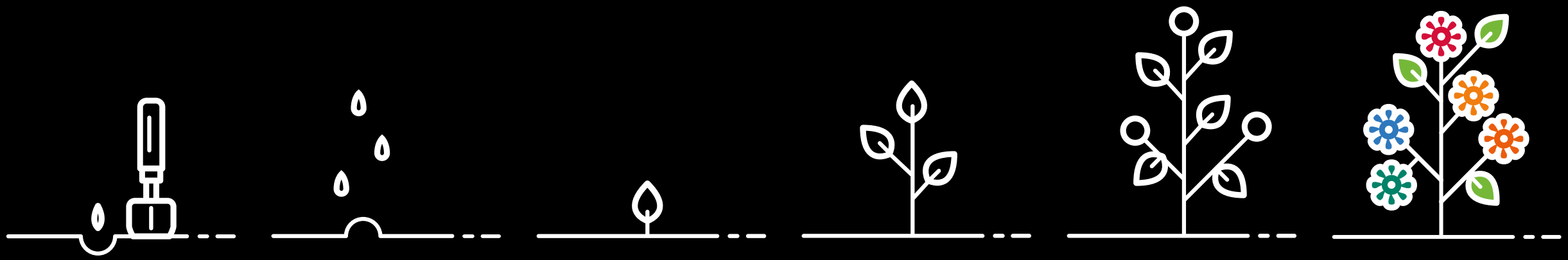
KISTERS

Empowering decisions of tomorrow

Experten für Umweltlösungen und IT.

Gegründet in	Weltweit fast	Umsatz	Mitarbeiter:innen
1963	**30 Standorte**	**€ 80 m**	**700**



Wegweisende Technologien	**Kunden-** orientiert	**Nachhaltig** im Herzen	**Empowering** decisions of tomorrow

Energie

Wegbereiter für die intelligente Nutzung erneuerbarer Energien.

Wir entwickeln digitale Lösungen, die in einem dynamischen Markt für Energie und Erneuerbare als leistungsfähige Werkzeuge für gute Entscheidungsfindung dienen und den Arbeitsalltag erleichtern.

Cloud-Lösungen

Lösungen für alle Marktrollen

Handel und Beschaffung

Vertrieb

Netzbetrieb

Metering

Smart Grid und Leittechnik

Prognose und Optimierung

„We are hacked!“

Krisenmanagement, Resilienz und Prävention

Dr. Markus Probst
KISTERS

KISTERS

Praxisbericht.

KISTERS

Der 10. November 2021...

Frankfurter Allgemeine
ZEITUNG FAZ.NET

Meldungen vom 10.11.2021
Artikel-Chronik

Zusammenarbeit angekündigt

Was die Erklärung von China und den USA für die Klimakonferenz bedeutet

In der heißen Phase der Klimaverhandlungen wollen China und die USA stärker zusammenarbeiten. Was beide erreichen wollen – und wie es sich auf das Ergebnis auswirken könnte. Mehr

Mission und Kolonialismus

Bis an die Ränder der Welt

Bernhard Maier gelingt eine Geschichte der christlicher Mission, die der Diskussion über deren Zusammenhang mit Kolonialismus eine sachliche Basis gibt. Neue Missionen werden aber nicht einbezogen. Mehr

„Wie Crocodile Dundee“

Australier wehrt Krokodil mit Gürtelmesser ab

In Queensland hat ein Salzwasserkrokodil einen Mann attackiert. Er hielt sich an einem Mangrovenzweig fest und verteidigte sich mit seinem Messer. Mehr

Kein Dreigestirn am 11.11.

