07 Starten Sie die Wiederherstellung der Daten

Funktionierende Backups sind der Schlüssel zur Bewältigung eines Ransomware-Angriffs. Prüfen Sie unbedingt vor einer Wiederherstellung der Daten, ob die Backups nicht ebenfalls kompromittiert wurden. Können Sie keine Backups einspielen – da fehlerhaft, infiziert oder grundsätzlich nicht vorhanden -, kann vereinzelt mit viel Glück auf ein freies Entschlüsselungstool zurückgegriffen werden, z. B. von www.nomoreransom.org. Bleiben auch hier die Erfolge aus, besteht abschließend die Option, verschlüsselte Systeme für eine künftige Entschlüsselungsmöglichkeit isoliert aufzubewahren.

lda.bayern.de/cr07

08 Denken Sie an Strafanzeige und Meldung nach Art. 33 DS-GVO

Im Falle eines Ransomware-Angriffes ist fast immer davon auszugehen, dass mindestens ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Kommen Sie daher Ihrer Meldeverpflichtung nach Art. 33 DS-GVO nach und melden Sie den Sicherheitsvorfall über den Online-Service des BayLDA. Ein Ransomware-Angriff stellt zudem eine Straftat dar, welche bei der Zentralen Ansprechstelle für Cybercrime (ZAC) des Bayerischen Landeskriminalamts angezeigt werden kann, um Ermittlungen gegen die Angreifer aufzunehmen. Dieser Schritt ist bei Cybercrime-Delikten im Interesse aller Geschädigten zu empfehlen.

lda.bayern.de/cr08

Vorfälle behandeln

Schritt für Schritt reagieren

Cyberangriffe können jeden treffen. Ein wichtiger Bestandteil der Cyberprävention ist es daher, sich auf mögliche Attacken auf die IT-Infrastruktur einzustellen und entsprechende Vorbereitungen zu treffen. Denn wenn die Systeme erst einmal verschlüsselt sind, ist es zu spät. Nur wer überlegt und gezielt handelt, kann größeren Schaden verhindern und einen Super-GAU im eigenen IT-Betrieb vermeiden.

Die im Flyer enthaltenen Schritte dienen als Ansatzpunkte für Maßnahmen, wenn das eigene Netzwerk angegriffen wird und Systeme durch Ransomware verschlüsselt sind. Auf www.lda.bayern.de gibt es weitere hilfreiche Tipps, die insbesondere auch den Datenschutz in solchen Situationen im Blick behalten. Zudem finden Sie dort Links zu anderen Sicherheitsbehörden, die zu diesem Thema Veröffentlichungen anbieten.

Cyberprävention
Mehr Sicherheit durch Datenschutz
www.lda.bayern.de

Herausgeber

Bayerisches Landesamt für Datenschutzaufsicht
Cybersicherheit und technischer Datenschutz
Promenade 18
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Erste Cyberhilfe

Schnell und effektiv handeln

8+

Reaktion auf Ransomware

Strukturiertes Vorgehen zur Schadensminimierung bei Verschlüsselungsangriffen

01 Handeln Sie strukturiert und effektiv im Team

Auch wenn die Zeit drängt und schnelles Handeln erforderlich ist: Bei einer Infektion mit Ransomware ist es wichtig, überlegt zu agieren. Verschaffen Sie sich zunächst einen Überblick über die Situation. Richten Sie hierzu ein interdisziplinäres Krisenteam ein und dokumentieren Sie detailliert die Vorkommnisse sowie alle ergriffenen Reaktionsmaßnahmen. Vorhandene Notfallpläne auf Papier helfen Ihnen, einen kühlen Kopf zu bewahren und die richtigen Schritte einzuleiten. Sollte Ihnen zum Teil das Fachwissen fehlen oder Sie sich durch die Situation überfordert fühlen, ist es ratsam, einen spezialisierten Dienstleister einzuschalten.

