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

21.03.2023

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] 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 mit der Veröffentlichung, falls Betroffene kein Geld zahlen.
Die Cyber-Kriminellen greifen sowohl Kleinbetriebe als auch Großunternehmen an, zur Minimierung des Entdeckungsrisikos oftmals am Wochenende oder vor Feiertagen.

Das Landeskriminalamt hat die Verschlüsselungsangriffe umfassend analysiert und Angriffsmuster sowie empfehlenswerte Sofortmaßnahmen zusammengefasst. Die folgenden Empfehlungen zeigen auf, wie Sie Schaden verhindern und 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.

Die vorgeschlagenen Maßnahmen erhöhen Ihre IT-Sicherheit. Absolute Sicherheit ist jedoch nicht garantiert. Bedenken Sie, dass trotz umgesetzter Sicherungsmaßnahmen ein Zugriff auf Ihr Netzwerk und Ihre Daten erfolgen kann. Beachten Sie deswegen unbedingt die technischen und organisatorischen Empfehlungen zum Thema **Sicherheitskopien** (Backups). 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[2] 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

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.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 und Software an. Veraltet sind Systeme und Software, die nicht regelmäßig und zeitnah 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. Es sich oftmals um Dateien, deren Schadenspotenzial nicht ersichtlich ist. Mit dem Aktivieren der Dateien startet die Schadsoftware, sofern keine technischen Gegenmaßnahmen eingerichtet sind.

Erstmaßnahmen nach einem Angriff

- Greifen Sie auf die Checkliste zurück.[3]
- Dokumentieren Sie alle Maßnahmen.
- Kontaktieren Sie Ihren IT-Dienstleister.
- Trennen Sie unverzüglich die Internetanbindung bzw. die internen Netzwerkverbindungen, insbesondere die Anbindung kritischer Systeme und Server.
- 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.

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf

- 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.[4]

Organisatorische Empfehlungen

- IT-Vertragsdienstleister unterstützen Sie bei der Bewältigung künftiger IT-Krisenlagen. Informieren Sie sich im Vorfeld über IT-Dienstleister mit dem Schwerpunkt Forensik. Die Möglichkeit der Alarmierung eines Dienstleisters sichern Sie sich mit einem Rahmenvertrag.
- Erstellen Sie eine Checkliste mit personellen Zuständigkeiten und allen relevanten internen und externen Kontaktdaten.[5] Die Liste sollte alle notwendigen Arbeitsschritte zur Krisenbewältigung beinhalten.[6] Berücksichtigen Sie die behördlichen Reaktionsempfehlungen.[7] Stellen Sie das Dokument auch in ausgedruckter Form allen zuständigen Beschäftigten zur Verfügung. Üben Sie die Umsetzung mit Ihrem Team.
- Die Checkliste für die IT-Fachkräfte sollte unbedingt den 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. Bereiten Sie ein alternatives E-Mail-Kommunikationssystem vor.

[4] https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden
[5] 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
[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html
[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD_2_0.pdf

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

Schulungs- und Sensibilisierungsmaßnahmen

- Gewährleisten Sie die regelmäßige **Fortbildung der IT-Fachkräf**te hinsichtlich aktueller Angriffsmuster und -methoden und technischer Gegenmaßnahmen.
- Schulen Sie Ihre Belegschaft bezüglich des Umgangs mit verdächtigen Beobachtungen. Veröffentlichen Sie die internen **Meldewege** zur Kontaktierung der zuständigen IT-Fachkräfte. Gewährleisten Sie die tolerante Fehlerkultur.
- Phishing-Gefahr: Sensibilisieren Sie alle Mitarbeiterinnen und Mitarbeiter. Betonen Sie, dass diese keine Links in elektronischen Nachrichten anklicken und auf sich daraufhin öffnenden Webseiten Zugangsdaten, Passwörter oder Bestätigungs-Codes für Benutzerkonten oder Fernzugriffsdienste eingeben dürfen. Die sich nach der Aktivierung des Links 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, Verknüpfungen und Programme zu verwenden.
- Kriminelle unternehmen Phishing-Versuche auch mittels Telefon. Sie geben sich telefonisch 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 nach telefonischer 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, Verknüpfungen und Programme. Verwenden Sie ein konkretes Passwort niemals für mehr als einen Dienst. Insbesondere das Passwort für das E-Mail-Konto darf nicht identisch sein mit dem Passwort des Fernzugriffsdienstes.

- Melden Sie festgestellte verdächtige Beobachtungen unverzüglich Ihren IT-Fachkräften. Erfragen Sie den Umgang mit dieser Situation.

Technische Empfehlungen

Die Prüfung und Umsetzung technischer Maßnahmen obliegt der IT-Fachebene.

