Bedingungen zum Siegel „BTC WASS Geprüfte Webapplikation“

BTC Business Technology Consulting AG

Inhaltsverzeichnis

1 Siegel „BTC WASS Geprüfte Webapplikation“

Die BTC bietet die Vergabe des Siegels „BTC WASS Geprüfte Webapplikation“ an.

Die Vergabe des Siegels setzt die Inanspruchnahme der „BTC Web Application Security Services“ zur Überprüfung der Webanwendung und ihrer IT-Infrastruktur voraus. Das Siegel ist nur für die getestete Webapplikation und ihrer IT-Infrastruktur gültig.

2 Bedingungen zur Siegelvergabe

Ausschlaggebend für die Risikobewertung aller Schwachstellen sind die im Penetrationstest vergebenen CVSS - Werte.

Das Common Vulnerability Scoring System[1], abgekürzt CVSS, ist ein Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in Computer-Systemen.

Die Vergabe des Siegels kann nur erfolgen, wenn die folgenden Bedingungen erfüllt sind:

- Kritisch priorisierte Schwachstellen wurden nicht identifiziert bzw. wurden innerhalb eines vorgegebenen Zeitrahmens von 60 Tagen nachweislich behoben.
- Mittel priorisierte Schwachstellen wurden nicht identifiziert bzw. wurden innerhalb eines vorgegebenen Zeitrahmens von 90 Tagen nachweislich behoben.
- Niedrig priorisierte Schwachstellen wurden nicht identifiziert bzw. in Abstimmung mit dem Kunden als vernachlässigbares Risiko eingestuft.
- Niedrig priorisierte Schwachstellen, die andererseits ein erhöhtes Risiko im Kontext der Webapplikation darstellen, müssen innerhalb eines vorgegebenen Zeitrahmens nachweislich behoben werden.

Wenn alle oben genannten Kriterien erfüllt werden, kann die Signierung als „BTC WASS Geprüfte Webapplikation“ erfolgen.

Wurden Schwachstellen behoben, die eine Siegelvergabe verhindern, erfolgt eine Prüfung in Form eines Stichprobentest isoliert für die kommunizierte Schwachstelle.

Im Angebot ist eine einmalige Stichprobe der behobenen Schwachstellen inbegriffen. Daher können durch Schwachstellen, die in der Stichprobe als nicht behoben erkannt werden, zusätzliche Kosten entstehen. Die Höhe der Kosten richtet sich nach dem entstandenen Aufwand der zu wiederholenden Stichprobenprüfung für die betreffende Schwachstelle.

Eine nachträgliche Signierung ist erst möglich, wenn die Bedingungen zur Siegelvergabe innerhalb der vorgegebenen Zeit erfüllt werden.

3 Einbindung des Siegels

Die BTC veröffentlicht einen Siegeleintrag zum getesteten System und stellt das Siegel zum Einbinden auf der Kundenwebsite bereit. Die Bilddatei des Siegels befindet sich dabei auf der BTC Website. Der Kunde kann die Bilddatei als verlinkte Bilddatei in seine Webapplikation einbinden. Das Siegel darf nur auf Systemen eingebunden werden, die mit BTC vorab in der Auftragsvergabe definiert wurden und den Kriterien aus Kapitel 1 entsprechen.

[1] https://www.first.org/cvss

4 Entzug und Aussetzung der Signierung

Unter verschiedenen Umständen behält sich die BTC, vor die Vergabe des Siegels auszusetzen oder das Siegel zu entziehen.

4.1 Aussetzung der Signierung

In den folgenden Fällen wird die Vergabe ausgesetzt:

- BTC erlangt Kenntnis über mittlere oder kritische Schwachstellen (nach CVSS) in der Webapplikation / der Website.
- An der Webapplikation oder ihrer IT-Infrastruktur werden maßgebliche Änderungen, wie Migration von Hardware / OS / Programmiersprache/-framework, durchgeführt.

Die Bilddatei des ursprünglichen Siegels wird mit dem Hinweis der Aussetzung versehen. Bei Beseitigung der Schwachstellen und erfolgreicher Stichprobenprüfung wird das Siegel wieder als erteilt dargestellt.

Für Schwachstellen, die durch die BTC auf erfolgreiche Behebung geprüft werden, können zusätzliche Kosten entstehen. Die Höhe der Kosten richtet sich nach dem entstandenen Aufwand der nachfolgenden Stichprobenprüfung.

