Hessisches Ministerium des Innern und für Sport

CYBER COMPETENCE CENTER HESSEN

Leistungsangebote des Hessen3C für Landkreise und Kommunen

CYBER COMPETENCE CENTER HESSEN

Vorstellung

Jörg Gaffga

Hessisches Ministerium des Innern und für Sport

Referat VII 12 - Hessen CyberCompetenceCenter (Hessen3C)

joerg.gaffga@hmdis.hessen.de

CYBER COMPETENCE CENTER HESSEN

Hessen3C

- Hessen CyberCompetenceCenter
  - Hessisches Ministerium des Innern und für Sport
  - Abteilung VII Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung
  - Referat VII 12
  - April 2019 gegründet
  - 49 Mitarbeiterinnen und Mitarbeiter
  - Hessen3C betreibt keine Strafverfolgung – alleinige Kompetenz Polizei & StA!
  - Enge Zusammenarbeit mit der hessischen Polizei, dem LfV und HLKA
  - Einbindung in nationale Organisationen (NCAZ)

CYBER COMPETENCE CENTER HESSEN

Hessen3C - Aufgabe

- Die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren sowie die Effizienz der Bekämpfung der Cyberkriminalität zu steigern

- Kernbereiche des Hessen3C sind die drei Säulen
  - Cybersecurity
  - Cybercrime
  - Cyberintelligence

- Beratung und Unterstützung von Landesverwaltung, Kommunen, KMU und KRITIS

CYBER COMPETENCE CENTER HESSEN

Herausforderung Cybersicherheit

- Digitalisierung ganzer Lebensbereiche schreitet munter voran
- Auch und gerade in der Verwaltung (OZG / digitale Vorgangsbearbeitung)
- Anfälligkeit für Hackerangriffe wird damit auch immer größer
- Bedeutung Cybersicherheit steigt damit
- Cybersicherheit ist die etwas verschämte Zwillingsschwester der Digitalisierung
- Bitterfeld (Sachsen-Anhalt) und Geisenheim (Rheingau-Taunus-Kreis)
- Kommunale Cybersicherheit gehört zur kommunalen Selbstverwaltung
- Land kann nichts vorschreiben
- Land kann aber unterstützen
- Finanzielle und organisatorische Herausforderung gerade für kleine und mittlere Kommunen

CYBER COMPETENCE CENTER HESSEN

Bund und Länder teilen sich die meisten Zuständigkeiten

EXTERNER LINK

OZG-Informationsplattform

Details zur Themenfeldarbeit

Eine besondere Herausforderung bei der Umsetzung des OZG liegt in den geteilten Zuständigkeiten von Bund und Ländern. Von den 575 OZG-Leistungen fallen derzeit 115 in die alleinige Verantwortung des Bundes. Die Digitalisierung dieser sogenannten Typ 1-Leistungen übernehmen die zuständigen Bundesressorts.

Anders ist es bei den föderalen Leistungen: 370 Leistungen sind zwar durch den Bund gesetzlich geregelt, werden aber von den Ländern vollzogen. Dabei handelt es sich um sogenannte Typ 2/3-Leistungen. Weitere 90 Leistungen vollziehen die Kommunen als Typ 4/5-Leistungen. Die Digitalisierung dieser Leistungen teilen sich die Länder auf.

