CYBER COMPETENCE CENTER HESSEN

Cybersicherheit – Lebensversicherung BCM

9. Kommunaler IT-Sicherheitskongress

Forum Factory Berlin, 24. April 2023

CYBER COMPETENCE CENTER HESSEN

Agenda

- Vorstellung Hessen3C
- Cyberbedrohung / Cyberlage
- Herausforderung Cybersicherheit
- Lebensversicherung BCM
- Tipps für präventives Handeln

Hessen3C

- Hessen CyberCompetenceCenter
  - April 2019 gegründet
  - Hessisches Ministerium des Innern und für Sport
  - Abteilung VII Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung
  - 49 Mitarbeiterinnen und Mitarbeiter

Hessen3C - Aufgabe

- Die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren sowie die Effizienz der Bekämpfung der Cyberkriminalität zu steigern
- Enge Zusammenarbeit mit der hessischen Polizei, dem LfV und HLKA
- Einbindung in nationale Organisationen (**N**ationales **C**yber **A**bwehr **Z**entrum NCAZ)
- Hessen3C betreibt Cyberresilienz - keine Strafverfolgung – alleinige Kompetenz Polizei & StA!
- Kernbereiche des Hessen3C sind die drei Säulen
  - Cybersecurity (Resilienz)
  - Cybercrime (Forensik)
  - Cyberintelligence
- Beratung und Unterstützung von Landesverwaltung, Kommunen und KMU

CYBER COMPETENCE CENTER HESSEN

Hessen3C

CYBER COMPETENCE CENTER HESSEN

Cyberbedrohungslage

- Aktuelle Lage wird von zwei Hauptfaktoren bestimmt:
  - Angriffskrieg Russland gegen die Ukraine
  - Organisierte Kriminalität
- Cyberbedrohungslage ist insgesamt sehr angespannt

CYBER COMPETENCE CENTER HESSEN

Cyberbedrohung für Kommunen

- Es kann jede Gemeinde, Stadt oder Landkreis zu jeder Zeit Opfer werden
- Keine Frage der Größe oder Bedeutung

CYBER COMPETENCE CENTER HESSEN

Herausforderung Cybersicherheit

- Anfälligkeit für Hackerangriffe nimmt zu („Ein Klick zuviel“)
- Bedeutung Cybersicherheit gewinnt erheblich an Gewicht
- Auf den Worst Case vorbereitet sein!

CYBER COMPETENCE CENTER HESSEN

Worst Case

instructions_read_me - Notepad

File Edit Format View Help

```
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://basta[redacted].onion/


Login ID: [redacted]


*!* To access .onion websites download and install Tor Browser at:

   https://www.torproject.org/ (Tor Browser is not related to us)

*!* To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.
```

CYBER COMPETENCE CENTER HESSEN

Lebensversicherung BCM

- Erstellen Sie ein BCMS (Business Continutiy Management System)
- Notfallkonzept, wie sie im Falle eines Totalausfalls der IT ihren Geschäftsbetrieb und ihre Verwaltung fortführen können
- Richten Sie ihre Organisation darauf aus!

CYBER COMPETENCE CENTER HESSEN

Lebensversicherung BCM

- **BCMS hat zwei zentrale Bausteine**
  - Betriebliches Fortführungskonzept
  - IT-Notfallmanagement

CYBER COMPETENCE CENTER HESSEN

Lebensversicherung BCM

- Empfehlung: BCMS gemäß Standard BSI 200-4

- Ein Notfallmanagementsystem nach BSI 200-4 durchläuft in einem PDCA*-Modell die Phasen
  - Planung und Konzeption zur Notfallvorsorge (Plan)
  - Erstellung eines Notfallhandbuchs zur Notfallbewältigung (Do)
  - Planung und Durchführung von Übungen und Tests (Check)
  - Permanente Aufrechterhaltung und Weiterentwicklung (Act)

