IS-Webcheck

Sicherheits-Check für Webauftritte durch das BSI

Einleitung

Ein *IS-Webcheck* („IS“ kurz für Informationssicherheit) testet Webauftritte oder deren Teilbereiche sowohl mit automatisierten als auch manuellen Verfahren auf Schwachstellen. Hierbei wird – wenn möglich – über das Internet auf die zu prüfenden Systeme zugegriffen, um vergleichbare Voraussetzungen wie bei einem Angriff zu erreichen.

Das BSI führt *IS-Webchecks* für Bundes- und Landesbehörden oder Betreibende Kritischer Infrastrukturen durch. Hierdurch sollen gängige Schwachstellen in deren Webauftritten aufgedeckt und den Betreibenden eine Hilfestellung gegeben werden, die eigenen Angebote besser abzusichern.

In dieser Kurzdarstellung wird die Vorgehensweise beschrieben, nach der das BSI grundsätzlich *IS-Webchecks* durchführt.

Beschreibung der getesteten Umgebung

Ein Webauftritt besteht meistens aus Kombinationen von Webservern, Webanwendungen und Datenbanken. Zum Schutz des Webauftritts werden üblicherweise vorgelagerte Sicherheitsgateways verwendet, bestehend aus Paketfiltern (kurz „PF“), Proxys und/oder Web Application Firewalls (kurz „WAF“). Diese sollen vor Angreifenden aus dem Internet schützen, indem die gesamte Kommunikation mit einer Unterscheidung zwischen schadhaftem und beabsichtigtem HTTP-Verkehr (Hypertext Transfer Protocol), analysiert sowie durch festgelegte Regeln gefiltert wird.

Obwohl hierdurch der Schutz der Systeme deutlich erhöht wird, können Angreifende unter Umständen weiterhin erfolgreich Angriffe durchführen. Durch eine eventuelle Fehlkonfiguration oder eine ausgenutzte Schwachstelle im Sicherheitsgateway, kann eine angreifende Entität trotzdem ein potenziell verwundbares System hinter dem Schutzwall vorfinden, wenn die Webanwendung selbst nicht ausreichend abgesichert ist.

Weiterhin ist zu beachten, dass Sicherheitsgateways oftmals eine Vielzahl von Systemen absichern und damit sehr generisch gegen Angriffe aufgestellt werden. Dadurch kann die Absicherung, die für eine Anwendung notwendig ist, für eine andere hinderlich sein. In einem solchen Fall werden häufig kurzfristig Regeln gelockert, ohne zu prüfen, ob hierdurch eine andere Anwendung angreifbar wird.

Darüber hinaus werden ausschließlich bekannte Angriffsmuster abgewehrt. Angreifende entwickeln jedoch täglich neue Methoden. Eine parameterbezogene Eingabevalidierung

innerhalb der Webanwendung kann an dieser Stelle viele Schwächen von vornherein ausschließen.

Grundsätzlich ist es daher nicht empfehlenswert, sich **allein** auf die (möglicherweise eingeschränkte) Schutzwirkung eines Sicherheitsgateways zu verlassen. Stattdessen sollte vor allem die Webanwendung so sicher wie möglich implementiert sein.

