IT-Notfallmanagement
die ersten 24 Stunden nach (und vor!) einer Kompromittierung

79. Betriebstagung DFN

TECHNISCHE UNIVERSITÄT DARMSTADT

Wer bin ich - Wo komme ich her

TECHNISCHE UNIVERSITÄT DARMSTADT

Dipl.-Inform. Jochen Becker

- Studium Diplom Informatik
- seit 2007 Mitarbeiter der TU Darmstadt im Hochschulrechenzentrum
- seit 2021 Leiter TUDa-CERT und stv. CISO der Stabsstelle Informationssicherheit des Präsidiums
- jochen.becker@tu-darmstadt.de
- @jb80evil:matrix.tu-darmstadt.de

Technische Universität Darmstadt (Stand 2022)

- gegründet 1877
- 325 Professorinnen und Professoren
- 2.706 wissenschaftliche Beschäftigte)
- 1.986 administrativ-technische Beschäftigte
- 132 Auszubildende
- 24.406 Studiendere in 120 Studiengängen
- an 5 Standorte mit 175 Gebäude
- 14 SFB/Transregios, 1 LOEWE-Exzellenz-Zentrum, 7 LOEWE-Exzellenz-Schwerpunkte, 5 DFG-Graduiertenkollegs, ...

Was habe ich vor

... die nächsten Minuten ...

TECHNISCHE UNIVERSITÄT DARMSTADT

Idealer Ablauf in 2 Varianten

Möglicher realer Ablauf

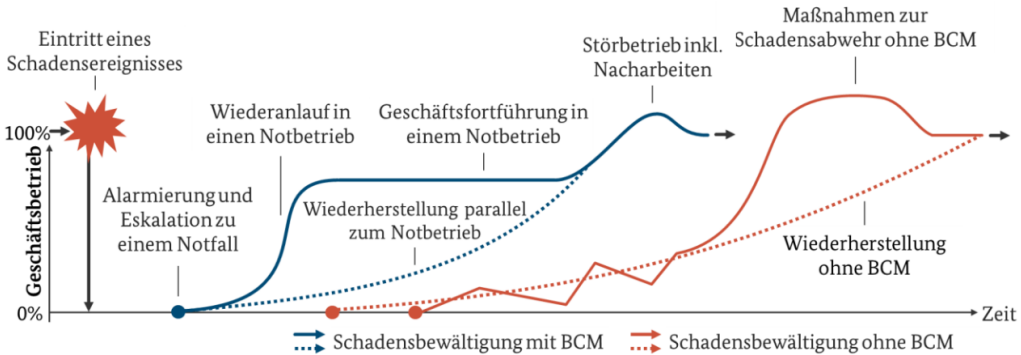
”Über den Tellerrand schauen und das Rad nicht neu erfinden”

Fazit

Bundesamt für Sicherheit in der Informationstechnik

Standard 200-4 - Business Continuity Management (BCM)

TECHNISCHE UNIVERSITÄT DARMSTADT



Bildquelle: BSI

Vorbereitet sein - BCM

”Was man hat, hat man”

TECHNISCHE UNIVERSITÄT DARMSTADT

- IT-Notfall und IT-Krisenmanagement etabliert
- IT-Notfallpläne vorhanden und Wiederherstellungs und Wiederanlaufpläne fertig und erprobt
- Vereinbarungen mit entsprechenden Servicepartnern geschlossen und diese eingearbeitet
- Beschäftigte und Nutzende geschult und bestens ausgebildet
- Aktuelle Systeme im Einsatz
- Personal stets bereit und verfügbar
- IT-Notfallsysteme vorhanden und parat
- Zertifizierten Betrieb nach BSI GS, ISO27xxx, TISAX, ...
- Kurz: *”alles gut”*

Vorbereitung - 24h davor

”Was man weiß, überrascht einen nicht”

TECHNISCHE UNIVERSITÄT DARMSTADT

- Aktuellen Netztopologieplan vorhanden
- Aktuelle IT-Gefahrenlage bewertet
- Aktuelle Risikoabschätzung der Gefahrenlage
- Vereinbarungen mit entsprechenden Servicepartnern geschlossen und diese eingearbeteit
- Beschäftigte und Nutzende geschult und bestens ausgebildet
- Aktuelle Systeme im Einsatz
- Akute bekannte Schwachstellen auf die aktuelle Bedrohung hin abgedichtet und überwacht
- CERT/SOC Mitarbeitende schauen sich die aktuellen Gefahren an und tauschen sich mit anderen Stellen aus

