HISOLUTIONS

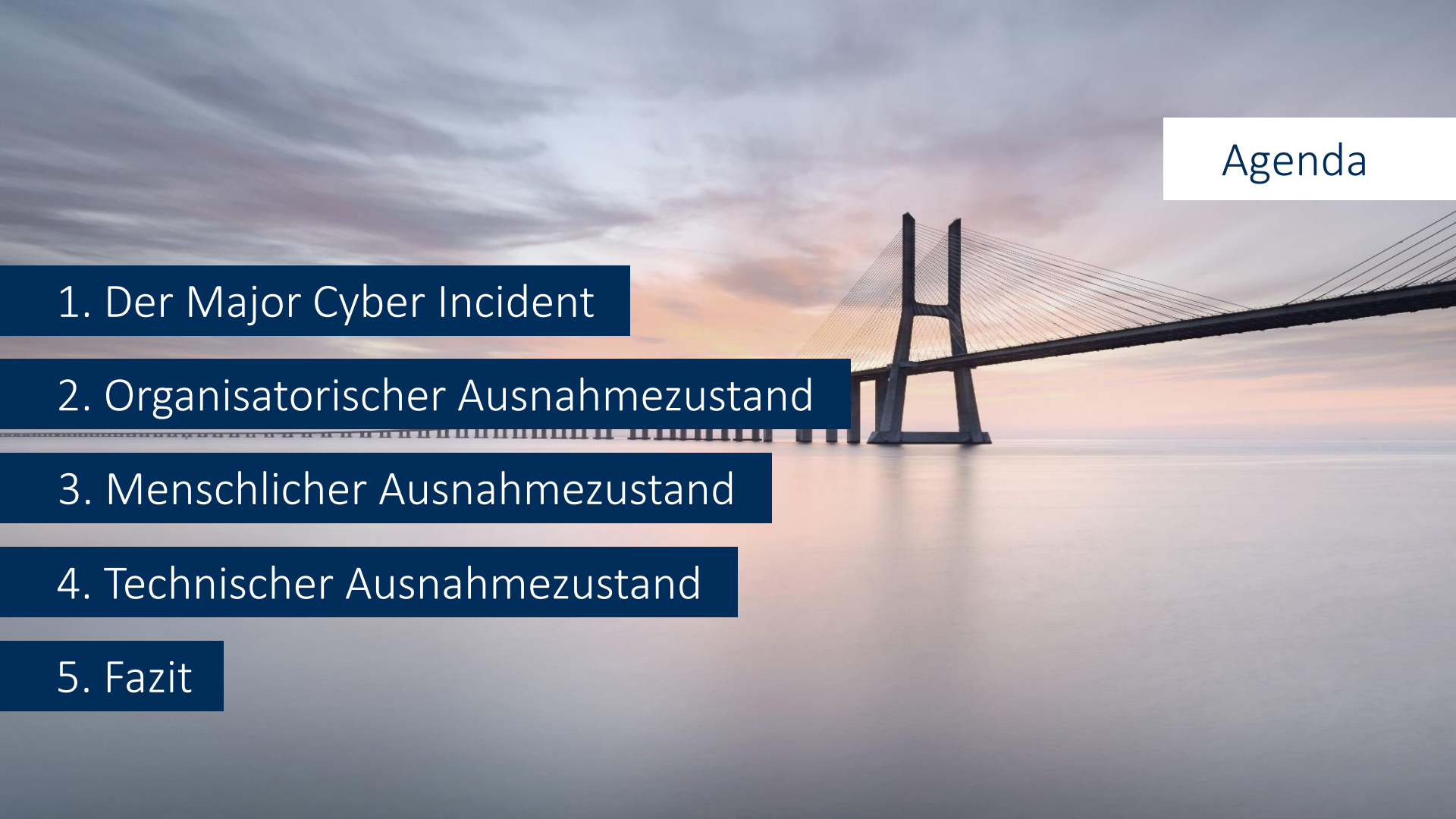
Aus Cyber-Unfällen gelernt

Über die Lehren der Incident Response und die Widersprüche zwischen Prävention und akutem Vorfall