  - *Plan-do-Check-Act

CYBER COMPETENCE CENTER HESSEN

Lebensversicherung BCM

- BCM ist in der Verantwortung der Verwaltungsspitze

CYBER COMPETENCE CENTER HESSEN

Lebensversicherung BCM

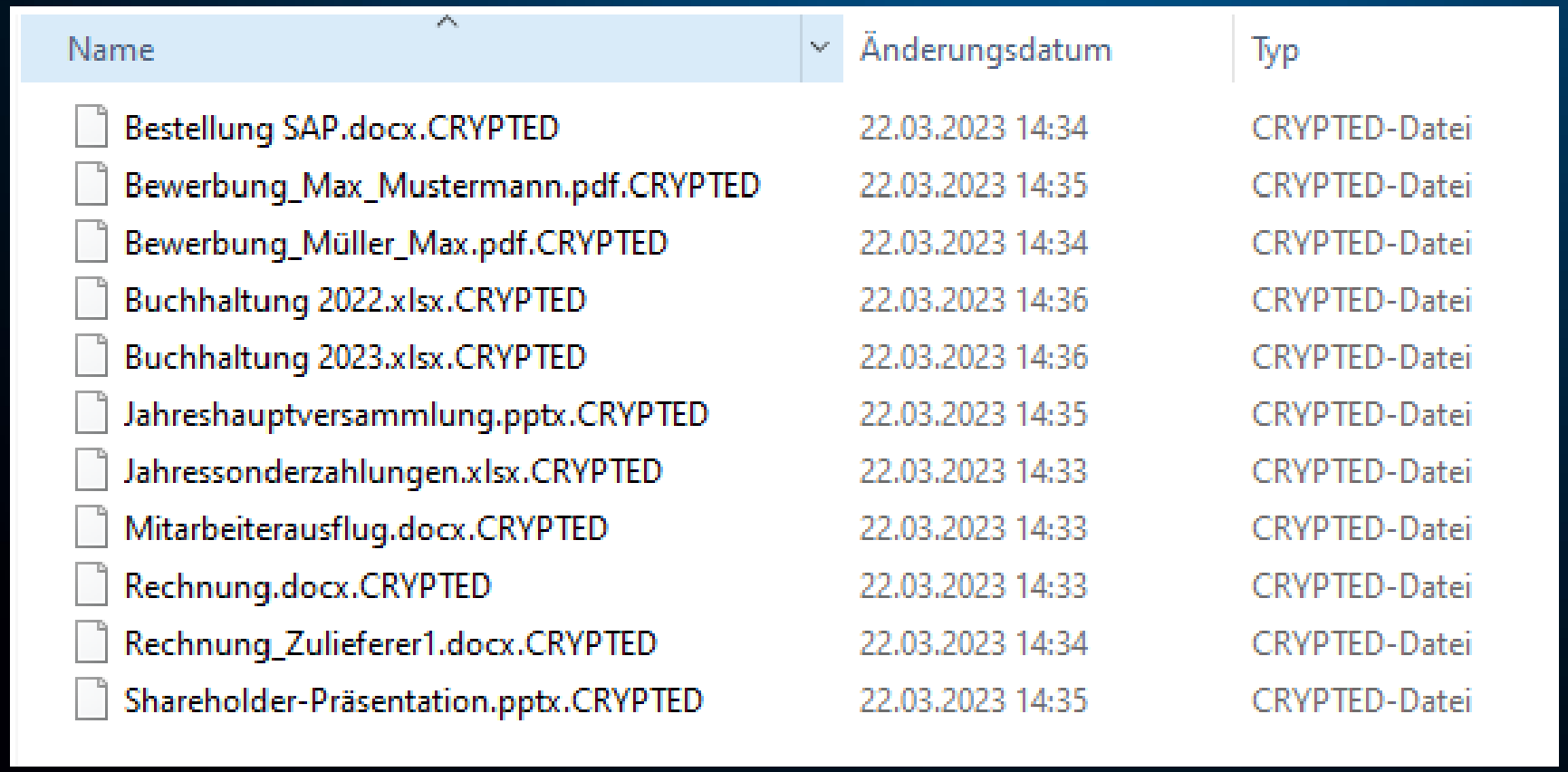
- Erstellung und Implementierung eines BCMS ist Aufgabe der Abteilung Organisation
- Erstellung und Implementierung BCM ist **keine** Aufgabe der IT!
- IT hat – wie alle Bereiche – gleichwohl wichtige Aufgaben i.R. eines BCM