Kölner Karnevalsprinz an Corona erkrankt

Beim diesjährigen Karnevalsauftakt am 11.11. in Köln wird es keine Auftritte des Dreigestirns geben. Der designierte Prinz Sven Oleff wurde trotz seiner Immunisierung positiv auf Corona getestet. Mehr

Ein Kriminalfall in 3 Akten

- Sofortmaßnahmen
- Vorfallmanagement
- Wiederaufbau

Image: (CC0) geralt / pixabay

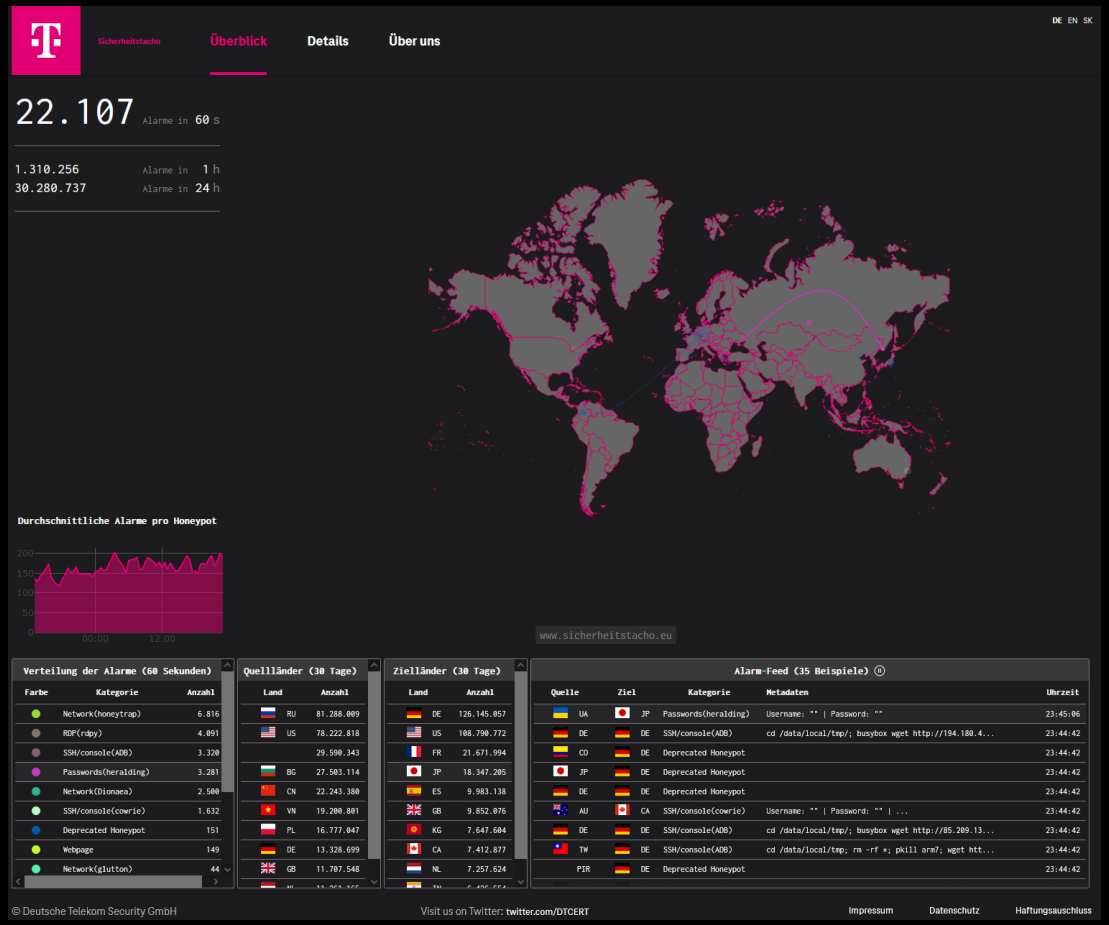
Eine Einordnung.

KISTERS

Cyberangriffe...

...sind leider Alltag.

Über 30 Millionen weltweite Angriffe tägl.
im Sicherheitstacho der Telekom.



https://www.sicherheitstacho.eu/start/main#/de/tacho

Der Business Case fliegt (Quelle: heise.de)

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

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

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

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

Ein Problem nicht nur für KISTERS

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".

