SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Update: IT-Sicherheitsmaßnahmen im Rahmen des aktuellen "Politleaks"

Nr. 2019-164159-1000, Version 1.0, 15.01.2019

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Im Dezember 2018 wurden gestohlene Daten deutscher Prominenter im Internet veröffentlicht. Seit dem 3. Januar 2019 sind diese Veröffentlichungen unter dem Schlagwort "Politleaks" in den Medien und daraufhin den Behörden bekannt geworden.

Die Bewertung der Hintergründe dieser Leaks und die Koordination der Ermittlungen obliegt den im Nationalen Cyber-Abwehrzentrum kooperierenden Behörden. In diesem Dokument stellt das BSI daher nur IT-technische Empfehlungen für Betroffene dar. Der Fokus dieses Dokuments liegt darauf Hilfestellung für möglicherweise Betroffene zu geben, damit diese Maßnahmen zur Bereinigung und Härtung ihrer Online-Konten ergreifen können sowie damit nicht-betroffene Personen ihre Online-Konten präventiv absichern können.

Empfehlungen

Die nachfolgenden Empfehlungen richten sich an Betroffene, deren Daten im Rahmen des Politleaks veröffentlicht wurden.

Die Bewertung der Hintergründe des aktuellen Vorfalls sowie die damit verbundene Ermittlungsarbeit obliegt den im Nationalen Cyber-Abwehrzentrum vertretenen Behörden. Für die Erstellung der Empfehlungen musste das BSI jedoch Arbeitshypothesen generieren. Diese Hypothesen sind wie folgt:

- Die gestohlenen Daten stammen nicht aus wenigen zentralen Datenbanken, sondern aus einer Vielzahl unabhängiger Quellen.
- Alle gesichteten veröffentlichten Daten lassen sich prinzipiell dadurch erklären, dass Zugangsdaten zu privaten E-Mail-Konten, Cloud-Diensten und Sozialen Netzwerken (mittels Phishing) gestohlen oder erraten wurden.
- Es gibt bislang keine Hinweise darauf, dass Schadsoftware zum Ausspähen von Daten eingesetzt wurde.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Die folgenden Maßnahmen gliedern sich in die Bereiche:

- Bereinigung (Maßnahmen, um einen möglicherweise weiterhin bestehenden Zugang der Täter zu unterbinden),
- Prävention (Maßnahmen, um zukünftige Angriffe zu verhindern oder zumindest zu erschweren),
- Detektion (Möglichkeiten zur Entdeckung einer Kompromittierung) und
- Reaktion (Maßnahmen zur Reaktion bei einer entdeckten erfolgreichen Kompromittierung oder dem Verdacht einer Kompromittierung).

Darüber hinaus sind auch die Basis-Maßnahmen der IT-Sicherheit zu beachten [1].

Maßnahmen zur Bereinigung

Unter der oben genannten Prämisse, dass Schadsoftware für die Politleaks keine Rolle gespielt hat, bestehen die Maßnahmen zur Bereinigung in der Änderung der Zugangsdaten zu E-Mail-Konten, Cloud-Anbietern und Sozialen Netzwerken.

Dabei ist die Reihenfolge entscheidend, mit der die Zugangsdaten verschiedener Accounts geändert werden. Grund dafür ist, dass für Accounts oftmals weitere E-Mail-Adressen als Rückfalloption für das Zurücksetzen von Passwörtern verwendet werden. Zu Beginn der Bereinigungsmaßnahmen sollte daher zunächst geprüft werden, wie Accounts miteinander verknüft sind. Anschließend sollte mit der Bereinigung von Accounts (meistens E-Mail-Konten) begonnen werden, die für das Zurücksetzen von Passwörtern verwendet werden. Als nächstes sollten die Passwörter von Accounts geändert werden, die für ein "Single-Sign-On" verwendet werden. Ein Beispiel hierfür ist Facebook, dessen Account verwendet wird, um sich bei anderen Diensten anzumelden. Anschließend sollten in loser Folge die verbliebenen Accounts zurückgesetzt werden. Dies sollte nicht nur für Accounts erfolgen, aus denen im Rahmen des aktuellen Vorfalls Daten veröffentlicht wurden, sondern präventiv auch für alle anderen Accounts - insbesondere alternative E-Mail-Konten, welche für eine Passwort-Zurücksetzen-Funktion hinterlegt wurden.

