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 gegen Ransomware

26.05.2022

Ransomware ist eine tägliche Bedrohung für die IT-Systeme von Unternehmen und Institutionen und kann zu massiven Beeinträchtigungen des Geschäftsbetriebes, Betriebsausfällen und hohen wirtschaftlichen Schäden führen.[1] Die Cyber-Kriminellen greifen sowohl Kleinbetriebe als auch Großunternehmen an, oftmals am Wochenende oder vor Feiertagen.
Als Ransomware wird ein Schadprogramm bezeichnet, das Daten auf IT-Systemen verschlüsselt und somit unbenutzbar macht. Für die Freigabe dieser Daten fordern die Kriminellen die Zahlung eines Lösegeldes. Häufig spähen sie zudem Daten aus und drohen, diese zu veröffentlichen, falls die Betroffenen kein Lösegeld zahlen.

Das Landeskriminalamt hat die Verschlüsselungsangriffe umfassend analysiert und Angriffsmuster sowie empfehlenswerte Sofortmaßnahmen zusammengefasst. Die folgenden Empfehlungen zeigen auf, wie Sie den Schaden begrenzen können und welche Schwachstellen am häufigsten genutzt werden. Das Dokument richtet sich sowohl an Führungskräfte kleiner und mittelständischer Unternehmen in Baden-Württemberg mit Microsoft-Systemen als auch an IT-Fachkräfte und IT-Dienstleister.

Welche Maßnahmen sind besonders wichtig?

Die vorgeschlagenen Maßnahmen stärken Ihre IT-Sicherheit. Absolute Sicherheit ist jedoch nicht garantiert. Bedenken Sie, dass trotz Sicherungsmaßnahmen ein erfolgreicher Angriff auf Ihr Netzwerk und Ihre Daten geschehen kann. Beachten Sie unbedingt sämtliche technischen und organisatorischen Empfehlungen zum Thema **Sicherheitskopien**. Üben Sie die **Wiederherstellung** des Netzwerks und der Datenbanken. Wichtig ist ein **IT-Notfallplan**, arbeiten Sie hierbei mit einer Checkliste. Bereiten Sie die Aufrechterhaltung der wichtigsten Geschäftsbereiche beim Ausfall der IT vor und üben Sie die praktische Umsetzung der Checkliste.

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

Wie gehen die Angreifer vor?

Die Polizei hat vier häufige Angriffswege festgestellt, denen jeweils mit technischen Gegenmaßnahmen (ab Seite 5) begegnet werden kann:

1. Die Täter greifen veraltete Rechner, Server, Software und Internetdienste an. Veraltet sind Systeme und Software, die nicht regelmäßig Sicherheits-Updates erhalten.
2. Phishing-Gefahr: Kriminelle spähen Zugangsdaten und Passwörter für Fernzugriffsdienste aus und greifen unberechtigt auf IT-Netzwerke zu.
3. Fehlerhaft konfigurierte Rechner, Server, Router, Firewalls oder Fernzugriffsdienste ermöglichen unberechtigte Zugriffe.
4. Kriminelle versenden Schadsoftware per E-Mail oder bieten über Links den Download solcher Dateien an. Hierbei handelt es sich oftmals um Office-Dokumente, deren Schadenspotenzial nicht ersichtlich ist. Mit dem Aktivieren der Dateien startet die Schadsoftware.

