1

Portalverbund Grundschutz		**Konvention** **PV-GS 1.4** **Ergebnis der AG**
Kurzbeschreibung	Um den technischen Betrieb und die Sicherheit im Portalverbund zu gewährleisten, wird ein technischer Mindeststandard (Grundschutz) definiert. Eine eigene Sub-Arbeitsgruppe der AG-IZ wird zu diesem Zweck eingerichtet.	
Editor:	Peter Reif (Wien)	Projektteam / Arbeitsgruppe **AG Integration und Zugänge (AG-IZ)** **Sub-Arbeitsgruppe AG-Policy** AG-Leiter: Michael Pellmann, MSc (Wien)
Beiträge von:	Rainer Hörbe, Florian Huchler (Vorarlberg), Harald Stradal (BM.I), u.a.	

3

4

1 Motivation

Um einen optimalen Betrieb des Portalverbundes zu gewährleisten, sind verschiedene technische Maßnahmen notwendig. Dazu gehört u.A. die Verwendung von IT auf dem neuesten sicherheitstechnischem Stand.

In Zusammenarbeit der PV-Teilnehmer sollen Maßnahmen definiert werden, die einen sicherheitstechnischen Mindeststandard definieren (Grundschutz). So kann man sich z.B. auf die Vermeidung von veralteten Übertragungsprotokollen einigen bzw. koordiniert auf aktuelle Sicherheitslücken reagieren. Eine eigene Sub-Arbeitsgruppe der AG-IZ wird zu diesem Zweck eingerichtet. Sie kann auch einzelne Portalverbundteilnehmer auf Sicherheitslücken oder ein unzureichendes internes Sicherheitsmanagement hinweisen.

2 Sub-Arbeitsgruppe Policy

Die Portalverbundteilnehmer beschicken die Sub-Arbeitsgruppe AG-Policy, die regelmäßig oder im Anlassfall Risiken und notwendige Sicherheitsmaßnahmen evaluiert, Richtlinien erarbeitet, Berichte und Revisionsprotokolle einfordert und Ergebnisse an die PV-Teilnehmer berichtet (Responsible Disclosure). Die notwendigen Sicherheitsmaßnahmen werden in dem Dokument [PVP SMA] beschrieben.

Alle für die PV-Teilnehmer relevanten Informationen werden unter Berücksichtigung der Responsible Disclosure zentral einsehbar gespeichert. Z.B. Risikobewertungen und Kommentare zu den Revisionsprotokollen.

3 Ziele

Erstellung und Wartung von sicherheitstechnischen Vorgaben (Security Controls), für die Infrastruktur des Portalverbundes (Stamm-, Anwendungsportale, Identity-Provider und Service-Provider). Die Anwendung der Controls soll in den Revisionsprotokollen laut PV-Revisionsleitfaden dokumentiert werden.

Security Controls können Übergangsfristen für bestimmte Produkte beinhalten, die aber spätestens mit Auslaufen des Supports für die jeweiligen Produkte enden.

Monitoringmaßnahmen bzw. Scans der Endpoints, um Schwachstellen aufzudecken und die Einhaltung der Vorgaben zu überprüfen.

Stichprobenartige Überprüfung der beim Depositar aufliegenden Revisionsprotokolle.

Erstellung von regelmäßigen Berichten über die Einhaltung der Controls.

4 Nicht-Ziele

Organisatorisch-rechtliche Controls werden im Revisionsleitfaden von der AG-Resi erstellt.

Eingriffe in die interne Sicherheit von PV-Teilnehmern.

Die PV-Teilnehmer haben weiterhin die Verantwortung eingehende Sicherheitsmeldungen auf Relevanz für ihre Portalinfrastruktur zu prüfen, die Sub-Arbeitsgruppe kann das nicht zur Gänze übernehmen.

5 Berichte

Die Sub-Arbeitsgruppe berichtet regelmäßig und im Anlassfall unter Berücksichtigung der Responsible Disclosure an den Depositar, die einzelnen PV-Teilnehmer bzw. an die AG-IZ oder die BLSG über den Status im Bezug auf den PV-Grundschutz der PV-Teilnehmer und die Ergebnisse der Monitoringmaßnahmen und Scans.

6 Zusammenarbeit mit anderen Stellen

Bei der Risikobewertung und Warnung vor Schwachstellen ist die Zusammenarbeit mit GovCert.at erwünscht.

7 Responsible Disclosure

Unter Responsible Disclosure wird in diesem Dokument verstanden, dass Portalverbundbetreibern eine gewisse Zeitspanne eingeräumt wird, in der sie ihre Schwachstellen beheben können, bevor die Information im eingeschränkten Kreis veröffentlicht wird.

Es werden außerdem keine Informationen über Schwachstellen nach außen gegeben, die die Sicherheit einzelner Portalverbundteilnehmer beeinträchtigen könnten.

8 PVP SMA

Die Sub-Arbeitsgruppe erstellt und wartet das Dokument „Portalverbund Sicherheitsmaßnahmen" [PVP SMA]. In diesem Dokument werden die für den Portalverbund aktuell gültigen technischen Sicherheitsmaßnahmen beschrieben. Es enthält allenfalls auch Kriterien zur sicherheitstechnischen Einstufung von Portalen, etwa in Form eines Farbschemas. Änderungen in dem Dokument werden von der AG-IZ beschlossen (Sitzung oder Umlaufbeschluss). Die Änderungen treten 4 Monate nach Beschluss in Kraft, bei Gefahr in Verzug, z.B. bei aktuellen Sicherheitslücken schon früher.

9 Referenzen

[PVP SMA] Portalverbund Sicherheitsmaßnahmen