



Besprechungsergebnis

Art der Besprechung: Arbeitssitzung Sektorkomitee Informationstechnologie
Datum: Freitag, 03.05.2019
Ort: SECO, Holzikofenweg 36, 3003 Bern, Raum HO36-2.238
Zeit: 10:00 – 15:30h
Vorsitz: Thomas Hilger SAS
Protokoll: Thomas Hilger SAS

Anwesend: Herr Christian Jenny, Bund, BAKOM
Frau Cornelia Enke, Bund, BIT
Herr Philippe Schwab Molnar, Bund, EDÖB
Herr Peter Stadlin, Fachexperte
Frau Liliane Mollet, insecor, Fachexpertin
Herr Thomas Schmitt, Fachexperte, get it services GmbH
Herr Matthias Bartholdi, SwissSign AG
Herr Michael Günther, SwissSign AG
Herr Timo Schmitt, SwissSign AG
Herr Reto Grubenmann, KPMG
Herr Thomas Moretti, QuoVadis
Herr Martin Lechmann, Swisscom
Herr Peter Weiss, Swiss Re
Herr Joseph Doekbrijder, S.W.I.S. Group
Herr Peter Reber, SQS
Herr Thomas Hilger, SAS
Herr Stephan Gehrke, SAS

Gäste/Referenten: Herr Jean-Maurice Geiser, Bund, BAKOM
Herr Urs Paul Holenstein, Bund, BJ
Herr Peter von Dach, Bund, ISB
Herr Igor Metz, Glue AG

Verteiler: Mitglieder Sektorkomitee
Leiter Ressort Metrologie und Ingenieurwesen

Traktanden	Ergebnis/Entscheid
1. Begrüssung, Vorstellung und Traktanden Teil 1: ISO-Themen und Datenschutz	Traktanden wurden genehmigt
2. Genehmigung Protokolls vom 23.06.2017	Das Protokoll wurde ohne Änderungen angenommen.
3. Internationale Entwicklung ISMS (Peter Weiss) - Informationen und Neuigkeiten zur Standardisierung - ISO/IEC 27017 / 27018	<p>Peter Weiss präsentiert die aktuelle Entwicklung der ISO-Normung auf diesem Gebiet und gibt einen Überblick über die Standard-Familie. Die wichtigsten Informationen:</p> <ul style="list-style-type: none"> - ISO/IEC 27001 wurde in der letzten Abstimmung bestätigt. Ev. wird eine Scope Revision in Betracht gezogen zusammen mit ISO/IEC 27002. - ISO/IEC 27002 wird überarbeitet (z.Zt. 3. WD) - ISO/IEC 27005 (risk management) wurde überarbeitet im July 2018 publiziert. - FDIS ISO/IEC 27102 (Guidelines for Cyber Insurance), Publikation wird im 2. Halbjahr 2019 erwartet. <p><u>Situation ISO/IEC 27017 / 27018:</u> Da am Markt immer wieder "missverständliche" Zertifizierungen mit diesen beiden Standards auftauchen hat die Workinggroup die Situation analysiert. Festzuhalten ist, dass die ISO/IEC 27017 und 27018 nur eine sektorspezifische Erweiterung der ISO/IEC 27002 darstellt und keinesfalls alleinstehend zertifiziert werden kann. Zertifizierungen sind nur nach ISO/IEC 27001 möglich, da nur dieser Standard entsprechende Anforderungen definiert.</p>
4. IT Service Management, ITSM (Thomas Schmitt) - Neuigkeiten - ITIL - ISO 20000-6:2017 - ISO/IEC 20000-1:2018	<p>Thomas Schmitt gibt einen Überblick über die Situation der ISO/IEC 20000 Normenlandschaft sowie über ITIL in der Schweiz.</p> <p>Die wichtigsten Neuerungen:</p> <ul style="list-style-type: none"> - ISO/IEC20000-6: Die Norm wurde am 6.6.2017 publiziert und die IAF hat eine 2-jährige Übergangsfrist beschlossen. Diese Übergangsfrist läuft im Juni 2019 ab. Nach Ablauf der Übergangsfrist wird das Mandatory Document IAF MD18 zurückgezogen. - ISOIEC 20000-1: Die Zertifizierungsnorm wurde überarbeitet und im September 2018 publiziert. Zertifizierungsstellen müssen bis Ende September 2019 einen Antrag auf Umstellung bei der SAS einreichen. Eine ZS wurde bereits umgestellt.
5. Informationen aus dem Bereich Datenschutz (Philippe Schwab Molnar) - DSG und VDSZ	<p>Herr Schwab informiert über die Situation beim Datenschutz. Es hat eine Äquivalenzüberprüfung der EU zum Datenschutz der Schweiz gegeben mit folgendem Ergebnis:</p> <p>Am 25. Mai 2018 ist in der EU die neue europäische Datenschutz-Grundverordnung (EU) 2016/679 in Kraft getreten. Gestützt auf Artikel 45 Absätze 3 und 4 der Verordnung überprüft die Europäische Kommission fortlaufend das Datenschutzniveau der Drittstaaten, welche wie die Schweiz über einen Angemessenheitsbeschluss der EU verfügen. Der nächste Bericht über das Datenschutzniveau der Schweiz ist für den Mai 2020 vorgesehen. Die Europäische Kommission berücksichtigt für den Bericht Informationen der Schweiz bis ca. Januar 2020.</p> <p>Die Beratung des 2ten Teils der Totalrevision DSG ist immer noch in der</p>