Erstmaßnahmen nach einem Angriff

- Greifen Sie auf die Checkliste zurück.
- Dokumentieren Sie alle Maßnahmen.
- Kontaktieren Sie Ihren IT-Dienstleister.
- Trennen Sie unverzüglich externe und interne Netzwerkverbindungen, insbesondere die Anbindung der kritischen Netzwerkbereiche.
- Isolieren Sie Backups, so dass diese nicht ebenfalls verschlüsselt werden.
- Schalten Sie noch nicht betroffene Rechner umgehend aus, um die Verschlüsselung weiterer Daten zu verhindern. Schalten Sie bereits verschlüsselte Rechner und Server nicht aus. Virtuelle Maschinen sollten angehalten und nicht heruntergefahren werden.
- Ändern Sie die Passwörter sämtlicher Admin-/Benutzer-Konten. Verwenden Sie hierfür einen geprüften und nicht betroffenen Rechner.
- Archivieren Sie festgestellte verdächtige Dateien und E-Mails.
- Sichern Sie erreichbare Protokolldaten und stellen Sie diese Ihrem IT-Dienstleister und der Polizei zur Verfügung. Autorisieren Sie Ihren Dienstleister, Daten und Informationen an die Polizei weiterzugeben.

- Erstatten Sie Strafanzeige bei der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg (Kontaktdaten siehe letzte Seite).
- Prüfen Sie Meldeverpflichtungen gegenüber der Datenschutzbehörde.[2]

Organisatorische Empfehlungen

- Informieren Sie sich im Vorfeld über IT-Dienstleister mit dem Schwerpunkt Forensik. Die Möglichkeit der Alarmierung eines Dienstleisters sichern Sie sich mit einem Rahmenvertrag. Der Vertragsdienstleister unterstützt Sie bei der Bewältigung künftiger IT-Krisenlagen.
- Erstellen Sie eine Checkliste mit personellen Zuständigkeiten und allen relevanten internen und externen Kontaktdaten.[3] Die Checkliste sollte alle notwendigen Arbeitsschritte zur Krisenbewältigung beinhalten.[4] Berücksichtigen Sie die behördlichen Reaktionsempfehlungen.[5] Stellen Sie das Dokument auch in ausgedruckter Form allen zuständigen Beschäftigten zur Verfügung. Üben Sie die Umsetzung mit Ihrem Team.
- Die Checkliste sollte einen ausführlich beschrifteten Netzplan Ihrer IT-Infrastruktur beinhalten. Aktualisieren Sie den Netzplan nach jeder relevanten Änderung der IT-Infrastruktur.
- Legen Sie mit der Checkliste die wesentlichen Systeme und Datenbanken fest und deren jeweilige Priorisierung im Zuge der eventuell notwendigen Wiederherstellung.
- Üben Sie die Aufrechterhaltung der Arbeitsfähigkeit der wichtigsten Geschäftsbereiche beim Ausfall der IT.
- Gewährleisten Sie die mobile telefonische Erreichbarkeit wichtiger Mitarbeiterinnen und Mitarbeiter für den Fall der Beeinträchtigung des Telefonsystems.
- Die Rekonstruktion des Netzwerks und der Daten im Schadensfall ist ein fachlich und zeitlich aufwendiger Prozess. Gewährleisten Sie entsprechende Expertise Ihrer IT-Fachkräfte. Reduzieren Sie den Aufwand im Ernstfall, indem

[2] https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden
[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/6_KonzepteEinfuehren/2_Inhalt/NVK_Inhalt_node.html
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html
[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.pdf

Sie den Wiederherstellungsprozess in allen Einzelheiten üben (Backup- und Disaster-Recovery).

Schulungs- und Sensibilisierungsmaßnahmen

- Gewährleisten Sie die regelmäßige **Fortbildung der IT-Fachkräfte** hinsichtlich aktueller Angriffsmuster und -methoden sowie geeigneter technischer Gegenmaßnahmen.
- Schulen Sie Ihre Belegschaft bezüglich des Umgangs mit verdächtigen Beobachtungen. Veröffentlichen Sie die internen **Meldewege** zur Kontaktierung der zuständigen IT-Fachkräfte.
- Phishing-Gefahr: Sensibilisieren Sie alle Mitarbeiterinnen und Mitarbeiter. Betonen Sie, dass diese keine Links in elektronischen Nachrichten anklicken und daraufhin Zugangsdaten, Passwörter oder Bestätigungs-Codes für Benutzerkonten oder Fernzugriffsdienste eingeben dürfen. Die sich nach dem Klicken öffnenden Webseiten können gefälscht sein und spähen alle einzugebenden Daten aus. Dies gilt auch für augenscheinlich vom eigenen Unternehmen oder dem eigenen IT-Dienstleister stammende Nachrichten. Zum Einloggen sind ausschließlich die vorgegebenen Lesezeichen und Verknüpfungen zu verwenden.
- Kriminelle unternehmen Phishing-Versuche auch mit dem Telefon. Sie geben sich beispielsweise als Angehörige eines IT-Dienstleisters aus und versuchen, Passwörter und Sicherheitscodes zu erfragen. Schulen Sie alle Mitarbeiterinnen und Mitarbeiter, die Fernzugriffsdienste nutzen. Sensible Zugangsdaten sind niemals weiterzugeben, auch nicht auf telefonische Aufforderung.

