DVGW
Service & Consult GmbH

DVGW
S&C

Gesetze, B3S WA, Eigenverantwortung und neues Denken

Björn Boos – Berater für Informationssicherheit

Gesetze: Übersicht

IT-SiG 2 vom 18.05.2021 (BGBl 27. Mai 2021)

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

BSI-KritisV Version 2

NIS 2.0 Richtlinie

Gesetze: IT-SiG 2 - § 7b

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes oder der in § 2 Absatz 10, 11 und 14 genannten Unternehmen Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, ….. Die Maßnahmen müssen sich auf einen vorher bestimmten Bereich von Internet-Protokolladressen, die regelmäßig den informationstechnischen Systemen

1. des Bundes oder

2. Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse

zugeordnet sind (Weiße Liste), beschränken.

Gesetze: IT-SiG 2 - § 8a

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.

Gesetze: IT-SiG 2 - § 8a
Beispiel – Intrusion Detection System

Meldungen

Eingang 30 | Überwacht 0 | Quittiert 0

Automatisch aktualisieren | Überwachen | Quittieren | Exportiere Meldungen

Erstes Auftreten	Wert	Endgeräte	Protokoll	Risikobewertung	
2021-06-01 11:37:09	(3) (3)	SCHRAML10_REDUN ⇄ 192.168.2.255	NetBIOS		PCAP herunterladen
2021-06-01 11:37:09	(1) (3) (3)	SCHRAML10_REDUN ⇄ 169.254.255.255	NetBIOS		PCAP herunterladen
2021-06-01 11:35:50	(2) (2) (2)	00:20:d5:01:df:97 ⇄ ff:ff:ff:ff:ff:ff (Broadcast)	ARP		PCAP herunterladen
2021-06-01 11:35:48	(2) (2) (2)	00:20:d5:02:83:c5 ⇄ ff:ff:ff:ff:ff:ff (Broadcast)	ARP		PCAP herunterladen
2021-06-01 11:35:06	(3) (6) (4)	PC-FERNZUGRIFF ⇄ 192.168.4.255	NetBIOS		PCAP herunterladen

DVGW S&C

Gesetze: Zweite Verordnung zur Änderung der BSI-Kritisverordnung

Übergangsfristen:

Branchenübergreifend muss festgeschrieben werden, dass für alle geänderten und neu eingeführten Anlagen zwei Jahre Zeit bis zum ersten Nachweis sowie sechs Monate für die Registrierung eingeräumt werden.

Anlagenbegriff „Software und IT-Dienste“ –

Es wird weitergehende Erläuterungen und Klarstellungen dazu geben

Betriebstechnischer Zusammenhang –

Es wird weitergehende Erläuterungen dazu geben

Gesetze: Zweite Verordnung zur Änderung der BSI-Kritisverordnung

Evaluierung der BSI-KritisV:

Die Wirtschaft und der UP KRITIS sollen in die Evaluierung eingebunden werden. Der Evaluierungsbericht wird allerdings nicht veröffentlicht (wg. § 10 Abs. 1 Satz 3 BSI-G)

Unterschreitung des Schwellenwertes

Im auf die Unterschreitung des Grenzwertes folgenden Jahr erlöschen die Verpflichtungen aus der Kritis-V.

Keine geänderten Schwellwerte → 500.000 EW bleiben der Richtwert

44 m^3 Wasserverbrauch / Person u. Jahr → 22 Mio. m^3 Schwellwert

Gesetze: Zweite Verordnung zur Änderung der BSI-Kritisverordnung Zeitplan

Anhörung der betroffenen Betreiber und Wirtschaftsverbände nach §10 Abs. 1 BSI-Gesetz am 26. Mai 2021, 13-15 Uhr

Kabinettsbeschluss: Juni 2021 (geplant)

Inkrafttreten: 1. Januar 2022 (geplant)

Registrierungs-/Meldepflicht: ab 2. April 2022 (§ 8b Abs. 3 BSI-G)

Nachweis Maßnahmen nach Stand der Technik:

2 Jahre nach erstmaliger Bestimmung als KRITIS-Betreiber (§ 8a Abs. 3 BSI-G)

Gesetze: NIS 2.0 Richtlinie

NIS 2.0 Richtlinie (Entwurf vom 16.12.2020) – legt Maßnahmen fest, mit denen in der Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll.

