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 Ransomware

Stand 25. Juli 2016

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben.[1] Die folgenden Empfehlungen richten sich an Wirtschaftsunternehmen und andere öffentliche und nicht-öffentliche Stellen in Baden-Württemberg. Die Realisierbarkeit der Maßnahmen bedarf einer konkreten Einzelfallprüfung.

Technische Prävention

- Scannen Sie ein- und ausgehende E-Mails auf Schadsoftware und entfernen Sie ausführbare Dateien.
- Nutzen Sie Spam-Filter, sodass möglichst wenig unerwünschte Mails den Endnutzer erreichen.[2]
- Verhindern Sie durch Ihren E-Mail-Server die Annahme externer Mails mit internem Absender (Anti-Spoofing[3]).
- Verhindern Sie die Ausführung aktiver Inhalte in E-Mails und Office-Dokumenten oder erlauben Sie deren Ausführung erst nach ausdrücklicher Bestätigung des Nutzers.
- Nutzen Sie für die E-Mail-Kommunikation (sowohl intern als auch extern) digitale Zertifikate/Signaturen um Absender zu verifizieren und die Manipulation von Nachrichten zu verhindern.[4]
- Blockieren Sie durch Ihre Firewall Zugriffe auf verdächtige IP-Adressen und Domains.

---

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI)

[2] BSI: E-Mail-Sicherheit *[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_098.html]*

[3] Der Begriff „Spoofing“ bedeutet allgemein die Verschleierung der eigenen Identität, was für Identitätsdiebstahl in vielfältiger Weise genutzt wird. Beim klassischen Phishing, Spear-Phishing oder Spam werden z.B. E-Mails mit gefälschten Absenderadressen verschickt. [Register aktueller Cyber-Gefährdungen und –Angriffsformen; *https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_026.html*]

[4] BSI: Wie verschlüsselt kommunizieren? *[https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Einsatzbereiche/einsatzbereiche.html]* Anleitung zur Nutzung von S/MIME *[https://www.ca.kit.edu/img/SMIME-Anleitung.pdf]*

- Überprüfen Sie durch einen Virenschutz in regelmäßigen Abständen Ihre Systeme. Häufig wird die Schadsoftware erst zu einem späteren Zeitpunkt durch aktualisierte Virensignaturen erkannt. Durch die Nutzung proaktiver Schutzmechanismen (beispielsweise cloudbasierte Analysen oder Verhaltensanalyse) kann die Erkennungsrate der Antivirensoftware verbessert werden. Aktualisieren Sie ihre Schutzsoftware regelmäßig.
- Deinstallieren Sie nicht benötige Software und führen Sie regelmäßige Updates für die eingesetzten Softwareprodukte und Betriebssysteme durch. Ein zentrales Patch-Management kann hierbei hilfreich sein.
- Gehen sie restriktiv mit der Vergabe von Benutzerrechten um. Sofern für bestimmte Dateien und Verzeichnisse auf Schreib- / Änderungsrechte verzichtet werden kann, vergeben Sie dort lediglich Leserechte. Über Administrationsrechte sollten möglichst wenige ausgewählte Personen verfügen. Schützen Sie alle Benutzerkonten mit starken Passwörtern und erhöhen Sie die Sicherheit sofern möglich durch Zwei-Faktor-Authentifizierung.[5]
- Prüfen Sie, ob das Remote Desktop Protocol (RDP) oder andere Fernzugriffssoftware aktiviert ist und ob diese zwingend benötigt werden. Deaktivieren Sie diese, falls darauf verzichtet werden kann.
- Sichern Sie Remotezugänge beispielsweise mittels Zwei-Faktor-Authentifizierung und kontrolliertem VPN-Zugriff ab.
- Deaktivieren Sie Macro-Elemente in Office-Dokumenten oder erlauben Sie deren Ausführung erst nach Bestätigung des Nutzers.[6] Nutzen Sie Office-Viewer zum Anschauen und Lesen verdächtiger Office-Dateien.
- Teilweise wird Ransomware als E-Mail-Anhang in Form von Javascript und VisualBasic-Skripten verteilt. Deaktivieren Sie daher die Ausführung von Skripten im Betriebssystem, sofern hierauf verzichtet werden kann.[7] Durch das Ändern der Standard-Dateizuordnung von Skript-Dateien kann durch Auswählen des Editors verhindert werden, dass die Skripte tatsächlich ausgeführt werden.
- Nutzen Sie Application-Whitelisting, um die Ausführung unerwünschter Programme zu verhindern.[8]
- Nutzen Sie die Möglichkeiten der Virtualisierung bestimmter Softwareprodukte (z. B. virtueller Browser). Sollten Sie auf die Nutzung konventioneller Browser angewiesen sein, so deaktivieren Sie aktive Inhalte (z. B. Flash, Java, Silverlight) oder erlauben Sie deren Ausführung nur nach Bestätigung des Nutzers.
- Prüfen Sie die Ablage geschäftskritischer Daten. Speichern Sie diese gegebenenfalls in physikalisch getrennten Netzwerken.