Empfehlungen für Mitarbeiterinnen und Mitarbeiter

- Beachten Sie die Hinweise zur Phishing-Problematik (E-Mail, Telefon, Karriereportale, Social Media, Messenger-Apps). Nutzen Sie zum Starten Ihrer Anwendungen und zum Einloggen ausschließlich die von Ihren IT-Fachkräften eingerichteten Lesezeichen und Verknüpfungen. Verwenden Sie ein Passwort niemals für mehr als einen Dienst.
- Melden Sie festgestellte verdächtige Beobachtungen unverzüglich Ihren IT-Fachkräften. Erfragen Sie den Umgang mit dieser Situation.

Technische Empfehlungen

- Richten Sie ein Datensicherungskonzept mit mehreren Backup-Ebenen ein.[6] Achtung: Ein im Netzwerk betriebenes Backup kann ebenfalls vom Angriff betroffen sein und verschlüsselt werden. Erstellen Sie aus diesem Grund fortlaufend aktuelle Sicherheitskopien Ihrer wichtigsten Daten mit so genannten **Offsite-Backups** und verwenden Sie hierfür beispielsweise externe Datenträger, Bandlaufwerke und unter bestimmten Umständen auch eine Cloud.[7] Erstellen Sie unbedingt auch Sicherheitskopien Ihrer Netzwerkumgebung wie Domänen und Active Directory. Trennen Sie nach der Erstellung der Kopien die Offsite-Backups wieder vom Netzwerk. Überprüfen Sie regelmäßig die Wiederherstellbarkeit. Verwenden Sie für die eventuell notwendige Wiederherstellung nicht das Original-Backup, sondern fertigen Sie zuvor eine Arbeitskopie an. Lagern Sie das Offsite-Backup im Idealfall an einem anderen physikalischen Standort.
- Jeder im Internet erreichbare Dienst oder Rechner ist angreifbar. Identifizieren Sie geschäftskritische Arbeitsbereiche. Unterbinden oder minimieren Sie die direkte Internetanbindung dieser Bereiche. Ausschließlich Fachkräfte sollten die Absicherung und Konfiguration Ihrer Systeme vornehmen.[8] Deaktivieren Sie Fernzugriffsdienste, falls Sie auf die Funktion verzichten können oder aktivieren Sie den Fernzugriff nur im Bedarfsfalle.
- Sichern Sie alle Dienste für Fernzugriffe und VPN unbedingt mittels **Mehr-Faktor-Authentisierung**.[9] Dies gilt insbesondere für die Fernwartungszugriffe Ihres eigenen IT-Dienstleisters und die Administratoren-Konten. Nutzerinnen und Nutzer sollten diese Dienste ausschließlich über zuvor eingerichtete Lesezeichen oder Verknüpfungen starten und niemals nach dem Klicken auf Links in Nachrichten oder Suchmaschinen. Richten Sie diese verbindlichen Verknüpfungen ein. Die Einrichtung von Zertifikaten bei Fernzugriffen erhöht zudem die Sicherheit.[10]
- Deaktivieren oder beschränken Sie unbedingt die Ausführbarkeit von **Makro**-Elementen in Office-Dokumenten aus externen Quellen. Hierzu können Sie

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.pdf
[7] 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
[8] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.pdf
[9] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf (Punkt 3)
[10] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html

beispielsweise administrative Gruppenrichtlinien einrichten.[11] Legitim verwendete Makros sollten zuvor durch die IT-Fachebene geprüft werden und nur digital signiert verwendbar sein.