4.2 Entzug der Signierung

In den folgenden Fällen wird dem Kunden das Siegel entzogen:

- BTC erlangt Kenntnis über den Missbrauch der Signierung
- BTC erlangt Kenntnis über jegliche Form von Betrug, der mit der signierten Webapplikation / Website in Verbindung steht.
- BTC erlangt Kenntnis über die Nichteinhaltung von gesetzlichen Bestimmungen.
- BTC erlangt Kenntnis über Aspekte des Kapitels 5.

Die Bilddatei des ursprünglichen Siegels wird mit dem Hinweis des Entzugs versehen.

5 Ausschluss bestimmter Angebote

Webapplikation die im Zusammenhang mit den folgenden Aspekten stehen, erhalten von BTC keine Signierung. Werden Webapplikationen nachträglich um diese Aspekte erweitert, erfolgt der Entzug nach Kapitel 4.2.

5.1.1 Produkte, deren Verkauf rechtlich untersagt ist

Hierzu zählen insbesondere, aber nicht ausschließlich, verbotene Waffen und Drogen.

Weiterhin betroffen sind Produkte, deren Verkauf rechtlich beschränkt ist, da die entsprechenden rechtlichen Voraussetzungen nicht erfüllt sind.

5.1.2 Schusswaffen und Munition

Hiervon erfasst sind alle Feuerwaffen, aber auch Druckluft-, Druckgas- und Federdruckwaffen, sofern diese nicht erlaubnisfrei erworben werden können.

5.1.3 Anscheinswaffen

Dies umfasst sowohl täuschend echt aussehende Imitate von Schusswaffen, als auch unbrauchbar gemachte Schusswaffen.

5.1.4 Problematische Angebote aus dem Bereich der Erotik

Als problematisch gelten Medien, Abbildungen und sonstige Inhalte, die nicht den allgemeinen ethischen oder moralischen Empfindungen entsprechen.

Weiterhin betroffen sind Artikel aus dem Bereich der Erotik, welche eine hohe Gefahr bleibender gesundheitlicher Schäden bergen.

5.1.5 Produkte mit nationalsozialistischem, rassistischem oder fremdenfeindlichem Bezug, auch sofern keine strafrechtliche Relevanz besteht

Dies gilt insbesondere für Artikel, die geeignet sind, eine nationalsozialistische Gesinnung nach außen zu tragen oder die das NS-Regime in unkritischer, verharmlosender oder verherrlichender Art und Weise darstellen.

5.1.6 Unechte Urkunden und Ausweise

Dies umfasst neben Nachahmungen amtlicher Ausweise auch unechte Zeugnisse oder Befähigungsnachweise.

5.1.7 Extraterrestrische Grundstücke und ähnliche Rechte

Jegliche Angebote zum Erwerb von Grundstückseigentum und ähnlichen Rechten im Weltall. Solche Transaktionen sind rechtlich nicht möglich.

5.1.8 Übersinnliche Leistungen

Betroffen sind Leistungen aus den Bereichen der Esoterik und der Magie – besonders, sofern diese Hilfe bei seelischen und psychischen Problemen versprechen.

5.1.9 Potentiell gesundheitsgefährdende Produkte

Als problematisch gelten insbesondere psychoaktive Substanzen, die zum Zweck des berauschenden Konsums angeboten werden.

6 Verzeichnis

Tabelle 1 – Änderungsverzeichnis

Version	Abschnitt	Gegenstand der Änderung	Autor	Datum
0.1	alles	Erstellung	Björn Kohnen	03.02.2015
0.2	1-4	Inhalterstellung	Björn Kohnen, Lars Meyer	15.11.2014
0.3	1-4	Weitere Inhaltserstellung	Björn Kohnen	03.02.2015
0.4	1-5	Weitere Inhaltserstellung	Björn Kohnen	05.02.2015
0.5	1-5	QS	Björn Kohnen	14.09.2015
0.6	1-5	QS	Dr. Walter Schultz	14.09.2015
0.7	1-5	QS	Torsten Oeltjen	15.09.2015
0.8	1-5	Überarbeitung	Björn Kohnen	15.09.2015
1.0	1-5	Verabschiedung	Björn Kohnen	15.09.2015
1.1	alles	Update Layout	Christian Bruns	28.02.2019