Gegen Ransomware: Checkliste Datensicherung

Version vom 02.11.2023, Autor: Mark Semmler GmbH (https://www.mark-semmler.de)

Disclaimer:

Die Inhalte dieses Dokuments wurden nach bestem Wissen und Kenntnisstand zusammengestellt und unterliegen einer Qualitätskontrolle. Die Komplexität und der ständige Wandel der Materie machen es jedoch erforderlich, Haftung und Gewähr auszuschließen, sofern nicht grobe Fahrlässigkeit oder Vorsatz vorliegen:

- Die vorliegenden Inhalte sind unverbindlich.
- Es kann keine Verantwortung für Schäden übernommen werden, die durch das Vertrauen auf Inhalte der Materialien oder durch anderen Gebrauch entstehen.

Die neueste Version dieses Papiers finden Sie hier:
https://www.mark-semmler.de/media/checkliste-datensicherung.pdf

Fehler, Verbesserungen, Anregungen und Kritik:
Geben uns Feedback z. B. über das Kontaktformular https://www.mark-semmler.de/kontakt.

Gegen Ransomware: Checkliste Datensicherung

– Seien Sie vorbereitet. –

Was ist Ransomware?

Ransomware (dt: Erpressungssoftware) ist Schadsoftware die Daten verschlüsselt, damit anschließend für deren Entschlüsselung hohe Lösegelder erpresst werden können. Sie wird mittlerweile von mehr als 100 professionell agierenden Tätergruppen eingesetzt und hinterlässt in jeder betroffenen IT eine Spur der Verwüstung: Ransomware legt innerhalb von Stunden Unternehmen lahm und verursacht massive, oft sogar existenzbedrohende Schäden.

Bis die Daten nach einem Ransomware-Vorfall wieder restauriert sind (falls dies überhaupt noch möglich ist) und die Schadsoftware wieder aus dem Netzwerk entfernt worden ist, bleibt das betroffene Unternehmen gelähmt – häufig fallen zentrale Geschäftsprozesse bis zu mehreren Wochen lang aus: keine Produktion, keine Verwaltung, keine Kommunikation; Lieferketten werden gerissen und wichtige Kunden, Geldgeber und Mitarbeiter verlieren ihr Vertrauen in das betroffene Unternehmen.

Weil (zu) viele Betroffene keinen anderen Ausweg mehr sehen als zu zahlen, verdienen die skrupellose Cyber-Kriminelle Unsummen, die von ihnen zum Teil wieder in neue Angriffswellen und in die Verbesserung der Angriffe investiert werden. Deshalb besteht eine anhaltend hohe Gefährdungslage. Jedes Unternehmen steht im Visier der Kriminellen – egal ob klein, mittel oder groß.

So viel steht fest: Ransomware ist eine reale Gefahr für jedes Unternehmen.

Wie werden Sie angegriffen?

Die Kriminellen führen Angriffswellen gegen möglichst viele Unternehmen durch und verwenden dabei Methoden, die seit Jahren bekannt aber leider viel zu häufig erfolgreich sind: E-Mails mit bösartigen Anhängen, Erraten von Passwörtern und das Ausnutzen wohl bekannter Sicherheitslücken, wenn verwundbare IT-Systeme im Internet exponiert sind führen zur Übernehme des ersten Rechners in der attackierten IT-Infrastruktur.

Die Gangster verwenden den ersten infizierten Computer als Sprungbrett für Angriffe gegen das restliche Unternehmensnetz: sie schlüpfen mit Hilfe professioneller Angriffswerkzeuge in die Rolle eines Administrators und übernehmen zentrale Computer (ihre Server). Dort angekommen sabotieren sie die Datensicherung, löschen Backups und deaktivieren im gesamten Netzwerk den Antivirus.

Damit sind Ihre Daten schutzlos den Gangstern ausgeliefert. Die Angreifer kopieren Ihre Unternehmensdaten, verteilen Ransomware auf alle Computer Ihres Netzwerks und verschlüsseln Ihren gesamten Datenbestend in einer konzertierten Aktion.

Was sollten Sie tun?

Die Angriffe der Gangster sind – wie oben erwähnt – wohl bekannt und lassen sich eigentlich zuverlässig abwehren. Hierzu ist es notwendig, dass einige wenige grundlegende Hausaufgaben gemacht werden, die für eine solide Informationsverarbeitung eigentlich selbstverständlich sein sollten. Dieses Dokument kann die entsprechenden Aufgaben nicht komplett aufzeigen – hierfür gibt es viele Leitfäden und Richtlinien, die speziell für mittlere, kleine und Kleinstunternehmen erstellt wurden und z. T. kostenfrei verfügbar sind.

