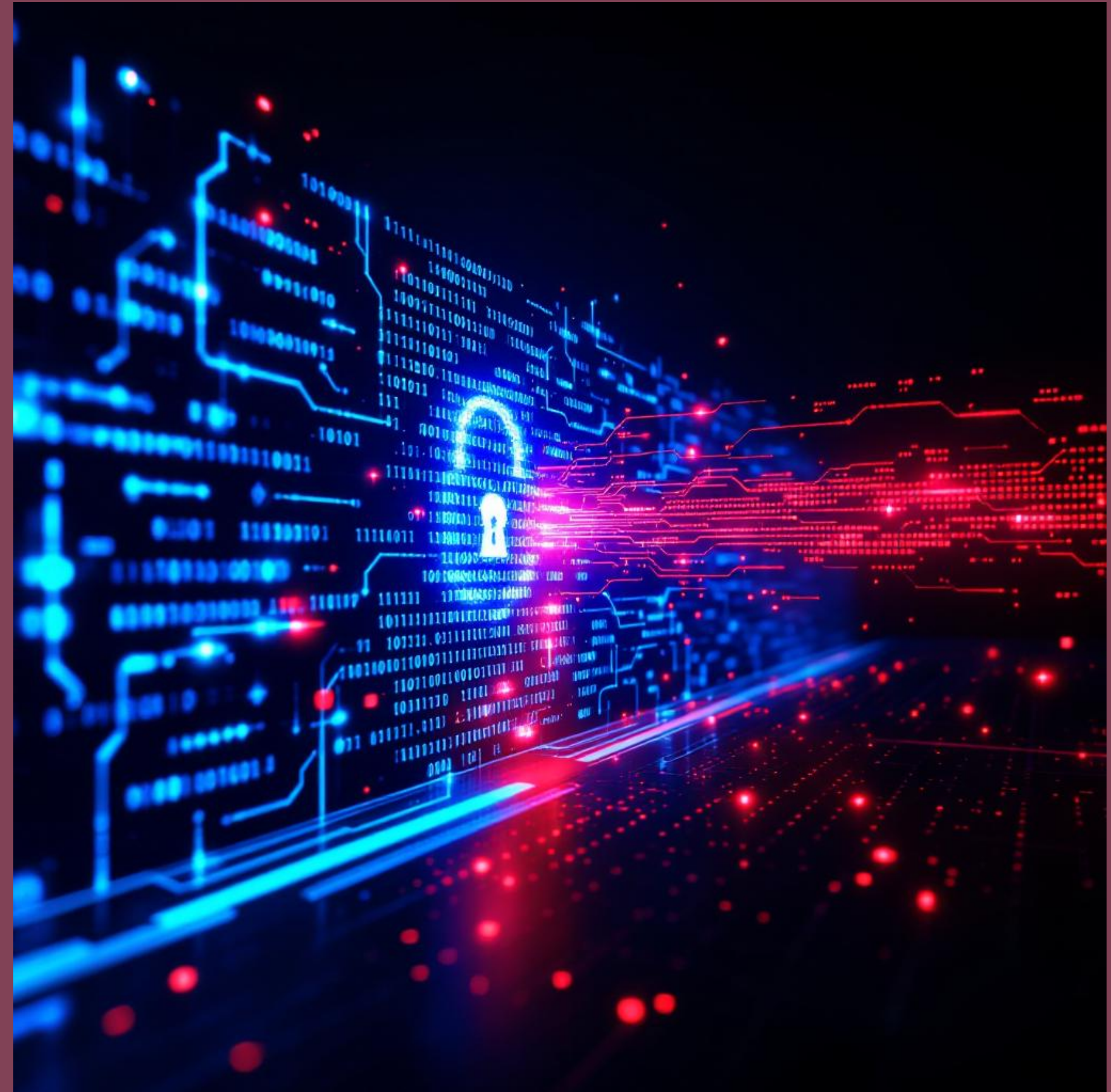


Der steinige Weg zur Resilienz

Theorie & Praxis im Rechenzentrum



zur Person

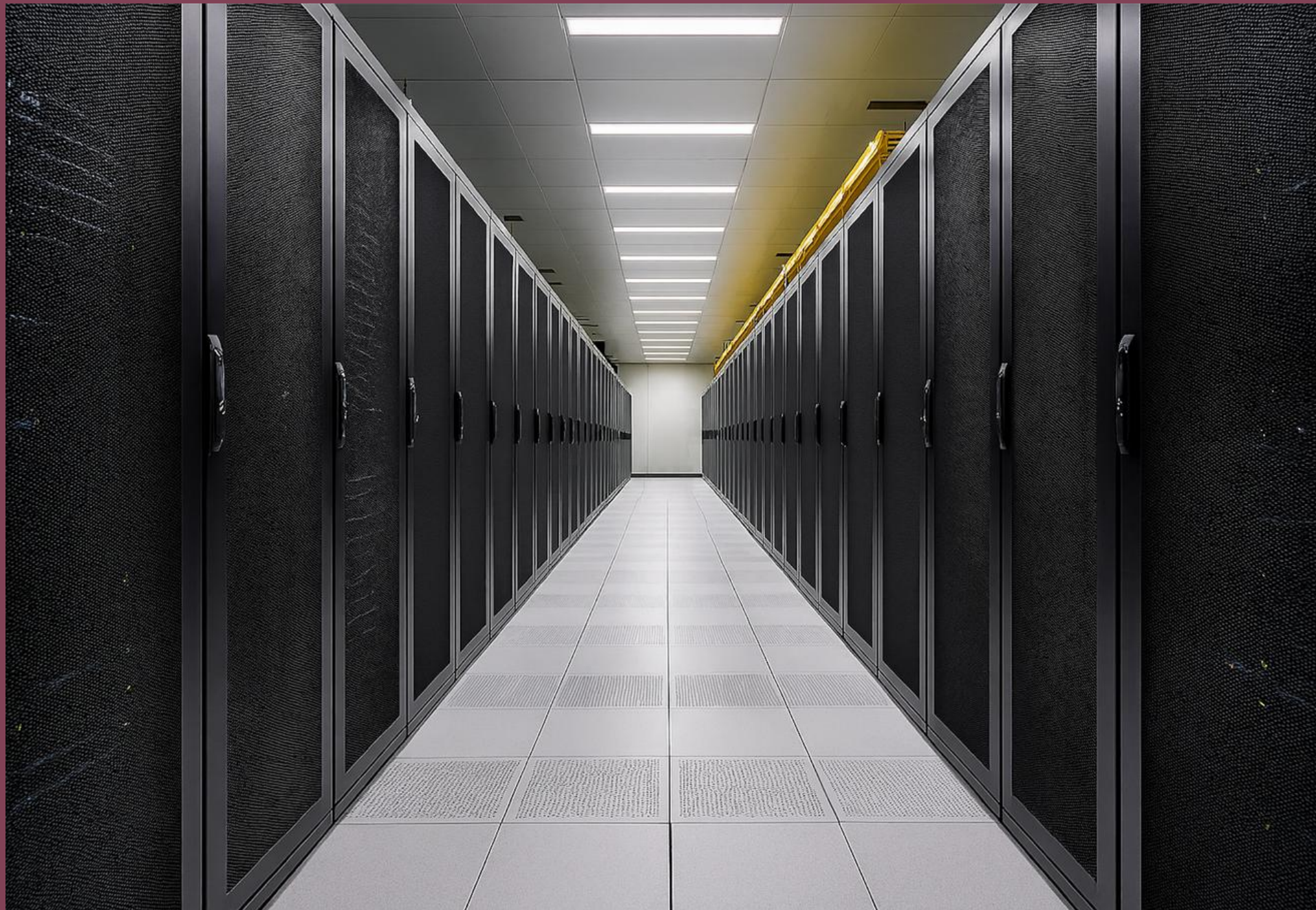
- CISO der SVD Büromanagement GmbH
- Geschäftsbereichsleiter für InfoSec & Datenschutz
- Risk Management
- Business Continuity Management
- ISO/IEC 27001 + 27701
- Security Operations Center