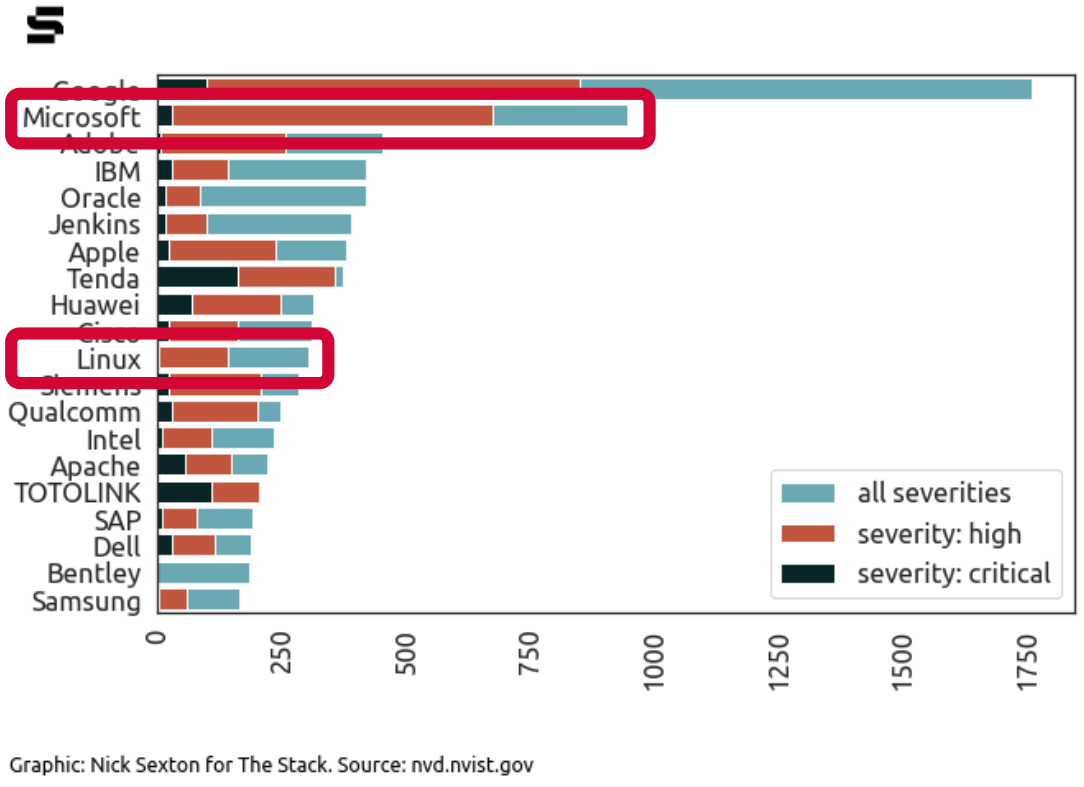
www.heise.de/ratgeber/Security-So-laufen-Ransomware-Angriffe-heute-ab-6457906.html?seite=all

- Eine Auswahl seitdem:

