Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Erfahrungen aus Ransomware-Angriffen

Stefanie Euler, Informationssicherheitsberatung für Länder und Kommunen
Maike Vossen, CERT-Bund, Grundsatz und Warn- und Informationsdienst (WID)
17/23/24.02.2022, Digital.Kommunal.Sicher – Informationssicherheit in der Kommunalverwaltung

Ransomware – Schlagzeilen aus Deutschland 2021

Software AG Opfer von Clop-Ransomware Attacke

KASEYA

Was über Ransomware-Betroffene in Deutschland bekannt ist

Ein großer Ransomware-Angriff hat Hunderte Unternehmen weltweit getroffen. Auch deutsche Firmen sind darunter, manche hatten aber offenbar Glück.

NACH CYBERANGRIFF AUF ANHALT-BITTERFELD

Spekulationen um Name der Hackergruppe - „Pay or Grief“ soll hinter Lösegeldforderung stecken

Cyberangriff: Stadtverwaltung Witten online nicht erreichbar

Ransomware legt Verwaltung von Schwerin und benachbartem Landkreis lahm

Autozulieferer aus Esslingen

Eberspächer meldet Cyberangriff

Ransomware-Attacke auf Medatixx: Großalarm im Gesundheitswesen

Cyber attack on the KISTERS Group: Expiry of the ultimatum and publication of captured data

Verschlüsselungstrojaner

MediaMarkt und Saturn offenbar von Ransomware betroffen

After ransomware attack, global logistics firm Hellmann warns of scam calls and mail

Digital healthcare: ransomware attack on Compugroup Medical

Cyber-Angriffe auf deutsche Verwaltung - Beispiele

Trojaner-Angriff im Burgdorfer Rathaus – LKA ermittelt

Computersystem des Kammergerichts offline

Trojaner-Befall: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm

Die Schadsoftware Emotet hat das Netzwerk der Stadtverwaltung Neustadt am Rübenberge gekapert. Bis mindestens Freitag bleiben die Bildschirme schwarz.

Zahlreiche Fälle von digitaler Erpressung in deutschen Behörden

In über 100 Fällen ist es Tätern gelungen, IT-Systeme von Behörden und öffentlichen Einrichtungen zu verschlüsseln.

LANDKREIS GÜNZBURG

Ransomware legt Verwaltung von Schwerin und benachbartem Landkreis lahm

20. Dezember 2019, 16:09 Uhr Kommunen - Frankfurt am Main

Aufräumen nach Trojaner-Attacke: Bad Homburg offline

Cyberkriminelle attackieren die Gemeindeverwaltung Kammeltal

Cyberangriff: Stadtverwaltung Witten online nicht erreichbar

NACH CYBERANGRIFF AUF ANHALT-BITTERFELD

Spekulationen um Name der Hackergruppe - „Pay or Grief“ soll hinter Lösegeldforderung stecken

Ransomware-Angriff auf

Landkreis Anhalt-Bitterfeld

- Erste Medienberichte am 05.07.2021
- „Wir sind nicht in der Lage, Dienstleistungen anzubieten.“
- Ausruf Katastrophenfall am 09.07.2021, Unterstützung durch BSI und BW, LKA ermittelt
- „Pay0rGrief“ veröffentlicht personenbezogene Daten
- Notinfrastruktur ist am 19.07.2021 einsatzbereit
- Prioritäre DL und Zahlungsfähigkeit am 03.08.2021 wiederhergestellt
- Beendung des Katastrophenfalls am 31.01.2022 (!)

Was jetzt?

BCM

→ (Zeit-)Kritische Geschäftsprozesse, Backup-Konzepte, Wiederanlaufplanung

Krisenstab

→ Stabsarbeit zum Koordinieren der Entscheidungsprozesse / Priorisieren, Medien betreuen, Kunden benachrichtigen/weiterversorgen, Personalplanung (MA-Fürsorge, Einsatz von Helfern)

→ **Frühzeitig Verantwortung** für den eigenen IT-Sicherheitsvorfall **übernehmen!**

Kein Berater und kein Helfer können Ihnen die Verantwortung und Zuständigkeit, sowie die zentralen Entscheidungen abnehmen.

Frühzeitige Reaktion nicht verpassen

- IT-Sicherheitsvorfälle können schon sehr frühzeitig durch Betriebsanomalien auffallen
- Frühzeitig Daten für spätere Analyse sammeln
- Frühzeitig intern eskalieren
- IT-Sicherheitsexpertinnen hinzuziehen, ggf. weitere(n) Dienstleister hinzuziehen. Vorfallsreaktion und IT-Betrieb funktionieren unterschiedlich
- Bestehende Quellen nutzen (z.B. BSI-Dokumente: „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ und „APT-Dienstleisterliste“)
- Infrastruktur schaffen und nutzen (Material, Räume, abgetrennte Bereiche)
- Trennung zwischen Vermutungen und Fakten helfen bei der realistischen Lageeinschätzung

Kräfte einteilen

- Die Reaktion auf einen IT-Sicherheitsvorfall ist ein Marathon mit Sprinteinlagen
  - Achten Sie auf Ihr Personal, schützen Sie es auch vor sich selbst
  - „Führungsrhythmus“ etablieren (z.B. morgendliche Lagebesprechung), aktive Pausenzeiten bestimmen
  - Versorgung nicht vergessen! (Getränke, Mahlzeiten, Obst)

„Dieser Angriff stellt daher für uns
ein von außen kommendes
unabwendbares, unvorhersehbares und nicht beeinflussbares Ereignis dar.“

NEIN, tut er nicht!

