

Incident Response nach LockBit 5.0-Angriffen: Zwei Fälle aus Deutschland

24.02.2026, 16:53 | IT, New Media & Software

Pressemitteilung von: *Benjamin Bansal, B.A., LL.M.*



Cyberangriffe mit Ransomware gelten in vielen Unternehmen noch immer als beherrschbares Risiko. Zwei aktuelle Vorfälle aus Deutschland zeigen jedoch, wie schnell moderne Angriffsszenarien etablierte Schutz- und Wiederherstellungsmechanismen aushebeln können. In beiden Fällen waren nicht nur produktive Systeme betroffen, sondern auch die vorhandenen Backup-Infrastrukturen vollständig kompromittiert. Der operative Geschäftsbetrieb kam zum Erliegen.

LockBit 5.0: Wenn Backups keine Rettung mehr bieten

Im Mittelpunkt der Angriffe stand die Ransomware-Variante LockBit 5.0, die seit Anfang 2026 erneut verstärkt in Deutschland beobachtet wird. Innerhalb weniger Wochen wurden zwei mittelständische Industrieunternehmen Ziel hochkoordinierter Attacken: ein Holzverarbeitender Betrieb sowie ein Automobilzulieferer mit stark virtualisierter IT-Umgebung. In beiden Fällen zeigte sich ein Angriffsmuster, das Sicherheitsverantwortliche zunehmend vor neue Herausforderungen stellt. Die Angreifer beschränkten sich nicht auf die Verschlüsselung produktiver Server, sondern nahmen gezielt auch Backup-Systeme ins Visier. Für die betroffenen Unternehmen stellte sich dabei früh die zentrale Frage, ob sich die LockBit 5.0 Ransomware entschlüsseln lässt oder ob alternative Wiederherstellungswege notwendig werden. Beim ersten Unternehmen wurden zwei virtualisierte Server sowie die angebundenen Backup-Volumes gleichzeitig verschlüsselt. Beim Automobilzulieferer nutzten die Täter eine Schwachstelle in der Firewall, um parallel auf Produktions- und Backup-Infrastruktur zuzugreifen. Das Ergebnis war die vollständige Verschlüsselung sämtlicher virtueller Maschinen sowie von mehr als einem Terabyte geschäftskritischer Daten. In beiden Fällen stuften die internen IT-Teams die Lage zunächst als Totalausfall ein, zentrale Geschäftsprozesse kamen vollständig zum Stillstand.

Forensische Analyse statt klassischer Wiederherstellung

Die Wiederherstellung der Systeme erfolgte nicht über konventionelle Backup-Rücksicherungen. Stattdessen kam eine umfassende Incident-Response-Analyse zum Einsatz, die alle verfügbaren Datenstrukturen und Systemzustände einbezog. Ziel war es, verbliebene Wiederanlaufpunkte innerhalb der kompromittierten Umgebungen zu identifizieren. „In beiden Fällen zeigte sich, dass klassische Wiederherstellungsmechanismen nicht mehr griffen, weil die Angreifer mit LockBit 5.0 gezielt auch die Backup-Infrastruktur in den Angriff einbezogen hatten“, sagt ein Ransomware-Spezialist von Digital Recovery. „Die Wiederherstellung musste daher auf forensischer Ebene innerhalb der kompromittierten

Systeme ansetzen“, so Digital Recovery. Nach Angaben des eingesetzten Incident-Response-Teams wurden dabei forensische Methoden genutzt, die auch unter laufenden Ermittlungen durch Behörden sowie in Abstimmung mit Cyber-Versicherern eingesetzt werden können. In beiden Fällen gelang es, kritische Systemzustände direkt aus den verschlüsselten virtuellen Maschinen zu rekonstruieren und schrittweise wiederherzustellen.

Geschäftsbetrieb unter Auflagen wieder aufgenommen

Trotz der Schwere der LockBit 5.0-Angriffe konnten beide Unternehmen ihren Betrieb nach kurzer Zeit in einem stabilisierten Zustand wieder aufnehmen. Zentrale Geschäftsprozesse wurden priorisiert wiederhergestellt, während parallel forensische Untersuchungen sowie sicherheitstechnische Nacharbeiten liefen. Die Fälle verdeutlichen, dass moderne Ransomware-Angriffe zunehmend darauf abzielen, klassische Wiederherstellungsstrategien vollständig zu neutralisieren und Unternehmen unter maximalen Zeitdruck zu setzen.

Steigende Anforderungen an Notfallkonzepte durch LockBit 5.0

Die beobachteten LockBit-5.0-Angriffe unterstreichen den wachsenden Handlungsdruck für Unternehmen mit stark vernetzten und virtualisierten Infrastrukturen. Backup-Strategien allein reichen in vielen Szenarien nicht mehr aus, um einen schnellen Wiederanlauf zu gewährleisten. Gefordert sind resiliente Architekturen, zusätzliche Schutzmechanismen sowie klar definierte Incident-Response-Prozesse, die auch unter extremen Bedingungen greifen.

Mehr zum Thema Incident Response, Backup-Architektur und Datenrettung nach Ransomware-Attacken findet man unter www.digitalrecovery.com/de.

Impressum:

Digital Recovery PHD GmbH
W-Tec Haus 4
Heinz-Fangman-Str. 2-6
42287 Wuppertal
info@digitalrecovery.de
www.digitalrecovery.com/de

Digital Recovery PHD GmbH

Heinz-Fangman-Str. 2-6
42287 Wuppertal
Deutschland

www.digitalrecovery.com/de

Portrait

Digital Recovery ist ein international aktives Datenrettungs- und Cyber-Resilienz-Unternehmen, das sich seit über 25 Jahren auf die Wiederherstellung verlorener oder verschlüsselter Daten für Unternehmen spezialisiert hat – von einfachen Festplatten über RAID-, NAS- und Serversysteme bis hin zu komplexen Ransomware-Vorfällen. Mit proprietärer Technologie wie TRACER, 24/7-Notfall-Support und einem globalen Netzwerk von Experten bietet das Unternehmen schnelle, technisch fundierte Lösungen, um auch in kritischen IT-Notfällen Daten zu retten und Ausfallzeiten zu minimieren.

News-ID: 1304833 • Views: 463 (Stand: 11.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1304833/Incident-Response-nach-LockBit-5-0-Angriffen-Zwei-Faelle-aus-Deutschland.html>