- Veraltete Systeme sind über das Internet leicht festzustellen und angreifbar. Beseitigen Sie diese vermeidbaren Sicherheitslücken. Installieren Sie zeitnah die von den Herstellern veröffentlichten **Updates** für alle Software- und Hardwareprodukte. Ein zentrales Patch-Management kann hilfreich sein.[12] Auch rein intern verwendete Systeme ohne direkte Internetanbindung, aber mit Anbindung zum Netzwerk, sind gefährdet. Auch hier sind Updates Pflicht. Prüfen Sie regelmäßig, ob die verwendeten Produkte von den Herstellern noch unterstützt werden. Ersetzen Sie zeitnah nicht mehr unterstützte Produkte. Aus Kompatibilitätsgründen erforderliche Ausnahmen sollten nur nach strenger Prüfung und mit angemessenen Sicherungsmaßnahmen möglich sein.[13]
- Trennen Sie Ihr IT-Netzwerk in verschiedene **Segmente**, um die unberechtigte Ausbreitung innerhalb des Netzwerks zu erschweren. Sichern Sie auch die internen Segmente mit separaten Firewall-Regeln und eindeutiger User-Authentisierung. Richten Sie sogenannte Pufferzonen im Netzwerk ein.[14] Prüfen Sie die Umsetzung eines technischen „Zero-Trust“-Konzepts.[15]
- Gehen Sie restriktiv mit der Vergabe von Benutzerrechten um.[16] Nur ausgewählte und fachkundige Personen sollten **Administrationsrechte** erhalten. Administrative Tätigkeiten sollten über gesicherte Rechner ohne Internetzugang erfolgen. Vergeben Sie ausschließlich Leserechte, wenn Schreib- und Änderungsrechte nicht zwingend nötig sind.
- Sichern Sie die verwalteten Anmeldedaten der Benutzerkonten vor Ausspähung und Missbrauch.[17] Namensbezeichnungen der Administratoren-Konten sollten nicht einfach zu erkennen sein. Wählen Sie Namensbezeichnungen, die **nicht auf hinterlegte Admin-Rechte hinweisen**. Gewährleisten Sie die Verwendung sicherer Passwörter mit mindestens zehn Zeichen, insbesondere für

[11] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_135.pdf
[12] 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
[13] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_145.pdf
[14] 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)
[15] https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF
[16] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf
[17] https://docs.microsoft.com/de-de/windows/security/identity-protection/credential-guard/credential-guard

Admin-Konten und Fernzugriffsdienste wie RDP.[18] Ein konkretes Passwort sollte niemals für mehr als einen Dienst gewählt sein. Speichern Sie niemals Passwortlisten im Netzwerk. Verhindern Sie das unautorisierte Anlegen neuer Benutzerkonten mit Admin-Rechten. Entziehen Sie ausgeschiedenen Mitarbeiterinnen und Mitarbeitern sowie ehemaligen Dienstleistern umgehend die Benutzerkonten und Berechtigungen. Reduzieren Sie die Anzahl der Domänen-Administratorenkonten auf das tatsächlich erforderliche Maß.

