KISTERS

Cybersicherheit – Schwachstellen entdecken mit Umweltmonitoring

Dr. Volker Bühner

Bau Akademie Ost - Digitalisierung und Innovation. Berlin, 09.02.23

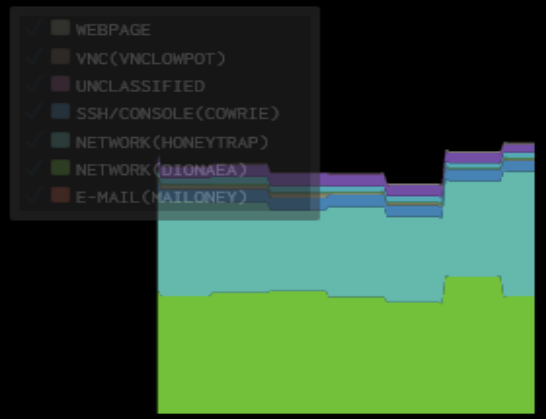
Der Sicherheitstacho zeigt die weltweiten Cyberangriffe auf die Honeypotinfrastruktur der DTAG sowie ihrer Partner an.

26834

Attacken in der letzten Minute

1226288 Attacken in den letzten **1** h

44117964 Attacken in den letzten **24** h



LIVE TICKER

DOMAIN	DATUM	QUELLE	ZIEL	ANGRIFFSTYP	PARAMETER
COMM	10:11:46	FR	HK	Network(honeytrap)	Attack on port 5038/tcp
COMM	10:11:45	FR	HK	Network(honeytrap)	Attack on port 5038/tcp
COMM	10:11:44	TH	US	Network(Dionaea)	Attack on port 445/tcp
COMM	10:11:43	TH	US	Network(Dionaea)	Attack on port 445/tcp
COMM	10:11:42	TH	US	Network(Dionaea)	Attack on port 445/tcp

TOP ATTACKER 2023-02

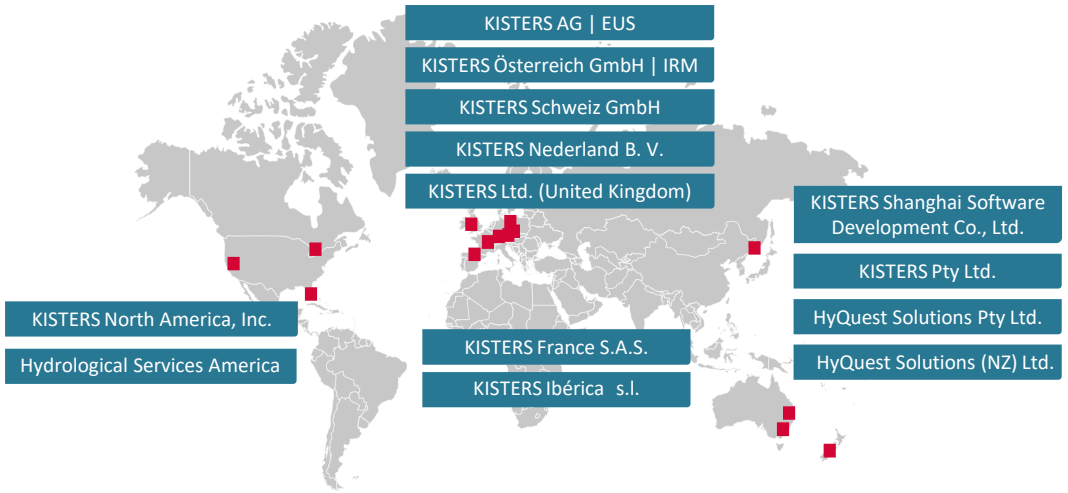
LAND	ATTACKEN
RU	24146772
US	12358974
NL	6618951
GB	5711260

Agenda

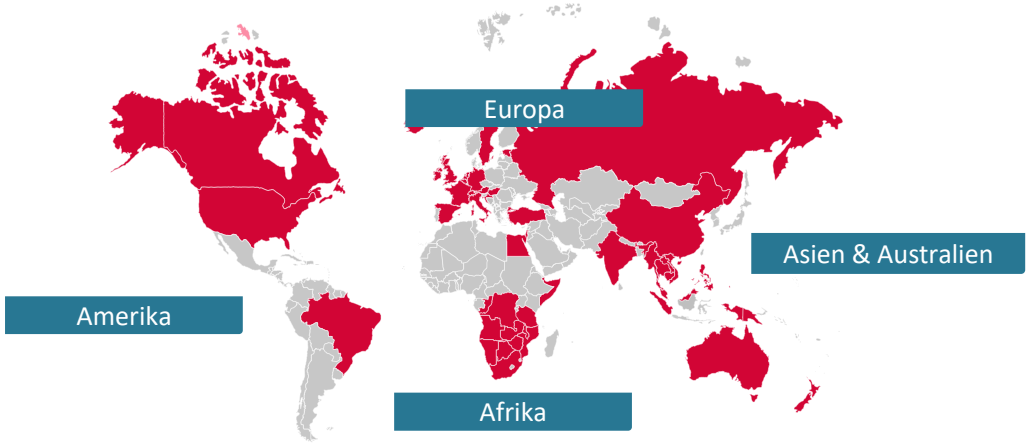
- Digitalisierung in der Energiewirtschaft
- Erfahrung und Auswirkungen nach einem Cyber-Angriff
- Der rechtliche Rahmen: KRITIS, IT-SiG 2.0
- (IT)-Umweltmonitoring: CVE-Tracking & Angriffserkennung mit Intrusion Detection Systemen (IDS)