Es ist empfehlenswert, die Bereinigungsmaßnahmen in einem Zug durchzuführen, um die Zeit zu minimieren, in der die Täter durch Querbeziehungen zwischen Accounts noch Zugriff behalten.

Für die Änderung der Passwörter gelten die Empfehlungen des BSI [2]. **Besonders hervorzuheben ist, dass grundsätzlich für jeden Account ein unterschiedliches, starkes Passwort verwendet werden sollte**. Bei der Verwaltung der Passwörter helfen Passwortmanager.

Da davon auszugehen ist, dass die Täter mithilfe gestohlener oder erratener Zugangsdaten vollen Zugriff auf Accounts hatten, sollte geprüft werden, ob Konfigurationsänderungen vorgenommen wurden. Besonders kritisch sind potenziell in E-Mail-Konten eingerichtete Weiterleitungsregeln, welche eine Kopie aller eingehender Nachrichten an die Täter senden. Falls vorhanden, müssen diese Weiterleitungen entfernt werden. Kritisch wären auch von den Tätern ergänzte Rückfalloptionen (Mobiltelefonnummern oder E-Mail-Adressen zum Zurücksetzen von Passwörtern). Diese Konfigurationen sollten ebenfalls geprüft und ggf. korrigiert werden.

Maßnahmen zur Prävention

Im aktuellen Fall wurden vor allem private Accounts kompromittiert. Gegen diese Angriffe schützen Maßnahmen, die von Personen einzeln umgesetzt werden sollten. Für zukünftige Fälle ist jedoch auch denkbar, dass dienstliche Accounts angegriffen werden. Daher werden nachfolgend auch Maßnahmen aufgeführt, die von Organisationen umgesetzt werden sollten.

Durch Personen einzeln umsetzbar

Online-Zugänge allgemein

- Verwendung starker Passwörter. Dabei sollte für jeden Zugang ein unterschiedliches Passwort gesetzt werden. Bei der Verwaltung von Passwörtern helfen Passwort-Manager. Passwörter für wichtige Online-Zugänge sollten regelmäßig geändert und zusätzlich auf Papier notiert an einem sicheren Ort (z. B. Safe) verwahrt werden. Weitere Empfehlungen zu Passwörtern unter [2].

- Wenn Zwei-Faktor-Authentisierung (2FA) vom Betreiber des Online-Dienstes angeboten wird, sollte diese aktiviert werden. Gegebenenfalls sollte ein Wechsel zu einem Anbieter in Betracht gezogen werden, der Zwei-Faktor-Authentifizierung unterstützt. Eine Liste von Online-Diensten, die 2FA unterstützen, ist unter [3] verfügbar. Eine exemplarische Übersicht über verschiedene Hilfeseiten zur Einrichtung von 2FA für verschiedene gängige Online-Dienste ist weiter unten in diesem Dokument unter "Anleitungen zur Einrichtung von Zwei-Faktor-Authentisierung" verfügbar.
  Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken. Dies ist üblicherweise ein Passwort sowie ein zweiter unabhängiger Faktor. Dieser zweite Faktor kann z. B. das Wissen über ein Einmalpasswort (z. B. eine per SMS an ein Mobiltelefon gesendete TAN), der Besitz eines Gegenstandes (wie z. B. ein physischer Schlüssel oder eines Sicherheitstokens) oder ein biometrischer Faktor wie etwa ein Fingerabdruck sein.
- Sicherheitsfragen (z. B. zum Zurücksetzen von Passwörtern) mindern dann den Schutz eines Accounts, wenn die Antwort auf eine Sicherheitsfrage einfacher zu erraten oder anderweitig zu erlangen ist als das eigentliche Passwort des Accounts. Daher sollten für die Antwort auf Sicherheitsfragen keine Informationen verwendet werden, die von einem Angreifer leicht recherchiert oder erraten werden können (z. B. Geburtsname der Mutter, Vorname des besten Freundes).