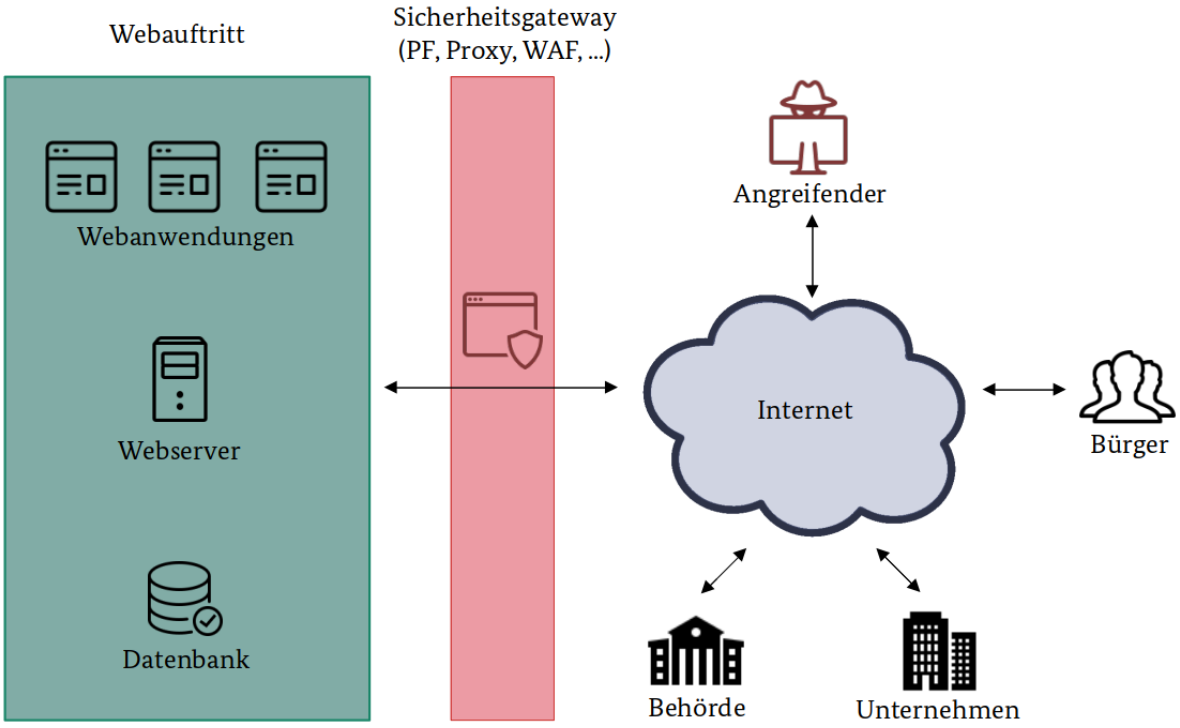

Abbildung 1: Zugriff auf einen Webauftritt[1]

Vorgehensweise

Aus den zuvor genannten Gründen konzentriert sich das BSI bei einem *IS-Webcheck*, auch wenn ein Sicherheitsgateway eingesetzt wird, nur auf die eigentliche Webanwendung.
Falls ein Live-Auftritt getestet wird, bedeutet das nicht, dass alle Schutzmaßnahmen abgeschaltet werden müssen. Lediglich für den Testzeitraum müssen entsprechende Freigaben in dem Sicherheitsgateway eingerichtet werden.

Ein Test des Webauftritts mit vorgeschaltetem Sicherheitsgateway liefert weniger klare Ergebnisse bezüglich der Webanwendung selbst, weswegen hiervon abgeraten wird. Um die korrekte Konfiguration und Wartung des Sicherheitsgateways zu überprüfen, empfiehlt das BSI, hierfür zusätzlich einen IS-Penetrationstest durchzuführen.

[1]Bildquelle: https://icons8.de/

Die grundsätzliche Durchführung eines *IS-Webchecks* erfolgt über das Internet, ausgehend vom Standort des BSI. Ausnahmen hiervon können gegebenenfalls vereinbart werden.

Um einen *IS-Webcheck* durchführen zu können, wird ein **schriftlicher Antrag** benötigt, welcher auf der Homepage des BSI zu finden ist[2] und insbesondere per E-Mail gestellt werden kann. Der Antrag wird von der oder dem IT-Sicherheitsbeauftragten, der IT-Leitung oder der Behördenleitung unterschrieben. Werden von der zu testenden Anwendung personenbezogene Daten verarbeitet, so müssen zusätzlich die oder der Datenschutzbeauftragte und der Personalrat hinzugezogen werden.

