Attingo

# Den Cyber-Erpressern auf der Spur

**Professionelle Datenrettung kann bei Ransomware-Befall helfen.**

Zielten Online-Erpresser anfänglich noch vorwiegend per Gießkannen-Prinzip auf Privatanwender mit verhältnismäßig geringen Lösegeld-Forderungen ab, wird mittlerweile kaum noch etwas dem Zufall überlassen. Wie Datenretter Attingo anhand von Anfragen in den vergangenen Monaten beobachten musste, werden immer häufiger gezielte Angriffe durchgeführt, die sich primär gegen große, teils globale Unternehmen richten, bei denen sich zum Beispiel über kompromittierte VPN Gateways mit 0-Day-Lücken Zugang auf das gesamte Netzwerk verschafft wird. Professionelle Cyberkriminelle zielen mittlerweile auf lukrative Ziele, bedenkt man die finanziellen Schäden, die eine vollständig zum Erliegen kommende IT-Infrastruktur dieser Größenordnung mit sich bringen kann.

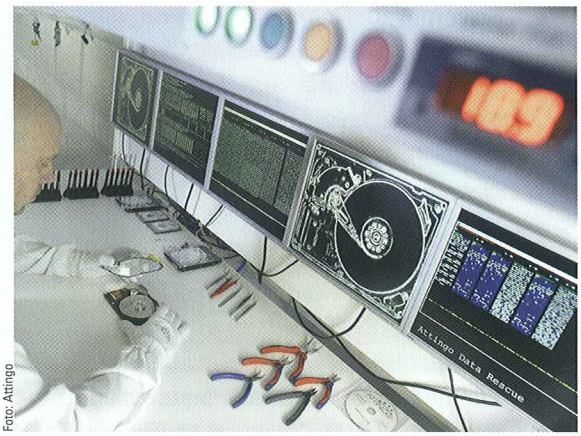


Foto: Attingo

*Für eine erfolgreiche Datenrettung bei verschlüsselten Daten ist eine Vielzahl von Faktoren entscheidend*

**Professionalisierung.** In nahezu allen Fällen solcher Ransomware-Attacken werden die Originaldaten verschlüsselt und die Backups auf Netzlaufwerken, Servern oder Tapes gelöscht bzw. überschrieben. „Wir haben zuletzt einen so fein abgestimmten Angriff erlebt, bei dem beim Kunden die Systemlaufwerke mit TrueCrypt Full Disk verschlüsselt wurden, da die Software ohnehin schon installiert war", erzählt Attingo-Geschäftsführer Nicolas Ehrschwendner.

Basierend auf diesen Erfahrungswerten hat der Datenretter Werkzeuge und Vorgehensweisen entwickelt, die in spezifischen Szenarien eine Datenrettung auch bei Ransomware-Verschlüsselung ermöglichen können. Für eine erfolgreiche Datenrettung bei verschlüsselten Daten ist eine Vielzahl von Faktoren maßgeblich entscheidend dafür, wie hoch die Chancen der Wiederherstellung der Daten sind und wie die Qualität des Ergebnisses ist (siehe Kasten).

**Königsweg Backup.** Was also tun, wenn die Unternehmensdaten plötzlich nicht mehr zugänglich sind und die Hacker eine „Lösegeldforderung" hinterlassen? Aus Sicht des Datenretters bestehen bei verschlüsselten Original-Daten Chancen bei (noch) unvollständig verschlüsselten Dateien – insbesondere bei Datenbanken, Archiven oder virtuellen Disk-Images. „Bessere Erfolge erzielen wir aber meist bei der (teils auch nur partiellen) Wiederherstellung von den gelöschten/vernichteten Backups", erklärt Ehrschwendner. „Hier besteht nur das Risiko, dass manche Angreifer so gewieft sind und die letzten Tage vor dem Platzen der Bombe bereits verschlüsselte Original-Daten sichern und somit das aktuellste Backup manchmal wertlos ist."

*Attingo*
*www.attingo.at*

## Entscheidende Faktoren für die Datenrettung bei Ransomware-Befall

- ***Um welche Ransomware handelt es sich?*** *Die eingesetzte Malware zu kennen ist entscheidend, um eine Einschätzung zu einer potenziellen Datenrettung abgeben zu können.*
- ***Wann wurde der Ransomware-Befall bemerkt?*** *Je eher der Cyber-Angriff bemerkt wurde, desto größer sind die Chancen einer Datenwiederherstellung.*
- ***Welche Daten wurden verschlüsselt?*** *Der Datentyp ist wie bei jeder Datenwiederherstellung ein entscheidender Faktor.*
- ***Gibt es eine Deadline von den Erpressern?*** *Die Analyse betroffener Server, NAS und Computer kann viel Zeit in Anspruch nehmen. Die Täter versuchen über die Ausübung entsprechenden Drucks eine Beauftragung von Datenrettungsdienstleistern zu unterbinden.*
- ***Was wurde bereits versucht, um Daten zu retten?*** *Erfahrungsgemäß wird in der Panik alles unternommen, um die Systeme wieder zum Laufen zu bekommen. Durch falsche Maßnahmen können die Chancen einer Datenrettung jedoch erheblich verringert werden.*
- ***Welche Systeme wurden befallen?*** *Welches Betriebssystem haben Sie im Einsatz, nutzen Sie Virtualisierungslösungen, gibt es eventuell alte Sicherungskopien?*