  Sind die Sicherheitsfragen nicht frei wählbar, sollten als Antworten erfundene Angaben bzw. zufällige Zeichenketten mit großer Länge hinterlegt werden.
  Sind die Sicherheitsfragen frei wählbar, können komplexe Fragen mit komplexen Antworten gewählt werden, die aus mehreren Wörtern, Zahlen und ggf. Sonderzeichen bestehen. In beiden Fällen muss gewährleistet sein, dass diese Angaben schwerer zu erraten sind als das Passwort des Accounts. Die Angaben zu Sicherheitsfragen sollten dann ebenfalls in einem Passwort-Safe oder auf Papier notiert an einem sicheren Ort verwahrt werden.
- Werden zusätzliche Accounts (z. B. alternative E-Mail-Adressen) für die Wiederherstellung eines Accounts verwendet, müssen diese ebenfalls mit einem starken Passwort abgesichert sein.
- Einige Online-Dienste zeigen bei der Anmeldung Informationen zur letzten erfolgreichen Anmeldung an. Das BSI empfiehlt, diese Informationen routinemäßig auf Plausibilität zu prüfen (Zeitpunkt, Anmeldungen von unbekannten Orten oder über unbekannte Geräte, parallele Sitzungen, etc.)
- Zugangsdaten für (wichtige) Online-Zugänge sollten nicht im Web-Browser gespeichert werden, da sie dort von Schadprogrammen ausgelesen werden können.
- Regelmäßige Bestandsaufnahme der genutzten Dienste und Accounts. Überprüfung der Sicherheitseinstellungen und ggf. vorhandenen Rechte bzw. Verknüpfungen und zu weiteren Diensten. Nicht mehr benötigte Accounts sollten gelöscht und die Anbieter zur Löschung aller Daten aufgefordert werden.

E-Mail

- Das BSI empfiehlt die generelle Nutzung von E-Mail-Verschlüsselung [4]. Einen Überblick über verschiedene Verschlüsselungsprogramme finden Sie unter [5].
- Sensible Informationen sollten nicht oder nur verschlüsselt per E-Mail versendet werden.
- Gesundes Misstrauen schützt vor Phishing-Angriffen und Schadsoftware [6].
- Es sollte abgewogen werden, private E-Mail-Konten (z. B. bei GMX, web.de, Google-Mail, etc.) nicht (mehr) geschäftlich zu nutzen. Bereits vorhandene geschäftliche Kommunikation sollte dann ggf. auf einem sicheren Rechner lokal archiviert und aus dem E-Mail-Konto gelöscht werden. Bei weiterer geschäftlicher Nutzung sollte eine Zwei-Faktor-Authentisierung für das E-Mail-Konto eingerichtet werden.
- Eine routinemäßige Prüfung, ob eigene E-Mail-Konten in öffentlich gewordenen Leaks enthalten sind [7], kann Ihnen helfen Gefährdungen Ihrer Konten einzuschätzen.
- Für den Abruf und Versand von E-Mails mittels mobiler Geräte, Apps oder Desktop-Clients wie Microsoft Outlook oder Mozilla Thunderbird müssen zwingend Protokolle mit Verschlüsselung (SSL/TLS) genutzt werden [8][9].
  Bei der Verwendung von unverschlüsselten Protokollen wird der Benutzernamen und das Passwort im Klartext übertragen! Überprüfen Sie alle E-Mail-Clients auf allen Geräten auf die Verwendung der korrekten Protokolle.

Clouds

- Sensible Informationen sollten nicht oder nur verschlüsselt in Clouds gespeichert werden.
- Informationen zu Risiken und Sicherheitstipps zur Cloud-Nutzung stellt das BSI unter [10] bereit.

- Überprüfung, ob Daten (z. B. Kontakte, Kalender, Fotos oder Datensicherungen) von (mobilen) Geräten automatisch zu Cloud-Diensten hochgeladen werden. Für sensible Daten sollte diese Funktion ggf. deaktiviert werden. Stattdessen sollten regelmäßig lokale Sicherungen der Daten durchgeführt werden.