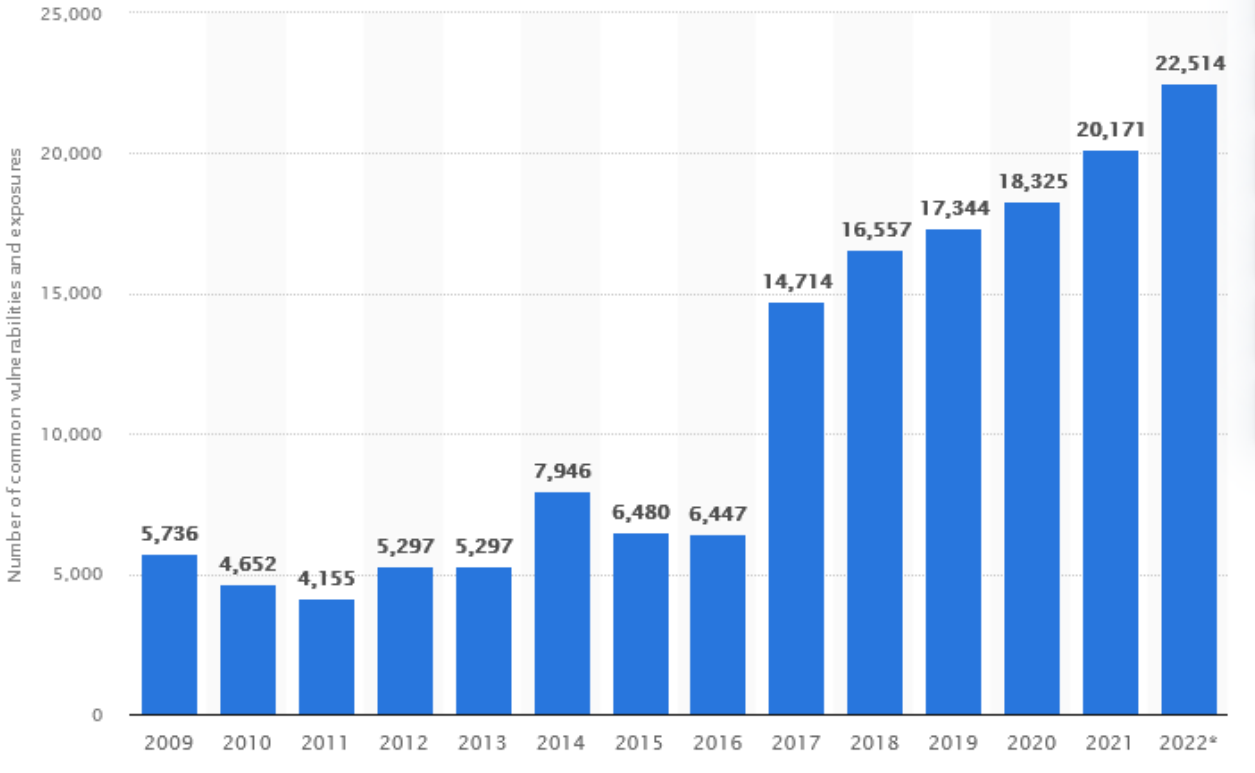
  (Quelle www.heise.de)

- 11.11.21 KISTERS (D)
- 09.02.22 vodafone, Portugal
- 17.02.22 red cross (CH)
- 28.02.22 Nvidia (US)
- 01.03.22 Satellite network KA-SAT (US)
- 12.04.22 Deutsche Windtechnik (D)
- 04.05.22 Sixt (car rental), Europe
- 12.06.22 Mainzer Stadtwerke (D)
- 12.06.22 entega Darmstadt (D)
- 12.10.22 WILKEN (D)
- 21.10.22 METRO (D)
- 26.10.22 enercity, Hannover (D)
- 31.12.22 SW & Stadt Potsdam (D)
- 12.01.23 British Royal Mail (UK)
- 17.01.23 Uni Duisburg-Essen (D)
- 20.01.23 T-Mobile (US)
- 23.01.23 Sky, TV
- 03.02.23 Universität Zürich (CH)
- 22.02.23 Energie Pool (CH)
- 10.03.23 Acronis (US)
- 14.03.23 Amazon Ring (US)
- 17.04.23 NCR (US)
- 24.02.23 NZZ (CH)
- 30.05.23 ABB (CH)
- 14.06.23 xplain (CH)
- 23.08.23 CloudNordic (DK)
- 01.11.23 Uni Hannover (D)
- 29.10.23 Boeing (US)
- 30.10.23 Südwestfalen-IT (D)
- 11.11.23 ICBC (China / US)
- 23.11.23 Cloudflare (US)
- 13.02.24 Varta (D)
- 15.02.24 PSI (D)
- 20.02.24 Schneider Electric(D)
- 23.02.24 Thyssenkrupp(D)
- 23.02.24 Wetzikon (CH)
- 26.03.24 NHS Scotland (UK)

Die Angriffsfläche wächst: vulnerabilities and exposures (CVEs) worldwide



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



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

KISTERS

Resilienz & Prävention.

