# Gefahr: Dreifache Erpressung

## Sichern Sie sich vor Ransomware ab!

Im ersten Quartal 2021 ist die Zahl von Ransomware-Attacken um 57 Prozent gestiegen. Im ersten Halbjahr 2021 sind doppelt so viele Unternehmen und Organisationen einem Angriff zum Opfer gefallen wie im ersten Halbjahr 2020. Und mit 1.000 von Ransomware betroffenen Unternehmen und Organisationen pro Woche ist ein neuer Höchststand erreicht. Fakt ist: Das Cybercrime-Geschäft floriert. Möglicherweise ist dafür auch eine neue Masche verantwortlich, die Cyberkriminelle für sich entdeckt haben: die dreifache Erpressung.

### So schützen Sie sich vor dreifacher Erpressung

- Zunächst schleusen Cyberkriminelle Ransomware in das Netzwerk ein. Dort werden Unternehmensdaten unbemerkt kopiert und auf die Server der Kriminellen weitergeleitet. Meist erfolgt so ein Datendiebstahl völlig unbemerkt. Danach werden sämtliche Unternehmensdaten
- Zu diesem Zeitpunkt stellen die Cyberkriminellen eine Lösegeldforderung, als Gegenleistung für die Entschlüsselung der Daten – und drohen mit einer Veröffentlichung der gestohlenen Daten, falls die Forderung nicht erfüllt werden sollte.
- NEU: Jetzt werden auch Lösegeldforderungen an Kunden, Geschäftspartner, Lieferanten und Patienten gerichtet; die Kontaktdaten dafür ziehen die Kriminellen aus den gestohlen Daten.

**Geben Sie Cyberkriminellen keine Chance, diese drei Hebel zu setzen – sichern Sie Ihr Netzwerk rechtzeitig ab!**

**Kontakt**

Lothringerstraße 53
52070 Aachen

Tel.: +49 (0) 241.515 767-10
Fax: +49 (0) 241.515 767-29

info@pronetix.de
www.pronetix.de

PRONETIX

## Druck auf Erpressungsopfer steigt

Die Angriffsopfer haben angesichts der dreifachen Erpressung auf jeden Fall noch einmal mehr zu verlieren. Denn: Die Datenschutzbehörden werden es sicher nicht gutheißen, wenn Drittopfer außerhalb des eigentlich betroffenen Netzwerks ebenfalls zu Schaden kommen. Für die Sicherheit der sensiblen Daten dieser Drittopfer sind Unternehmen, Organisationen und Co. nämlich verantwortlich. Es drohen letztlich hohe finanzielle Verluste – unter anderem durch die IT-Störung, ihre Behebung, mögliche Lösegeldzahlungen, Image-Verluste und eben Strafzahlungen wegen des Verstoßes gegen den Datenschutz.

## So schützen Sie sich vor dreifacher Erpressung

- Auch an freien Tagen ist Vorsicht geboten: Die meisten Ransomware-Attacken erfolgten 2020 am Wochenende. Möglicherweise sind Adressaten von Malware-Kampagnen dann weniger aufmerksam.
- Spielen Sie Sicherheitspatches sofort aus: Sobald Hersteller ein Sicherheitsupdate ausspielen, ist die Lücke offiziell bekannt – und Cyberkriminelle stürzen sich direkt darauf. Sicherheitspatches sollten daher immer direkt nach Erscheinen ausgespielt werden.
- Schulen Sie die Security Awareness: Cyberkriminellen gelingt es immer wieder, mit ihren Attacken Mitarbeitende so zu manipulieren, dass sie auf Ransomware-Attacken hereinzufallen. Die Schulung der Security Awareness hat daher eine Schlüsselfunktion.
- Nutzen Sie eine Anti-Ransomware-Lösung: Es gibt inzwischen spezielle Tools, die durch Ransomware ausgelöste Anomalien erkennen, Bei Auffälligkeiten schrillen direkt die Alarmglocken.
- Beobachten Sie Ihr Netzwerk: Die dreifache Erpressung braucht einige Vorbereitung und die Ransomware ist längst im System, bevor die eigentliche Erpressung beginnt. Daher sollte das Netzwerk regelmäßig auf eine Infektion überprüft werden.

## Wir sichern Ihr Unternehmen ab!

Auf Wunsch erarbeiten wir ein wasserdichtes IT-Sicherheitskonzept für Sie. Bausteine darin können die Untersuchung Ihres Netzwerks auf Schwachstellen mit einem IT-Sicherheitscheck, die Implementierung effizienter Sicherheitslösungen, ein regelmäßiges Patch-Management und sogar die Schulung Ihrer Mitarbeiter zur Security Awareness sein.

**Mit umfassenden Maßnahmen setzen wir Cybersicherheit für Sie um und verhindern die dreifachen Erpressung!**

**Kontakt**

Lothringerstraße 53
52070 Aachen

Tel.: +49 (0) 241.515 767-10
Fax: +49 (0) 241.515 767-29

info@pronetix.de
www.pronetix.de

PRONETIX