IS-Webcheck

Sicherheits-Check für Webauftritte durch das BSI

Einleitung

Ein *IS-Webcheck* testet Webauftritte oder deren Teilbereiche mit automatisierten Verfahren auf Schwachstellen. Hierbei wird - wenn möglich - über das Internet auf die Angebote zugegriffen, um einem Angriff vergleichbare Voraussetzungen zu nutzen.

Das BSI führt *IS-Webchecks* grundsätzlich nur für Bundesbehörden oder Institutionen im besonderen staatlichen Interesse durch. Hierdurch sollen gängige Schwachstellen in deren Webauftritten aufgedeckt werden und den Betreibern 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 Sicherheitsgateways bestehend aus Paketfiltern, Proxies und/oder Web-Application-Firewalls (WAF) verwendet.

Das vorgelagerte Sicherheitsgateway soll vor Angreifern aus dem Internet schützen. Wird hier ein herkömmlicher Paketfilter oder ein einfacher Proxy eingesetzt, so findet die Filterung im Regelfall auf Protokollebene statt. Hierbei liegt wahrscheinlich eine Konfiguration vor, die den kompletten http-Verkehr durchlässt. Es findet keine Unterscheidung statt, ob schadhafter http-Verkehr oder beabsichtigter Verkehr vorliegt, sodass kein wirklicher Schutz des Webauftritts stattfindet.

Bei erweiterten Proxies oder WAFs findet eine Analyse des http-Verkehrs statt und nach vorher festgelegten Kriterien werden Teile daraus herausgefiltert.

Auch wenn hierdurch der Schutz der Systeme deutlich erhöht wird, können Angreifer unter Umständen weiterhin in die Systeme eindringen. Bei einer eventuellen Fehlkonfiguration oder einer ausgenutzten Schwachstelle im Sicherheitsgateway, findet ein Angreifer trotzdem ein potenziell verwundbares System hinter dem Schutzwall vor, wenn die Webanwendung nicht selbst ausreichend abgesichert ist.

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

Darüber hinaus werden innerhalb eines Sicherheitsgateways bekannte Angriffsmuster abgewehrt. Findige Angreifer entwickeln jedoch täglich neue Methoden, Angriffe durchzuführen. Eine parameterbezogene Eingabevalidierung innerhalb der Webanwendung kann hier viele Schwächen von vornherein ausschließen.

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

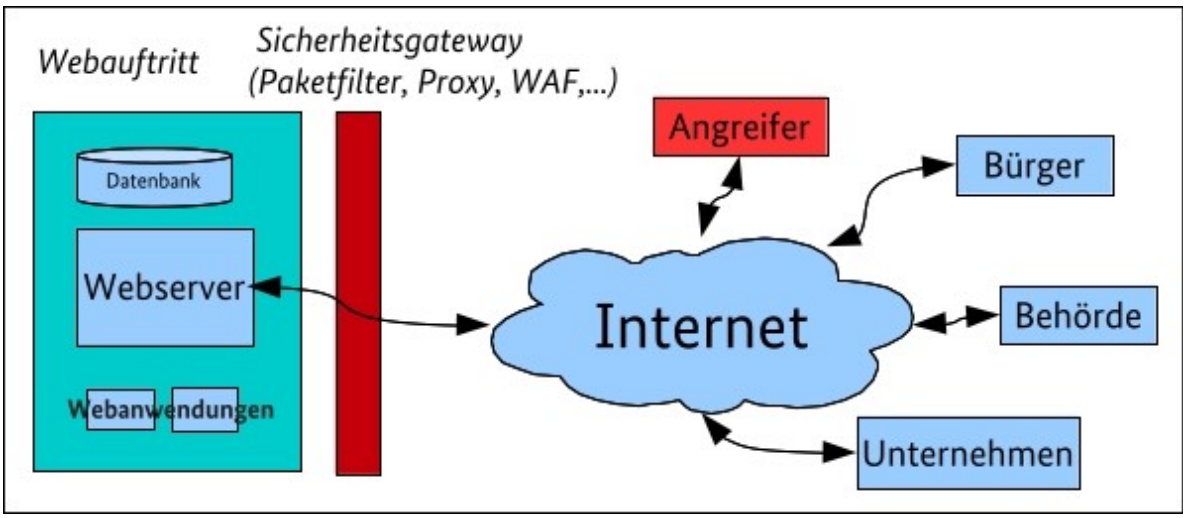

Abbildung 1: Zugriff auf Webauftritt

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 die Zeitspanne der Tests, müssen für das Testteam Freigaben in dem Sicherheitsgateway freigeschaltet werden.

