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

IT-Sicherheitsmaßnahmen im Rahmen des aktuellen "Politleaks"

Nr. 2019-163986-1000, Version 1.0, 04.01.2019

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Seit Dezember 2018 wurden offenbar gestohlene Daten von deutschen Prominenten im Internet veröffentlicht. Seit dem 3. Januar 2019 sind diese Veröffentlichungen unter dem Schlagwort "Politleaks" in den Medien und daraufhin den Behörden bekanntgeworden.

Die Bewertung der Hintergründe dieser Leaks und die Koordination der Ermittlungen obliegt den im Nationalen Cyber-Abwehrzentrum kooperierenden Behörden, hier insbesondere BKA, BfV, BND, BBK, Kdo CIR und BSI. In diesem Dokument stellt das BSI daher nur die IT-technischen Empfehlungen für Betroffene dar. Der Fokus liegt darauf, den evtl. noch bestehenden Zugang der Täter zu unterbinden und die eigenen Daten gegen zukünftige Angriffe zu schützen.

Bei den folgenden Empfehlungen stand die rasche Bereitstellung von Maßnahmen im Vordergrund.

Empfehlungen

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

Wie bereits geschildert, liegt die Bewertung der Hintergründe und die Ermittlungsarbeit bei den im Nationalen Cyber-Abwehrzentrum vertretenen Behörden. Für die Erstellung der Empfehlungsliste musste das BSI jedoch Arbeitshypothesen generieren. Diese Hypothesen sind wie folgt:

- Die 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 Postfächern, Cloud-Diensten und Sozialen Netzwerken (mittels Phishing) gestohlen oder erraten wurden.
- Es gibt bisher keine Hinweise auf Schadsoftware-Infektionen als Quelle der Daten.

* 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 solche, die den Zugang der Täter unterbinden ("Bereinigung"), und solche, die zukünftige Angriffe verhindern ("Prävention").

Maßnahmen zur Bereinigung

Unter der oben genannten Prämisse, dass Schadsoftware für die Politleaks keine Rolle gespielt hat, bestehen die Maßnahmen zur Bereinigung im Ändern der Zugangsdaten zu Postfächern, Cloud-Anbietern und Sozialen Netzwerken.

Dabei ist die Reihenfolge, mit der die Zugangsdaten verschiedener Accounts geändert werden, entscheidend. Dies liegt daran, dass für Accounts oftmals andere Postfächer als Rückfalloption für das Zurücksetzen von Passwörtern verwendet werden. Zu Beginn der Bereinigungsmaßnahmen sollte daher kurz geprüft werden, wie Accounts miteinander zusammenhängen. Anschließend sollte mit den Accounts (meistens Postfächer) begonnen werden, die für das Zurücksetzen von Passwörtern verwendet werden. Als nächstes sollten die Passwörter von Accounts geändert werden, die als "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 restlichen Accounts zurückgesetzt werden. Dies sollte nicht nur für Accounts erfolgen, die vom Datenleak betroffen waren, sondern alle, die mit denselben Passwörtern benutzt wurden, oder deren Passwort-Zurücksetzen-Funktion auf ein kompromittiertes Postfach verweist.

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

Beim Ändern der Passwörter gelten die Empfehlungen des BSI [1]. Besonders hervorzuheben ist im Rahmen dieses Vorfalls, dass für jeden Account ein unterschiedliches, starkes Passwort verwendet werden sollte. Bei der Verwaltung der Passwörter helfen Passwortmanager (siehe [1]).

Da davon auszugehen ist, dass die Täter mithilfe gestohlener Zugangsdaten vollen Zugriff auf Accounts hatten, sollte geprüft werden, ob Konfigurationsänderungen vorgenommen wurden. Besonders kritisch sind Weiterleitungen in Postfächern, die dafür sorgen würden, dass eingehende Nachrichten an Adressen der Täter weitergeleitet werden. Falls vorhanden, sollten diese Weiterleitungen entfernt werden. Kritisch wären auch von den Tätern ergänzte Rückfalloptionen (Mobilnummern oder E-Mailadressen zum Zurücksetzen von Passwörtern). Diese Konfigurationen sollten auch geprüft und ggf. korrigiert werden.

Maßnahmen zur Prävention

Im Fall des Politleaks scheinen vor allem private Accounts kompromittiert worden zu sein. 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 im folgenden auch Maßnahmen aufgeführt, die von Organisationen umgesetzt werden sollten.