(Basis-)Maßnahmen gegen Ransomware

Patches und Updates
Zeitnahe Aktualisierung der eingesetzten Software; unverzügliches Einspielen von Patches und Sicherheitsupdates; kein Einsatz von veralteten/nicht mehr unterstützten Produkten

Absicherung von externen Zugängen
2-Faktor Authentifizierung; starke Passwörter; Einsatz von VPN; Reduzierung der verfügbaren „Anschlusspunkte“

Ausführungsverhinderung / Whitelisting
Nur explizit freigegebene Programme dürfen vom Nutzer überhaupt gestartet werden; Einschränken von Makros

Strikte Rollen- und Rechtetrennung bei Administration
Verschiedene administrative Accounts für Clients und Server; keine Verwendung von privilegierten Accounts für das „Surfen im Internet“ oder andere; nicht-administrative Tätigkeiten

Backups
Regelmäßige Backups von geschäftskritischen Daten; außerhalb des Backup-Vorgangs sind diese physikalisch vom Netz getrennt; Wiedereinspielen der Backups wird regelmäßig getestet

BCM / Notfallplanung
Handbücher und Leitfäden für den „worst-case“ erstellt und geübt; alternative Kommunikationswege; Reaktion auf Presseanfragen; Wichtige Namen, Nummern und Kontakte offline und physikalisch (Papier) verfügbar

Fazit:

Ransomware-Abwehr hilft Ihrer gesamten IT-Sicherheit

- Es ist keine Frage des **OB**, sondern eine Frage des **WANN**!
- Sie wissen was passieren kann und Sie sind mitverantwortlich!
- Es gibt viel zu tun - Fangen Sie JETZT an!
- Was brauchen Sie denn noch? Die Fälle sind öffentlich, die Schäden bekannt …
- Jetzt investieren ist billiger, als wochenlang eingeschränkt zu sein und neu aufzubauen.
- Wenn Sie glauben, bereit alles getan haben – nicht drauf ausruhen, lieber regelmäßig checken und aktualisieren

BSI Good Practice Sammlung (Auszug)

Hintergrundinformationen Ransomware, Sensibilisierung

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_**Managementabstract-Angriffe**.html

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/**Themen/Ransomware**.pdf

BCM Vorbereitung, BIA-Prozesspriorisierung

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/**bsi-standard-200-4_Business_Continuity_Management**_node.html

Notfallmanagement, Krisenstabsarbeit:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/**Standard_200-4_Bewaeltigung**.pdf

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/**Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall**.pdf

Mitarbeiter-Hilfen (Spin-off aus Wahlsicherheit):

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/**Infos-fuer-Kandidierende**/Info-fuer-Kandidierende/kandidierende_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/**Leitfaden-Kandidierende**.html