Die mit Abstand wichtigste Sicherheitsmaßnahme stellen wir Ihnen jedoch hier vor: eine Datensicherung, die den Namen „DatenSICHERung“ auch wirklich verdient.

Auf der nächsten Seite haben wir Ihnen deshalb einige grundlegenden Anforderungen auf den Punkt gebracht und als einfache Checkliste aufgeführt. Beantworten Sie sich selbst die 12 Fragen und diskutieren sie diese z. B. mit Ihrem Administrator und/oder Ihrem Systemhaus.

Wenn Sie eine oder sogar mehrere Fragen mit einem „NEIN“ beantworten müssen besteht akuter Handlungsbedarf. Überarbeiten Sie in diesem Falle Ihre Datensicherung zeitnah.

Wenn Sie von einem Systemhaus betreut werden: Lassen Sie sich schriftlich bestätigen, dass Ihre Datensicherung die aufgeführten Anforderungen erfüllt. Akzeptieren Sie kein einziges „NEIN“ in der Checkliste – egal wie die Begründung lautet.

Checkliste für Ihre Datensicherung

– Jedes „NEIN“ bedeutet: Es besteht Handlungsbedarf. –

Speicherorte: Wo sind die wichtigsten Daten?

JA	NEIN	
☐	☐	Es wurde analysiert, welche Programme für den Geschäftsbetrieb wichtig sind und wo diese ihre Daten ablegen – die Speicherorte der wichtigen Applikationen sind bekannt.
☐	☐	Die Geschäftsführung hat verbindlich geregelt, wo die Mitarbeiter ihre Daten ablegen müssen – die Speicherorte für die Daten der Mitarbeiter sind festgelegt.

Strategie

JA	NEIN	
☐	☐	Im Zuge der Datensicherung werden alle Speicherorte der wichtigen Applikationen und alle Speicherorte der Mitarbeiter (also alle wichtigen Daten des Unternehmens) gesichert.
☐	☐	Für jeden Speicherort wurde von der Geschäftsleitung festgelegt, in welchem Rhythmus er gesichert werden muss, damit im Falle eines Falles dem Unternehmen kein wesentlicher Datenverlust entsteht.
☐	☐	Die Datensicherung setzt das Mehr-Generationen-Prinzip um. Es gibt z. B. zusätzliche Wochen-, Monats- und Jahressicherungen, um bei Bedarf auf mehrere Versionen der gesicherten Daten zurückgreifen zu können.
☐	☐	Für die Datensicherung werden mehrere Medien eingesetzt. Dabei ist sichergestellt, dass der Ausfall eines Mediums nicht zum Verlust von wesentlichen Teilen der gesicherten Daten führt.
☐	☐	Die Datensicherungen werden an mehr als einem Standort gelagert, damit die gesicherten Daten auch bei einem größeren Schadensereignis verfügbar bleiben.

(IT-)Infrastruktur

JA	NEIN	
☐	☐	Die Geschäftsführung hat eine(n) MitarbeiterIn benannt, der/die für die Datensicherung verantwortlich ist. Er/sie kontrolliert, dass die Datensicherung ordnungsgemäß durchgeführt wird.
☐	☐	Der Netzwerkverkehr von und zu den für die Datensicherung eingesetzten IT-Systemen ist auf das für die Funktionsfähigkeit absolut notwendige Minimum beschränkt (die Backup-Systeme sind vom restlichen Unternehmensnetz möglichst umfassend getrennt bzw. komplett gekapselt).
☐	☐	Sämtliche administrativen Zugänge der für die Datensicherung eingesetzten IT-Systeme werden unabhängig von der restlichen IT verwaltet (es sind so genannte „lokale“ Konten) und sie verfügen über eigene, exklusive Authentifizierungsmerkmale.

Wiederanlauf

JA	NEIN	
☐	☐	Für jeden Speicherort gibt es einen Wiederanlaufplan (Kochrezept), der bei einer Störung oder einem Ausfall die Wiederherstellung der dort gespeicherten Informationen sicherstellt.
☐	☐	Die Wiederanlaufpläne werden jährlich und nach jeder Aktualisierung getestet, indem einer der gesicherten Speicherorte nach dem Zufallsprinzip gesichert und testweise (z. B. in einer Testumgebung oder auf einem ausgemusterten IT-System) wiederhergestellt wird.