Dresdner Abwassertagung 2026

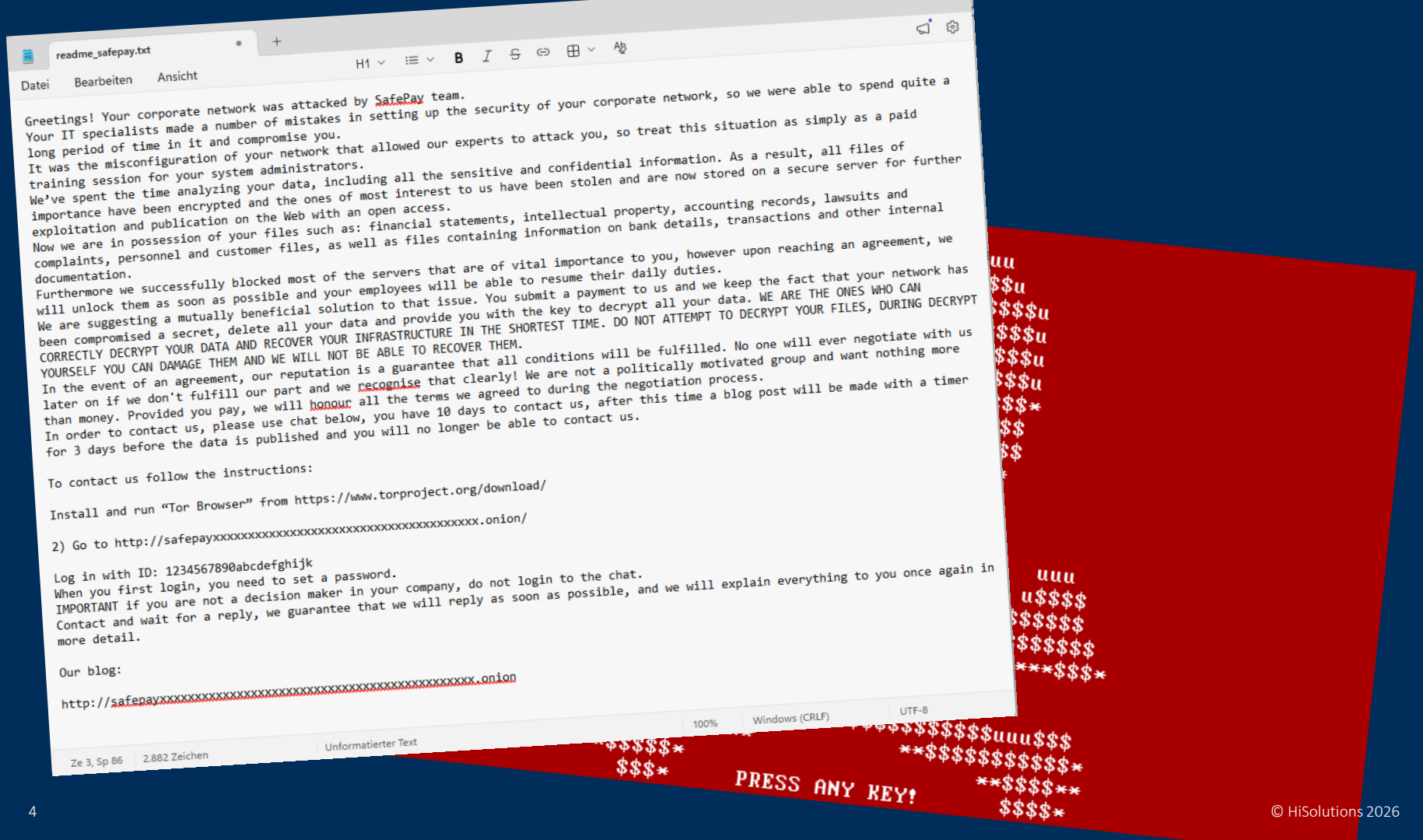
Jan Rähm

Agenda

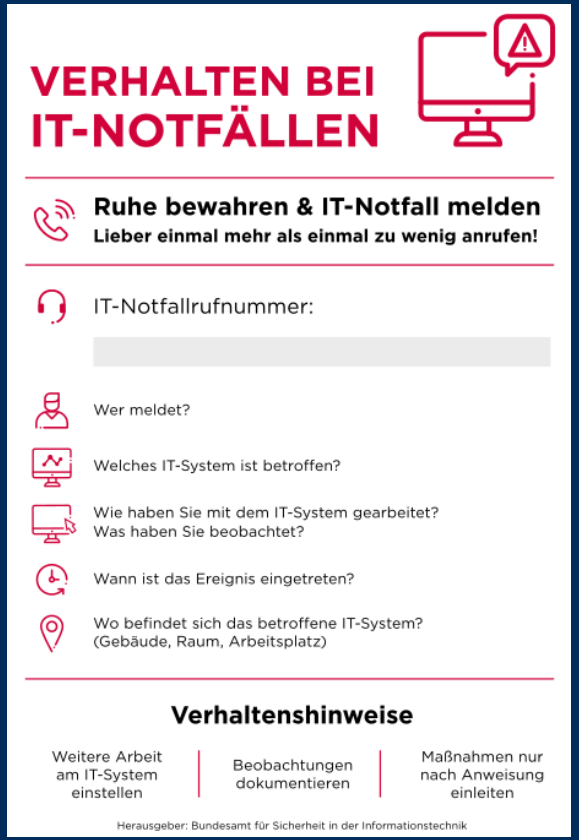


1. Der Major Cyber Incident
2. Organisatorischer Ausnahmezustand
3. Menschlicher Ausnahmezustand
4. Technischer Ausnahmezustand
5. Fazit

1. Der Major Cyber Incident



2. Organisatorischer Ausnahmezustand



VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Bild: www.bsi.bund.de

auf dem Server verschlüsselt

Meldeketten mit veralteten Nummern

nie unter Stress getestet

IT-Abteilung informiert alle per Mail:
„Wir wurden gehackt. Wirklich“

Pressemitteilung sagt „vorsorglich abgeschaltet“

gar nichts gesagt

3. Menschlicher Ausnahmezustand


Bild: energepic.com / pexels.com

Leugnung

Ärger

Feilschen

Depression

Akzeptanz

Eine IT-Krise ist kein Sprint,
Eine IT-Krise ist ein Marathon!

Bild: Pietro Rampazzo, unsplash.com

3. Technischer Ausnahmezustand

Bild: Florian Hirzinger, CC BY-SA 3.0

Unsere Firewall loggt … für sieben Tage.

Unsere E3-Lizenz enthält Logging!

Der Log-Server liegt auf dem HyperV.

4. Fazit

Bild: Martina Nolte / CC BY-SA 3.0 DE

Es ist keine Frage, OB es passiert – sondern WANN – und ob Sie dann vorbereitet sind.

Der schlimmste Zeitpunkt, Notfallplan zum ersten Mal zu lesen, ist während des Major Cyber Incidents.

Wasseraufbereitungs- und -behandlungsanlagen hören nicht auf zu arbeiten, weil die IT steht. Sie zu weiter steuern zu können, ist die Herausforderung.

2022 – Fallbeispiel ASG (Abwasser- u. Straßenreinigungsbetrieb der Stadt Gifhorn)

https://www.youtube.com/watch?v=OazNTpO9J9I

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com