Eine Übersicht über die Zuständigkeiten bei Bund, Ländern und Kommunen

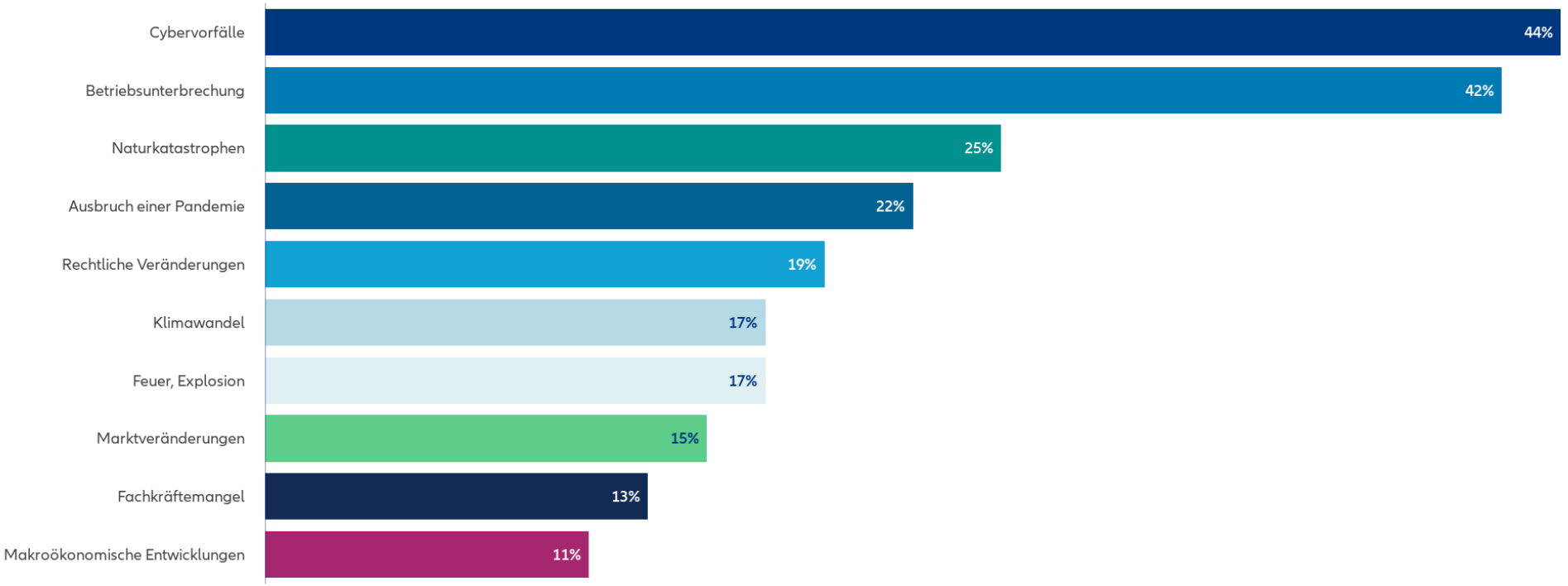
Quelle: https://www.onlinezugangsgesetz.de

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

CYBER COMPETENCE CENTER HESSEN

Herausforderung Cybersicherheit

- Digitalisierung ganzer Lebensbereiche schreitet munter voran
- Auch und gerade in der Verwaltung (OZG / digitale Vorgangsbearbeitung)
- Anfälligkeit für Hackerangriffe wird damit auch immer größer
- Bedeutung Cybersicherheit steigt damit
- Cybersicherheit ist die etwas verschämte Zwillingsschwester der Digitalisierung
- Landkreis Anhalt-Bitterfeld (Sachsen-Anhalt) und Stadtverwaltung Geisenheim (Rheingau-Taunus-Kreis)
- Kommunale Cybersicherheit gehört zur kommunalen Selbstverwaltung
- Land kann nichts vorschreiben
- Land kann aber unterstützen
- Finanzielle und organisatorische Herausforderung gerade für kleine und mittlere Kommunen