KISTERS auf einen Blick

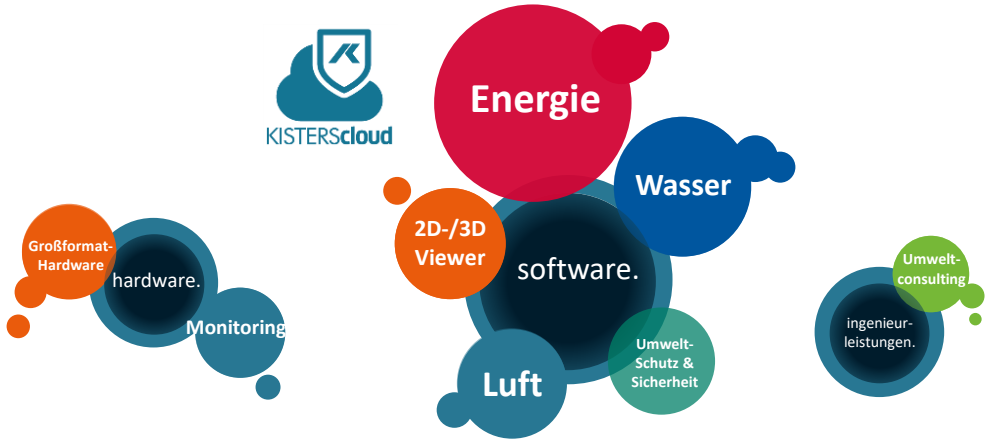
Die KISTERS Gruppe



Eine starke Kundenbasis



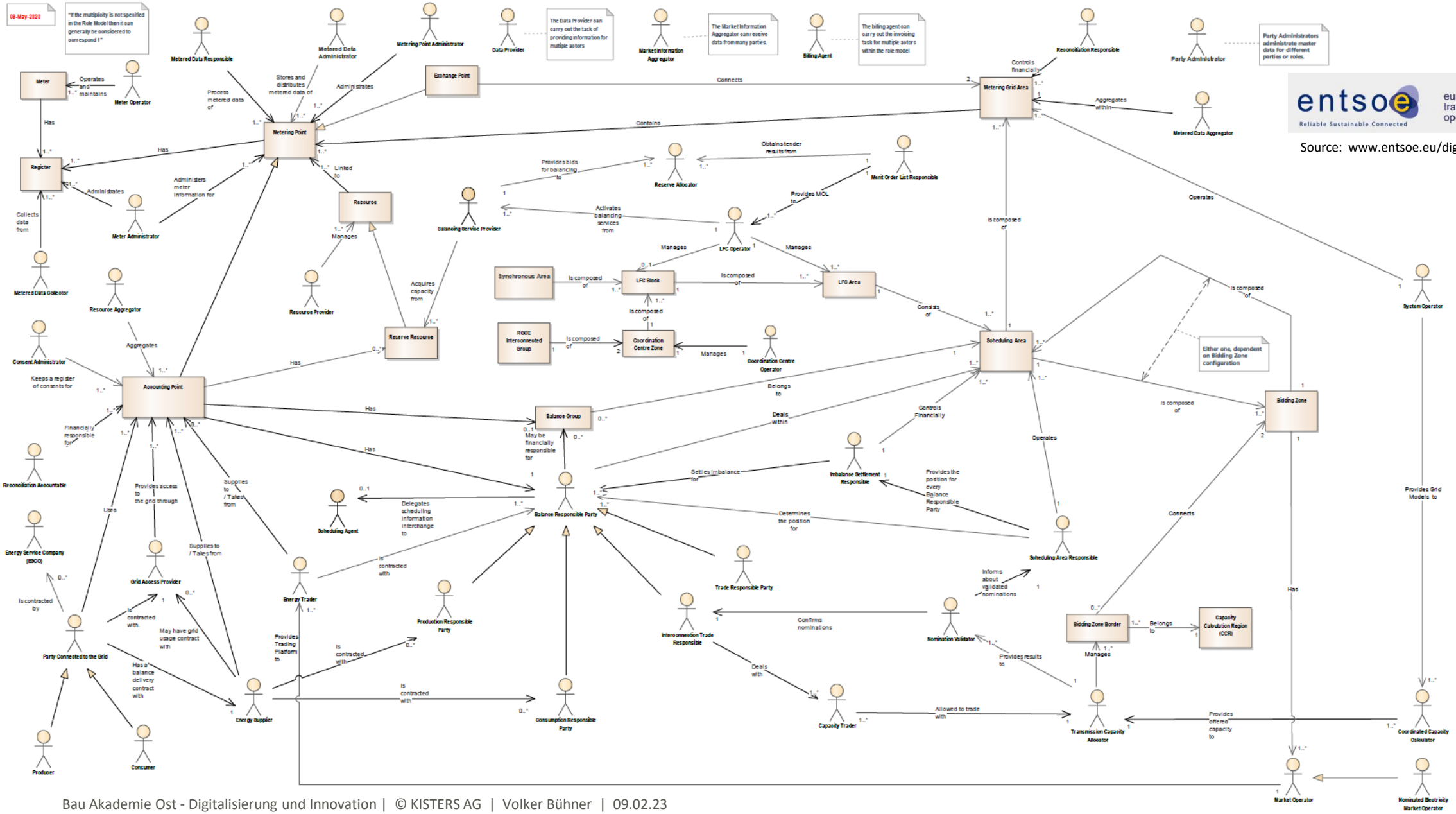
Märkte & Softwareprodukte



Unternehmenszahlen

Kennzahlen	22
Anzahl fester Mitarbeiter	> 700
Anzahl Business Units	6
Anzahl Tochtergesellschaften	14