Mobile Geräte

- Mobile Geräte (Smartphones, Tablet, Laptops) können leicht verloren gehen bzw. gestohlen werden. Aus diesem Grund sollten alle Daten auf diesen Geräten verschlüsselt werden.
- Smartphones und Tablets sollten mit einer mindestens 6-stelligen PIN geschützt werden. Eine PIN ist alternativen Entsperr-Mechanismen wie Wischgesten oder Fingerabdruck-Sensoren vorzuziehen, da diese einen geringeren Schutz bieten und Angreifer immer wieder neue Wege finden, diese auszutricksen.
- Verwendung verschlüsselter VPN-Tunnel bei der Nutzung von fremden Netzwerken oder öffentlichen WLANs, um ein Ausspähen von Informationen zu verhindern [11] [12].
- Drahtlosschnittstellen (WLAN, Bluetooth, NFC) sollten deaktiviert werden, wenn diese nicht genutzt werden.
- Verschiedene häufig genutzte Apps (wie z. B. der Messenger WhatsApp) übermitteln alle Kontakte im Adressbuch des Mobiltelefons an den Anbieter. In sensiblen Bereichen sollte die Nutzung solcher Apps vermieden werden. Auch viele unscheinbare Apps (z. B. Taschenlampen) versuchen Kontaktinformationen (z. B. für Werbezwecke) auszuspähen. Bei der Installation von Apps sollten daher die verlangten Berechtigungen genau geprüft und ein Zugriff auf Kontakte nur in begründeten Fällen gewährt werden, wenn dies zur Funktionsweise der App zwingend erforderlich ist.
- Weitere Empfehlungen zur Absicherung von mobilen Geräten stellt das BSI unter [13] zur Verfügung.

Weitere grundlegende Maßnahmen

- Regelmäßige Installation von Sicherheitsupdates für Betriebssysteme und alle installierten Anwendungen. Prüfen Sie insbesondere, ob für die Betriebssysteme der von Ihnen verwendeten mobilen Geräte noch Sicherheitsupdates bereitgestellt werden.
- Verifikation von Accounts für Soziale Netzwerke (z. B. Twitter).

Von Organisationen (Partei/Fraktion/Verband) umsetzbar:

- Umsetzung von Maßnahmen zum Schutz vor Angriffen per E-Mail [14].
- Organisations-Webmail (wie Outlook Web Access):
  Je nach Nutzungsart und -häufigkeit sollte entschieden werden, Webmail entweder zu deaktivieren, nur über ein VPN zugreifbar zu machen oder durch Zwei-Faktor-Authentisierung abzusichern.
  Erläuterung: In den letzten Monaten wurden wiederholt Angriffsversuche beobachtet, in denen die Täter Domainnamen registrierten, die den offiziellen Webmail-Domains ihrer Opfer ähnelten. Funktionsträgern wurden anschließend Phishing-Mails im Namen des IT-Supports der eigenen Organisation zugeschickt, in welchen die Empfänger aufgefordert wurden, sich auf der manipulierten Webseite mit ihren Zugangsdaten einzuloggen. Mit den ausgespähten Zugangsdaten hatten die Täter anschließend vollständigen Zugriff auf die Postfächer der Opfer.
- IT-Sicherheitstraining:
  Etablierung regelmäßiger Sensibilisierungskampagnen zu schädlichen E-Mails (Phishing, Schadsoftware), vor allem für VIPs und Funktionsträger (auch nicht-politische Funktionen wie Öffentlichkeitsarbeit, Redenschreiber, Social-Media-Team, Rechnungswesen - jeweils ggf. fokussieren auf die Leitungsrolle oder öffentlich recherchierbare Mitarbeiter). Täter scheinen sich vor allem auf die genannten Rollen und Funktionen zu fokussieren, da in deren Postfächern die interessantesten Inhalte erwartet werden.
- Verdächtige E-Mails:
  Es empfiehlt sich, eine zentrale Stelle in der Organisation einzurichten, an die verdächtige E-Mails weitergeleitet werden können. Die zentrale Stelle kann die E-Mails technisch bewerten und ggf. auf Authentizität prüfen.
- Protokollierung:
  Um Angriffe detektieren oder nachträglich analysieren zu können, sollten Logdaten (mindestens von E-Mail-Servern, Webmail-Servern und VPN-Servern) erhoben, an zentraler Stelle gesichert und regelmäßig ausgewertet werden.
- Vorbereitung von Pressestatements:
  Um im Fall von Dokumenten-Veröffentlichungen schnell reagieren zu können, sollte ein Entwurf für ein Pressestatement vorbereitet werden.