Ereignis - Stunde 0 - Variante einfach

TECHNISCHE UNIVERSITÄT DARMSTADT

- Der Angriff läuft mindestens ein IT-System wird kompromitiert
- Die Endpoint Protection erkennt sofort den Einbruch und isoliert das System
- Die nutzende Person erkennt die Anomalie und ruft sofort im CERT an
- Das CERT isoliert die Nahe Umgebung, schaut in Log File und Netflow-Analyse-Daten
- Analyse ergab kleiner Problem und weitere Gefährdung unwahrscheinlich
- CISO wird informiert
- Beteiligte Nutzende und Admins werden informiert

Bewältigung - 24h danach - Variante einfach

TECHNISCHE UNIVERSITÄT DARMSTADT

- *Lessons learned*
- Berichte werden erstellt und verteilt
- Einbruchsstelle wird genauer untersucht
- Awarenessmaßnahmen und - schulungen werden gegebenenfalls angepasst
- Fall ist abgeschlossen

Ereignis - Stunde 0 - Variante schwer

TECHNISCHE UNIVERSITÄT DARMSTADT

- Der Angriff läuft die System werden kompromitiert
- Einbruch wird erkannt
- Einbruchsstelle wird isoliert
- Es wird erkannt das ein großer Schaden zu erwarten ist
- IT-Notfallmanagement greift
  - IT-Krisenstab wird aktiviert (BAO nach BSI 200-4)
  - Einrichtung wird heruntergefahren
  - Notbetrieb wird angesagt
  - Notbetrieb wird aktiviert
- CERT/SOC voll tätig um mit Admins die Analyse zu machen
- dezentrale Admins und Nutzende warten auf Information

Bewältigung - 24h danach - Variante schwer

TECHNISCHE UNIVERSITÄT DARMSTADT

- IT-Notbetrieb wird ausgerollt
- Handlungsfähigkeit wird wieder hergestellt
- Wiederherstellungsbetrieb läuft an
- Betroffene Systeme werden begonnen zu analysieren
- Unterstützung kommt über Verträge und andere CERT
- Der IT-Krisenstab koordiniert die IT-Notfallteams
- Öffentlichkeitsarbeit und interne Kommunikation erfolgt aus dem IT-Krisenstab heraus

Soweit zu einem möglichen Ideal Zustand

Möglicher realer Ablauf

”Was man nicht hat, hat man nicht”

TECHNISCHE UNIVERSITÄT DARMSTADT

- Mangelwirtschaft
- Diskussionen um Zuständigkeiten und Zugriffe aus Systeme und Daten
- Mangelnde Informationen zur IT-Landschaft
- Personalknappheit und -ausfälle
- BCM noch nicht wirklich im Wert erkannt
- CERT/SOC noch nicht aktiv dauerhaft installiert

In diesem Ablauf werden folgende Personenrollen betrachtet

Nutzenden **Betreiber / Admin** **CERT / SOC** **Verantwortliche**

Vorbereitung - 24h davor

”Was Beteiligte so alles machen”

TECHNISCHE UNIVERSITÄT DARMSTADT

Nutzenden

- Sollte Schulungen besuchen
- Neues (sicheres) Passwort mache ich *nächste Woche*
- Das Programm brauche ich für ...
- Gut das ich mein eigener Admin bin

Betreiber / Admin

- Systemdoku *muss ich noch schreiben*
- Notfallpläne *werden noch erstellt*
- Wiederanlaufpläne *brauch ich ne Vorlage*
- Rufnummern finde ich schon
- Monitoring *führen wir noch ein*

CERT / SOC

- Notfallmanagement *arbeiten wir dran*
- Überwachungs-systemeinführung wartet wir auf Infos
- Lage sieht aktuell nicht gut aus
- Kollegen warnen uns

Verantwortliche

- Machen wir ein Projekt draus
- *könnte Forschung behindern/ein-schränken*
- IT-Sicherheit kostet Geld
- Sehen oft ihren eigenen Bereich als Prio 1

Ereignis - Stunde 0

"Der Überraschungsmoment"

TECHNISCHE UNIVERSITÄT DARMSTADT

Nutzenden

- Services gehen nicht
- Beschwerden
- Tickets öffnen
- ...
- Langsame Realisierung
- ggf. Stillschweigen
- "*Ich* habe keinen Link geklickt"

Betreiber / Admin

- "SCH....."
- Suchen nach der Quelle
- Ahnen es wird viel Arbeit werden
- Suche nach Passworten
- Suche nach Dokumentation der Vorgänger:innen

CERT / SOC

- "SCH....."
- Bereiche Abschalten?
- Alles Abschalten?
- Bedrohung Abwägen

Verantwortliche

- Suchen nach den Technikern
- ...
- Denken an Presse
- Wollen führen
- Wollen leiten

Bewältigung - 24h ähm 24 Wochen danach

"... und jetzt ..."

