Was trägt alles zur Sicherheit einer Website bei?

Intention

Dieses Pattern zählt verschiedene Punkte auf, die zur Absicherung der eigenen Website beitragen können.

Problemstellung

Im Laufe der letzten Jahre stieg die Anzahl der Angriffe auf Websites. Vor allem Webshops und Websites die mit Nutzerdaten hantieren sind extrem davon betroffen. Es stellt sich die Frage, wie die eigene Seite vor solchen Angriffen geschützt werden kann?

Szenario

Angriff ist die beste Verteidigung! Um die Sicherheit von Websites zu testen, werden oft selbst bekannte Angriffe auf diese ausgeführt. Sollte ein Angriff gelingen, so hat man eine Schwachstelle ausfindig machen können, um die man sich kümmern sollte.

Lösung

- Zugriff auf den Webserver sollte nur von einem sicheren System aus geschehen.
    - Ein sicheres System besitzt die aktuellsten Sicherheitsupdates und ist im besten Fall mit einem Virenscanner ausgestattet.
- Keine externe Hardware (vor allem aus unbekannten Quellen) an Systeme oder Server Hardware anschließen.
    - Datenträger oder sonstige Hardware vor dem Anschließen mit einem Virenscanner auf Schadsoftware überprüfen.
- Anzahl der Admin Accounts limitieren.
    - Admins haben in einem System alle Rechte. Daher sollten nur Experten oder verantwortliche Accounts Administratorrechte besitzen.
- Sichere Admin-Passwörter verwenden.
    - Studien belegen, längere Passwörter (10 Zeichen oder mehr) sind generell sicherer als kurze (auch wenn kurze Passwörter Sonderzeichen verwenden).
- 2-Faktoren-Authentifizierung.
    - Für den Fall, dass ein Angreifer ein Passwort in Erfahrung gebracht hat, bietet eine 2-Faktoren-Authentifizierung eine weitere Sicherheitsbarriere.
- Benutzergruppen einrichten und Zugriffsrechte setzen.

    - Lese und Schreibrechte für jeden Benutzer oder jede Benutzergruppe separat setzen. Wichtige oder systemrelevante Dateien werden dadurch vor Manipulation sowie vor dem Zugriff Unberechtigter geschützt.
- Sich über bekannte Angriffe und Sicherheitslecks informieren.
    - Hier findet man eine gute Anlaufstelle.
- Verschlüsselung der Kommunikation (*HTTPS*)
    - Dies dient der Datensicherheit beim Datenaustausch, zudem hilft eine Verschlüsselung die Datenintegrität zu gewährleisten.
- Aufruf der Seite nur mit einer verschlüsselten Verbindung erlauben.
    - Jegliche Kommunikation mit der Website findet ausschließlich verschlüsselt statt.
    - Wird eine Seite mit http://www.secpatt.at aufgerufen, leitet diese automatisch auf https://www.secpatt.at weiter.
    - *HSTS Header* verwenden um *HTTPS* zu erzwingen
- Regelmäßige Backups
    - Backups tragen dazu bei sich abzusichern. Beschädigte oder korrumpierte Dateien, können mit Hilfe eines Backups wiederhergestellt werden.
    - Einige Hoster erstellen automatisiert selbstständig Backups. Es empfiehlt sich die Leistungen des eigenen Hosters zu prüfen und bei Bedarf auf diesen Service zuzugreifen.
    - Mehr zu diesem Thema bietet das Pattern: „**Wann und wie oft sollte man Updates installieren?**“
- Plugins und Software aus vertraulichen Quellen verwenden
    - Software oder Plugins für ein *CMS* (z.B. WordPress) nur aus vertraulichen Quellen herunterladen und verwenden. Ist die Quelle einer Software-Applikation unbekannt, sollte diese nicht verwendet werden.
    - Eine vertrauliche Quelle für WordPress-Plugins wäre beispielsweise: https://de.wordpress.org/plugins/. Bei den Applikationen sollte man generell auf die Bewertung und Erfahrungsberichte von anderen Nutzern achten, um potenzielle Probleme zu vermeiden.
- Sicherheits-Plugins für CMS verwenden
    - Sicherheits-Plugins für ein CMS sind eine gute Ergänzung.
    - Plugins sollten nur aus vertrauenswürdigen Quellen geladen bzw. erworben werden. Es empfiehlt sich die Ratings und Reviews der einzelnen Plugins durchzulesen.
- Website mit ScanTools auf Sicherheitslecks testen.
- Virenscanner können ebenfalls ein Einfallstor für Viren oder Malware sein
    - Verwendung etablierter und bekannter Virenscanner, die mit Updates aktuell gehalten werden.
- *XSS* Prävention
    - Benutzereingaben überprüfen um somit das Einschleusen von HTML, URL und JavaScript zu unterbinden.
    - Für bekannte *CMS* gibt es hierfür auch Plugins.
- Prävention von *SQL-* oder *Code-Injection*
    - Mehr herzu in folgendem Blogpost: https://blog.varonis.de/sql-injection-verstehen-erkennen-und-verhindern/

Beispiele

Regelmäßige Updates
Um die Sicherheit der Website sowie der Systeme, die auf den Webserver zugreifen zu gewährleisten, muss auf die Aktualität der Software geachtet werden. Im Pattern: „**Wann und wie oft sollte man Updates installieren?**“ wird im Detail darauf eingegangen.

Verschlüsselte Kommunikation mit der Website
Im Pattern „**Wie verschlüssele ich die Kommunikation mit meiner Website?**“ wird beschrieben wie man eine *SSL / TLS* Verschlüsselung in die eigene Seite integriert.

ScanTools
Sofern die Seite sowie die Systeme abgesichert sind, empfiehlt es sich die Seite mit **ScanTools** auf bekannte Schwachstellen zu überprüfen. ScanTools überprüfen verschiedenste Sicherheitsaspekte einer Website und zeigen eventuelle Schwachstellen im System auf. Mehr Informationen zu diesem Thema liefert das Pattern „**Wie überprüfe ich die Sicherheit meiner Webseite?**“.

Sich über Gefahren informieren

- https://www.heise.de/security/
- http://seclists.org

Unterbinden von *XSS (Cross Site Scripting)*

Folgende Seiten geben Auskunft darüber wie man *XSS* unterbinden kann:

- https://www.php-kurs.com/cross-site-scripting-xss-unterbinden.htm
- https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

HSTS Header mit Apache Server

Mit folgendem Code in der .htaccess Datei kann eine verschlüsselte Verbindung erzwungen werden, sofern die Website es unterstützt:

```
# Use HTTP Strict Transport Security to force client to use secure connections only

Header set Strict-Transport-Security "max-age=3600" env=HTTP
```

Mehr hierzu unter: https://www.cyon.ch/support/a/wie-aktiviere-ich-http-strict-transport-security-hsts-fur-meine-website

Referenzen

Studien zum Thema Passwort-Sicherheit (Zugangsberechtigung erforderlich):

https://ieeexplore.ieee.org/abstract/document/6234434/?part=1
https://dl.acm.org/citation.cfm?id=1753384

Mehrfaktoren-Authentifizierung:

https://www.onlinesicherheit.gv.at/praevention/konten_und_passwoerter/mehrfaktor-authentifizierung/249584.html

Keywords

Sicherheit, Verschlüsselung, Authentifizierung