Hackerangriffe - Empfehlenswerte Maßnahmen nach erfolgreichen Angriffen

Freitag, 25 Januar 2019

https://www.datenschutz.de/hackerangriffe-empfehlenswerte-massnahmen-nach-erfolgreichen-angriffen/

Aktuelle Meldung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 24.01.2019

Nach einem erfolgreichen Hackerangriff auf eigene Geräte oder Accounts gibt es eine Reihe von Standard-Maßnahmen, die sich für den Betroffenen empfehlen. Sie fallen unterschiedlich aus, je nachdem, ob ein eigenes Gerät (PC, Laptop, Smartphone usw.) betroffen ist oder ein Account im Internet gehackt wurde.

Besonders zu empfehlen ist, sich vor einem Hackerangriff diese Maßnahmen in Ruhe durchzulesen und zu überlegen, was davon auf die eigene Situation passt und auf welche Daten, Geräte oder Accounts man besonders dringend angewiesen ist. Dann sollten entsprechende Sicherungsmaßnahmen (etwa Backups/Sicherungskopien) durchgeführt werden. Der beste Moment dafür ist genau: jetzt.

Bitte lesen Sie diese Hinweise und weitere Informationen (vgl. links unter 8.) genau durch, bevor Sie zur Tat schreiten. Auch die richtige Reihenfolge der Maßnahmen ist von Bedeutung.

1. Bei Angriff auf eigenes Gerät

- Gerät ausschalten und physisch vom Internet und anderen Netzwerken trennen.
  Hinweis: Damit kann die Schadsoftware nicht weiter ausgeführt werden. Üblicherweise ist es sinnvoll, die Aktivitäten der Schadsoftware zu unterbrechen, um den Schaden möglichst gering zu halten.
  (Allerdings kann ein Verschlüsselungstrojaner dann auch nicht den Schlüssel an den Erpresser versenden; dann ist es dem Erpresser auch nicht möglich, die Datenträger wieder zu entschlüsseln).
- Ändern Sie alle Passwörter von allen Diensten, die sie auf diesem Gerät verwendet haben. Angreifer haben diese häufig abgegriffen und können damit z. B. in Social Media Accounts eindringen. Siehe auch Punkt 2.
- Das Gerät von Experten begutachten lassen.
- Das Gerät mit einer Start-DVD o.ä. starten.
  Evtl. versuchen, wichtige Daten zu retten, dabei aber nicht den Infektionsherd weiter verbreiten. Bei Problemen vgl. b.
- Die Festplatte des Rechners anschließend auf jeden Fall komplett löschen (formatieren) und das System komplett neu installieren. Da Schadsoftware zuvor die vollständige Kontrolle über den Rechner hatte, konnte sie beliebige Komponenten nachladen und tief im System verankern. Nur in sehr wenigen Ausnahmefällen auf diese Vorsichtsmaßnahme verzichtet werden und der Rechner trotzdem von der Schadsoftware befreit werden.

2. Bei Angriff auf eigenen Account (E-Mail/online-Banking/Social Media)

Ändern Sie die Zugangsdaten (Passwörter und dergleichen) zu dem kompromittierten Gerät oder Dienst. Hinweise für eine sinnvolle Auswahl von Passwörtern siehe unter https://www.baden-wuerttemberg.datenschutz.de/hinweise-zum-umgang-mit-passwoertern/

Falls das nicht möglich ist, z.B. weil der Angreifer das Passwort selbst bereits geändert hat (und auch das Erzeugen eines neuen Passwortes nicht weiterführt), bleibt nur die Kontaktaufnahme zum Anbieter bzw. Plattformbetreiber. Notieren Sie sich die wichtigsten Kontaktdaten jetzt, später verlieren Sie damit wertvolle Zeit.

Überprüfen Sie genau, welche Geräte und Dienste bzw. Online-Konten betroffen sind. Setzen Sie neue Zugangsdaten (Passwörter) zuerst bei den Diensten ein, mit denen Sie andere Konten zurücksetzen können. Dies sind in der Regel ihre E-Mail-Accounts!