- Richten Sie ein Datensicherungskonzept mit mehreren Backup-Ebenen ein.[8] 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 beispielsweise externe Datenträger, Bandlaufwerke oder unter bestimmten Umständen auch eine Cloud.[9] Erstellen Sie auch Sicherheitskopien Ihrer Netzwerkumgebung wie Domänen und Active Directory. Trennen Sie die Offsite-Backups nach der Erstellung der Kopien wieder vom Netzwerk. Überprüfen Sie regelmäßig die Wiederherstellbarkeit. Lagern Sie das Offsite-Backup im Idealfall an einem anderen physikalischen Standort. Verwenden Sie für die eventuell notwendige Wiederherstellung nicht das Original-Backup, sondern fertigen Sie zuvor eine Arbeitskopie an.
- Im Internet erreichbare Dienste, Rechner und Server sind über das Internet angreifbar. Insbesondere die direkte Internetanbindung ohne Verwendung von beispielsweise Reverse Proxy, WAF und VPN stellt ein Risiko dar. Identifizieren Sie geschäftskritische Arbeitsbereiche. Unterbinden oder minimieren Sie die Internetanbindung dieser Bereiche. Ausschließlich Fachkräfte sollten die Absicherung und Konfiguration Ihrer Systeme vornehmen.[10] Deaktivieren Sie Fernzugriffsdienste, falls Sie auf die Funktion verzichten können oder aktivieren Sie den Fernzugriff nur im Bedarfsfall.
- Sichern Sie alle Anwendungen für Fernzugriffsdienste und VPN unbedingt mittels **Mehr-Faktor-Authentisierung** (MFA oder 2FA).[11] Aktive Fernzugriffe sollten niemals unbegrenzt verwendbar sein. Erstellen Sie automatisierte Time Outs. Diese Empfehlungen gelten insbesondere für die Fernwartungszugriffe Ihres eigenen IT-Dienstleisters und die Administratoren-Konten. Nutzerinnen und Nutzer sollten Fernzugriffsdienste ausschließlich über zuvor eingerichtete Lesezeichen, Verknüpfungen oder Programme starten und niemals nach dem

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2023.pdf
[9] 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
[10] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.pdf
[11] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf (Punkt 3)

Klicken auf Links in Nachrichten oder Suchmaschinen. Richten Sie diese verbindlichen Verknüpfungen ein. Die Einrichtung von Zertifikaten bei Fernzugriffen erhöht zudem die Sicherheit.[12]

- Deaktivieren oder beschränken Sie unbedingt die Ausführbarkeit von **Makro**-Elementen in Office-Dokumenten aus externen Quellen. Hierzu können Sie beispielsweise administrative Gruppenrichtlinien einrichten.[13] 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 verwendeten Software- und Hardwareprodukte. Ein zentrales Patch-Management kann hilfreich sein.[14] Ebenso gefährdet sind intern verwendete Systeme ohne Internetanbindung, aber mit Netzwerkanbindung. Auch hier sind Updates Pflicht. Prüfen Sie regelmäßig, ob die verwendeten Produkte von den Herstellern noch unterstützt werden. Ersetzen Sie nicht mehr unterstützte Produkte zeitnah. Aus Kompatibilitätsgründen erforderliche Ausnahmen sollten nur nach strenger Prüfung und unter Berücksichtigung angemessener Sicherungsmaßnahmen möglich sein.[15]
- 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.[16] Prüfen Sie die Umsetzung eines technischen „Zero-Trust“-Konzepts.[17]
- Gehen Sie restriktiv mit der Vergabe von Benutzerrechten um.[18] Nur ausgewählte und fachkundige Personen sollten **Administrationsrechte** erhalten. Vergeben Sie ausschließlich Leserechte, wenn Schreib- und Änderungsrechte nicht zwingend nötig sind.[19] Administrative Vornahmen sollten ausschließlich über gesicherte Rechner ohne Internetzugang erfolgen und niemals mittels

[12] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html
[13] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_135.pdf
[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2023.pdf
[15] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_145.pdf
[16] 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)
[17] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf
[18] 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
[19] https://learn.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts

Fernzugriffsanwendungen. Sichern Sie herausragende Konten wie Administratoren und Domänen mit MFA. Insbesondere die Konfigurationen kritischer Systeme wie Firewall und Backup sollte nur lokal und ausschließlich unter Verwendung einer MFA möglich sein.