KISTERS

Maßnahmen auf mehreren Ebenen

1. Organisatorische Maßnahmen

Image: (CC0) geralt / pixabay

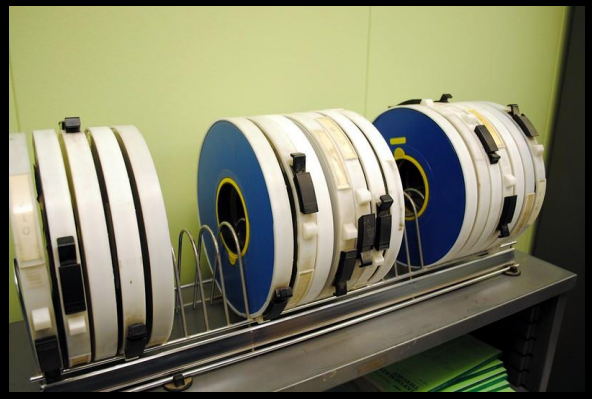


Image: (CC BY-SA 2.0) Andrew Adams / flickr

Maßnahmen auf mehreren Ebenen

1. Organisatorische Maßnahmen

2. Schutz der eigenen Systeme

Image: (CC0) geralt / pixabay

Netzwerkstruktur und Softwarebetrieb

- Schnelle Sicherheitspatches:
  Nutzung von Software in der jeweiligen Herstellercloud

Image: (CC0) Squid7085 / Wikimedia Commons

- Starke Zugriffsbeschränkungen:
  2FA, feingranulares Berechtigungssystem

- Starker Netzwerkschutz zur Erschwerung von „lateral movement“:
  Firewallregeln und Netzwerksegmentierung

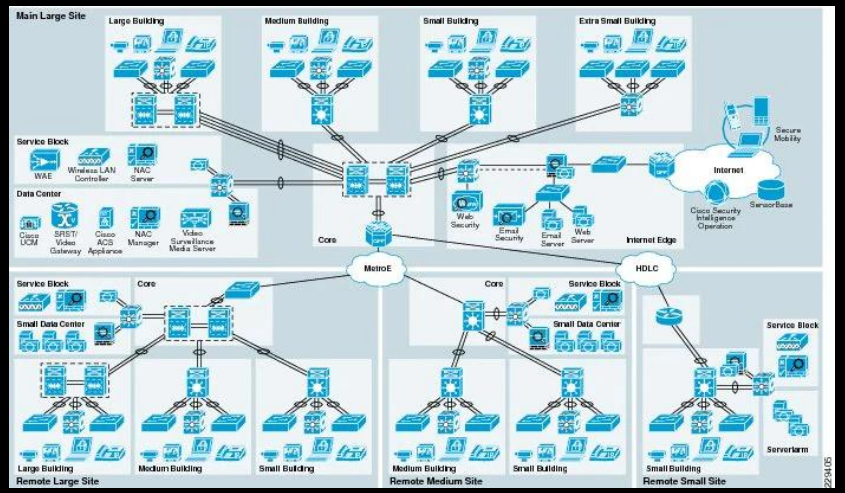
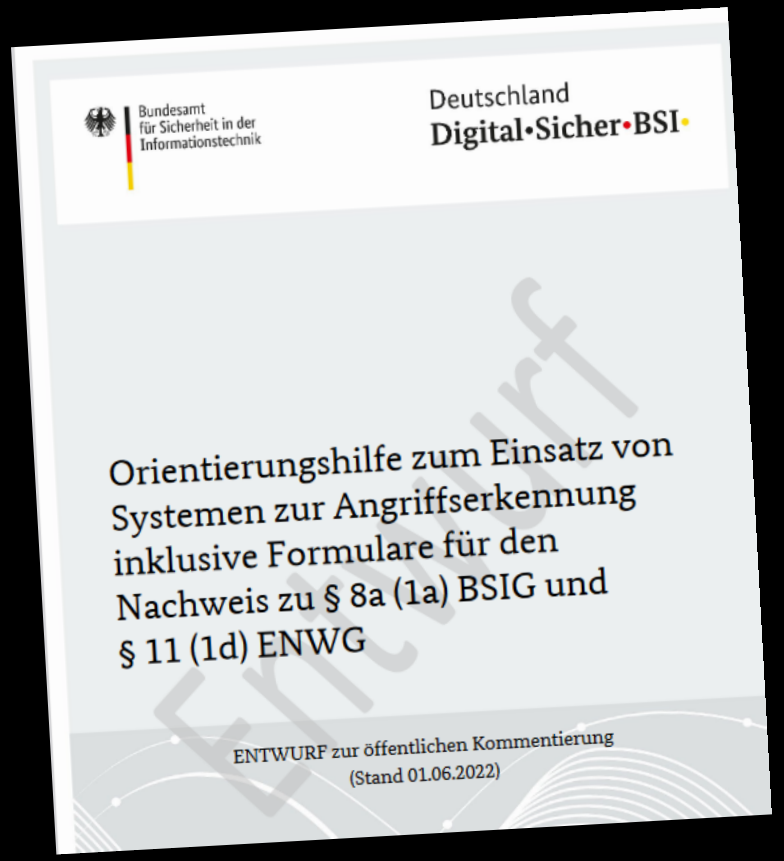


