AZ: 09 561 / 06
wissOR Bernd Beule Informationssicherheitsbeauftragter (ISB)
Produkt-Nr. P8000-01
Kostenstelle K8200

Dessau, 08.03.2021
HR 2322

Anforderungen an externe Webseiten oder Fachanwendungen des UBA im Web

Dieses Dokument beschreibt Anforderungen an den Aufbau und Betrieb von Internetpräsenzen von Fachinformationssystemen einer Bundesbehörde, die insbesondere die IT-Sicherheit betreffen. Daraus resultieren ggf. Betriebsorte, Techniken und Pflichten für Fachbetreuer und Betreiber. Einige Angaben sind optional und als Vorschläge gedacht, von denen bei nachgewiesenem Bedarf dokumentiert abgewichen werden kann; andere Vorschläge sind jedoch obligatorisch. Dies ist dann entsprechend vermerkt.
Die Anforderungen an die IT-Sicherheit von Webanwendungen des Bundes legt das Bundesamt für Sicherheit in der Informationstechnik (BSI, https://www.bsi.bund.de/) fest. Empfehlungen des BSI sind für Bundesbehörden und somit auch für das UBA nach spätestens 12 Monaten verpflichtend umzusetzen. Diese Pflichten kann das UBA dann an die Mitarbeiter und Fachbetreuer von Internetpräsenzen weitergeben. Basis hierfür sind das BSI-Gesetz (BSIG) und der Umsetzungsplan Bund (UP-Bund) zum Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI).

0. Sicherheitsbewusstsein zum Betrieb von Webanwendungen

Für einen sicheren Betrieb von außen erreichbarer Webanwendungen ist für Fachbetreuer und Betreiber folgendes zu verinnerlichen.

Webanwendungen sind ubiquitär, d.h. sie sind 7 Tage, 24 Stunden und von überall aus der gesamten Welt per Internet erreichbar. Länderspezifische Feiertage, Tag und Nacht oder lokale Öffnungs- bzw. Betriebszeiten von Behörden oder Betreibern spielen daher KEINE Rolle. Es muss also jederzeit damit gerechnet werden, dass bei Bekanntwerden einer Sicherheitslücke aus Sicherheitsgründen eine sofortige Aktion an oder mit der Webanwendung erforderlich sein kann. Kann das UBA dies aus dienstrechtlichen o.a. Gründen nicht leisten, muss der Betreiber der Webanwendung diese Reaktionsanforderung in Abhängigkeit vom Schutzbedarf der Fachanwendung übernehmen.

Gemäß BSI werden Behördenwebseiten regelmäßig angegriffen und/oder konkrete, vertrauliche Daten abgezogen. Diese Meldungen werden dann presseöffentlich und sind somit bekannt. Viel gefährlicher ist aber der heimliche und nicht öffentliche Angriff auf Webseiten – i.d.R. durch sog. 0-Day-Exploits. In 2014 wurden drei große Sicherheitslücken zu Webanwendungen bekannt:

- *Heartbeat / Heartbleed* http://de.wikipedia.org/wiki/Heartbleed
- *Shellshock* http://de.wikipedia.org/wiki/Shellshock_%28Sicherheitsl%C3%BCcke%29
- *Poodle* http://de.wikipedia.org/wiki/Poodle