lda.bayern.de/cr01

02 Lokalisieren und isolieren Sie die befallenen Systeme

Oft sind mehrere Clients und Server infiziert: Finden Sie heraus, welche Abschnitte und Systeme Ihres Netzwerkes konkret befallen sind. Führen Sie aktiv Virenscans durch, um Bedrohungen aufzuspüren. Protokolldateien helfen Ihnen, Auffälligkeiten im Netzwerk, bei DNS-Auflösungen oder in Firewalls zu erkennen. Sobald infizierte Systeme gefunden wurden, sollten diese schnellstmöglich isoliert und deren Kommunikationsmöglichkeiten (z. B. LAN, WLAN, Bluetooth, USB) getrennt werden. Prüfen Sie zudem alle Administratorenkonten hinsichtlich Legitimität und Kompromittierung, um eine weitere Ausbreitung der Ransomware zu verhindern.

lda.bayern.de/cr02

03 Suchen und schließen Sie das Einfallstor der Cyberattacke

Um Ihre Systeme vor der akuten Bedrohung zu schützen, ist es wichtig, die Ursache des Angriffs schnellstmöglich aufzuspüren. Die häufigsten Einfallstore bei Ransomware-Attacken sind erfolgreiche Phishing-Kampagnen oder die Ausnutzung bestehender Sicherheitslücken auf Grund veralteter Patch-Stände. Suchen Sie deshalb nach ausgenutzten Schwachstellen und vorhandenen Angriffspunkten. Eine später notwendige Datenwiederherstellung und die Wiederaufnahme des Betriebs können nur auf gehärteten Systemen sicher ablaufen, bei denen das Einfallstor der Cyberattacke geschlossen wurde.

lda.bayern.de/cr03

04 Bestimmen Sie die Ransomware-Variante

Finden Sie anhand der Lösegeldforderung, der Dateiendung der verschlüsselten Daten oder mit Hilfe von seriösen Online-Diensten heraus, um welchen Ransomware-Typ es sich handelt. Danach können Sie prüfen: Gibt es freie Entschlüsselungstools? Wie gehen die Täter im Regelfall vor? Welche möglichen Konsequenzen drohen (z. B. Veröffentlichung der abgezogenen Daten auf einer Leak-Page im Darknet)? So können Sie das Ausmaß besser einschätzen und zielgerichtet auf den Angriff reagieren. Vorsicht: Eine Kontaktaufnahme oder gar Zahlung des Lösegeldes an die Angreifer birgt weitere Gefahren und sollte vermieden werden.

lda.bayern.de/cr04

05 Bewerten Sie das Risiko für die betroffenen Personen

Nachdem Sie sich ein erstes Bild vom Schadensausmaß machen konnten, ist es Ihnen möglich abzuschätzen, welche personenbezogenen Daten von dem Vorfall betroffen sind. Bei Ransomware ist es mittlerweile sehr wahrscheinlich, dass die Daten vor der Verschlüsselung auch – zumindest teilweise – ausgeleitet wurden. Eine vorläufige Risikoeinschätzung für die betroffenen Personen sollte somit frühzeitig erfolgen, um gerade bei einem drohenden hohen Risiko angemessen zu reagieren. Denken Sie zudem an die interne Kommunikation gegenüber Ihren Beschäftigten, die vom Vorfall in unterschiedlichem Ausmaß betroffen sein können.

lda.bayern.de/cr05

06 Setzen Sie die infizierten Systeme neu auf

In der Regel hilft bei einem Befall mit Ransomware nur das Neuaufsetzen der betroffenen Systeme, da eine Bereinigung von Schadcode nicht oder nur sehr schwer möglich ist. Zudem könnten mögliche Backdoors ansonsten schnell übersehen werden. Alle neuaufgesetzen Systeme, die wieder in das Netzwerk integriert werden sollen, sind mit aktuellen Sicherheitsupdates zu versorgen. Ein besonderes Augenmerk ist dabei auf das Active Directory zu richten: Denken Sie daran, Administratoren-Passwörter zu ändern und das AD zu säubern. Je nach Schadensausmaß kann auch das Neuaufsetzen des kompletten AD notwendig sein.

lda.bayern.de/cr06