Richtlinien sind Rechtsakte der Europäischen Union, die aber nicht unmittelbar in den Ländern gelten, sondern von den Mitgliedstaaten in nationales Recht umgewandelt werden müssen (Gegensatz ist eine Verordnung, z.B. Datenschutz-Grundverordnung)

Gesetze: NIS 2.0 Richtlinie

Artikel 2 - Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission angesehen werden.

Kommentar BDEW: Anwendungsbereich der Richtlinie (Artikel 2 + Anhang): Die vorgeschlagene Ausweitung des Anwendungsbereichs sollte nur die Unternehmen von systemischer Relevanz umfassen. Ausnahmemöglichkeiten für Kleinst-, kleine und mittlere Unternehmen der Energie- und Wasserwirtschaft sollten auch zukünftig möglich sein *(keine Anwendung der EU-KMU-Definition).*

Gesetze: NIS 2.0 Richtlinie

Artikel 31 (Entwurf)

Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen gemäß diesem Artikel bei Verstößen gegen die in dieser Richtlinie festgelegten Verpflichtungen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Stellungnahme BDEW: Der Höchstbetrag sollte jedoch bei 2 Mio. € liegen und nicht in Relation zum Jahresumsatz stehen.

Zum B3S WA

B3S WA v.3

Anwendungsfälle sind 3 dazu gekommen:

AR 6 - Datenverbindung über Netzwerke anderer Anbieter (Mobilfunk etc. in Abgrenzung zu AR 2)

AR 7 - Virtualisierung der Infrastruktur

AR 8 - Einsatz von IoT Geräten

Es gilt das zum Zeitpunkt der Genehmigung geltende Grundschutzkompendium.

Grundschutzkatalog ist raus

Zur Einordnung von Trinkwasserversorgungsunternehmen als kritische Infrastruktur nach KritisV

Eigenverantwortung: Wasserversorger nach Größe

WVU mit betrieblicher Wassergewinnung von ... bis unter ... m3	1 000 m³	Anzahl WVU	Versorgungs-anteil	Gruppierung
unter 10 000	2367	532	0,06%	
10 000 - 20 000	3361	238	0,08%	
20 000 - 30 000	4224	174	0,10%	
30 000 - 50 000	8530	216	0,21%	
50 000 - 100 000	33124	448	0,80%	
100 000 - 200 000	90342	621	2,17%	
200 000 - 300 000	100655	407	2,42%	
300 000 - 500 000	159770	405	3,85%	9,69%
500 000 - 1 Mill.	358051	498	8,62%	
1 Mill. - 10 Mill.	1645004	617	39,60%	48,22%
10 Mill. oder mehr	1748348	42	42,09%	42,09%
Insgesamt	4153776	4198	4153776	

© 2016 Destatis Fachserie 19 Reihe 2.1.1 – Öffentliche Wasserversorgung

Eigenverantwortung: Eine einfache Frage

Wollen wir selbst die Digitalisierung oder scheuen wir uns vor den Veränderungen, die sie zwangsweise mit sich bringt?

IT = Informationstechnik

OT = Operational Technology (Steuerungstechnik)

„Zwischen IT und OT unterscheiden wir schon bereits seit 2018 nicht mehr. Die eingesetzten Technologien und Protokolle sind mittlerweile identisch.“

Heiko Althoff,
Abteilungsleiter Informationstechnologien - EMSCHERGENOSSENSCHAFT/LIPPEVERBAND

Eigenverantwortung: Schwachstellen kennen und managen

Common Vulnerabilities and Exposures (deutsch: Häufige Schwachstellen und Anfälligkeiten) sind seit 1999 der Industriestandard.

Die Liste der CVEs wird von der MITRE-Corporation zusammen mit CVE Numbering Authorities verwaltet.