Strategie

- business-driven
- Prävention vor Reaktion
- Rennrad (schauen)

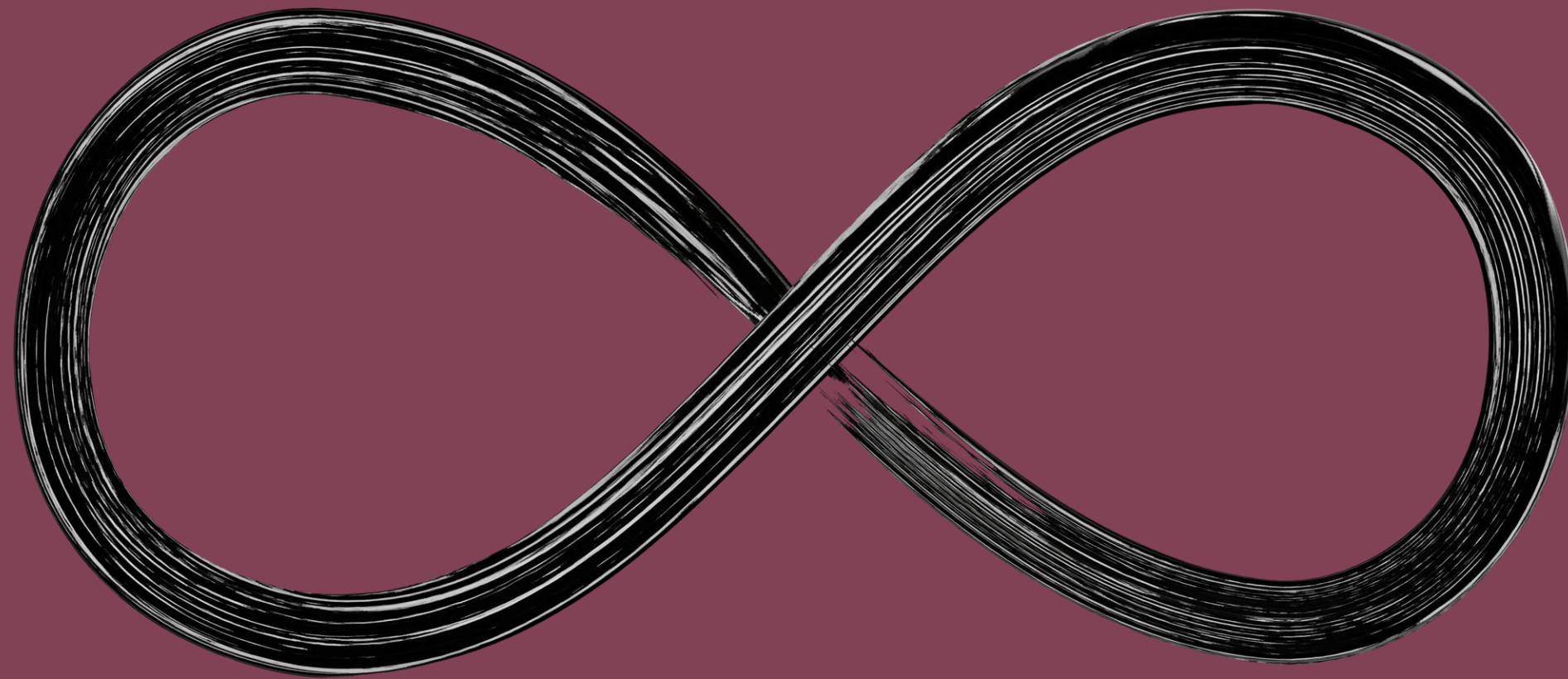


SVD - wer ist das?



