Baden-Württemberg

LANDESKRIMINALAMT

ZENTRALE ANSPRECHSTELLE CYBERCRIME
TELEFON 0711 5401-2444, FAX 0711 5401-2505
E-MAIL CYBERCRIME@POLIZEI.BWL.DE, INTERNET WWW.LKA-BW.DE/ZAC

Handlungsempfehlungen zur Ransomware

26. Mai 2021

Ransomware sind Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder verhindern und nur gegen Zahlung eines Lösegeldes wieder freigeben. Hierfür verwenden die Cyber-Kriminellen so genannte **Verschlüsselungstrojaner**. Ransomware-Attacken sind eine alltägliche Bedrohung für alle Unternehmen und öffentliche Einrichtungen. Sie können zu **massiven Beeinträchtigungen des Geschäftsbetriebes und hohen wirtschaftlichen Schäden** führen[1]. Die Umsetzung der polizeilich empfohlenen Maßnahmen bedarf einer konkreten Einzelfallprüfung.

Präventionsempfehlungen:

- Binden Sie sich an einen spezialisierten **IT-Vertragsdienstleister**, den Sie in einer Cyber-Krisenlage alarmieren können.
- Erstellen Sie einen **IT-Notfallplan (Checkliste)** mit abzuarbeitenden Stichpunkten und allen relevanten Kontaktdaten. Stellen Sie die Checkliste auch in ausgedruckter Form allen zuständigen Beschäftigten zur Verfügung. Üben Sie die Umsetzung mit Ihrem Team.
- Richten Sie mehrstufige Backup-Ebenen Ihrer Sicherheitskopien ein. Ein durchgehend im Netzwerk betriebenes Backup kann ebenfalls vom Angriff betroffen sein und verschlüsselt werden. Erstellen Sie deswegen regelmäßig aktuelle **Offside**-Backups (beispielsweise Bandlaufwerke, externe Datenträger, unter bestimmten Umständen auch Cloud[2]) und überprüfen Sie deren Integrität und Wiederherstellbarkeit. **Üben Sie die Wiederherstellung des Netzwerkes und der Daten.**

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.html

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf und https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf

- Prüfen Sie, ob das Remote Desktop Protocol (RDP) oder andere Fernzugriffsdienste aktiviert sind und ob Sie diese zwingend benötigen[3]. Deaktivieren Sie diese, falls Sie auf die Funktion verzichten können. Die Konfigurationseinstellungen sollten von Fachkräften vorgenommen werden.
- Sichern Sie alle Dienste für Fernzugriffe unbedingt mittels **Zwei-Faktor-Authentisierung** und kontrolliertem VPN-Zugriff ab[4]. Dies gilt auch für die Fernwartungszugriffe Ihres eigenen IT-Dienstleisters.
- Deaktivieren Sie mittels administrativer Gruppenrichtlinien die Ausführbarkeit von **Makro**-Elementen in Office-Dokumenten aus externen Quellen oder erlauben Sie deren Ausführung erst nach Prüfung und Bestätigung durch IT-Fachkräfte.[5]
- **Trennen Sie die Netzwerksegmente** (Office- und Produktivnetzwerk) und sichern Sie auch die internen Segmente mit separaten Firewall-Regeln und eindeutiger User-Authentisierung. Richten Sie im Netzwerk „Pufferzonen“ (DMZ)[6] ein.
- Deinstallieren Sie nicht benötigte Software und führen Sie **regelmäßige Updates** für die eingesetzten Remote-Lösungen, Software, Hardware und Betriebssysteme durch. Ein zentrales Patch-Management kann hierbei hilfreich sein.[7]
- Gehen sie restriktiv mit der Vergabe von Benutzerrechten um. Nur ausgewählte und fachkundige Personen sollten Administrationsrechte erhalten. Vergeben Sie **ausschließlich Leserechte** auf bestimmte Dateien und Verzeichnisse, sofern auf Schreib- und Änderungsrechte nicht nötig sind.
- Verwenden Sie moderne Dienste zur **Erkennung von abweichenden Verhaltensmustern im Netzwerk**. [8] Gewährleisten Sie auch die regelmäßige manuelle Prüfung abweichenden Verhaltens, beispielweise atypische IP-Adressen und Zugriffszeiten oder ungewöhnliche Datentransfers.