Image: (©) Cisco

Systeme zur Angriffserkennung

- MUSS-Kriterien lt. BSI

Thema	Anforderung
Rahmenbedingungen	Notwendige Technologie, Organisation und Personal müssen vorhanden sein.
Angriffsmuster	Informationen zu Schwachstellen eingesetzter Systeme und zu Angriffen müssen eingeholt werden.
Plattform	Die zur Angriffserkennung notwendige Hardware und Software muss auf dem aktuellen Stand sein.
Signaturen	Die Signaturen zur Detektion müssen aktuell gehalten werden.
Konfiguration	Systeme müssen so konfiguriert werden, dass bekannte Möglichkeiten der Schwachstellenerkennung genutzt werden.



Maßnahmen auf mehreren Ebenen

1. Organisatorische Maßnahmen

2. Schutz der eigenen Systeme

3. Schutz der Kundensysteme

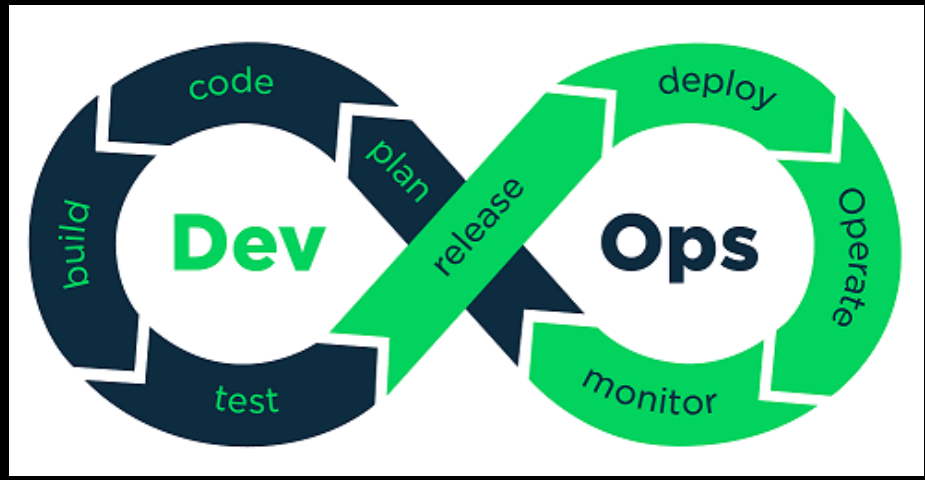
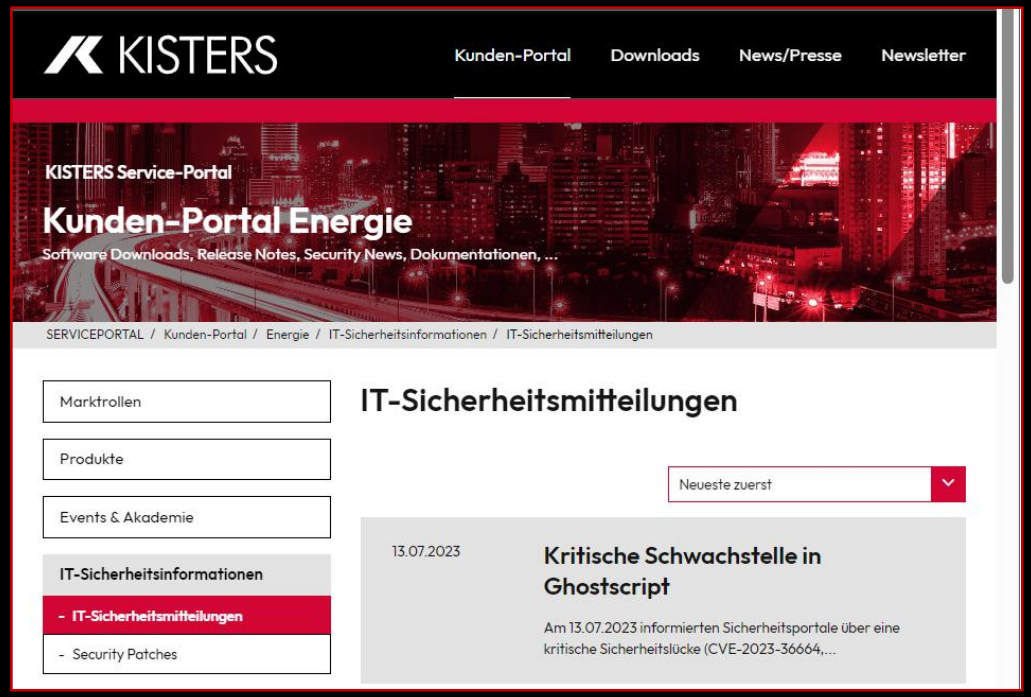
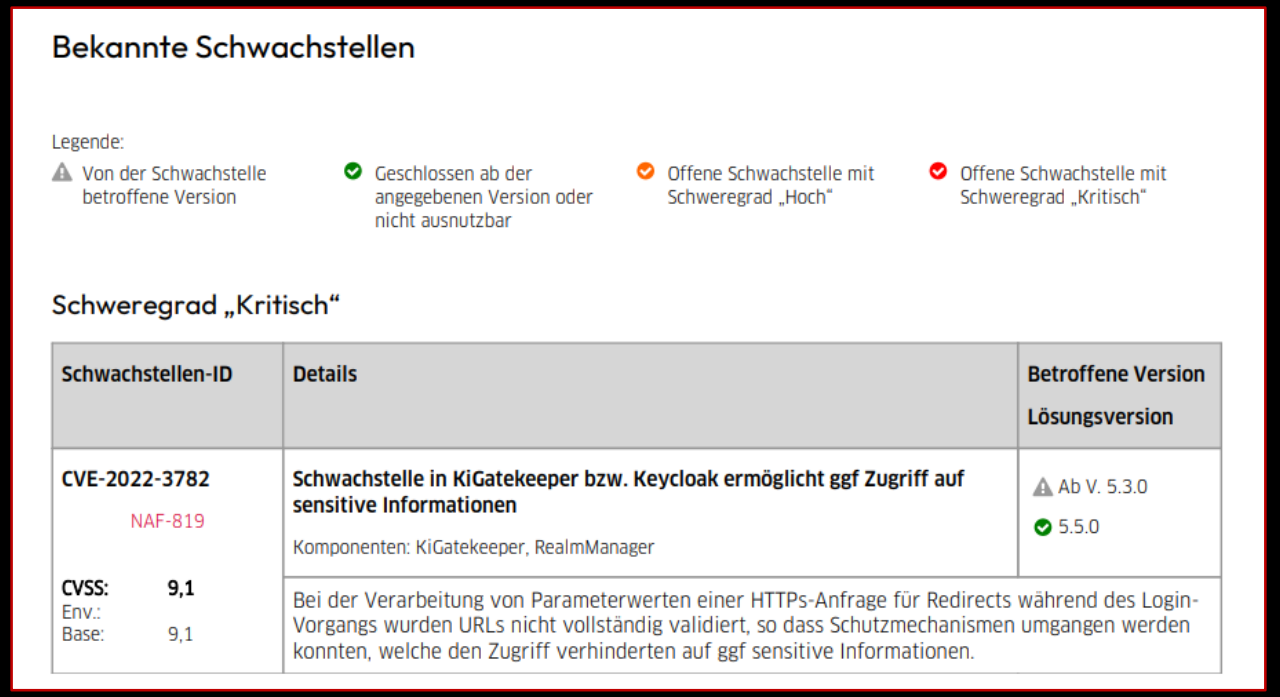


