Was ist während oder nach einem Hackerangriff zu tun?

Intention

Dieses Pattern soll eine Art Leitfaden sein, im Falle eines Hackerangriffs auf die eigene Website.

Problemstellung

Websitebesitzer erkennen meist erst relativ spät, dass die eigene Seite gehackt wurde. Offensichtlich ist es jedoch, wenn Besucher der Website durch den Browser darauf aufmerksam gemacht werden, dass die Seite unsicher ist. In einem solchen Fall muss schnell gehandelt werden um den (Image-)Schaden zu minimieren.

Szenario

Man wird von Seitenbesuchern oftmals darauf aufmerksam gemacht, dass die Browser davor warnen die Website zu besuchen. Dies ist ein guter Indikator dafür, dass man aktiv werden sollte.

Lösung

Erst einmal Ruhe bewahren**. Wenn man selbst eine Lösung kennt und es sich zutraut, die Situation unter Kontrolle zu bringen zu, sollten folgende Punkte nach und nach abgearbeitet werden:**

- Den eigenen Computer auf Viren und Malware überprüfen
    - Damit man sicher gehen kann, dass man nicht selbst das Einfallstor für die Angreifer gewesen ist.
- Den Webhoster kontaktieren
    - Webhoster sind mit dieser Art von Problem tagtäglich konfrontiert, dementsprechend können sie einem unter Umständen weiterhelfen.

Die nachfolgenden Schritte sollten nur über ein sicheres System durchgeführt werden:

- Admin-Accounts überprüfen und Passwörter ändern
    - Zuallererst sollten die Admin-Accounts überprüft werden. Ist ein Login möglich, ist es sinnvoll sicherheitshalber das Passwort zu ändern.
    - Dies sollte bei allen Accounts durchgeführt werden, die Zugriff auf das CMS, den Webserver oder auf die Datenbank haben.
    - Ist der Zugriff auf einen Account mit dem bekannten Passwort nicht möglich, so ist dieser Account mit großer Wahrscheinlichkeit kompromittiert worden.
        - Das Passwort dieses Accounts muss in diesem Fall geändert werden.
        - Um komplett sicher zu gehen, empfiehlt es sich diesen Account zu löschen.
        - Automatisches blocken aller IP-Adressen, von denen versucht wird, sich weiterhin mit den Login-Daten des gelöschten Accounts anzumelden.
- Backup der Seite erstellen
    - Auch wenn die Seite gehackt oder infiziert wurde, lohnt es sich, diese abzusichern. Einerseits um nachzuvollziehen was geändert wurde und welche Dateien geändert wurden, aber auch um Beweise zu sichern mit denen man gegebenenfalls Schadensersatzansprüche geltend machen kann.
- Website Offline setzen
    - Damit die Seite keinen weiteren Schadcode verteilen kann.
- Logfiles überprüfen
    - Logfiles können Auskunft darüber geben woher oder auch von wem der Angriff stammen kann und wie sich die Angreifer Zugriff auf das System verschafft haben.
- Daten auf dem Webspace löschen
    - Damit sind nicht nur die Daten auf dem FTP Server gemeint, sondern auch die Datenbank.
- Passwörter zur Sicherheit noch einmal ändern

Fürs erste ist damit sichergestellt, dass kein weiterer Schaden mehr von der Seite ausgehen kann.

Folgende Schritte sind optional durchführbar:

- Sich bei einer der offiziellen Meldestelle für Internetkriminalität melden und den Fall erklären
    - E-Mail: against-cybercrime@bmi.gv.at
        - In der Mail sollte erklärt werden worum es sich handelt und was passiert ist. Die Meldestelle wird versuchen eine Lösung anzubieten oder zumindest auf Stellen zu verweisen, die einem weiterhelfen können.
        - Die Erstattung einer Anzeige via Meldestelle ist derzeit leider noch nicht möglich.
- Bei Straftaten durch konkrete Personen ist eine Anzeige bei jeder Polizeidienststelle möglich.
- Cyber-Security-Hotline für Unternehmen (Kostenlos für Mitglieder der WKO): 0800 888 133
    - Weitere Informationen hierzu: https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html

