Kommentierung der Entwurfsfassung der TR-03172 - Portalverbund

Dokument TR-03172-3 Onlinedienst

Firma/Organisation:	Databund e.V.	**Namen bzw. Ansprechpartner:**	Databund-Geschäftsstelle

Kapitelnummer	Kapitelname	Anforderung/Absatz/Abbildung/Tabelle	Kurzbeschreibung	Kommentar/Vorschlag/Frage/Kritik
A3.4.02	Build- und Releasemanagement			Das Release SOLLTE signiert werden, die Signatur muss aber validiert werden. Dies steht im Widerspruch und sollte präzisiert werden.
A3.5.01	Infrastruktur			Wenn eine Verschlüsselung gefordert wird, wie soll hier die Schlüsselverwaltung aussehen? Wenn verschlüsselt wird, wie sieht die Weiterverarbeitung in nachgelagerten Systemen aus? (DMS, E-Akte, etc.). Dies sollte präzisiert werden.
A3.7.01	Kommunikation			Wie ist in diesem Fall die Allowlist zu verstehen? Eingehend oder Ausgehend? Worauf bezieht sich die Allowlist auf die Dokumentation oder die Anwendung? Dies sollte präzisiert werden.
A3.7.03	Kommunikation			EV-SSL-Zertifikate spielen in den heutigen Browsern keine Rolle mehr. Für den Nutzer sind Unterschiede beim Zertifikat auf den ersten Blick nicht mehr erkennbar und bieten daher keinen wirklichen Mehrwert in Hinblick auf die Sicherheit.
A3.7.05	Kommunikation			Bezieht sich DNSSEC in diesem Fall auch z. B. auf einen ausgehenden E-Mail-Transport? Dies sollte präzisiert werden.
A3.8.04	Drittsoftware	Alle verwendete (Dritt-) Software MUSS auf aktuellem Stand gehalten werden, damit eventuell vorhandene bzw. neue Schwachstellen nicht die Webanwendung bzw. den Webservice gefährden können. Informationen über identifizierte Schwachstellen werden regelmäßig und zeitnah über einschlägige Mailinglisten und Informationsdienste, z.B. den Warn- und Informationsdienst (WID) von CERT-Bund veröffentlicht. Wenn Schwachstellen in verwendeter Software bekannt werden MÜSSEN die relevanten Updates kurzfristig eingespielt werden. Software, die nicht länger vom Hersteller oder Entwickler gewartet wird, DARF NICHT verwendet werden.	Diese Anforderung ist grundsätzlich nachvollziehbar. Allerdings ist es so, dass im Rahmen einer modernen Software-Entwicklung ein komplexes Antragsystem teilweise mehrere Hundert Basisbibliotheken wie z. B. XML-Parser und andere Komponenten aus dem OpenSource-Bereich eingesetzt werden. Dies ist aus vielen Gründen notwendig, unter anderem weil eine signifikant höhere Fertigungstiefe ("Eigenfertigung") weder wirtschaftlich noch sicherer wäre. Diese Bibliotheken werden in sehr vielen Kontexten eingesetzt, was sich auch in den CVE-Meldungen widerspiegelt. Die gemeldeten Sicherheitslücken können ggf. nur in ganz bestimmten Kontexten ausgenutzt werden oder betreffen bestimmte Teilfunktionen. Folglich sind die meisten Sicherheitsmeldungen für ein bestimmtes System nicht relevant. Durch die pauschale und undifferenzierte Anforderung müssten aber sehr viele Patches unnötiger Weise erstellt, qualitätsgesichert und über den Staging-Prozess in Produktion gebracht werden. Zudem besteht das Risiko, dass durch neue Versionen Sicherheitslücken oder funktionale Fehler eingeschleust werden. Diese Anforderung bindet erhebliche Kapazitäten, ohne einen tatsächlichen Sicherheitsgewinn zu bieten.	Wie ist hier die Definition "auf dem aktuellem Stand" zu verstehen? Nicht jedes Update schließt Sicherheitslücken und/oder Schwachstellen. Wann wird eine Software nicht mehr gewartet? Ab welcher Definition soll ein außerplanmäßiges Update erfolgen (Schwere der Schwachstelle)? Mit einem kurzfristigen Update werden ggf. weitere Softwareprobleme durch fehlende Tests geschaffen. Nur weil keine Updates erfolgen, heißt es nicht, dass die Software nicht aktuell ist. Dies sollte präzisiert werden.