Traktanden	Ergebnis/Entscheid
	<p>ersten Staatspolitischen Kommission, der SPK-Nationalrat. Ende Mai 2019 ist das Thema in der nächsten Sitzung traktandiert, aber eine Einigung ist noch nicht in Sicht. Nach Abschluss durch die SPK-N, wird das Revidierte DSG in der SPK-Ständerat behandelt, eventuelle Differenzen bereinigt und das Parlament muss das Gesetz am Schluss verabschieden.</p> <p>Aus heutiger Sicht scheint es nicht möglich zu sein, bis im Januar 2020 der Europäischen Kommission einen mindestens durch die Volksvertreter un-widersprochenen Entwurf eines totalrevidierten DSG präsentieren zu können. Die Gefahr besteht somit, dass die Schweiz kurz- oder langfristig über keinen Angemessenheitsbeschluss der EU im Datenschutz mehr verfügt.</p> <p>Zudem ist für die Anerkennung der Äquivalenz auch noch die Unterzeichnung der Konvention Nr. 108+ durch die Schweiz nötig.</p> <p>Das jetzt angeglichene Schengen-Datenschutzgesetz (SDSG, SR 235.3) hat gemäss Bericht der Europäischen Kommission auch noch etwas Nachholbedarf. Siehe dazu auch den Bericht von SRF. D.h. die bisherigen Umsetzungen sind suboptimal.</p>
<p>6. Informationen Zertifizierung allgemein (Stephan Gehrke)</p>	<p>Der Technische Leiter Zertifizierung berichtet über allgemeine Aktivitäten der EA im IAF im Bereich der Zertifizierung und im Besonderen über IAF Aktivitäten zur Überarbeitung der ISO/IEC 27006. Eine weitere wichtige Norm im Committee Draft Status ist die ISO/IEC 27552 (CD) Privacy information management system.</p>
<p>7. Themenvorschläge für die nächste(n) Sitzung(en)</p>	<p>—</p>
<p>Mittagessen</p>	
<p>8. Begrüssung, Vorstellung, Traktanden zum zweiten Teil der Sitzung „Themen betreffend PKI“ Genehmigung Protokoll der letzten Sitzung</p>	<p>Die Traktanden wurden genehmigt Das Protokoll von der letzten Sitzung vom 23.06.2017 wurde ohne Änderung genehmigt.</p>
<p>9. Informationen PKI / ZertES (Christian Jenny) - Aktueller Stand - Neuerungen/Änderungen - Umsetzung</p>	<p>Neue Versionen von relevanten ETSI Normen wurden veröffentlicht, u.a.:</p> <ul style="list-style-type: none"> - ETSI EN 319 411-2 (2018-04) Policy Requirements for Trust Service Providers - ETSI EN 319 412-5 (2017-11) Certificates Profiles-QC Statements <p>Art. 7 VZertES ermöglicht nun die Videoidentifikation, dies entspricht den eIDAS Anforderungen gem. Art 24, 1, d. Allerdings fehlen derzeit Kriterien für Konformitätsbewertung. Akkreditierung und Konformitätsbewertung ist derzeit nicht möglich. Ein ETSI "new work item" wurde vorgeschlagen. Anpassungen bzw. eine Harmonisierung bez. Personenidentifizierung wird es im Rahmen der eID-Ausführungsbestimmungen geben.</p>
<p>12. Informationen PKI / ZertES (Urs Paul Holenstein, Peter von Dach) - Behördenzertifikate - eGov Signaturvalidator</p>	<p>Die Einführung der Behördenzertifikate ist ein wichtiger Schritt im Rahmen des elektronischen Behördenverkehrs. Ein Konzept wird Mitte Jahr erwartet. Weiteres Ziel ist, dass "Validator.ch" schnell und eindeutig über die Validität des Zertifikates Auskunft geben kann.</p> <p>Weiteres Vorgehen:</p> <ul style="list-style-type: none"> - Konzept erstellen - Vernehmlassung bei den CSP - Finalisierung Konzept Behördenzertifikat - Umsetzung im Anhang zur TAV des BAKOM

Sektorkomitee Informatiksicherheit

Arbeitssitzung vom 03.05.2019

Traktanden	Ergebnis/Entscheid
13. Diverses - Verschiedenes - Themenvorschläge	Gewünschte Themen wären:
9. Ort und Datum nächste Sitzung	Für den Bereich PKI wird gewünscht, dass die Sitzungen halbjährlich organisiert werden. Nächste Sitzung wird Q4/2019 gewünscht (doodle-Umfrage) im SECO, Holzikofenweg 36, 3003 Bern

Bern, 12.08.2019 /hit