- Sichern Sie die verwalteten Anmeldedaten der Benutzerkonten vor Ausspähung und Missbrauch.[20] Namensbezeichnungen der Konten und Gruppen der Administratoren 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 Admin-Konten und Fernzugriffsdienste wie VPN und RDP.[21] Ein konkretes Passwort sollte niemals für mehr als einen Dienst verwendbar 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 die zugewiesenen Benutzerkonten und Berechtigungen umgehend. Reduzieren Sie die Anzahl der Administratoren- und Domänenkonten auf das tatsächlich erforderliche Maß. Trennen Sie Administratoren-Konten von E-Mail-Konten.
- Prüfen Sie zusätzlich zur Absicherung mittels MFA die Einführung moderner passwortloser Authentisierungsverfahren, insbesondere für Administratoren-Konten und für Anwendungen mit hohem Risiko.
- Verwenden Sie moderne Dienste zur Detektion abweichender Verhaltensmuster im Netzwerk.[22] Prüfen Sie regelmäßig auch manuell abweichende Verhaltensmuster, beispielweise atypische IP-Adressen und Zugriffszeiten sowie ungewöhnliche Datentransfers (Volumen, Ziele, Quellen).
- 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 automatisiert oder mindestens einmal täglich. Größere Netzwerke können zusätzlich mit speziellen Lösungen wie Endpoint-Protection gesichert werden.
- Die Kriminellen sind in der Regel auf die Installation von Trojanern und weiterer Software angewiesen. Blockieren Sie administrativ die **Ausführbarkeit**

[20] https://docs.microsoft.com/de-de/windows/security/identity-protection/credential-guard/credential-guard
[21] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
[22] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.pdf

nichtautorisierter Dateien, auch in den Benutzerprofilen der Anwender (Portable Apps). Beschränken Sie die Ausführbarkeit im Netzwerk und auf Rechnern ausschließlich auf konkret festgelegte arbeitsnotwendige Programme (Whitelist)[23] und nutzen Sie Windows-Schutzfunktionen wie SRP, AppLocker und WDAC. Beschränken Sie Windows Script Host und MSHTA. Recherchieren Sie regelmäßig aktuelle Indikatoren (IoC) häufig verwendeter Angriffswerkzeuge wie Cobalt Strike[24] und Mimikatz und erfassen Sie die IoC in Ihren Sicherheitssystemen zur Detektion und Blockierung.

- 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.[25]
- Im Falle eines Angriffs kann die Analyse der **Protokolldaten** Hinweise auf den Angriffsweg und ausgenutzte Sicherheitslücken des betroffenen Netzwerks ergeben. Aktivieren Sie im Alltag die möglichst umfangreiche und langfristige Protokollierung Ihrer Systeme.[26] Sichern Sie die Protokolldaten vor Manipulation und Löschung im Zuge eines Cyberangriffs.
- Die Snapshot-Funktion bietet spezielle Möglichkeiten zur zeitnahen Zurücksetzung und Wiederherstellung von Virtuellen Maschinen (VM). Üben Sie das hierfür notwendige Vorgehen. Sichern Sie die gespeicherten Snapshots vor Manipulation und Löschung im Zuge eines Cyberangriffs.
- Verhindern Sie mit technischen Gruppenrichtlinien und ähnlichen Maßnahmen die Ausführbarkeit externer und aktiver Inhalte wie ActiveX, JavaScript oder OLE in E-Mails, PDF- und Office-Dokumenten.[27]
- Unterbinden Sie über **unsichere Privatrechner** Ihrer Mitarbeiterinnen und Mitarbeiter vorgenommene Fernzugriffe. Beachten Sie die Einrichtungsempfehlungen für Arbeitsplätze im Home-Office.[28] Setzen Sie ein sogenanntes „Mobile Device Management“ um.[29]
- Aktivieren Sie den Ransomware-Schutz Ihrer verwendeten Anti-Viren-Lösung. Dieser Schutz bietet jedoch keine umfassende Absicherung.

[23] https://docs.microsoft.com/de-de/windows-server/identity/software-restriction-policies/software-restriction-policies
[24] https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-148a
[25] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf (S.21)
[26] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html
[27] https://support.microsoft.com/de-de/office/sperren-oder-entsperren-externer-inhalte-in-office-dokumenten-10204ae0-0621-411f-b0d6-575b0847a795
[28] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf
[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-ManagementV2_0.pdf

- 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, IMG, HTA, DLL, LNK. Beachten Sie insbesondere passwortgeschützte Dateien oder Dateicontainer.
- Virtualisieren Sie die für Ihre Belegschaft nutzbare Internetumgebung.[30]
- Blockieren Sie Zugriffe von und auf einschlägige IP-Adressen und Domains[31] sowie das Onion-/TOR-Netzwerk.
- Gefahr Datenausspähung: Prüfen Sie die Erforderlichkeit der Netzanbindung von Speicherorten sensibler Daten. Speichern Sie diese gegebenenfalls verschlüsselt und in getrennten Netzwerksegmenten.
- Richten Sie TPM und HSM ein zur Gewährleistung der Zugriffssicherheit.
- Führen Sie regelmäßig Tests Ihrer Systeme auf Schwachstellen durch.[32]

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



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

[30] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_047.pdf
[31] https://docs.microsoft.com/de-de/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide
[32] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html