3. Änderung von Zugangsdaten anderer Geräte/Dienste

Ändern Sie auch die Zugangsdaten anderer Geräte oder Dienste, wenn diese gleich/ähnlich dem kompromittierten Passwort sind. Verwenden Sie immer unterschiedliche Passwörter für unterschiedliche Dienste!

4. Prüfung des kompromittierten Geräts/Accounts auf Veränderungen

- Wurden Daten verändert oder gelöscht?
  Dann sollten sie ggf. wiederhergestellt werden.
- Wurden Nachrichten versandt, Rechtsgeschäfte getätigt o.ä.?
  Dann kann sich ein Hinweis an Empfänger oder andere Dritte anbieten (auch: Widerruf, Anfechtung von Erklärungen).
- Wurden sonstige Handlungen getätigt, die sich negativ auswirken können? Z.B. unter Vorspiegelung der „gekaperten“ Identität rechtswidrige Inhalte erstellt oder abgerufen?
  Dann kann sich ebenfalls die Information Dritter, auch der Polizei oder Staatsanwaltschaft anbieten.
- Falls das E-Mail-Konto kompromittiert wurde:
  Wurden durch den Angreifer neue Passwörter für andere Dienste beantragt, die per E-Mail versandt wurden? Da der Angreifer diese E-Mails gelöscht haben kann, sollten andere Konten, die mit der E-Mail-Adresse verknüpft sind, geprüft werden. Passwörter ändern nicht vergessen!
- Ähnliches gilt für Konten bei denen man sich mit Zugangsdaten anderer Konten anmeldet („Single-Sign-On“, z.B. Facebook-Login).

5. Anzeige erstatten

Anzeige bei Polizei oder Staatsanwaltschaft ist möglich und sinnvoll. Vorsicht: Durch Maßnahmen zur Beendigung des Angriffs bzw. zur Behebung der Schäden können Spuren vernichtet werden. Kontaktieren Sie im Zweifel vorher die Polizei.

6. Eigene Pflichten erfüllen

Sind Sie selbst Verantwortlicher oder Auftragsverarbeiter im Sinne der DS-GVO, so sind folgende Maßnahmen geboten:

- Einbeziehen des eigenen Datenschutzbeauftragten
- Prüfen und verbessern der wohl unzureichenden technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO. Falls menschliches Versagen (z.B. E-Mail-Anhang mit Malware geöffnet): Schulungen und Virenschutz verbessern.
- Prüfen der Meldepflicht gegenüber der Datenschutz-Aufsichtsbehörde nach Art. 33 DS-GVO.
- Prüfen einer Benachrichtigungspflicht gegenüber den betroffenen Dritten nach Art. 34 DS-GVO.

7. Weitere Maßnahmen

Weitere Maßnahmen sind abhängig vom technischen Zugriffsweg, von der Art der Daten und der Schutzbedürftigkeit der Betroffenen. Z.B.

1. Sperrung von kompromittierten Kredit- u.ä. Karten (Karten-Sperr-Notruf 116116).
2. Können Angriffe auf Dritte nun einfacher erfolgen? Dann Dritte und/oder Datenschutz-Aufsichtsbehörde warnen.
3. Sind Daten unbefugt im Internet veröffentlicht worden? Dann den jeweiligen Anbieter und/oder Hosting-Provider benachrichtigen und um Löschung (Art. 17 DS-GVO) ersuchen. Ist dies nicht erfolgreich, siehe Punkt 8.
4. Betreiber von Suchmaschinen können aufgefordert werden, verletzende oder ehrenrührige Treffer auszublenden (vgl. dazu die Informationen der Suchmaschinenbetreiber, zu Google etwa https://support.google.com/websearch/troubleshooter/3111061).

Wer hilft weiter?

- Datenschutz-Aufsichtsbehörden, z.B. https://www.baden-wuerttemberg.datenschutz.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de
- Das BSI hat dazu auch wichtige Tipps zu Hackerangriffen veröffentlicht: https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_fuer_Betroffene_von_Datenleaks_08012019.html
- Landeskriminalamt Baden-Württemberg, https://lka.polizei-bw.de/
- Bundeskriminalamt (BKA), https://www.bka.de

Die Pressemitteilungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg können hier abgerufen werden.