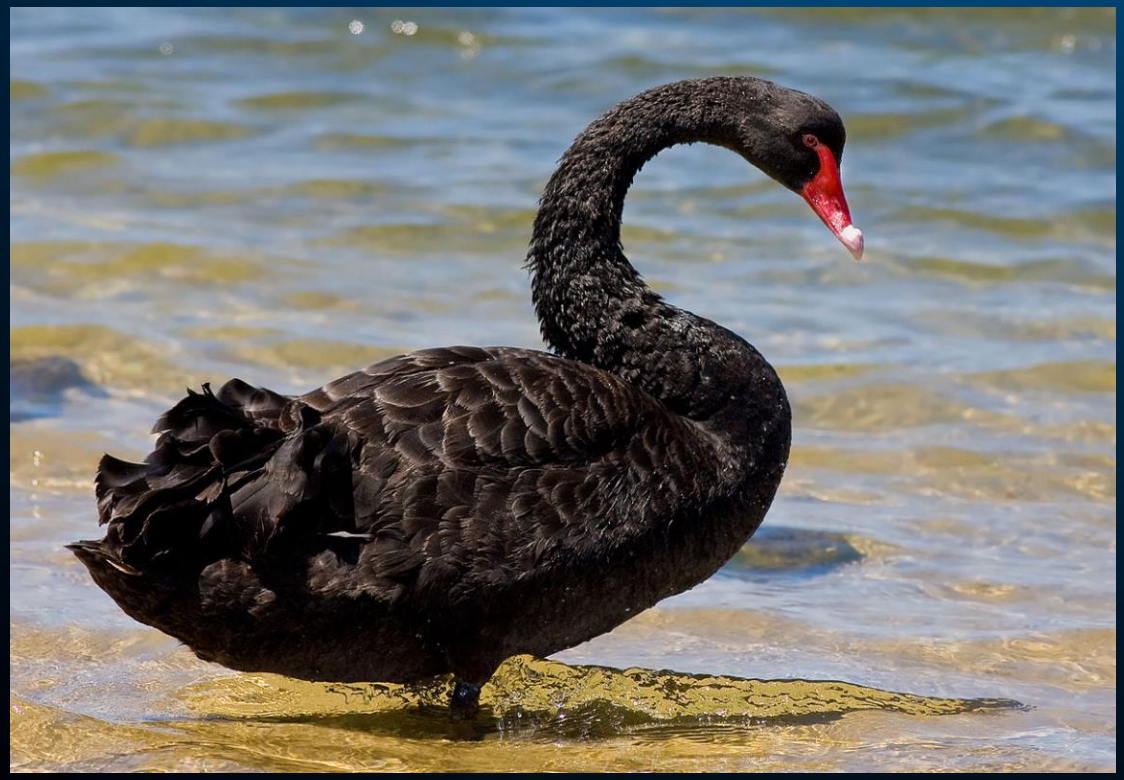
CYBER COMPETENCE CENTER HESSEN

Hessen3C & Kommunen

- Kommunales Dienstleistungszentrum Cybersicherheit KDLZ-CS
  - Beratungsangebot für Kommunen i.S. IT-Infrastruktur
  - Partnerschaft Hessen3C mit ekom21
  - Analyse der bestehenden Infrastruktur vor Ort
  - Dienstleistungs-Pakete je nach Gemeindegröße
  - Kostenfrei für die Kommunen
  - Start im Jahr 2016
  - Insgesamt 340 Kommunen sind vorstellig geworden
  - 1.005 Beratungstermine durchgeführt
  - Daraus resultierten 294 fortgeschrittenen Maßnahmen

CYBER COMPETENCE CENTER HESSEN

Nassim Nicholas Taleb → „schwarze Schwäne“



Quelle: https://de.wikipedia.org/wiki/Black_Swan_(Risiken)

CYBER COMPETENCE CENTER HESSEN

Neues Angebot: HECAAZ L/K

- **H**essisches **C**yber**A**bwehr**A**usbildungs**Z**entrum **L**and/**K**ommunen
  - Gemeinsames Projekt von Hessen3C mit ekom21
  - Unterstützt von den Kommunalen Spitzenverbänden
  - Angebot für alle 443 Städte, Gemeinden und Landkreise
  - Schulungsangebot, das die Bediensteten im Bereich Cyber- und IT-Sicherheit schulen und befähigen soll
  - Stufe 1: Durchführung von möglichst ortsnahen mobilen IT-Schulungslabors
    - Ortsnah = In jedem Landkreis für die jeweils kreisangehörigen Städte & Gemeinden
  - Stufe 2: Verstetigung des Aus- und Fortbildungsangebots an der Hessischen Hochschule für öffentliches Management und Sicherheit (HöMS) unter dem Themenfeld „Cybersicherheit für Kommunen“
    - Neuer Angebotszweig, der von der HöMS aufgebaut wird

CYBER COMPETENCE CENTER HESSEN

Format Schulungen

- Kostenfrei für die Kommunen
- Kosten werden vollständig vom Land getragen
- Veranstaltungsdauer: 3 Tage
- Thema: Betriebliches Kontinuitätsmanagement (Business Continuity Management BCM)
  - Inhalte zum Notfall- und Krisenmanagement sowie zur Notfallvorsorge werden behandelt und erarbeitet

- Tagesworkshops zu spezifischen Fachthemen sind in Planung

CYBER COMPETENCE CENTER HESSEN

Qualität Schulungen

- Schulungen erfolgen durch BCM-zertifizierte Trainer der ekom21
- Schulungen erfolgen sehr praxisbezogen und in Gruppenarbeit
- Kein Frontalunterricht!
- 8 bis 12 Teilnehmerinnen oder Teilnehmer pro Veranstaltung
- Zielgruppe der Schulungen sind Bedienstete aus den Bereichen Verwaltungsleitung / Organisation / IT-Betrieb
- BCM ist in der Hauptsache eine Aufgabe Organisation
- Planung geht von i.d.R. 2 Bediensteten pro Kommune und Schulung aus
- Die technische und operative Durchführung der Veranstaltungen obliegt der ekom21
- Gegebenenfalls notwendiges technisches Equipment wird durch die ekom21 erbracht
  - (Vorabstimmung zwischen ekom21 und Landkreisbeauftragten notwendig).