Ein Test auf den Webauftritt mit vorgeschaltetem Sicherheitsgateway liefert keine klaren Ergebnisse bzgl. der Webanwendung selbst, weswegen hiervon abgeraten wird. Um die Sicherheit des Sicherheitsgateways selbst zu testen, empfiehlt das BSI, dass hierfür zusätzlich ein IS-Penetrationstest vor Ort durchgeführt wird.

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

Jeder *IS-Webcheck* startet mit einem Erstgespräch. Je nach Umfang wird dieses telefonisch oder aber auch persönlich durchgeführt. Bei dem Gespräch werden die Randbedingungen geklärt. Hierbei wird beispielsweise erfragt, ob eine WAF eingesetzt wird oder die Methodik nach ISO 100-2 und 100-3 eingehalten wurde und die relevanten Maßnahmen der BSI-Grundschutz-kataloge umgesetzt sind. Eine ebenfalls wichtige Frage, die im Vorfeld der Tests zu klären ist, ist, ob das Webangebot selbst gehostet wird oder über einen externen Dienstleister. Ist Letzteres der Fall, so muss dieser in den Auftrag eingebunden werden.

Sind sich beide Seiten über die Vorgehensweise einig, erfolgt die schriftliche Beauftragung des BSI (gerne auch per E-Mail). Der Antrag wird von dem IT-Sicherheitsbeauftragten oder dem IT-Leiter der Behörde unterschrieben. Werden von der zu testenden Anwendung personenbezogene Daten bearbeitet, so müssen der Datenschutzbeauftragte und der Personalrat hinzugezogen werden.

Nach Eingang des Antrags wird ein Termin vereinbart, wann die zum *IS-Webcheck* gehörenden Tests durchgeführt werden. Es ist wichtig, dass bei diesem Termin ein kompetenter Ansprechpartner der Behörde bzw. des Hosters die getesteten Systeme vor Ort beobachtet. Einerseits kann er hierdurch die potenziellen Wege von Angreifern direkt verfolgen und andererseits ggf. gefundene Schwachstellen sofort nach Abschluss der Tests beseitigen.

Die BSI-Tester führen zwar keine destruktiven Tests durch, bei vorliegenden Fehlkonfigurationen oder unbeseitigten Schwachstellen kann es durch die *IS-Webchecks* aber dennoch zu kurzen Abstürzen einzelner Systeme kommen. Auch hierbei ist wichtig, dass jemand vor Ort diese negativen Reaktionen sofort beheben kann. Aus diesem Grund sollten betroffene Kunden oder Mitarbeiter über die stattfindenden Tests ebenfalls benachrichtigt werden.

Je nach Fall werden die *IS-Webchecks* mehrfach (bei Bedarf auch an verschiedenen Terminen) durchgeführt.

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

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

Berichterstellung

Der durch das BSI erstellte Bericht gliedert sich entsprechend der Kritikalität der gefundenen Schwachstellen. Für jede gefundene Schwachstelle wird anhand eines Beispiels die Gefahr beschrieben und Maßnahmen-Empfehlungen zur Beseitigung der vorgefundenen Sicherheitslücken bzw. zur allgemeinen/speziellen IT-Sicherheit aufgelistet.

Maßnahmenempfehlung

Das BSI empfiehlt allgemeine Maßnahmen zur Sicherheit von Webanwendungen in allen Ebenen der installierten IT-Architektur (Webanwendung, Sicherheitsgateway) zu implementieren, zu pflegen und entsprechend zukünftigen Erfordernissen weiterzuentwickeln.

Über diese Grundschutzmaßnahmen hinaus, können bei einem *IS-Webcheck* einige die Architektur des getesteten Webauftritts betreffenden spezifischen Schwachstellen gefunden werden. Im Bericht werden zu den Schwachstellen besondere Handlungsempfehlungen gegeben, die den Betreibern des Webauftritts helfen sollen, die Sicherheit weiter zu erhöhen.

Abgrenzung

Ein *IS-Webcheck* stellt nur eine Momentaufnahme dar, da täglich neue Sicherheitslücken bekannt werden und außerdem jeder Webauftritt ein dynamisches System darstellt. Um nicht nur für den Augenblick die Sicherheit zu erhöhen, wird empfohlen, den *IS-Webcheck* regelmäßig zu wiederholen.

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

Um die Sicherheit weiter zu erhöhen, wird empfohlen, zusätzliche Prüfmethoden wie IT-Pentests auf die beteiligten Systeme oder Codeanalysen einzusetzen.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
- Referat C23 -
Postfach 20 03 63
53133 Bonn

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