A3.9.06	Dateiupload		Wie soll der Umgang mit False-Positives erfolgen? Gegen welche Signaturen soll auf Schadsoftwaren geprüft werden? Wann ist die Definition Schadsoftware erreicht? Dies sollte präzisiert werden.
A3.9.08	Dateiupload		Wie wird das in der Cloud strukturiert sein? Sinnvoll ist hier ein getrennter Bereich, der zugriffsgeschützt ist und eine Ausführung von Dateien nicht möglich ist. Zudem sollte geprüft werden, ob nur Lesen-Zugriffe möglich sind.
A3.10.07	Authentisierung, Authentifizierung und Autorisierung	Den Fach- und Systemadministratoren SOLLTE eine Möglichkeit gegeben werden, sich über ungewöhnliche Anmeldevorgänge informieren zu lassen.	Was ist mit ungewöhnlich gemeint? Dies sollte präzisiert werden.
A3.10.12	Authentisierung, Authentifizierung und Autorisierung		Wie ist hier Webservice zu verstehen? Die Zugriffsregelung sollte für den gesamten Onlinedienst gelten. Dies sollte präzisiert werden.
A3.11.02	Anbindung eines Servicekontos nach TR-03160		In der Praxis wird die Rückmeldung vom IdP signiert und vom SP (Service-Provider) validiert, die Authentifizierungs- und Autorisierungsinformationen unterliegen dieser Prüfung in der Regel nicht.
A3.11.04	Anbindung eines Servicekontos nach TR-03160		Wie sollen die übergebenen Daten an nachgelagerte Systeme (Fachverfahren) weitergegeben werden? Diese Daten werden für die Bearbeitung des Antrages und die Rückmeldung dort zwangsweise benötigt (z. B. Postkorb-Handle). Dies sollte präzisiert werden.
A3.12.02	Sessionmanagement und Caching		Das HTTP-Protokoll hält keine ständige Verbindung!
A3.16.02	Konfiguration		Was ist hier gemeint? Der Browser? Browser-Abläufe können nicht vollständig
A3.19	Verknüpfung von Antragsdaten und Nutzeridentität		Da die Servicekonten derzeit keine kryptografische Maßnahmen ergreifen, sind die Fachverfahren derzeit ausschließlich für die Integrität zuständig (siehe A3.19.01).
A3.19.01	Verknüpfung von Antragsdaten und Nutzeridentität		Findet in der Praxis weder bei der BundID noch bei MUK auf Basis von Elster statt. Bei beiden Konten werden keine Signaturen übermittelt. Die übermittelten Daten sind nachträglich nicht prüfbar. Wer erstellt das geforderte Siegel und wie soll das Siegel prüfbar sein? Dies sollte präzisiert werden.
A3.20.03	Antrag absenden		siehe A3.19.01, ist hier die Übermittlung der Daten an das Fachverfahren z. B. per Fit-Connect explizit gefordert? Die Daten müssen in diesem Fall vor der Übertragung automatisch entschlüsselt und dann wieder mit dem Zertifikat des Empfängers verschlüsselt werden. Dies sollte präzisiert werden.
A3.20.06	Antrag absenden		Woher stammt das Siegel? Wie ist dieses prüfbar? Wie ist hier das Wort "Kopie" zu verstehen? Wenn z. B. ein XML-Format an das Fachverfahren übermittelt wird, wird dies an den Antragsteller in Kopie übermittelt oder ist hier eher eine leserliche Version (z. B. PDF) gefordert? Wie soll mit Anhängen umgegangen werden? Problem: Antrag kann mehrere GB haben. Dies sollte präzisiert werden.