CYBER COMPETENCE CENTER HESSEN

Schulungstermine / Zeitplan

- 68 Schulungstermine für das Jahr 2022
- Weitere Schulungstermine wird es für das 1. HJ 2023 geben
- Planungen HECAAZ L/K gehen von mindestens 90 Schulungsveranstaltungen aus
- Konkrete Terminplanung erfolg durch die ekom21 in Abstimmung mit dem Ansprechpartner/Koordinator des Landkreises
  - Bündelung der Kommunikation
- Start HECAAZ erfolgt am 23. Mai 2022

CYBER COMPETENCE CENTER HESSEN

Leistungen Landkreise

- Es wird gebeten, seitens der Landkreise einen Ansprechpartner zu benennen
- Aufgabe / Funktion: Abstimmung mit der ekom21
  - Koordination der Kommunen im jeweiligen Landkreis
- Meldung Ansprechpartner bitte an ekom21 und Hessen3C

- Wünschenswert: Unterstützung in Form von mietfreien Räumlichkeiten

CYBER COMPETENCE CENTER HESSEN

Unsere weiteren Angebote für Sie …

CYBER COMPETENCE CENTER HESSEN

Hessen Leak Checker

- Hiermit werden dienstliche E-Mail-Adressen ausfindig gemacht, die entgegen dem Willen des Betroffenen in Datenlecks veröffentlicht wurden
- Stehen diese in Verbindung mit anderen Daten und Passwörtern, ergibt sich hieraus eine potentielle Gefährdung der Informationssicherheit

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Warn- und Informationsdienst

- Aktuelle Informationen zur Sicherheitslage, bekannt gewordene Sicherheitslücken und Phishing-Kampagnen!
- Werktäglicher Schwachstellenbericht!
- Kostenlos!
- TLP-Verpflichtung ist Voraussetzung!

CYBER COMPETENCE CENTER HESSEN

https://mip.bsi.bund.de/Anlage_1_TLP-Merkblatt.pdf

Die TLP-Stufen

TLP:WHITE Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

TLP:GREEN Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

TLP:AMBER Eingeschränkte interne und organisationsübergreifende Weitergabe

Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis *Kenntnis nur, wenn nötig* weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen.

Hierfür muss er sicherstellen, dass die Dritten das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:RED Persönlich, nur für bekannte Empfänger

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Beratung und Prävention

Durchführung von Vortragstätigkeiten / Awareness-Veranstaltungen in Sachen IT-Sicherheit!

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Beratung und Prävention

Durchführung von Vortragstätigkeiten / Awareness-Veranstaltungen in Sachen IT-Sicherheit!

Schwerpunktthemen:

- Ausspähen von Daten/Identitätsdiebstahl/Datendiebstahl
- Preisgabe persönlicher Daten
- Phishing/Ransomware etc.
- Aktuelle Betrugsphänomene

Hessisches Ministerium des Innern und für Sport

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Notfall Hotline

Jederzeit erreichbar!

0611 / 353 – 9900

24/7 Erreichbarkeit

cert@hessen3c.hessen.de

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

- Beratung zum IT-Krisenmanagement
  - Organisation und Abläufe im Krisenstab
  - Innere und äußere Kommunikation

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

- Beratung in der Analyse / Forensik
  - Breite Erfahrung / nicht öffentliche Informationen
  - IT-forensische Sicherungen nach polizeilichen Standards
  - Zugang zu BSI und anderen Sicherheitsbehörden

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

- Beratung zur Wiederherstellung
  - best practises, **aber …**

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

- Beratung zur Wiederherstellung
- **Aber …** Hessen3C kann nicht:
  - Eigene Vorbereitung ersetzen
  - Eigene Spezialisten oder Dienstleister ersetzen

CYBER COMPETENCE CENTER HESSEN

Hessen3C – Incident Response / MIRT

Bei schweren IT-Sicherheitsvorfällen unterstützt das Hessen3C im Incident Response

- Bei Bedarf erfolgt die Unterstützung durch unser **MIRT** (mobile incident response team) vor Ort

CYBER COMPETENCE CENTER HESSEN

Vielen Dank für Ihre Aufmerksamkeit!

CYBER COMPETENCE CENTER HESSEN

? ? ? ? ? ?

Fragen