ku/Ergebnisse Sitzung AG IT-Sicherheit am 07.02.2025 in Siegburg

Teilnehmende: Michael Schmidt (AV), Dr. Heiko Althoff (EGLV), Ulrich Molitor (EV), Niclas Schlothane (EV), Florian Haus (LINEG), Christof Döring (NV), Frank Steinwender (RV), Jürgen Sluytermann (WTV), Marcel Brühl (WTV), Dr. Sonja Haas (WTV), Ralf Dittrich (WVER), Florian Fußberger (WVER), Wilhelm Frings (WVER), Jennifer Schäfer-Sack (agw), Petra Kuhr (agw)

entschuldigt: Patrick Zolper (BRW), Sigurd Sommer (LINEG), Jens Becker (NV), Andreas vom Stein (RV), Fabian Noack (RV), Stefan Kremer (WTV), Christoph Hachenberg (WV)

Gast: Rolf Tenner (StEB Köln)

Tagesordnung:

0. **Begrüßung, Ergänzungen der Tagesordnung**
1. **Austausch B3S (Herr Tenner, StEB Köln)**
2. **Aktuelles aus der agw (kurz)**
3. **Erarbeitung eines Konzeptes für ein Unterstützungsnetzwerk und erste Überlegungen Angriffsszenario**
    a. Warum ist es sinnvoll?
    b. Abwehr-/Angriffsszenario – was wollen wir?
    c. Arbeitspakete schnüren
    d. Abstimmung weiteres Vorgehen
4. **Bericht aus den Verbänden, allgemeiner Austausch und Diskussion**
    a. Austausch zu Softwareprodukten, Auditoren, Lizenzmodellen
    b. Next Shift KI, Governance- und Security-Fragen
    c. Gemeinsame Diskussion
5. **Verschiedenes**
    a. Neuer Termin mit Besichtigung des Cyber-SOC des KDW in Essen im Sommer 2025

TOP 0: Begrüßung, Ergänzungen der Tagesordnung

Frau Schäfer-Sack begrüßt die Teilnehmenden im Namen der agw, insbesondere dankt Sie Herrn Rolf Tenner von der StEB Köln für die Bereitschaft, heute als Gast und Referent teilzunehmen. Herr Sluyterman begrüßt die Teilnehmenden im Namen des WTV und gibt Informationen zum allgemeinen Ablauf der Sitzung und der Organisation des weiteren Tages. Die im Vorfeld den Teilnehmenden zugegangene Tagesordnung wird ohne Änderungen angenommen. Frau Schäfer-Sack gibt einen kurzen Überblick über die Arbeit der agw und die Genese der agw AG IT-Sicherheit. Es folgt eine Vorstellungsrunde.

Die Teilnehmenden beschließen, sich zukünftig im Rahmen der Arbeitsgruppe mit Du anzureden.

TOP 1: Austausch B3S (Herr Tenner, StEB Köln)

Herr Tenner stellt anhand eines Foliensatzes die Änderungen im Branchenstandard Wasser/Abwasser (B3S WA Edition 2023) vor. Der B3S WA stellt einen Minimalstandard mit den Anforderungen aus

dem IT-Grundschutz-Kompendium dar. Eine Fortschreibung erfolgt alle zwei Jahre. Nach Abschluss der KRITIS-Gesetzgebung ist eine Fortschreibung alle drei Jahre geplant. Im Jahr 2023 haben sich einige Neuerungen ergeben hinsichtlich der Anzahl der Anwendungsfälle und der allgemeinen Struktur. Zusätzlich wurden Doppelungen gestrichen und eine Reduzierung der Anzahl der Anforderungen vorgenommen. Die Änderungen sorgen insgesamt für eine Verschlankung und wird von den Teilnehmenden ausdrücklich begrüßt.

Herr Tenner verweist zudem auf eine aktuelle Veröffentlichung des BSI zur „Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN)“. Die Konkretisierung des Schemas zur Reife- und Umsetzungsgradbewertung bei der § 8a BSIG-Nachweisprüfung bindet die Bewertung der Reife- und Umsetzungsgrade durch die Prüfer an festgelegte Kriterien. Sie ist spätestens für beim BSI eingereichte Prüfergebnisse mit einem Ende der Prüfung nach dem 01.04.2025 anzuwenden.

Der Foliensatz wird den Teilnehmenden im Nachgang zur Verfügung gestellt.

Die Teilnehmenden danken Herrn Tenner für die Vorstellung der Änderungen. Die Verbände, die bereits die Umstellung auf den B3S WA 2023 durchgeführt haben, bestätigen, dass die Anwendung einfacher geworden ist.

Die Teilnehmenden diskutieren intensiv über die unterschiedlichen Normen und Standards im Bereich der Informationssicherheit. In den Verbänden werden derzeit vor allem der Branchenstandard Wasser/Abwasser und die ISO/IEC 27001 angewendet. Das BSI-Grundschutz-Kompendium wird von einigen Beratern als Standard gefordert. Die Teilnehmenden tauschen sich zu den Vor- und Nachteilen der unterschiedlichen Standards aus. Festzuhalten ist, dass der B3S WA ein guter und eignungsfestgestellter Standard explizit für die Wasserwirtschaft ist.

Insbesondere vor dem Hintergrund der Umsetzung der NIS2-Richtlinie in deutsches Recht rückt die Betrachtung des gesamten Verbands in den Vordergrund. Die Umsetzung in deutsches Recht sowohl der NIS2-Richtlinie als auch der CER-Richtlinie verzögert sich derzeit aufgrund der vorgezogenen Neuwahl des Deutschen Bundestages wahrscheinlich bis Mitte 2025. Der B3S WA wird nach dem Abschluss des deutschen Umsetzungsprozess der EU-Richtlinien erneut angepasst werden. Nach Einschätzung einiger Teilnehmender wird der Umsetzungsprozess auch Auswirkungen auf die Trennung von OT/IT in den Verbänden haben. Die Teilnehmenden werden sich darüber über die agw weiterhin eng austauschen.