Durch Personen einzeln umsetzbar:

- Verwenden starker Passwörter, idealerweise bei jedem Account unterschiedlich (vgl. [1])
- Wenn vom Anbieter angeboten, Aktivierung von Zwei-Faktor-Authentisierung. Ggf. Wechsel zu einem Anbieter, der Zwei-Faktor-Authentifizierung unterstützt ([2])
- Es empfiehlt sich, beim Login routinemäßig die angegebene letzte Login-Zeit auf Plausibilität zu prüfen (Logins von unbekannten Orten oder über unbekannte Geräte, fehlgeschlagene Logins, parallele Sitzungen etc.)
- E-Mails zu verschlüsseln erhöht den Aufwand für die Täter. Für Webmail empfiehlt das BSI die Browser-Erweiterung Mailvelope
- Prüfen, ob eigene Accounts mithilfe von öffentlich zugänglichen Informationen angreifbar sind, z. B. die Beantwortung von Sicherheitsfragen zum Zugriff oder dem Zurücksetzen des Passworts
- In öffentlichen WLANs Nutzung verschlüsselter VPN-Tunnel, um ein Ausspähen von Informationen im WLAN zu verhindern
- Prüfen, ob Daten (für Backups oder Fotoalben etc.) automatisch zu Cloud-Diensten hochgeladen werden. Diese Funktion ggf. deaktivieren oder für sensible Daten vermeiden.
- Prüfen, welche Apps automatisiert Kontaktlisten zum Anbieter übermitteln, und diese Apps entweder meiden oder nicht für sensible Inhalte benutzen

- Prüfen, ob eigene E-Mail-Konten bereits in öffentlich gewordenen Leaks enthalten sind [3].

- Private Mailpostfächer (GMX, Web.de, Google-Mail, etc.):
  Je nach Nutzungsart und -häufigkeit sollte abgewogen werden, private Postfächer entweder nicht mehr geschäftlich zu nutzen (bereits vorhandene geschäftliche Mails sollten dann ggf. auf einem sicheren Rechner lokal archiviert und aus dem Online-Webspeicher gelöscht werden), oder falls vom Anbieter angeboten um Zwei-Faktor-Authentifizierung zu erweitern

Durch die Organisation (Partei/Fraktion/Verband) umsetzbar:

- Organisations-Webmail (wie Outlook Web Access o. ä.):
  Je nach Nutzungsart und -häufigkeit sollte entschieden werden, Webmail entweder zu deaktivieren, nur per E-Mail-Client oder VPN zugreifbar zu machen, oder durch Zwei-Faktor-Authentisierung abzusichern.
  Erläuterung: In den letzten Monaten wurden wiederholt Angriffsversuche beobachtet, in denen die Täter Domains registrierten, die den offiziellen Webmail-Domains ähnelten. Funktionsträgern wurden Mails im Namen des IT-Supports zugeschickt, die die Empfänger aufforderten, sich auf der manipulierten Webseite mit ihren Zugangsdaten einzuloggen.
- IT-Sicherheitstraining:
  Sensibilisierung zu Phishing und Schadsoftware-Anhängen, 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).
  Erläuterung: Die Täter scheinen sich vor allem auf die oben genannten Rollen und Funktionen zu fokussieren, da in deren Postfächern die relevantesten Inhalte erwartet werden.
- Verdächtige Mails:
  Es empfiehlt sich, eine zentrale Stelle in der Organisation einzurichten, an die verdächtige Mails weitergeleitet werden können. Die zentrale Stelle kann die Mails bewerten und ggf. auf Authentizität prüfen.
- Logging:
  Um Angriffe detektieren oder nachträglich analysieren zu können, sollten Logdaten (mindestens von E-Mail-Servern, Webmail-Servern und VPN-Servern) erhoben werden und an zentraler Stelle gesichert werden.
- Pressestatement:
  Um im Fall von Dokumenten-Veröffentlichungen schnell reagieren zu können, sollte ein Entwurf für ein Pressestatement vorbereitet werden. Die En-Marche-Kampagne wies beispielsweise sehr professionell darauf hin, dass Dokumente gefälscht oder aus dem Kontext gerissen sein können, und warnte vor voreiligen Schlüssen.

Links

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

[2] Liste von Webseiten, die eine Zwei-Faktor-Authentifizierungen erlauben: https://twofactorauth.org/

[3] Auswahl von Leak-Datenbanken zur Recherche:

https://sec.hpi.de/ilc/

https://haveibeenpwned.com/

https://monitor.firefox.com/

https://breachalarm.com/

BSI für Bürger Schutzmaßnahmen & Risiken

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

Fremde WLANs - https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/FremdeWLAN/fremdeWLAN_node.html

Passwörter - https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Sichere Einrichtung Ihrer Software - https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungSoftware_node.html

Spam, Phishing & Co -https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/spamPhishingCo_node.html

Verschlüsselung - https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html

Virtual Private Networks (VPN) - https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/VPN/VPN_Virtual_Private_Network_node.html

Anleitungen zur Einrichtung von Zwei-Faktor-Authentifizierungen

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

Google - https://www.google.com/landing/2step/

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/

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/