- Verwenden Sie moderne Dienste zum Erkennen abweichender Verhaltensmuster im Netzwerk.[19] Prüfen Sie regelmäßig auch manuell auf abweichendes Verhalten, beispielweise atypische IP-Adressen und Zugriffszeiten sowie ungewöhnliche Datentransfers.
- Die Kriminellen sind in der Regel auf die Installation von Trojanern und weiterer Software angewiesen. Blockieren Sie administrativ die **Ausführbarkeit nichtautorisierter Dateien**. Beschränken Sie die Ausführbarkeit im Netzwerk und auf Rechnern ausschließlich auf konkret festgelegte arbeitsnotwendige Programme (Whitelist).[20]
- In das Netzwerk eingedrungene Angreifer nutzen oftmals die weitreichenden Möglichkeiten der **PowerShell** zur Maximierung des Schadens. Schränken Sie die Verwendung der Powershell unbedingt ein oder unterbinden Sie diese Möglichkeit.[21]
- Verhindern Sie beispielsweise mit technischen Gruppenrichtlinien die Ausführbarkeit externer und aktiver Inhalte wie ActiveX, JavaScript oder OLE in E-Mails, PDF- und Office-Dokumenten.[22]
- Die Snapshot-Funktion bietet spezielle Möglichkeiten zur zeitnahen Zurücksetzung von Virtuellen Maschinen (VM). Snapshots können VM schnell wiederherstellen. Üben Sie das hierfür notwendige Vorgehen. Sichern Sie die Speichersysteme der Snapshots unveränderlich und ausschließlich lokal.
- Beachten Sie die Einrichtungsempfehlungen für Arbeitsplätze im Home-Office.[23] Unterbinden Sie über **unsichere Privatrechner** Ihrer Mitarbeiterinnen

[18] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
[19] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.pdf
[20] https://docs.microsoft.com/de-de/windows-server/identity/software-restriction-policies/software-restriction-policies
[21] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf (S.21)
[22] https://support.microsoft.com/de-de/office/sperren-oder-entsperren-externer-inhalte-in-office-dokumenten-10204ae0-0621-411f-b0d6-575b0847a795
[23] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf

und Mitarbeiter vorgenommene Fernzugriffe. Setzen Sie ein sogenanntes „Mobile Device Management“ um.[24]

- Aktivieren Sie den Ransomware-Schutz Ihrer verwendeten Anti-Viren-Lösung. Dieser Schutz bietet jedoch keine umfassende Absicherung.
- Überprüfen Sie Ihre Systeme in regelmäßigen Abständen mit einem Virenschutz. Häufig wird die Schadsoftware erst zu einem späteren Zeitpunkt mit aktualisierten Virensignaturen erkannt. Aktualisieren Sie Ihre Schutzsoftware mindestens einmal täglich. Größere Netzwerke können zusätzlich mit speziellen Lösungen wie Endpoint Protection gesichert werden.
- Scannen Sie automatisch ein- und sowie ausgehende E-Mails und heruntergeladene Daten auf Schadsoftware. Entfernen Sie aus den Anlagen ausführbare Elemente und sonstige kritische Dateiformate, beispielsweise ISO, DLL, LNK. Beachten Sie insbesondere übersandte oder passwortgeschützte Dateien.
- Blockieren Sie Zugriffe von und auf das Onion-/TOR-Netzwerk, einschlägige Domains und IP-Adressen.[25]
- Gefahr Datenausspähung: Prüfen Sie die Erforderlichkeit der Netzanbindung von Speicherorten sensibler Daten. Speichern Sie diese gegebenenfalls verschlüsselt und in getrennten Netzwerken.
- Führen Sie regelmäßig Tests Ihrer Systeme auf Schwachstellen durch.
- Im Falle eines Angriffs kann die Analyse der Protokolldaten Hinweise auf den Angriffsweg und eventuell ausgenutzte Sicherheitslücken des betroffenen Netzwerks ergeben. Aktivieren Sie im Alltag die möglichst umfangreiche und langfristige Protokollierung Ihrer Systeme. Sichern Sie die Protokolldaten vor Manipulation und Löschung im Zuge eines Cyberangriffs.

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf
[25] https://docs.microsoft.com/de-de/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide

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

Zentrale Ansprechstellen Cybercrime der Bundesländer

Die Kontaktdaten der Zentralen Ansprechstellen Cybercrime für Unternehmen und Behörden im Bundesgebiet können Sie auf der folgenden Webseite nachlesen: www.polizei.de/zac