Werden derartige Sicherheitslücken bekannt, versuchen Angreifer aus der gesamten Welt automatisch per Skript, verwundbare Systeme zu finden. Die Eigentümer der Webanwendung (z.B. Bundeshörde) oder der Schutzbedarf der Inhalte sind dabei zunächst für die Angreifer uninteressant. Angreifer platzieren dann - eine entsprechende Ausnutzbarkeit der gefundenen Lücke vorausgesetzt - vielmehr auf verwundbaren Systemen ihre eigenen Programme oder Hintertüren für einen späteren Besuch, um die fremden Webseiten als Werkzeug zu missbrauchen, z.B. zum Massenversand von Spam, für DDoS-Angriffe (http://de.wikipedia.org/wiki/Denial_of_Service), um Trojaner zu verbreiten, u.a. Untaten im Netz. Daher müssen bekannt gewordene Sicherheitslücken in Webanwendungen und den basierenden Webservern schnellstmöglich – manchmal sogar sofort - geschlossen bzw. Webauftritte notfalls temporär vom Netz genommen werden und nicht erst beim nächsten Treffen von Fachbetreuer und Betreiber oder in einer Woche. Ansonsten läuft die Bundeshörde Gefahr, als Teil eines illegalen Webangriffs bekannt zu werden und das sollte das UBA tunlichst vermeiden. Gehen konkrete Angriffe von unseren Webseiten aus, sind auch wir haftbar – unabhängig davon, ob wir selber aktiv geworden sind oder Externe unsere Webanwendung missbrauchen.

Die folgenden drei Betriebsorte sind alternativ.

5.1 Rechenzentrum einer Bundesbehörde

Dies kann im Prinzip die jeweilige Bundesbehörde selber sein. Das UBA ist jedoch nicht in der Lage, eine 7x24 - Verfügbarkeit zu gewährleisten, da das Rechenzentrum nachts und am Wochenende nicht besetzt ist. (Anm.: Die 7x24 – Verfügbarkeit ist zu unterscheiden von der 7x24 – Erreichbarkeit, die für das UBA-RZ sicher gestellt ist. Dies bedeutet aber eben nicht automatisch eine 7x24 – Verfügbarkeit.) Andere Bundesbehörden, bei denen bereits Webanwendungen des UBA betrieben werden sind:

- Zentrum für Informationsverarbeitung und Informationstechnik
- Bundesanstalt für Landwirtschaft und Ernährung (http://www.ble.de/)
- Bundesverwaltungsamt (http://www.bva.bund.de/)
- Deutscher Wetterdienst https://www.dwd.de/DE/Home/home_node.html)
- ...

Die Rechenzentren des Zivit und des BVA werden inzwischen im ITZ-Bund zusammengefasst: https://www.itzbund.de/DE/Home/home_node.html. Hinzu kommen weitere Dienstleister des Bundes, z.B.: https://www.bwi.de/ , die zum **Dienstleistungsverbund des Bundes** zusammengefasst werden. Der Betrieb von Webanwendungen ist im **Dienstleistungsverbund des Bundes** anzustreben.

Vorteil:
Bundesbehörden sind verpflichtet, die Sicherheitsanforderungen für Bundeswebseiten zu erfüllen. Weiterhin sind sie verpflichtet, auf Sicherheitswarnungen des BSI gemäß den Vorschriften zu reagieren. Das erspart dem Auftraggeber UBA die Festlegung diverser Details zur IT-Sicherheit.
Nachteil:
Ggf. werden in den Rechenzentren nicht alle technischen Plattformen unterstützt, die wünschenswert wären oder funktional erforderlich sind.

5.2 Ein Betreiber, der nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert ist

Die Zertifizierung bedeutet, dass der Betreiber prinzipiell in der Lage ist, die Sicherheitsanforderungen des BSI zu erfüllen. Wichtig ist hier der Zusatz „auf Basis von IT-Grundschutz".
Vorteil:
Der Betreiber verfügt über die erforderliche Infrastruktur, Technik, Personal und Organisation, um die Sicherheitsanforderungen des Bundes erfüllen zu können.
Nachteil:
Ob und wie dies für eine konkrete Webanwendung genutzt wird, muss aber detailliert im Vertrag festgehalten werden.
Weiterhin werden dort ggf. nicht alle Techniken unterstützt, die wünschenswert wären oder fachlich erforderlich sind.