CYBER COMPETENCE CENTER HESSEN

IT-Notfallpan

- Die IT-Abteilung muss sich auch auf Worst Case vorbereiten!
- Kritische Prozesse identifizieren und festlegen
- Wiederherstellung der Prozesse priorisieren

CYBER COMPETENCE CENTER HESSEN



Name	Änderungsdatum	Typ
Bestellung SAP.docx.CRYPTED	22.03.2023 14:34	CRYPTED-Datei
Bewerbung_Max_Mustermann.pdf.CRYPTED	22.03.2023 14:35	CRYPTED-Datei
Bewerbung_Müller_Max.pdf.CRYPTED	22.03.2023 14:34	CRYPTED-Datei
Buchhaltung 2022.xlsx.CRYPTED	22.03.2023 14:36	CRYPTED-Datei
Buchhaltung 2023.xlsx.CRYPTED	22.03.2023 14:36	CRYPTED-Datei
Jahreshauptversammlung.pptx.CRYPTED	22.03.2023 14:35	CRYPTED-Datei
Jahressonderzahlungen.xlsx.CRYPTED	22.03.2023 14:33	CRYPTED-Datei
Mitarbeiterausflug.docx.CRYPTED	22.03.2023 14:33	CRYPTED-Datei
Rechnung.docx.CRYPTED	22.03.2023 14:33	CRYPTED-Datei
Rechnung_Zulieferer1.docx.CRYPTED	22.03.2023 14:34	CRYPTED-Datei
Shareholder-Präsentation.pptx.CRYPTED	22.03.2023 14:35	CRYPTED-Datei

CYBER COMPETENCE CENTER HESSEN

Präventiv im Tagesgeschäft handeln

- Cybersicherheit bedeutet sich über Gefahren bewusst sein und stringente Resilienz zu betreiben
- Es kann jede Gemeinde, Stadt oder Landkreis zu jeder Zeit Opfer werden
- IT-Infrastruktur anhand aktueller Erkenntnisse bzw. Erfordernisse auf Schwachstellen prüfen

CYBER COMPETENCE CENTER HESSEN

Tipps

- Software und Schutzsysteme auf aktuellstem Stand halten
  - bereitstehende Softwareaktualisierungen (Updates) zum Abdichten bekannter Sicherheitslücken umgehend installieren!
- Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter
  - MA über Gefahren aufklären und richtiges Verhalten schulen
  - Schulungen regelmäßig wiederholen (Fortbildung verpflichtend)
- „Starke“ Passwörter verbindlich vorsehen
  - Variante 1 (technische Lösung): „Zwei-Faktor-Authentifizierung“
  - Variante 2: Komplexe Passwörter (Groß-/Kleinschreibung, Sonderzeichen, Zahlen)

Tipps

- IT-Systeme technisch aufrüsten, wo immer geboten
  - Ständige Aufgabe
  - IT-Systeme regelmäßig professionell auf Schwachstellen scannen lassen!
  - Nicht am falschen Punkt sparen!
- IT-Systeme intelligent strukturieren und schützen
  - Trennung von Systemen wo immer geboten
  - Grundsatz Netzwerk-Architektur: Zero trust!
  - Zwei-Faktor-Authentifizierung
- Lebensversicherung Backup
  - Kein Backup = kein Mitleid
  - Backup richtig machen
  - Backup-System besonders schützen

CYBER COMPETENCE CENTER HESSEN

Tipps

- Warnschüsse ernst nehmen und proaktiv reagieren!
  - Erfolglose Hackerangriffe professionell forensisch analysieren
  - Ergebnisse und Empfehlungen technisch bzw. systemisch umsetzen

CYBER COMPETENCE CENTER HESSEN

Zusammenfassung

- Nehmen Sie sich aktiv des Themas Cybersicherheit an!
- Stärken Sie proaktiv und präventiv Ihre IT-/Netzresilienz!
- Schulen Sie regelmäßig Ihre Mitarbeiterinnen und Mitarbeiter!
- Bereiten Sie sich auf den Worst Case vor!

CYBER COMPETENCE CENTER HESSEN

Fragen / Diskussion

CYBER COMPETENCE CENTER HESSEN

Danke für die Aufmerksamkeit !