[3] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.pdf
[4] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf (Punkt 3)
[5] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_135.pdf
[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.pdf (Seite 3)
[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.pdf
[8] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.pdf

- Schützen Sie alle Benutzerkonten mit starken Passwörtern und erhöhen Sie die Sicherheit im Idealfall durch eine Zwei-Faktor-Authentisierung. Dies gilt ebenso für Zugriffsmöglichkeiten auf verwendete Firewalls.
- Nutzen Sie Application-Whitelisting, um die Ausführung unerwünschter Programme zu verhindern. Blockieren Sie die Ausführbarkeit aller nichtautorisierten Dateien durch Anwenderinnen und Anwender.
- Blockieren Sie Zugriffe von und auf das „Onion"-Netzwerk, einschlägige Domains und IP-Adressen.
- Scannen Sie eingehende sowie ausgehende E-Mails auf Schadsoftware und entfernen Sie ausführbare Dateien.
- Verhindern Sie die Ausführung aktiver Inhalte in E-Mails, PDF- und Office-Dokumenten.
- Gewährleisten Sie die Sichtbarkeit der vollständigen Absender-E-Mail-Adresse für die E-Mail-Empfänger in Ihrer Institution. Allen Anwenderinnen und Anwendern sollten Dateiendungen standardmäßig angezeigt werden.
- Nutzen Sie für die jegliches E-Mail-Kommunikation digitale Zertifikate und Signaturen zur Verifizierung des Absenders. Damit verhindern Sie Manipulationen von Nachrichten.[9]
- Nutzen Sie die Möglichkeit der Virtualisierung bestimmter Softwareprodukte. Nutzen Sie beispielweise eine „Sandbox".
- Prüfen Sie die Ablage geschäftskritischer Daten. Speichern Sie diese gegebenenfalls verschlüsselt und in getrennten Netzwerken.
- Beachten Sie die Einrichtungsempfehlungen für Arbeitsplätze im Home-Office[10]. Setzen Sie ein „Mobile Device Management" für Ihre Mitarbeiter um[11].
- Führen Sie regelmäßige Tests auf Schwachstellen Ihrer Systeme durch.
- Überprüfen Sie mit einem Virenschutz in regelmäßigen Abständen Ihre Systeme. Häufig wird die Schadsoftware erst zu einem späteren Zeitpunkt durch aktualisierte Virensignaturen erkannt. Aktualisieren Sie ihre Schutzsoftware mindestens einmal täglich.

[9] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html; Anleitung zur Nutzung von S/MIME: https://www.ca.kit.edu/img/SMIME-Anleitung.pdf

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf

Verhaltensprävention für Mitarbeiterinnen und Mitarbeiter:

Informieren Sie in Form von Mitarbeiterschulungen oder Awareness-Kampagnen über die Gefahren und Infektionsursachen von Ransomware. Mit präparierten E-Mails können Sie den Sensibilisierungsgrad der Beschäftigten überprüfen.

Verhaltensempfehlung für Mitarbeiterinnen und Mitarbeiter:

- Prüfen Sie bei eingehenden E-Mails die Absenderadresse auf Authentizität und den Inhalt auf Schlüssigkeit.
- Öffnen Sie keine verdächtigen Dateien und folgen Sie keinen unbekannten Links, die Sie per E-Mail erhalten haben.
- Halten Sie im Zweifel Rücksprache mit den IT-Ansprechpartnerinnen und -partner Ihres Unternehmens und melden Sie Auffälligkeiten.

Maßnahmen nach einer Infektion[12]:

- Greifen Sie auf den vorhandenen IT-Notfallplan zurück.
- Kontaktieren Sie Ihren IT-Dienstleister.
- Trennen Sie unverzüglich externe und interne Netzwerkverbindungen.
- Schalten Sie relevante Rechner und Server umgehend aus, um die Verschlüsselung weiterer Daten zu verhindern.
- Isolieren Sie Backups, so dass diese nicht ebenfalls verschlüsselt werden.
- Sichern Sie relevante Dateien, die Aufschluss über den Infektionshergang geben können. Hierzu zählen beispielsweise Logfile-Protokolldaten und verdächtige E-Mails.
- Ändern Sie sämtliche Benutzer- und Netzwerkkennwörter, sofern diese durch den Vorfall kompromittiert sein könnten.
- Erstatten Sie Strafanzeige bei der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg.

[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

Zentrale Ansprechstelle Cybercrime (ZAC):

Die ZAC dient als zentraler Ansprechpartner der Polizei für die Wirtschaft und Behörden von Baden-Württemberg in allen Belangen des Themenfeldes Cybercrime.

Erreichbarkeit der ZAC:
Telefon: +49 (0)711 5401 2444
E-Mail: cybercrime@polizei.bwl.de

Informationen:

- Ransomware - Bedrohungslage, Prävention & Reaktion
  https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

- Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime der Länder und des Bundes
  http://www.polizei.de/zac