Wie stelle ich einen Hackerangriff fest?

Intention

In diesem Pattern wird beschrieben, mit welchen Methoden festgestellt werden kann, ob die eigene Website gehackt wurde.

Problemstellung

Bei einem perfekten Verbrechen werden sprichwörtlich keine Spuren hinterlassen. Im Internet keine Spuren zu hinterlassen ist jedoch schwerer als man denkt. Dennoch kann es Laien schwer fallen Spuren nach oder während einer Cyber-Attacke zu finden. Durch fehlendes Fachwissen, können viele Spuren übersehen oder gar nicht erst gefunden werden. In solchen Fällen ist das Feststellen eines Hackerangriffs auf die eigene Website reine Glückssache.

Szenario

Ein Hacker verschaffte sich unbemerkt Zugriff auf die eigene Onlinepräsenz.

Lösung

Folgende Punkte können darauf hinweisen, dass eine Seite gehackt wurde:

- Der Webhoster hat die Seite deaktiviert.
- Verdächtige Nachrichten / Bilder / Texte oder Popups tauchen auf, wenn die Website besucht wird (unter anderem durch *Ransomware*, *Defacement der Website*).
- Links auf der Website leiten auf andere Inhalte weiter (*Phishing*, *Spamvertised* Content).
- Die eigene Seite leitet auf eine andere Seite weiter (*Hijacking*).
- Passwörter für den/die Adminaccount(s) funktionieren nicht mehr.
    - **ACHTUNG** – Sollte dies zutreffen, muss man alle Geräte auf Schadsoftware überprüfen von denen man auf diesen Account zugegriffen hat.
- Es sind Programme, *Widgets*, *Plugins* oder Features installiert, die vorher nicht installiert waren.
- Nutzerbeschwerden über verschiedenste Kanäle (z.B. per Mail) häufen sich.
- Neue Unterseiten mit anderem Inhalt.

Sofern einer oder mehrere dieser Punkte zutreffen, hat sich mit größter Wahrscheinlichkeit jemand Zugriff auf die Seite verschafft.

Folgende Schritte können unternommen werden, sofern Erfahrung mit der Linux Shell vorhanden ist:

- Logs nach verdächtigen Aktivitäten durchsuchen.
    - Logins von unbekannten *IP Adressen*
    - Fehlgeschlagene Login-Versuche
- Prozesse auf dem Server durchsuchen und nach Programmen oder Aktivitäten suchen, die einem nicht bekannt sind.
- Netzwerkkonnektivität des Servers überprüfen.
- Nach verdächtigen oder unbekannten Ordnern oder Dateien suchen und diese gegebenenfalls überprüfen.
    - .htaccess Dateien
    - .php, .html Dateien
    - Mediendateien
    - Datum der letzten (Datei-)Änderung überprüfen
- Cron Jobs überprüfen.

Sofern festgestellt wird, dass die Seite einer Cyberattacke zum Opfer gefallen ist kann das Pattern „Was ist während oder nach einem Hackerangriff zu tun?“ weiterhelfen.

Beispiele

Defacement

Beim Defacement wird der sichtbare Bereich der Seite verändert. Üblich sind Texte oder Bilder, die darauf hinweisen, dass die Seite eine Cyber-Attacke zum Opfer fiel. Sofern die eigene Seite

betroffen ist, sollte diese Offline genommen werden. Danach empfiehlt es sich ein Backup aufzuspielen und dieses mit den aktuellsten Updates zu versorgen. Sobald dies erledigt ist, kann die Seite wieder online gehen.

Logfiles überprüfen (Apache Server, englisch)

- https://httpd.apache.org/docs/2.4/logs.html

Alle laufenden Prozesse auf dem Server anzeigen (Linux, englisch)

- https://www.cyberciti.biz/faq/show-all-running-processes-in-linux/

Gefährliche bzw. unerwünschte Prozesse erkennen (Linux, englisch)

- https://ma.ttias.be/how-to-identify-the-bad-processes-on-a-hacked-linux-box/

Cron-Jobs überprüfen

- https://cronjob-tipps.de/was-cronjobs-sind-und-wofuer-sie-gut-sind/

Cron-Jobs auflisten bzw. anzeigen lassen (englisch)

- https://www.cyberciti.biz/faq/linux-show-what-cron-jobs-are-setup/

Onlinetools verwenden, die nach verdächtigen Inhalten suchen (z.B. Google Conditional Hacks) oder Auskunft über den Status geben:

- Google Tool zum Überprüfen der Website: https://transparencyreport.google.com/safe-browsing/search
- Überprüft ob Spam-Links, versteckte Weiterleitungen oder ähnliches auf der Seite zu finden sind: http://isithacked.com
- Dieses Tools überprüft ob die Website *URL* in einer Phishing-Datenbank auftaucht oder bei Google als schädlich gelistet wurde: https://aw-snap.info/utilities/is-flagged.php, https://sitecheck.sucuri.net
- Diese Seite überprüft ob Viren oder Malware über eine Website verteilt werden: https://www.virustotal.com/#/home/url
- Abruf einer Seite "Wie durch Google": https://support.google.com/webmasters/answer/6066468?hl=de

Wurden meine Daten gehackt?

Die untenstehenden Seiten zeigen ob persönliche Identitätsdaten im Internet veröffentlicht wurden. Dabei wird mit Hilfe einer E-Mail-Adresse ein Datenabgleich durchgeführt und überprüft ob bereits Daten in Internet-Datenbanken kursieren.

- https://haveibeenpwned.com
- https://breachalarm.com
- https://sec.hpi.de/ilc/search

Referenzen

https://developers.google.com/web/fundamentals/security/hacked/how_do_I_know_if_site_hacked
https://developers.google.com/web/fundamentals/security/hacked/
https://www.csoonline.com/article/2457873/data-protection/signs-youve-been-hacked-and-how-to-fight-back.html
https://www.strato.de/faq/article/1089/Woran-erkenne-ich-dass-meine-Webseite-gehackt-wurde.html
https://www.checkdomain.de/blog/allgemein/website-gehackt-jetzt/
https://codex.wordpress.org/FAQ_My_site_was_hacked
https://symetris.ca/blog/my-websites-been-hacked-now-what
https://www.whoishostingthis.com/resources/website-hacked-checklist/
https://www.cyberciti.biz/faq/

Keywords

Hacking, Cyber-Attacke, Prävention, Server