5.3 Beliebiger anderer Betreiber

Es kann selbstverständlich für Fachanwendungen auch jeder andere Betreiber für den Betrieb einer Webanwendung gewählt werden, der die gewünschten oder erforderlichen Techniken unterstützt. Ausnahme sind hier Webanwendungen, die nur für Bundesbehörden sind. Diese dürfen gemäß Erlass „Netze des Bundes (NdB)" nicht mehr extern betrieben werden.
Neben diesem freien Wahlvorteil ergibt sich aber ein erheblicher Nachteil:
Zum Betrieb einer Bundeswebseite sind die Sicherheitsanforderungen für diese exakt einzuhalten. Dies muss dann im Detail vertraglich vereinbart und vom Betreiber nachgewiesen werden.

Konkret bedeutet dies:

Der Betreiber erfüllt den IT-Grundschutz des BSI:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

6.2 Betriebssystem und Software

Für die Wahl des Betriebssystems gibt es keine Vorgaben.

Als Webbeschreibungssprache ist aktuell HTML 5 zu wählen. Auf die Verwendung von Adobe Flash ist nach Möglichkeit zu verzichten.

Der Einsatz weiterer Sprachen ist auf das notwendige Minimum zu beschränken. Denn jede weitere Sprache vergrößert die Anzahl potentieller Sicherheitslücken.

Grundsätzlich sind für Webanwendungen nur Betriebssysteme, Datenbanken, Webserver, Sprachen u.a. Programme zu verwenden, die noch vom Hersteller unterstützt werden. Dies sichert ein Bereitstellen von Updates und Patches durch den Hersteller. Betriebssysteme, Datenbanken und Sprachen, die nicht mehr vom Hersteller supported werden, stellen für den Nutzer, Betreiber und das UBA ein nicht zu kalkulierendes Sicherheitsrisiko dar. Stellt ein Hersteller den Support für eine Version ein, informiert er darüber i.d.R. mit einigen Monaten Vorlauf. Bereits im Betrieb befindliche Webanwendungen haben in diesem Falle unverzüglich zu reagieren und auf vom Hersteller unterstützte Programmversionen zu migrieren. Die Wahl bekannterer Programmiersprachen etwa schützt dabei in der Regel davor, dass das Produkt komplett eingestellt wird und der Migrationsaufwand dadurch sehr hoch wird. Die Verantwortung, dass nur vom Hersteller unterstützte Programmversionen in Webanwendungen verwendet werden, liegt beim Fachbetreuer der Webanwendung im UBA. Dieser kann die Verantwortung auf den Betreiber übertragen, muss dies jedoch im Vertrag klar und eindeutig regeln. Das UBA wird Programme, die vom Hersteller nicht mehr unterstützt werden, vollständig aus dem IT-Betrieb des UBA entfernen, um die IT des UBA ausreichend vor Angriffen zu schützen. Für Fachbetreuer von Webanwendungen und damit für den Betrieb von Webanwendungen besteht kein Anspruch darauf, dass das UBA nicht mehr unterstützte Programme bereit hält. Denn hier ist das Sicherheitsrisiko höher einzuschätzen als das Schutzziel der Verfügbarkeit der Webanwendung.

6.3 Content Management System

Wird ein Content-Management-System (CMS) verwendet, so bietet der Bund den Government Site Builder (GSB) an, für den es einen Bundesrahmenvertrag für das Hosting beim BVA gibt:
https://produkt.gsb.bund.de/DE/GSB-Services/Rahmenvertraege/Rahmenvertraege_node.html
Selbstverständlich kann der GSB auch von einem anderen Betreiber gehostet werden.
Vorteil:
Der Bund garantiert sowohl für die Sicherheit dieses Softwareproduktes als auch des Hostings, wenn beim BVA gehostet wird.
Nachteil:
Ggf. erfüllt dieses Produkt nicht alle fachlichen Anforderungen an die Umsetzung eines Fachverfahrens.

Selbstverständlich kann auch ein anderes CMS verwendet werden. Dann sind jedoch die Anstriche
- 5.3 Modellierung IT-Grundschutz, Baustein Software (hier dann das CMS),
- 8 Rollen- und Rechtekonzept,
- 9 Notfallmanagement und
- 11 weitere Anforderungen (z.B. Barrierefreiheit)

dieses Vermerkes zu berücksichtigen und vor Inbetriebnahme umfassend zu dokumentieren.