Marktrollenmodell Energiewirtschaft



ERS

entsoe
Reliable Sustainable Connected
european network of transmission system operators for electricity

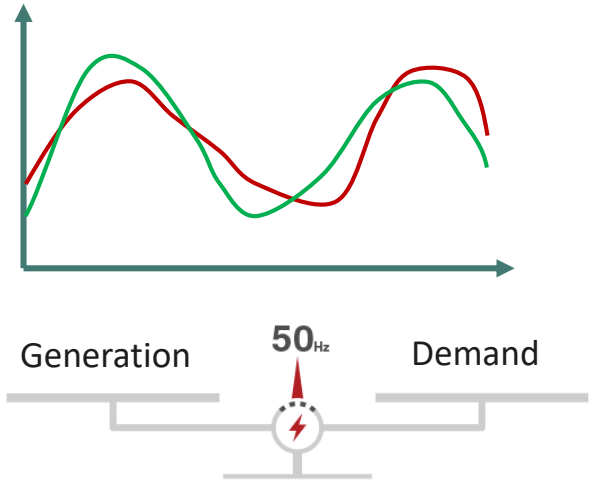
Source: www.entsoe.eu/digital/cim/role-models/

Digitalisierung in der Energiewirtschaft

Digitalisierte Prozesse ohne manuellen Eingriff

Regelkreise mit direktem Eingriff

- Regelenergie inkl. europäischem Stromaustausch
- Netzleittechnik
- Digitale Schutztechnik



Marktkommunikation

- Aggregation aller Handelsgeschäfte zu Fahrplänen
- Bilanzierung auf Ebene der Bilanzkreisverantwortlichen (BKV) und Übertragungsnetzbetreiber (TSO)
- Redispatch (1.0 und 2.0): BKV, Betreiber, DSO und TSO
- Kundenwechselprozesse (Lieferantenwechsel, MSB Wechsel)

Cyberangriffe: Eine Auswahl (Quelle: heise online)

KISTERS

Hackerangriff: Über 3000 Temposünder kommen ohne Strafe davon

Bei einem **Cyberangriff** im Oktober 2021 waren Server der Schweriner IT- und Servicegesellschaft (SIS) und des Kommunalservice Mecklenburg (KSM) durch eine Schadsoftware teilweise verschlüsselt worden.…

07.04.2022 | heise online

Witten: Bei Cyberangriff erbeutete Daten im Darknet veröffentlicht

Nachdem beim **Cyberangriff** erbeutete Daten der Stadt Witten im Darknet veröffentlicht worden sind, ruft der Bürgermeister zu Wachsamkeit auf.…

17.11.2021 | heise online

Rotes Kreuz: Gezielter Cyberangriff erfolgte über ungepatchte Sicherheitslücke

Der **Cyberangriff** auf das Internationale Komitee vom Roten Kreuz (IKRK) war eine gezielte Aktion, ausgenutzt wurde eine ungepatchte Sicherheitslücke in einem Single-Sign-On-System.…

17.02.2022 | heise online

Funke Mediengruppe registriert Cyberangriffe auf Zeitungswebseiten

Es ist nicht das erste Mal, dass öffentlich bekannt wurde, dass es einen **Cyberangriff** auf die Funke Mediengruppe gab. Im Dezember 2020 hatte sich schon einmal eine solche Attacke ereignet – mit schweren Folgen.…

26.02.2022 | heise online

"Terroristischer Akt": Vodafone Portugal nach Cyberattacke komplett ausgefallen

Nähere Einzelheiten zur Art des Angriffs nannte Vaz nicht, bezeichnete den **Cyberangriff** aber als "terroristischen" und "kriminellen" Akt. Vodafone Portugal arbeite daran, alle Dienste wiederherzustellen, dies stelle sich aber als "langwierig" dar.…

09.02.2022 | heise online

Cyberangriff führt zu Einschränkungen für Kunden beim Autovermieter Sixt

Der Autovermieter Sixt hat eine Cyberattacke eingestanden. Eigenen Angaben zufolge sei der Angriff frühzeitig eingedämmt worden, sodass die Auswirkungen…

04.05.2022 | heise online

Nvidia: Cyber-Attacke unbekannter Tragweite, Hersteller schlägt angeblich zurück

Nvidia ist offenbar Opfer einer Cyber-Attacke geworden. Eine Hacker-Gruppe behauptet, Zugriff auf vertrauliche Mitarbeiterinformationen und Daten erlangt…

28.02.2022 | heise online

Satelliten-Störung: Tausende Windräder nicht steuerbar

Das Unternehmen gehe einem vermuteten **Cyberangriff** nach und habe ein Sercurity-Unternehmen damit beauftragt, berichtet die Nachrichtenagentur Reuters ….

01.03.2022 | heise online

Cyberangriffe: Der business case fliegt (Quelle: heise online)

KISTERS

https://www.heise.de/news/Knapp-die-Haelfte-der-Ransomware-Opfer-zahlt-Loesegeld-7067219.html

Knapp die Hälfte der Ransomware-Opfer zahlt Lösegeld

Zwei Drittel der Befragten gaben demnach an, im vergangenen Jahr Opfer einer Ransomware-Attacke gewesen zu sein. 2020 waren es 37 Prozent gewesen – ein Anstieg von rund **80** Prozent....

27.04.2022 | heise Security

Ransomware: USA setzen Kopfgeld auf Mitglieder der Conti-Gruppe aus

Im vergangenen Jahr etwa gelang es **Conti**, das irische Gesundheitssystem teilweise lahmzulegen ....