Frau Schäfer-Sack gibt einen Hinweis auf ein Praxisseminar des KDW im Mai dieses Jahres, in dem die Anforderungen aus der NIS2-Richtlinie und deren praktische Umsetzung bei den Betreibern intensiv thematisiert werden wird. Da nach Rücksprache mit Herrn Derler nur eine begrenzte Anzahl an Plätzen zur Verfügung steht, ist eine frühzeitige Anmeldung erforderlich. Das Save-the-Date wird im Nachgang der Sitzung an die Teilnehmenden verteilt werden.

TOP 2: Aktuelles aus der agw (kurz)

Angesichts der fortgeschrittenen Zeit wird dieser Tagesordnungspunkt verkürzt dargestellt. Die Hinweise auf den Umsetzungsstand des NIS2-Umsetzungs- und des KRITIS-Dachgesetzes wurden bereits unter TOP 1 thematisiert. Die EU hat in beiden Fällen ein Vertragsverletzungsverfahren gegen

Deutschland eingeleitet. Vor diesem Hintergrund bereiten sich die meisten Mitgliedsverbände der agw bereits jetzt schon intensiv auf die Umsetzung der NIS2-/CER-Gesetzgebund in den Verbänden vor.

Ein Überblick über die Schwerpunkte in den Wahlprogrammen der demokratischen Parteien im Vorfeld der Bundestagswahl insbesondere hinsichtlich der Themen IT-Sicherheit, Digitalisierung und Künstliche Intelligenz wird angesichts der fortgeschrittenen Zeit nicht gewünscht.

TOP 3: Erarbeitung eines Konzeptes für ein Unterstützungsnetzwerk und erste Überlegungen Angriffsszenario

Frau Schäfer-Sack stellt kurz die Genese dieses Vorhaben sowie den Beschluss der Mitgliederversammlung für ein gemeinsames Unterstützungsnetzwerk und Angriffsszenario vor.

Herr Sluyterman führt in die Thematik ein. Wichtig ist die gemeinsame Ableitung eines Scopes, unter dem die Verbände sich versammeln können. Die Szenarien reichen von Stromausfällen, Satellitenstörungen, Cyberangriffen, Lieferkettenproblemen bis hin zum Fall der Bündnis-/Landesverteidigung.

Die Teilnehmenden diskutieren über die Abgrenzung und die vermutlich betroffenen Bereiche. Im Falle eines Angriffs ist in erster Linie die IT betroffen, die OT nur in vereinzelten Fällen. Die Ausprägungsstufen können klein, mittel und ein Totalausfall sein. Auch müsste über eine gemeinsame Vorgehensweise und ggfs. eine gemeinsame Kommunikationsweise gegenüber Behörden diskutiert werden.

Die Einbindung des SOC KDW als Unterstützung im Notfall kann nur funktionieren, wenn die Verbände eigenes Personal dafür abstellen, da die fachliche Expertise in den Verbänden liegt. Allerdings hält das KDW in ihren Räumlichkeiten Infrastruktur vor, die im Falle einer Kompromittierung des eigenen Netzes genutzt werden können. Bei der Ableitung des Scopes muss auch geklärt werden, wie weit der Rahmen des Unterstützungsnetzwerkes gezogen wird. Dies gilt es im weiteren Verlauf zu diskutieren. Wichtig ist ebenso die Frage der Kommunikation im Falle eines Cyber-Angriffs. Hier müssen alternative Kommunikationswege mitgedacht werden.

Der Zeitpunkt der Entscheidungsfindung wurde ebenfalls diskutiert, da dieser für den Verlauf der Krise von großer Bedeutung ist. Betroffene Verbände berichten darüber, dass in den ersten drei Stunden nach einem Angriff es nicht möglich sei, gemeinsam zu agieren. Dies ist allerdings die Zeit, in der der größte Schaden entsteht. Eine Unterstützung durch die Verbände wäre erst ab Stunde drei sinnvoll, wenn es um die Analyse des Angriffs geht und den Wiederaufbau des Systems. Hier kann ein Tandemgespann in jedem Fall sehr hilfreich sein.

Darüber hinaus tauschen sich die Teilnehmenden über eine 24/7-IT-Rufbereitschaft im Verband aus. Diese ist bislang nicht in allen Verbänden vorhanden.

Es wird vereinbart, dass Herr Sluyterman und Herr Dr. Althoff einen ersten Aufschlag eines Konzeptes formulieren werden, die den Teilnehmenden rechtzeitig vor dem nächsten Termin bei EGLV in Essen nach den Sommerferien 2025 zur Verfügung gestellt wird. In der nächsten Sitzung wird darüber eine Diskussion stattfinden.

TOP 4: Bericht aus den Verbänden, allgemeiner Austausch und Diskussion

Angesichts der fortgeschrittenen Zeit wird dieser Tagesordnungspunkt bilateral in die Mittagspause verschoben.

TOP 5 Verschiedenes

Die nächste Sitzung wird nach den Sommerferien 2025 bei EGLV in Essen stattfinden. Die Terminfindung wird digital nach der Sitzung erfolgen. Im Anschluss an die nächste Sitzung ist zudem ein Besuch beim KDW in Essen und eine Besichtigung des SOC KDW geplant.

Im Anschluss an die Sitzung erfolgt ein gemeinsames Mittagessen und die Besichtigung des Wasserwerks des Wahnbachtalsperrenverbands.

gez. J. Schäfer-Sack