TECHNISCHE UNIVERSITÄT DARMSTADT

Nutzenden

- Können nicht arbeiten
- Müssen vor Ort kommen
- Organisieren sich mit Privatgeräten
- Leiden

Betreiber / Admin

- Schwitzen
- Suchen die Ursache
- Setzen neu auf
- Wollen alles sicherer machen
- Wollen sofort wieder online gehen
- Mehrarbeit

CERT / SOC

- "SCH....."
- Quelle suchen
- Systeme abdichten
- Admins unterstützen und besänftigen
- Vermitteln zwischen Dienstleistern und Admins und Verantwortlichen
- Mehrarbeit

Verantwortliche

- Suchen nach (den) Technikern
- Lesen Pressemitteilungen
- Wollen führen
- Wollen leiten
- Die wichtigsten System sind jeweils ihre
- Kosten werden realisiert

Zusammengefasst

TECHNISCHE UNIVERSITÄT DARMSTADT

Vorbereitet

- lässt schnelle Handlungen zu,
- sorgt dafür, dass jede:r weiß was zu tun ist,
- stellt eine einheitliche Wissensbasis zur Verfügung,
- dämmt eine Gefahr schnell und effektiv ein,
- sorgt für gezieltes reagieren selbst im total Ausfall und
- zentrale Koordination kann greifen.

Unvorbereitet

- Entsteht oft Aufgrund von *klaren Zuständigkeiten*
- Chaosphasen treffen härter, damit sollte man umgehen können
- Häufig rettet persönliches Engagement einzelner die Situation
- Bereiche mit guten Personal priorisieren sich nach vorne
- Oft leider die Wahrheit
- Von niemandem gewünscht

Was mache ich noch so

TECHNISCHE UNIVERSITÄT DARMSTADT

¸Jochen Becker

- Helfer im THW > 30 Jahre
- Ausbilder und Prüfer
- Fachberater
- ausgebildeter Zugführer
- Leiter THW-Führungsstellen/LuK
- Elbe 2002 und 2013
- Schneechaos Münsterland 2005
- Flüchtlingswelle 2015/2016
- Sturm 2019 Kreis Offenbach
- Starkregen 2021 (Ahrtal)

Technisches Hilfswerk

- gegründet August 1950
- Gesetzlicher Auftrag
  1. technische Hilfe im Zivilschutz,
  2. Einsätze und Maßnahmen im Ausland im Auftrag der Bundesregierung,
  3. **Bekämpfung von Katastrophen, öffentlichen Notständen und Unglücksfällen größeren Ausmaßes** auf Anforderung der für die Gefahrenabwehr zuständigen Stellen sowie
  4. Unterstützungsleistungen und Maßnahmen im Sinne der Nummern 1 bis 3, die das Technische Hilfswerk durch Vereinbarung übernommen hat.

Blick über den (eigenen) Tellerrand

”Wie der Alltag einen prägt”

TECHNISCHE UNIVERSITÄT DARMSTADT

- Rettungsdienst
  - Ersthelfendenausbildungen für alle
  - Rettungsdienst
  - Notärzte
- Notfallmedizin
  - Kliniken
  - Spezialkliniken

- Katastrophenschutz und Zivilschutz
  - KRITIS
  - Vorhaltung für den Ernstfall
  - Trainieren für den Ernstfall
  - Dezentrale Verteilung
  - Unterstützende Arbeitsweise
  - Einheitliche Technologie (Bundesstandards)

Zusammenarbeit mit übergreifenden Zuständigkeiten - Hand in Hand

Blick über den (eigenen) Tellerrand

”Fragen die gestellt werden sollten”

TECHNISCHE UNIVERSITÄT DARMSTADT

- Was haben andere?
- Wer kann mir helfen?
- Mit wem kann ich zusammenarbeiten?
- Wer könnte mit mir zusammenarbeiten?
- Muss ich alles selbst machen?
- Muss ich alles selbst können?
- Muss ich alles selbst haben?