07.05.2022 | heise online

Cybergang Conti: Interne Daten geleakt - 2,8 Milliarden US-Dollar erbeutet

Das **Conti**-Mitglied befindet sich offenbar auch in der Ukraine. Schmerzhafte Datenlecks Das erste Paket enthält interne Jabber-Protokolle von **Conti** von Ende Januar 2021 bis Ende Februar 2022....

01.03.2022 | heise Security

Nach Cyberangriff auf Fraunhofer-Institut in Halle Daten im Darknet angeboten

Wann der **Cyberangriff** stattfand, ließ der LKA-Sprecher offen. Auch über die mögliche Täterschaft wollte der Sprecher nicht spekulieren. Er mahnte jedoch an, dass in Sachsen-Anhalt mittlerweile jedes dritte Unternehmen von Cyberkriminalität betroffen sei....

04.05.2022 | heise online

Wind turbine giant Vestas confirms data breach following 'cybersecurity incident'

Adam Bannister 22 November 2021 at 13:20 UTC
Updated: 23 November 2021 at 08:46 UTC

Cyber-attacks | Denmark | Critical Infrastructure

Danish company has also 'initiated a gradual and controlled reopening of all IT systems'

Vestas, the world's largest supplier of wind turbines, has revealed that data has been compromised following a suspected cyber-attack.

In a statement posted today (November 22), the Danish energy giant said it "has already initiated a gradual and controlled reopening of all IT systems" after shutting down several operational IT systems as a precaution following a "cybersecurity incident" on Friday (November 19).

News of the incident first emerged on Saturday (November 20) when the company warned that "customers, employees, and other stakeholders may be affected by the shutdown".

Cyberangriffe: KISTERS AG (Quelle: heise online)

KISTERS

https://www.heise.de/ratgeber/Security-So-laufen-Ransomware-Angriffe-heute-ab-6457906.html?seite=all

Massive Cyber-Angriffswelle auf Behörden, Onlineshops & Co.

Die mittelständische Kisters AG aus Aachen war nach einem **Cyberangriff** in der Nacht vom 10. auf den 11. November nicht mal mehr telefonisch über ihre Festnetznummer erreichbar....

06.12.2021 | c't Magazin

Die in der Öffentlichkeit kaum bekannte Kisters AG, die unter anderem Software für kritische Infrastrukturen aus den Sektoren Energie und Wasser anbietet, wurde Ende 2021 von Ransomware heimgesucht. Welche Auswirkungen dies für die Kunden des Unternehmens, namhafte Betreiber kritischer Infrastrukturen, noch haben wird, ist noch nicht abzusehen. Jedoch hatte die Bundesnetzagentur zwischenzeitlich in einem vom Unternehmen veröffentlichten Schreiben die Beeinträchtigung von Marktprozessen bekannt gegeben und die "fristgerechte Übersendung der für die Bilanzkreis- und Netznutzungsabrechnung zu erwartenden Messwerte und Nachrichten ausgesetzt".

Eine Auswahl (Quelle www.heise.de)

- 09.02.22: Vodafone, Portugal
- 17.02.22: red cross, Switzerland
- 28.02.22: Nvidia, US
- 01.03.22: Satellite network KA-SAT, Europe
- 12.04.22: Deutsche Windtechnik
- 04.05.22: Sixt (car rental), Europe
- 12.06.22: Mainzer Stadtwerke
- 12.06.22: entega Darmstadt, Germany
- 12.10.22: WILKEN, Ulm, Germany
- 21.10.22: METRO, Germany
- 26.10.22: enercity, Hannover, Germany
- 25.11.22: prophete
- 31.12.22: SW & Stadt Potsdam
- 12.01.23: British Royal Mail
- 17.01.23: Uni Duisburg-Essen
- 20.01.23: T-Mobile US
- 23.01.23: Sky TV
- 03.02.23: Universität Zürich

Mitteilung der Bundesnetzagentur

Konsequenz: Verschiebung der Marktformatanpassungen

Beschlusskammern > Beschlusskammer 6 > Netzzugang / Messwesen > Marktkommunikation 2022

Mitteilung Nr. 27: Verschiebung der Umsetzung der Datenformate einschließlich der Marktkommunikation 2022 auf den 01.10.2022