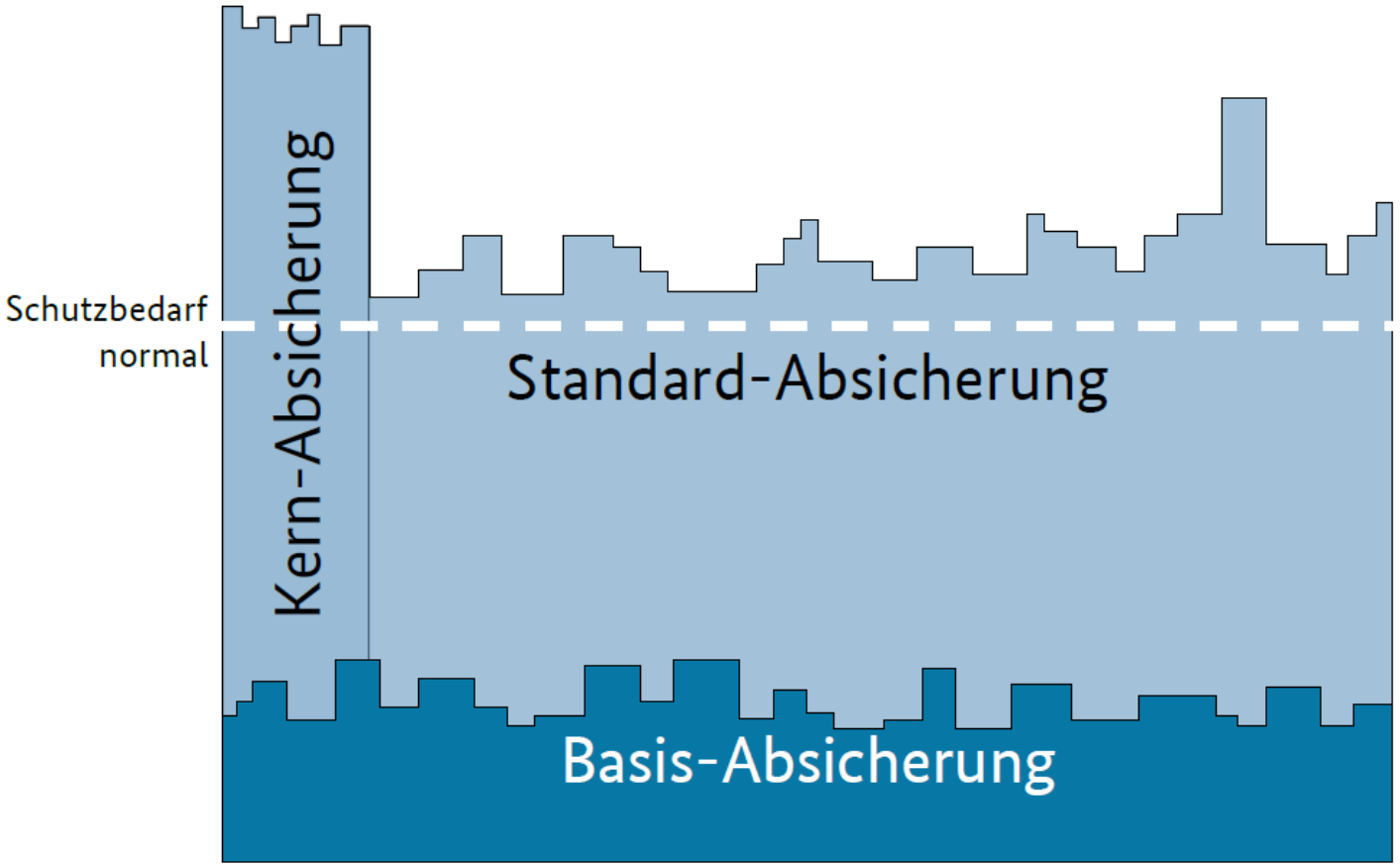
IT-Grundschutz

IT-Grundschutz verfolgt einen ganzheitlichen Ansatz.

Infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsanforderungen helfen, ein Standard-Sicherheitsniveau aufzubauen, um geschäftsrelevante Informationen zu schützen.

An vielen Stellen werden bereits höherwertige Sicherheitsanforderungen geliefert, die die Basis für sensiblere Bereiche sind.

BSI-Standard 200-2
Überblick Vorgehensweisen



IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“

Zielgruppe:

- Dieses IT-Grundschutz-Profil richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen

Zielsetzung:

- Das Profil erleichtert den Einstieg in die Informationssicherheit und hilft, die gröbsten Schwachstellen aufzudecken, welche zu beseitigen sind, um möglichst schnell das Sicherheitsniveau anzuheben

Informationssicherheitsberatung für Länder und Kommunen

Die Zielgruppe

BSIG - §3 Abs. 1,
Nr. 13a, Nr. 14 & Abs. 2

16 Bundesländer
10.800 Kommunen

Bedarfe und
Herausforderungen
kennenlernen

Chancen nutzen

Konzepte und Strategien

Kooperativ und
Komplementär

Beratung Länder

Individuelle und
zielgruppenspezifische
Beratungsprojekte

Informationssicherheits-
management,
Sicherheitskonzeption,
IT-Grundschutz

Beratungsprozess

BSI-Kostenverordnung

Gremien

AG Informationssicherheit
des IT-PLR

Kommission der IuK
Informationssicherheit

Beratung Kommunen

Multiplikatoren

Kommunale
Spitzenverbände

Sicherheits-Anforderungen
an Ebenen-übergreifende
Verfahren

Einstieg in die Basis-
Absicherung

IT-Grundschutz-Profile

Arbeitshilfen, Blaupausen

Praxis-Checks

Sicherheitsberatung-Regional@bsi.bund.de

BSI Good Practice Sammlung (Auszug)

Sicherheitsberatung für Länder und Kommunen

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitsberatung/Laender-und-Kommunen/laender-und-kommunen_node.html

Interner Bereich für Länder und Kommunen

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitsberatung/Laender-und-Kommunen/Infos_int_Bereich/infos_int_bereich_node.html

IT-Grundschutz-Standards

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

IT-Grundschutz-Kompendium

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf

IT-Grundschutz-Profile

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/Profile/itgrundschutzProfile_Profile_node.html

IT-Grundschutz Hilfsmittel

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Hilfsmittel_und_Anwenderbeitraege/Hilfsmittel_Anwenderbeitraege_node.html

Fragen?

Deutschland
Digital•Sicher•BSI•

Kontakt

Stefanie Euler
BL 12: Informationssicherheitsberatung für Länder und Kommunen
stefanie.euler@bsi.bund.de
Tel. +49 (0) 228 99 9582 5112

Maike Vossen
OC 21: CERT-Bund, Grundsatz und Warn- und Informationsdienst (WID)
maike.vossen@bsi.bund.de
Tel. +49 (0) 228 99 9582 4157

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
Twitter: **@BSI_Bund @certbund**

Bundesamt
für Sicherheit in der
Informationstechnik