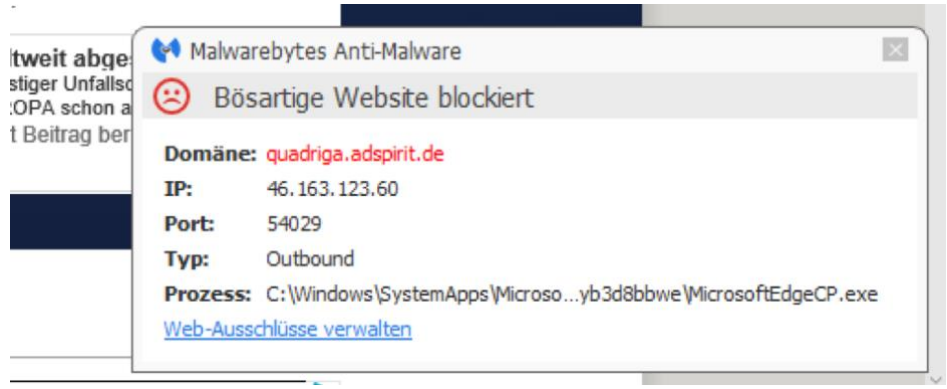
- Die Seite aus einem Backup neu hochladen
    - Wenn regelmäßig Backups erstellt wurden, kann nach einer vorherigen Überprüfung auf Unversehrtheit ein Backup der Seite hochladen werden.
    - **Nicht vergessen, danach die Passwörter sicherheitshalber zu ändern!**

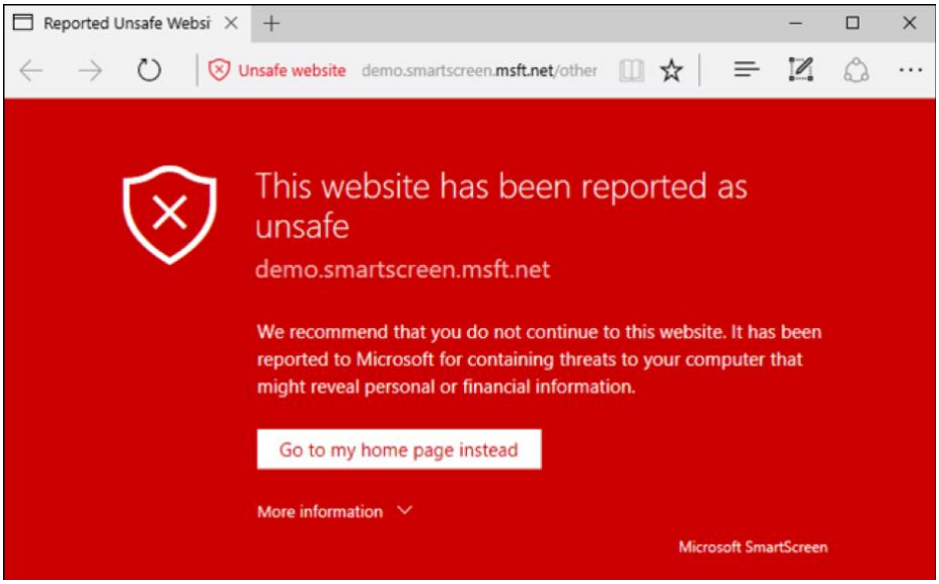
Achtung! – Wenn man nicht selbst Herr der Lage werden kann, empfiehlt es sich, dies einem Experten zu überlassen.

Beispiele

Warnungen vor bösartigen Websites

Sofern eine Seite als bösartig eingestuft wurde, zeigen Webbrowser entsprechende Warnungen an. Falls beim Besuch der eigenen Seite eine solche Warnungen auftaucht, sollte schnellstmöglich etwas unternommen werden.





Backups erstellen

Wie Backups erstellt werden und wann dies getan werden sollte, wird in Pattern „**Wann und wie sollte man Backups erstellen?**“ erläutert.

DDoS Attacken

Sollte die eigene Seite nicht mehr erreichbar sein oder der Fehler 503 auftauchen, kann es sein, dass der Seite momentan ein DDoS Angriff widerfährt. Mehr zu diesem Thema findet man im Pattern: „**Was kann man gegen DDoS Attacken tun?**“.

Referenzen

https://www.onlinesicherheit.gv.at/erste_hilfe/meldestellen/249337.html
https://www.hosttest.de/artikel/webseite-gehackt-was-tun-1062.html

Keywords

Hacker, Sicherheit, Backups, Meldestelle