Vor der Durchführung eines *IS-Webchecks* wird ein **Erstgespräch** durchgeführt, um die Rahmenbedingungen und technischen Details zu klären. Es wird, je nach Ausführlichkeit des Antrags, beispielsweise erfragt, ob eine WAF eingesetzt wird oder relevante Maßnahmen nach BSI IT-Grundschutz umgesetzt wurden. Eine ebenfalls wichtige Frage im Vorfeld ist, ob das Webangebot selbst oder über einen externen Dienstleistenden gehostet wird. Ist Letzteres der Fall, so muss dieser in den Auftrag eingebunden werden.

Im Anschluss an den darauffolgenden **Vertragsabschluss** wird ein Termin vereinbart, an dem die zum ***IS-Webcheck*** gehörenden Tests durchgeführt werden. Es ist wichtig, dass zu diesem Zeitpunkt eine kompetente Ansprechperson der Behörde bzw. des Hosters die getesteten Systeme beobachtet. Einerseits können hierdurch die potenziellen Wege von Angreifenden direkt nachverfolgt, andererseits gegebenenfalls gefundene Schwachstellen beseitigt werden.

Das BSI-Prüfteam führt zwar keine destruktiven Tests durch, dennoch kann es aufgrund von Fehlkonfigurationen oder Schwachstellen durch die *IS-Webchecks* zu Abstürzen einzelner Systeme oder zu einem (teilweisen) Datenverlust kommen. Auch hierbei ist wichtig, dass jemand vor Ort diese negativen Reaktionen sofort beheben kann, und dass aktuelle Datensicherungen vorliegen. Aus diesem Grund müssen betroffene Kunden oder Mitarbeitende ebenfalls über die stattfindenden Tests informiert werden.

Nach Abschluss des *IS-Webchecks* wird ein umfangreicher **Bericht** erstellt, der den Beteiligten ausgehändigt wird.

Die Ergebnisse und alle während der Tests gewonnenen Erkenntnisse werden vertraulich behandelt.

Bericht und Maßnahmenempfehlung

Der durch das BSI-Prüfteam erstellte Bericht gliedert sich entsprechend der Kritikalität der gefundenen Schwachstellen. Für jede dieser wird anhand eines Beispiels die davon ausgehende Gefahr beschrieben.

[2]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Antrag_Webcheck.pdf

Außerdem werden Maßnahmenempfehlungen zur Beseitigung der detektierten Sicherheitslücken beziehungsweise zur Steigerung des allgemeinen/speziellen IT-Sicherheitsniveaus aufgelistet. Dabei werden sowohl fundamentale Grundschutz- als auch individuelle Maßnahmen thematisiert.

Abgrenzung

Ein *IS-Webcheck* stellt nur eine Momentaufnahme dar, da täglich neue Schwachstellen bekannt werden, und außerdem jeder Webauftritt ein dynamisches System darstellt. Um das Sicherheitsniveau nicht nur für den Augenblick zu erhöhen, wird empfohlen, den *IS-Webcheck* regelmäßig, mindestens alle drei Jahre, zu wiederholen.

Ein *IS-Webcheck* zeigt, wie andere Sicherheitsprüfungen auch, welche Sicherheitslücken zum Prüfzeitpunkt mit vertretbarem Untersuchungsaufwand und den vereinbarten Methoden gefunden wurden. Er liefert keine Garantie dafür, dass alle Schwachstellen tatsächlich gefunden werden. Durch die *IS-Webchecks* kann aber ein hohes Maß an zusätzlichem Sicherheitsgewinn bewirkt werden, der die Betreibenden von Webauftritten im Internet gut gegen Angriffe schützt.

Um das Sicherheitsniveau weiter zu erhöhen, wird empfohlen, zusätzliche Prüfmethoden – beispielsweise IS-Penetrationstests oder Codeanalysen – auf die beteiligten Systeme anzuwenden.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
– Penetrationstests –
Postfach 20 03 63
53133 Bonn

E-Mail: it-pentest@bsi.bund.de