Bei der Veröffentlichung von Daten der En-Marche-Kampagne in Frankreich 2017 wurde beispielsweise sehr professionell darauf hingewiesen, dass Dokumente gefälscht oder aus dem Kontext gerissen sein könnten, und vor voreiligen Schlüssen gewarnt.

Warnung von Kontakten

Im Sinne der Datenschutzgrundverordnung sollten Betroffene von denen Daten abgeflossen sind, alle ihre Kontakte, für die sie verantwortlich sind, über diesen Sachverhalt informieren. Denn durch die Veröffentlichung entstehen auch für sekundär Betroffene Risiken:

1. Phishing: In Phishing-Angriffen können die abgeflossenen Informationen gezielt genutzt werden, um eine Vertrauensbeziehung zu einem Opfer aufzubauen, etwa indem aus einer veröffentlichten Originalmail des Opfers zitiert wird. Hierdurch könnte das Opfer dazu verleitet werden, nicht-öffentliche Informationen preiszugeben. Im Zweifel sollten diese beim Sender nachfragen.
2. Schadprogramme: Durch die Veröffentlichung von E-Mail-Adressen besteht die Gefahr, dass die Eigentümer Ziel von Spam und Angriffen mit Schadsoftware werden. Einige Tätergruppen nutzen hierbei gezielt ausgespähte Kommunikationsbeziehungen zwischen Absender und Empfänger aus [14].
   Hier helfen z.B. aktuelle Betriebssysteme, Anwendungen und Antivirenprodukte.
3. Passwort-Rate-Angriffe: Die veröffentlichten E-Mail-Konten können verstärkt Angriffen ausgesetzt sein, bei denen gezielt versucht wird, durch das Raten von Passwörtern (auch durch Variation verlorener geänderter alter Passwörter) Zugriff auf die E-Mail-Konten zu erlangen. Als Schutzmaßnahmen helfen hier vor allem sichere Passwörter sowie ein zweiter Faktor.
   Dies wird ggf. zu Sperrungen von Accounts nach vielen Fehlversuchen führen. Schlechte Passwörter können zu einer erneuten Kompromittierung führen.

Maßnahmen zur Detektion

Eine Überprüfung des Verlaufs der Anmeldungen bei einem Online-Konto kann Hinweise geben, ob unrechtmäßig auf den Account zugegriffen wurde. Nachfolgend eine Auswahl von Beschreibungen für verschiedene gängige Online-Dienste, wie dies dort überprüft werden kann.

Facebook

- Überprüfung der vorhandenen An- und Ab-Meldungen im Facebook-Profil unter "Einstellungen" -> "Deine Facebook-Informationen" -> "Zugriff auf deine Informationen" -> "Sicherheits- und Login-Informationen" -> "An- und Abmeldungen"
  (https://www.facebook.com/ *Platzhalter Account-URL* /allactivity?log_filter=loginslogouts&category_key=loginslogouts&privacy_source=access_hub)

Twitter

- Verlauf der Accountzugriffe unter "Einstellungen und Datenschutz" -> "Deine Twitter Daten" -> "Account-Verlauf" -> "Verlauf der Accountzugriffe" Alle anzeigen
  (https://twitter.com/settings/your_twitter_data/logins)

GMX

- Postfach-Zugriffe: Aktive Sitzungen: https://hilfe.gmx.net/sicherheit/sitzungen/sitzung.html
- Postfach-Zugriffe: Apps zurücksetzen: https://hilfe.gmx.net/sicherheit/sitzungen/zugang.html

Web.de

- Postfach-Zugriffe: Aktive Sitzungen: https://hilfe.web.de/sicherheit/sitzungen/sitzung.html
- Postfach-Zugriffe: Apps zurücksetzen: https://hilfe.web.de/sicherheit/sitzungen/zugang.html

Google

- Letzte Kontoaktivität: https://support.google.com/mail/answer/45938
- Kontowiederherstellung: https://www.google.com/recovery

Maßnahmen zur Reaktion

Vorbereitung erweiterter Analysen

Verdächtige E-Mails, Daten, Screenshots oder sonstige Artefakte, die mit der Kompromittierung oder dem Verdacht einer Kompromittierung in Verbindung stehen, sollten gesichert und mit einem Zeitstempel versehen werden, damit diese für weitere Analysen im Rahmen von Strafverfolgung zur Verfügung stehen. Auf eine voreilige Löschung ist zu verzichten, wenn geplant ist eine Strafanzeige zu erstatten.