---

[5] Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte.
[https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html]

[6] Deaktivieren von VBA in Office 2013 *[https://technet.microsoft.com/de-de/library/ee857085.aspx#changevba]*
Geschützte Ansicht in Office 2013 *[https://technet.microsoft.com/de-de/library/ee857087.aspx]*

[7] Disabling Windows Script Host *[https://technet.microsoft.com/en-us/library/ee198684.aspx]*
Restricting the Ability to Run Scripts *[https://technet.microsoft.com/en-us/library/ee198679.aspx]*

[8] Anwendungsschutz vor ungepatchten Schwachstellen mittels EMET
[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_040.html]
Sicherer Einsatz von Microsoft AppLocker v1.0
[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_117.html]

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-0 · Telefax 0711 5401-3355
stuttgart.lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de

- Erstellen Sie regelmäßig externe Backups und überprüfen Sie deren Integrität und Wiederherstellbarkeit. Stellen Sie sicher, dass die Backups durch einen Verschlüsselungstrojaner nicht unmittelbar mitverschlüsselt werden.
- Führen Sie regelmäßige Penetrations- und Vulnerabilitätstests Ihrer Systeme durch.
- Erstellen Sie einen IT-Notfallplan und üben Sie dessen Umsetzung mit Ihren Mitarbeitern.

Verhaltensprävention für Mitarbeiter:

Informieren Sie in Form von Mitarbeiterschulungen oder Awareness-Kampagnen über die Gefahren und Infektionsursachen von Ransomware.
Durch simulierte Phishing-Mails kann der Sensibilisierungsgrad der Mitarbeiter überprüft werden.

Verhaltensempfehlung für 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. Dateiendungen wie .exe, .scr, .js, .vbs, .chm, .bat, .com, .msi, .jar, .scf, .pif, .hta (Aufzählung nicht abschließend) weisen auf ausführbare Dateien hin, die mitunter unerwünschte Änderungen am PC vornehmen.
- Wichtige Daten sollten auf Netzlaufwerken und nicht lokal abgelegt werden, da lokale Dateien unter Umständen nicht vom Backup umfasst werden.

Maßnahmen nach einer Infektion

- Trennen Sie unverzüglich die Netzwerkverbindung von infizierten Rechnern.
- Schalten Sie betroffene Geräte umgehend aus, um die Verschlüsselung weiterer Daten zu verhindern.
- Isolieren Sie Backups, damit diese nicht ebenfalls verschlüsselt werden.
- Sichern Sie relevante Dateien, die Aufschluss über den Infektionshergang geben können. Hierzu zählen beispielsweise Log-Dateien oder 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.

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-0 · Telefax 0711 5401-3355
stuttgart.lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de

Zentrale Ansprechstelle Cybercrime

Die ZAC dient als zentraler Ansprechpartner 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

Links

- BSI: Lagedossier Ransomware vom 07.07.2016
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lagedossiers/Lagedossier_Ransomeware.html
- BSI: Ransomware - Bedrohungslage, Prävention & Reaktion vom 11.03.2016
  https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Ransomware_11032016.html
- BKA: Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime
  http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html
- Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime der Länder und des Bundes
  http://www.polizei.de/nn_196750/Polizei/DE/Einrichtungen/ZAC/zac__node.html?__nnn=true