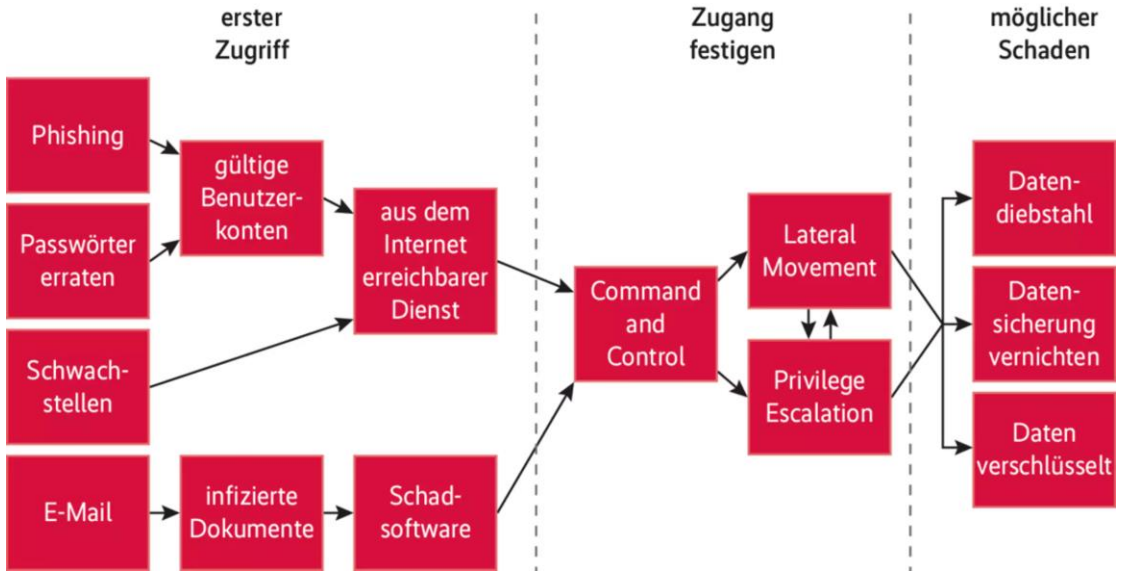
02.02.2022

An die Beschlusskammern 6 und 7 haben sich zahlreiche Unternehmen gewandt und mitgeteilt, dass der fristgerechten Implementierung der für den Umsetzungsstichtag 01.04.2022 vorgesehenen neuen Datenformate gegenwärtig schwerwiegende Hindernisse entgegenstehen.

Nach hier vorliegenden Informationen ergibt sich dies insbesondere aus einem im November 2021 stattgefundenen Hacker-Angriff auf einen unter anderem für die Energiebranche tätigen Softwarehersteller und IT-Dienstleister, dessen Entwicklungsarbeit für die Umsetzung der aktuell zu erledigenden Datenformatanpassungen dadurch um mehrere Monate zurückgeworfen worden ist. Betroffen von dieser Verzögerung sind nach Kenntnis der Beschlusskammern mehrere hundert Unternehmen und Marktrollen in den Sparten Strom und Gas.

Typischer Angriffsvektor

https://www.heise.de/ratgeber/Security-Ransomware-Angriffsmuster-und-wie-man-sich-vor-ihnen-schuetzt-6457415.html?seite=all



Etappen bei Ransomeware-Angriffen und Gegenmaßnahmen

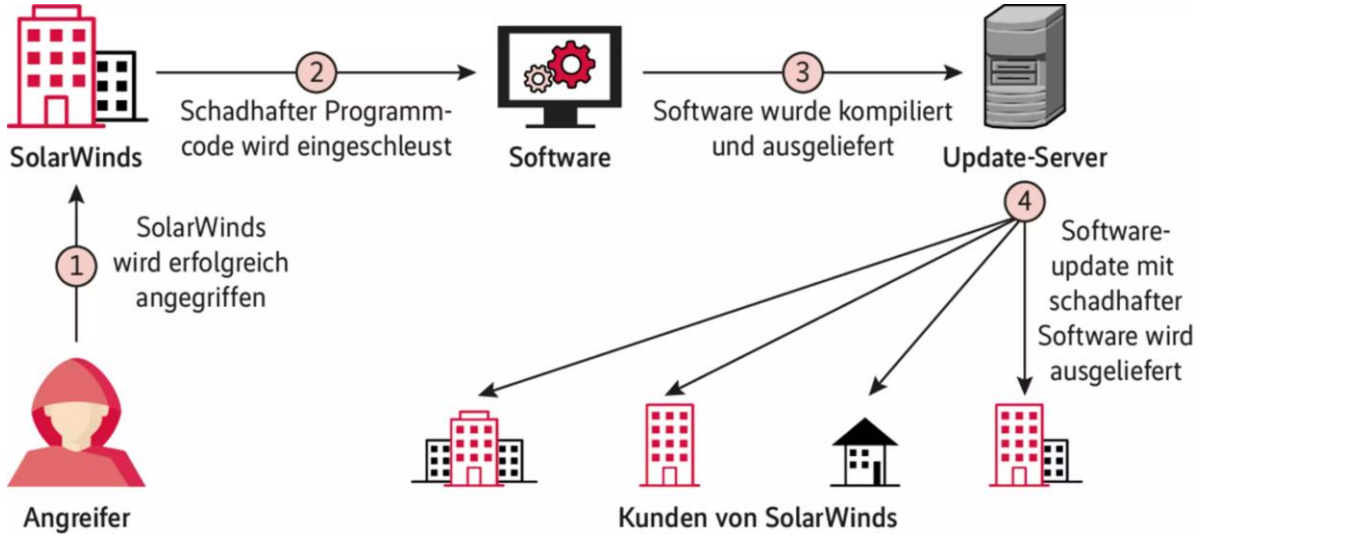
Angriffsart	Verteidigung und Abwehr	Software/Dienstleistung
Phishing (Abgriff von Nutzerdaten)	MitarbeitersensibilisierungMulti-Faktor-AuthentisierungDetektion und Reaktion	SIEM-SystemMFA-LösungSchulungsanbieter für PhishingE-Mail-/Webfilter
Brute-Forcing (Passwort erraten)	MitarbeitersensibilisierungMulti-Faktor-AuthentisierungPasswortmanagerDetektion und Reaktion	SIEM-SystemMFA-LösungSchulungsanbieter für IT-SicherheitPasswortsafe
Schwachstellen (z. B. Exchange)	Absicherung des UnternehmensnetzwerksSysteme/Software zeitnah patchenAbsicherung der Clients und ServerDetektion und ReaktionNetzwerksegmentierung	SIEM-SystemNetwork Access Controlzentrales Patch-ManagementCMDBSchwachstellenscannerIDS-/IPS-Systeme
E-Mail (Ransomware)	MitarbeitersensibilisierungAbsicherung der Clients und ServerDetektion und Reaktion	SIEM-SystemSchulungsanbieter für IT-SicherheitE-Mail-/WebfilterEndpoint-Protection-Software
aus dem Internet erreichbarer Dienst	Systeme/Software zeitnah patchenAbsicherung der Clients und ServerDetektion und Reaktion	SIEM-SystemApplication-GatewayIDS-/IPS-Systemezentrales Patch-ManagementCMDBSchwachstellenscanner
Ausführen von Schadsoftware	Systeme/Software zeitnah patchenAbsicherung der Clients und ServerDetektion und Reaktion	SIEM-SystemEndpoint-Protection-Softwarezentrales Patch-ManagementCMDBSchwachstellenscanner
Kommunikation mit Command-and-Control-Server	Absicherung des UnternehmensnetzwerksDetektion und Reaktion	SIEM-SystemNext-Gen-Firewall-SystemEinsatz von ProxysNetflow-Analysen
Lateral Movement	striktes Identitäts- und BerechtigungsmanagementAbsicherung des UnternehmensnetzwerksSysteme/Software zeitnah patchenAbsicherung der Clients und ServerDetektion und Reaktion	SIEM-SystemEndpoint-Protection-Softwarezentrales Patch-ManagementCMDBSchwachstellenscannerNetwork Access ControlIdentity ManagementIDS-/IPS-Systeme
Privilege Escalation	striktes Identitäts- und BerechtigungsmanagementPasswortmanagerAbsicherung der Clients und ServerDetektion und Reaktion	SIEM-SystemMFA-LösungIdentity ManagementIDS-/IPS-Systeme