Gegebenenfalls Strafanzeige erstatten

Stellen Sie gegebenenfalls Strafanzeige bei einer erfolgten Kompromittierung Ihrer Online-Konten. Privatpersonen wenden sich hierzu an ihre lokale Polizeidienststelle. Unternehmen wenden sich an die bundesweit eingerichteten Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC) [15]. Nehmen Sie idealerweise direkt Protokolldaten, Screenshots sowie weitere vorliegende Informationen mit, um den Fall möglichst genau zu schildern.

Links

[1] BSI für Bürger: Basisschutz für Computer & Smartphone
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/BasisschutzGeraet_node.html

[2] BSI für Bürger: Passwörter
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

[3] Übersicht von Online-Diensten, die eine Zwei-Faktor-Authentifizierungen anbieten

https://twofactorauth.org/

[4] BSI für Bürger: Verschlüsselt kommunizieren

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/verschluesselt_kommunizieren_node.html

[5] E-Mail Verschlüsselung in der Praxis
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_in_der_Praxis_node.html

[6] BSI für Bürger: Spam, Phishing & Co
https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/spamPhishingCo_node.html

[7] Auswahl von Leak-Datenbanken zur Recherche:

- Identity Leak Checker des Hasso-Plattner-Instituts: https://sec.hpi.de/ilc/
- Have I Been Pwned: https://haveibeenpwned.com/
- Firefox Monitor: https://monitor.firefox.com/
- BreachAlarm: https://breachalarm.com/

[8] E-Mail-Verschlüsselung

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/email_verschluesselung_node.html

[9] Verschlüsselung in der mobilen Kommunikation

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/VerschluesselungMobil/Verschluesselung_in_der_mobilen_Kommunikation/Verschluesselung_in_der_mobilen_Kommunikation_node.html

[10] BSI für Bürger: Cloud: Risiken und Sicherheitstipps

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/CloudComputing/GefahrenRisiken/gefahrenrisiken_node.html

[11] BSI für Bürger: Öffentliche WLAN
https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/FremdeWLAN/fremdeWLAN_node.html

[12] BSI für Bürger: Virtual Private Networks (VPN)
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/VPN/VPN_Virtual_Private_Network_node.html

[13] BSI für Bürger: Schutz für Smartphone und Co.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

[14] ACS: Maßnahmen zum Schutz vor Emotet und anderen Angriffen per E-Mail

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

[15] ACS: Kontakt zu Strafverfolgungsbehörden

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html

Übersicht von Hilfeseiten zur Einrichtung von Zwei-Faktor-Authentisierung für verschiedene gängige Online-Dienste

Amazon - https://www.amazon.de/gp/help/customer/display.html?nodeId=202073820

Apple - https://support.apple.com/de-de/HT204915/

Google - https://www.google.com/landing/2step/
https://landing.google.com/intl/de/advancedprotection/ (Programm "Erweiterte Sicherheit")
https://support.google.com/accounts/answer/46526 (Kontosicherheit erhöhen)

Microsoft - https://support.microsoft.com/de-de/help/12408/microsoft-account-how-to-use-two-step-verification/

Microsoft Office365 - https://docs.microsoft.com/de-de/office365/admin/security-and-compliance/set-up-multi-factor-authentication/

Posteo - https://posteo.de/hilfe/was-ist-die-zwei-faktor-authentifizierung-und-wie-richte-ich-sie-ein

Facebook - https://de-de.facebook.com/help/148233965247823/

Instagram - https://help.instagram.com/566810106808145/

LinkedIn - https://www.linkedin.com/help/linkedin/answer/544/turning-two-step-verification-on-and-off

Signal - https://docs.appsignal.com/user-account/two-factor-authentication.html

Telegram - https://telegram.org/blog/sessions-and-2-step-verification/

Twitter - https://help.twitter.com/de/managing-your-account/two-factor-authentication/

WhatsApp - https://faq.whatsapp.com/de/android/26000021/