6.4 Verwendung von Erweiterungen oder Plug-ins

Bei der Verwendung von Erweiterungen oder Plug-ins für Webanwendungen gilt das Minimalprinzip. Es dürfen nur Erweiterungen verwendet werden, die fachlich erforderlich sind – keine „Nice-to-have Strategie". Die Verwendung jedes Plug-ins ist zu dokumentieren:
- Verwendungszweck
- Hersteller
- Technische Abhängigkeiten (z.B. von Bibliotheken)
- Versionsnr. und Datum

Wie jede andere verwendete Software ist auch jedes Plug-in aktuell zu halten. Insbesondere sind bekannt gewordene Sicherheitslücken umgehend zu schließen.

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_1.pdf?__blob=publicationFile&v=5
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=10

Eine Analyse der Webverbindung mit https://www.ssllabs.com/ssltest/ muss mindestens ein „grünes A" ergeben, am besten ein „A+".

7.3 Authentifizierung

Ist die Webanwendung nicht ausschließlich read-only, sondern sind für eine oder mehrere Funktionen Anmeldungen mit einer Authentifizierung erforderlich, so sind mindestens folgende Standards einzuhalten:

- Passwortgüte nach der Authentifizierungsrichtlinie des UBA, aktuell bedeutet dies mindestens 10 Zeichen aus 3 Zeichenklassen
- keine Übertragung oder Speicherung der Klartextpassworte, sondern nur verschlüsselte Übertragung und Speicherung der Hashwerte
- Mehrfach-Hash (mindestens 100-fach)
- Verwendung der SALT-Technologie auf Serverseite (http://de.wikipedia.org/wiki/Salt_%28Kryptologie%29)

Grundsätzlich gelten die Standards der Authentifizierungsrichtlinie UBA unter:
http://ubanet/websites/Security/regelungen/UBARegelungen/Forms/AllItems.aspx

Es existiert weiterhin zum Hashverfahren ein ENISA-Report (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report) mit Empfehlungen, welche Algorithmen in welcher Weise zu verwenden sind. Weiterhin sollte unbedingt darauf geachtet werden, dass keine eigenentwickelten Software-Bibliotheken zur Authentifizierung und für Krypto-Operationen verwendet werden; stattdessen sind unbedingt bewährte Standard-Bibliotheken einzusetzen.

8. Ansprechpartner, Rollen + Rechte Konzept

8.1 Ansprechpartner

Der Betreiber benennt Ansprechpartner und Vertreter, die für Sicherheitswarnungen 7 x 24 erreichbar sind. Dies können bei unterschiedlichen Zuständigkeiten für

- Netzwerk,
- Betriebssystem,
- Datenbank oder
- Fachanwendung

auch unterschiedliche Ansprechpartner sein; im Idealfall ist es ein Ansprechpartner.
Hierzu sind jeweils E-Mail Adresse; Festnetznummer und Mobilnummer zu hinterlegen.

8.2 Rechte und Rollen Konzept

Bei Webanwendungen, die über read-only hinaus auch Interaktion von unterschiedlichen Personen erlauben, ist ein Rollen-und-Rechte-Konzept zu erstellen und dessen technische Umsetzung zu dokumentieren.

9. Business Continuity Management

Es ist das Business Continuity Management (BSI-Standard 200-4) nachzuweisen (s. auch Abs. 5.3). Folgende Anstriche sind besonderes zu dokumentieren:

Bundesbehörde dürfen nicht über eine Webanwendung ungewollt den Raum der Bundesbehörde verlassen.

Diese Fassung der Richtlinie ist vom 08.03.2021.

Umweltbundesamt, Wörlitzer Platz 1, 06844 Dessau
Bernd Beule Informationssicherheitsbeauftragter (ISB) E-Mail: it-sibe@uba.de