Lessons learned

Sicherungen sind elementar, aber…

- Verteiltes, geo-redundantes Rechenzentrum / Cloud: Bei Ransomware Angriff kein Gewinn
- ISO 27001 Zertifizierung, eigener CISO: Hilfreich, aber keine Garantie
- Sicherungen sind natürlich elementar. Nur, sind diese sicher / nicht kompromittiert?
- Segmentierungen (Netzwerk, Grundschutzempfehlungen des BSI)
- Drohszenario Supply-Chain-Attack

https://en.wikipedia.org/wiki/Supply_chain_attack



https://www.heise.de/ratgeber/Security-Ransomware-Angriffsmuster-und-wie-man-sich-vor-ihnen-schuetzt-6457415.html

Entwicklung / Betrieb sicherer Softwarelösungen

KISTERS

Sichere Software erfordert einen sicherheitsorientierten Entwicklungsprozess

- Alle Schritte des Entwicklungsprozesses müssen Sicherheitsaspekte berücksichtigen
- Alle Werkzeuge im Entwicklungsprozess müssen sichere Entwicklung unterstützen
- Alle beteiligten Personen/Rollen im Entwicklungsprozess müssen sicherheitsbewusst sein
- Alle Phasen des Software Lebenszyklus (Entwicklung & Betrieb) müssen einbezogen werden

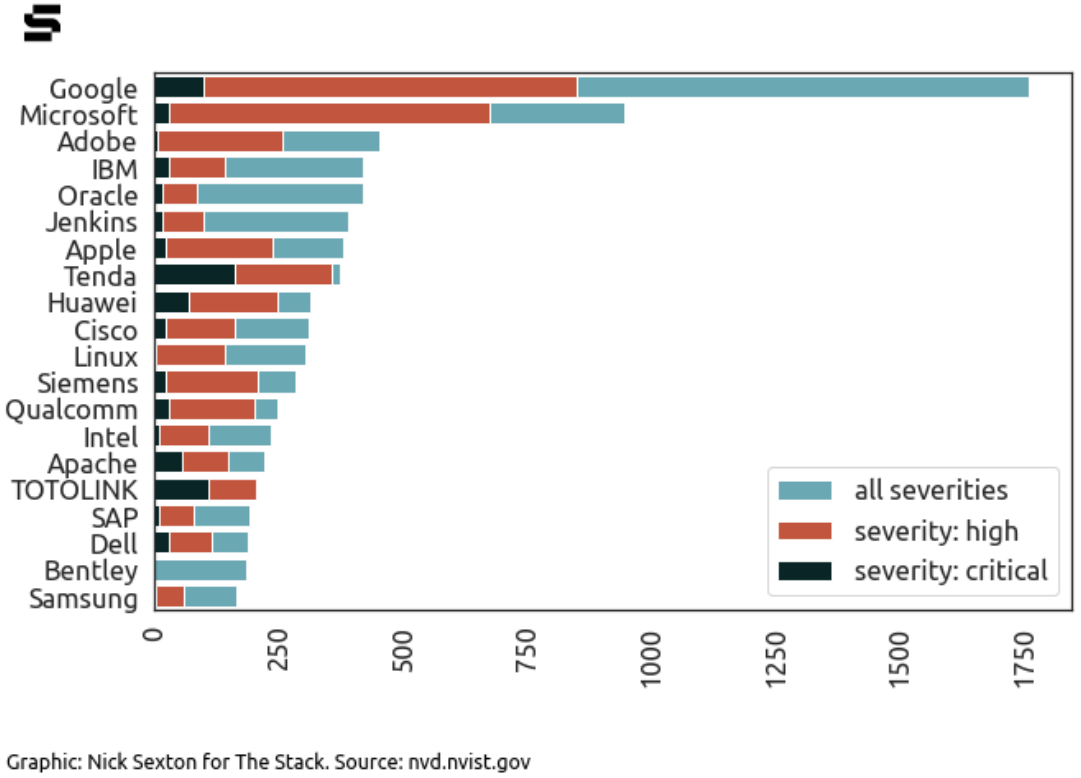
- Deswegen scannen wir alle Softwarebuilds auf (neue) CVE
- Bedingt eine Liste (Software Bill of Materials (SBOM)) über alle ausgelieferten Versionen / Kundeninstallationen
- Direkte, automatisiere Benachrichtigung der Kunden