Für deutsche Steuerungen ist die Numbering Authority das CERT@VDE (Bestandteil des VDE e.V.) zuständig.

OASIS Common Security Advisory Format (CSAF) mit relevanter Unterstützung u. a. von BSI, NIST und MITRE soll automatisieren.

Neues Denken: Was ist spezifisch an den Steuerungen für die Wasserversorgung?

Neues Denken: Kritische Infrastruktur darf nicht im Internet betrieben werden!

Erste Konsequenz: Sofortige Stilllegung des Internets

- Das ist nämlich auch kritische Infrastruktur.

Entscheidung Bundespost zur Digitalisierung
aller Ortsvermittlungsstellen → 1979
Offizielle Betriebsaufnahme in Deutschland → 1989
ISDN befindet sich aktuell „in Abschaltung“

Punkt-zu-Punkt Verbindungen → gestern
Risiken durch Infiltration in digitale Netze → schon lange

Aber: Wer die Risiken nicht managen will, kann die Vorteile nicht nutzen!

© Wikipedia – Briefmarke von 1988

Neues Denken: Zero Trust – ein unglücklicher Name
Aber eine coole Methodik

Kein

- Gerät
- Anwender
- Dienst

sowohl innerhalb des eigenen Netzes als auch außerhalb des eigenen Netzes ist vertrauenswürdig, also wird allen misstraut.

- Alle Geräte müssen registriert sein (Attestation Service)
- Alle Anwender müssen sich authentifizieren (Active Directory)
- Alle Dienste müssen autorisiert sein (Attribute Authority)

Erst dann wird eine Kommunikation ermöglicht.

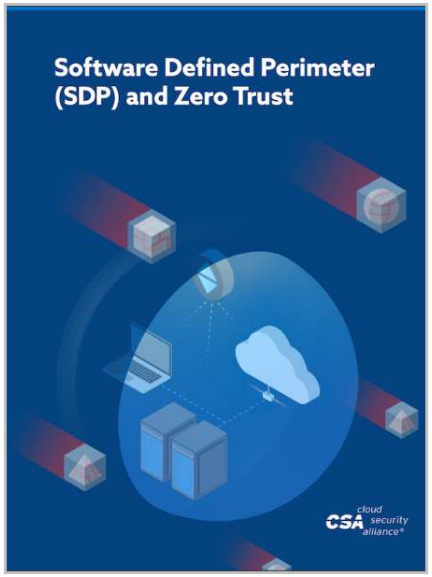
Neues Denken: SDP - Woher kommt der Denkansatz

DISA (Defense Information Systems Agency) seit 2005

- Black Core Network-Initiative innerhalb des Global Information Grid

Heute weiterentwickelt von Cloud Security Alliance

Google IBM Security Microsoft



Öffentliche Demo zum Runterladen:

http://sdpcenter.com/test-sdp/

https://github.com/WaverleyLabs

DVGW S&C

Zu Zero-Trust und SDP

Neues Denken: Software Whitelisting / Blacklisting – Ein Beispiel

Blacklisting ist die Funktion jeder Virenschutzsoftware

Ausführungsverhalten von unerwünschter Software bei aktiviertem Software Whitelisting

Benutzer	**Software Restrictions** (seit WinXP - 2001)	**Applocker** (seit Win7 - 2008)	**Code Integrity – WDAC** (seit Win10 – 2017)
Standardbenutzer	nicht startbar	nicht startbar	nicht startbar
Administrativer Benutzer	nicht startbar	nicht startbar	nicht startbar
Systemkonto	startbar	startbar	nicht startbar

Software Whitelisting - der bessere Virenschutz - IT- und Medienzentrum - Universität Rostock (uni-rostock.de)

Gesetze, B3S, Eigenverantwortung und neues Denken

Björn Boos – Berater für Informationssicherheit

DVGW Service & Consult GmbH
Björn Boos +49 228 9188-93126
björn.boos@dvgw-sc.de – www.dvgw-sc.de