- Beispiele aus dem THW
  - Dienstvorschrift 1-100, ”Führung und Einsatz”
  - Dienstvorschrift 1-101, ”Handbuch Führen im Technischen Hilfswerk”
- so ähnlich auch bei Feuerwehr, Rettungsdienst, Bundeswehr
- finden sich in der IT-Sicherheit wieder
  - BSI Standards 200-1 bis 200-4
  - Ausbildung zum Digitaler Ersthelfer (seit 2021)

Vorbereit sein mal anders gedacht oder gesagt

”Was man haben könnte, hätte man”

TECHNISCHE UNIVERSITÄT DARMSTADT

- *”In Krisen Köpfe kennen”*
- Erreichbarkeiten sicherstellen
- Notfallverfahren ohne IT - *mit Stift und Zettel* - planen
- Orte und Stellen definieren, wer findet sich wann wo
- Meldeketten definieren, wer ist *mein* nächster Kontakt
- *Etwas annehmen und persönliche Punkte zurückstellen können*
- Vorbereitung und Vorhaltung kostet immer extra Geld (Inverstion in die Zukunft?)
- Zur Einführung von IT-Sicherheit Veränderungen im Gewohnten vornehmen

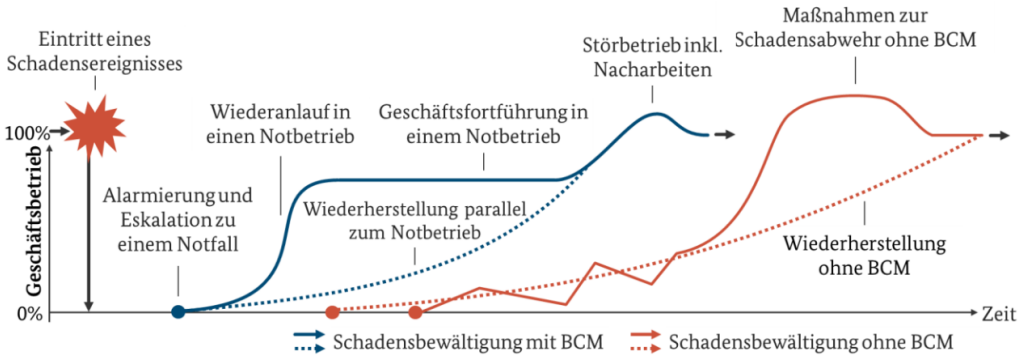
”Tips aus meiner Sicht als CERT-Leiter”

TECHNISCHE UNIVERSITÄT DARMSTADT

- Auf oberere Managementebene das klare Ziel Informationssicherheit benennen und stützen
- IT-Sicherheitsmaßnahmen nicht als Einschränkung sehen, sondern als Schutz der eigenen Arbeit
- CERT als operative Einheit mit dediziertem eigenem Personal ausstatten
- Informationen aus den zentralen Bereichen dem CERT zur Verfügung stellen
  - Netflowdaten ´
  - Servicelisten / Kernprozesse / Geschäftsprozesse inkl. Dringlichkeit
  - Assetmangement und Netzdiagramme inkl. Tunnelstrecken
  - Login- und Accountdaten
- Informationen die noch nicht vorhanden sind sammeln lassen, ggf. mit Priorität
- Gefahrenpotentiale aufzeigen und gemeinsam lösen wollen (Schwachstellenmanagement)
- Zentralen und gemeinsamen Betrieb so viel wie möglich
- Outsourcing und Cloud mitberücksichtigen und bedenken - nicht immer ein Gewinn

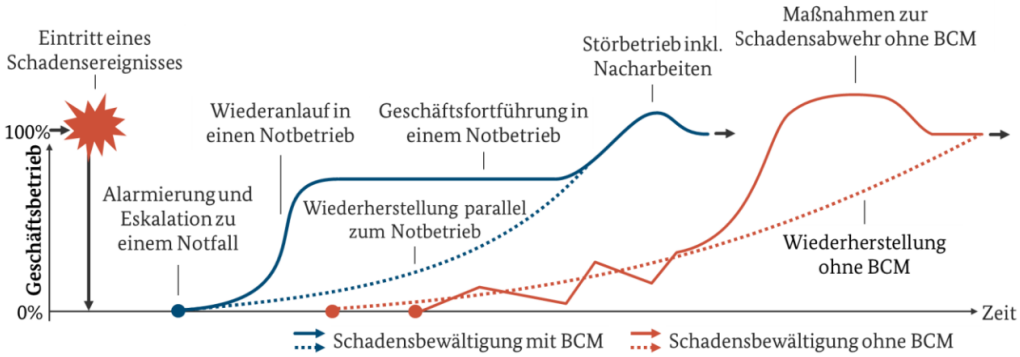
zurück zum Anfang

Standard 200-4 - Business Continuity Management (BCM) - Vorbereitet sein



Bildquelle: BSI

Danke und Zeit für Fragen



Bildquelle: BSI