Image: (©) GitLab

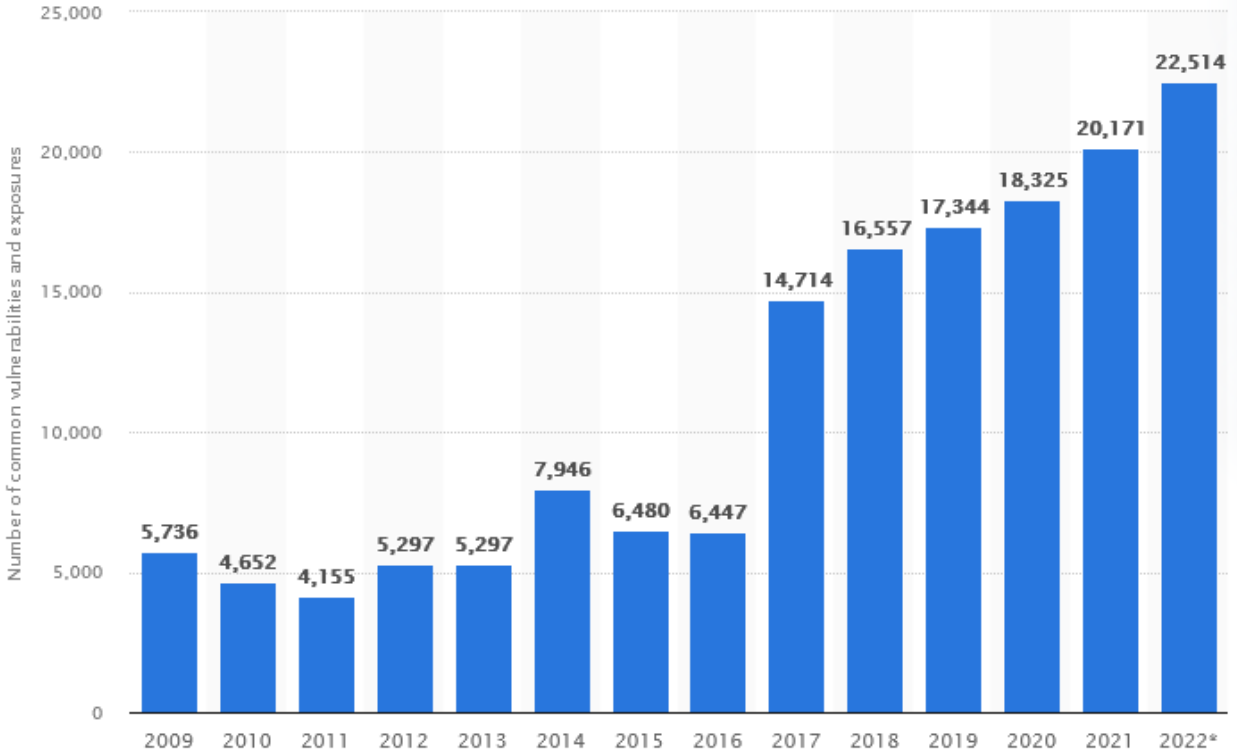
security vulnerabilities and exposures (CVEs) worldwide

KISTERS

Das Problem wächst



Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov



https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

IT-SiG 2.0

„Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“: 28.05.21

Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,

1. die in Kritischen Infrastrukturen eingesetzt werden,
2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
   a) zu einem Ausfall oder
   b) zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder
   c) zu Gefährdungen für die öffentliche Sicherheit führen können
3. und die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift
   a) als kritische Komponente bestimmt werden oder
   b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

Betrifft u.a. Soft- und Hardwarekomponenten in SCADA-Systemen, VPPM, o.ä.