Image: (©) GitLab

CVE-Bewertung und Behebung

- Geschwindigkeit im gesamten Prozess ist gefragt!
- Bei der Bewertung, bei der Behebung und bei Bereitstellung und Installation
- Der Entwicklungsprozess muss entsprechend ausgerichtet werden





Bekannte Schwachstellen

Legende:

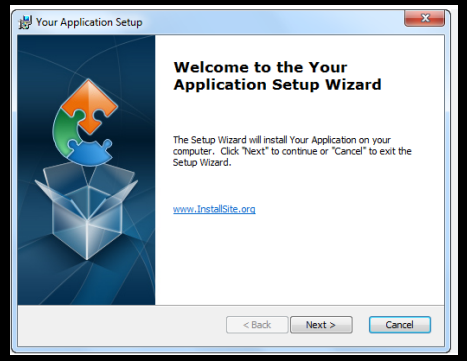
- ⚠ Von der Schwachstelle betroffene Version
- ✔ Geschlossen ab der angegebenen Version oder nicht ausnutzbar
- Offene Schwachstelle mit Schweregrad „Hoch“
- Offene Schwachstelle mit Schweregrad „Kritisch“

Schweregrad „Kritisch“

Schwachstellen-ID	Details	Betroffene Version Lösungsversion
CVE-2022-3782 NAF-819 **CVSS:** **9,1** Env.: Base: 9,1	**Schwachstelle in KiGatekeeper bzw. Keycloak ermöglicht ggf Zugriff auf sensitive Informationen** Komponenten: KiGatekeeper, RealmManager Bei der Verarbeitung von Parameterwerten einer HTTPs-Anfrage für Redirects während des Login-Vorgangs wurden URLs nicht vollständig validiert, so dass Schutzmechanismen umgangen werden konnten, welche den Zugriff verhinderten auf ggf sensitive Informationen.	⚠ Ab V. 5.3.0 ✔ 5.5.0

Container-Deployment und Cloud-first-Strategie

msi / installer



Containertechnologien

Container (single node)

docker

Container (multi node)

kubernetes

OPENSHIFT

RKE

Azure Kubernetes Service (AKS)

Vor 2022 — 2025 ff

„Es ist nicht die Frage, OB sondern WANN.“

KISTERS

Thank you

Dr. Markus Probst
Leiter Geschäftsbereich Energie

KISTERS