NUN?

Zahlen Sie kein Lösegeld, da dies die Angreifer nur ermutigt. Wenden Sie sich an die Behörden und suchen Sie professionelle Hilfe und schliessen Sie eine Cyberversicherung ab.