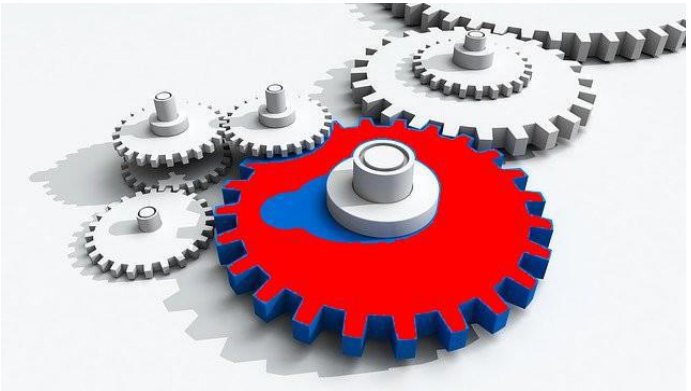
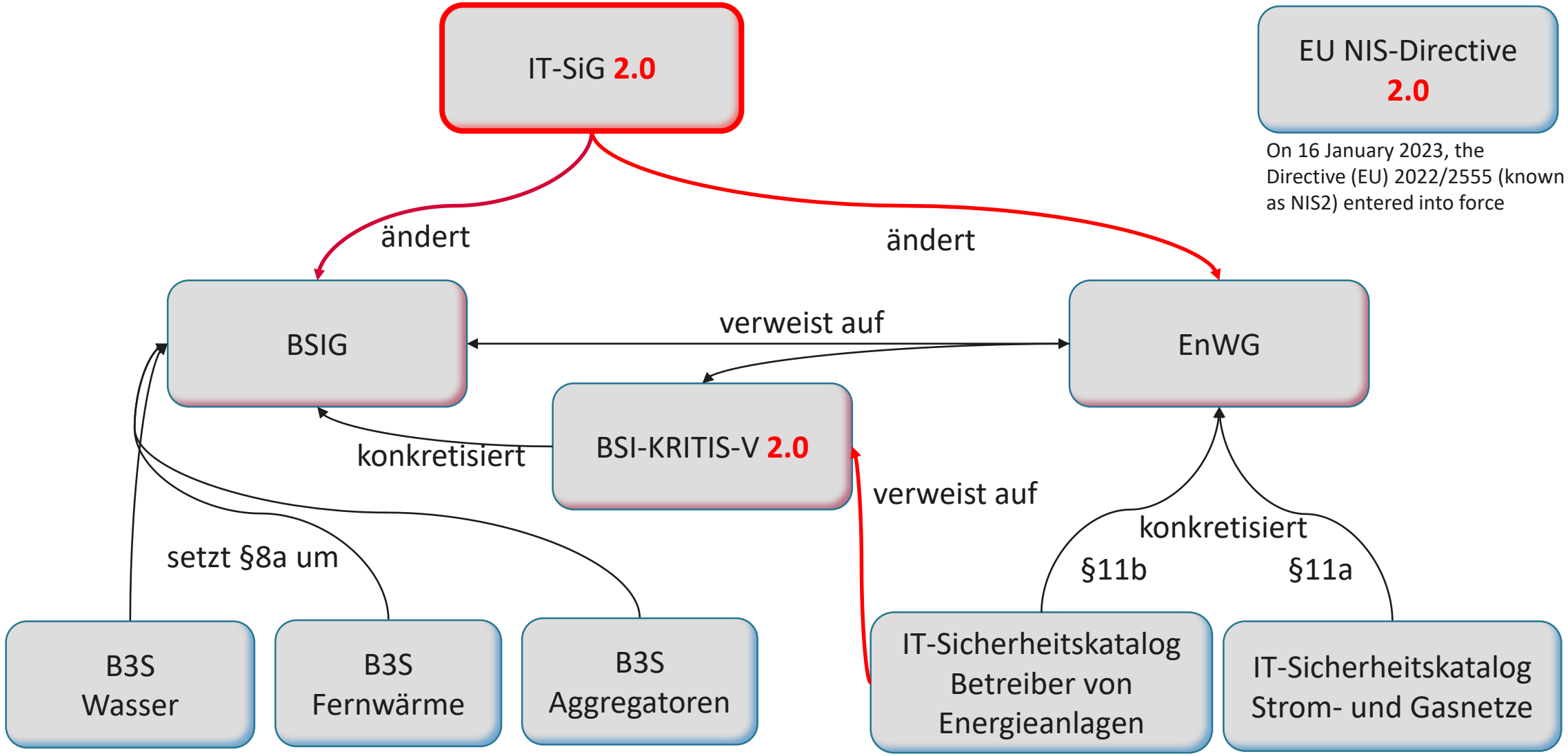


Image: (CC0) qimono / pixabay

Gesetzlicher Rahmen IT-SiG 2.0

KISTERS



IT SiG 2.0: Neue Pflichten für KRITIS Betreiber

System zur Angriffserkennung (1/2)

- Warum ein System zur Angriffserkennung?
  - Angreifer haben Erfolg weil die Sichtbarkeit in den komplexen Netzwerken fehlt
  - Es fehlen Mechanismen, um schädliche und korrekte Kommunikation zu unterscheiden
  - Angreifer lassen sich Zeit und spionieren zunächst aus

- Systeme zur Angriffserkennung gehören explizit zu den technischen und organisatorischen Sicherheitsvorkehrungen
- Bedrohungen müssen mittels Mustererkennung identifiziert und abgewehrt werden.
- Der Einsatz ist spätestens zum **01.05.23** verpflichtend.

Image: pixabay.com

IT SiG 2.0: Neue Pflichten für KRITIS Betreiber

KISTERS

System zur Angriffserkennung (2/2)

- Es gibt zwei Ansätze von Intrusion Detection Systemen (IDS), die auch kombiniert werden können:
  - Automatisierte Analyse von Logdateien, Prozessen und Rechnerknoten – Host-based IDS (HIDS)
  - Monitoring des Netzwerkverkehrs – Network-based IDS (NIDS)
- Darüber hinaus gibt es Security Information and Event Management Systeme (SIEM): Erkennt komplexe Angriffssituationen aus Ereignissen aus verschiedenen (Teil-)Systemen
- Der Einsatz eines IDS muss auf die Anforderung eines OT Netzwerks (Operational Technology) ausgelegt sein.
- Problem: Systeme zur Angriffserkennung erzeugen eine Menge an Fehlalarmen. Die Meldungen müssen zeitnahe ausgewertet und interpretiert werden, damit ein möglicher echter Angriff erkannt wird.

Fazit

Cyberangriffe lassen sich nicht verhindern sondern nur erschweren

- Minimierung der Auswirkungen eines erfolgreichen Angriffs:
  - Segmentierungen (Netze, Systeme, Domänen)
  - Alternative Kommunikationskanäle und -konzepte
  - Vorher (!) Konzepte und Checklisten erstellen
- Minimierung der Angriffsfläche:
  - CVEs umgehend bewerten und fixen
  - IDS / SIEM
- Hochautomatisierte Marktprozesse (nicht nur in der Energiewirtschaft) sind auf IT angewiesen
- Berücksichtigung des monetären und personellen Aufwands zur Absicherung und Aktualisierung von Software und Systemen

Vielen Dank für Ihre Aufmerksamkeit!

Volker Bühner
Dr.-Ing.

Head of BU Energy
Head of EUS GmbH
Branch Manager Dortmund

KISTERS AG EUS GmbH
Rhenus-Platz 3
59439 Holzwickede - Germany
Tel.: +49 2301 18591 12
Fax: +49 2301 18591 55
Cell: +49 172 71817 98

www.kisters.eu

volker.buehner@kisters.de