- zentraler Backoffice Dienstleister in der österr. SV
- bedient verschiende Geschäftsfelder
- von IKT über FM & Beschaffung bis Druck & Bau
- Personalstand: ca. 500
- 7500 Clients, 2800 Server

Resilienz



...der Weg dort hin



**Nicht die Stärksten überleben,
auch nicht die Intelligentesten,
sondern die, die am besten auf
Veränderungen reagieren**

(Charles Darwin)

Information Security

Information Security

Was wollen wir schützen?

Welche/n Standard/s ziehen wir heran?

Wie gehen wir vor?

Information Security

Best Practice?

- Erhebung des Status Quo
- Analyse der Gaps
- risikobasierter Ansatz bei der Umsetzung
- Erstellung verbindlicher, zentraler Dokumente
- Step-by-step
- wiederkehrend

Management Commitment

bei SVD?

- ursprüngliches Ziel: ISO/IEC 27xxx Zertifizierungen
- regulatorische Anforderungen erfüllen
- damalige Reise: 2+ Jahre

Information Security

news ORF.at

Cyberattacke: Daten von 1,5 Millionen Schweden veröffentlicht

16. September 2025, 15.27 Uhr

Nach einer Cyberattacke gegen einen IT-Dienstleister sind persönlichen Daten von 1,5 Millionen Schweden veröffentlicht. Das Datenleck gehe auf einen Cyberangriff auf den System Miljödata am Wochenende 23. und 24. August zurück, teilte schwedische Staatsanwaltschaft am Montag mit. Schwedische Medien zufolge waren vor allem Stadtverwaltungen und private Unternehmen betroffen.

Die Untersuchung des Datenlecks sei im Gange, sagte Staatsanwältin Sandra Helgadottir. Eine Gruppe mit dem Namen Datacarry, die zu der Attacke bekannt, sagte Helgadottir. Die Ermittlungen konzentrierten sich darauf, die Verantwortlichen hinter der Cyberattacke zu identifizieren. „Derzeit gibt es keine Hinweise, dass eine ausländische Macht daran beteiligt ist“, sagte die Staatsanwältin.

Hacker forderten Geld

Schwedische Medien berichteten, die Hacker hätten zuvor (umgerechnet rund 150.000 Euro) gefordert und mit der Veröffentlichung der Daten gedroht. Miljödata hatte am Wochenende erklärt, dass die Daten im Darknet veröffentlicht worden seien. Es handelte sich unter anderem um Namen, Adressen und Kontaktdaten. Die Zahl der Betroffenen entspricht fast 15 Prozent der schwedischen Bevölkerung von 10,6 Millionen Bürgern.

news ORF.at

Cyberangriff auf Innenministerium aufgedeckt

30. August 2025, 10.17 Uhr

Ein Cyberangriff auf die IT-Infrastruktur des Innenministeriums (BMI) ist vor mehreren Wochen aufgedeckt worden. Wie das Ministerium heute bekanntgab, wurden Unregelmäßigkeiten in einem der Büro-IT-Systeme des BMI registriert. Dahinter steckte jedoch ein gezielter und professioneller Angriff.

Konkret kam es dabei zu unberechtigten Zugriffen auf Mailserver des BMI. Aktuell ist eine Einschränkung des externen E-Mail-Verkehrs die Folge der ergriffenen Sicherheitsmaßnahmen.

Rund 100 der etwa 60.000 E-Mail-Accounts des BMI waren in Teilbereichen davon betroffen, wobei sensible Inhalte grundsätzlich nicht per Mail kommuniziert werden. Mitarbeiterinnen und Mitarbeiter mit diesen Accounts wurden laut BMI jedenfalls direkt informiert, die betroffenen Systeme isoliert sowie externe IT-Sicherheitsfachleute hinzugezogen, das sei in einem derartigen Fall üblich.

Daten und Informationssysteme nicht betroffen

Das BMI unterstrich, dass die Erfüllung der polizeilichen Kernaufgaben zu keinem Zeitpunkt des Angriffs beeinträchtigt war, „die Arbeitsfähigkeit ist vollumfänglich gegeben, und die wesentlichen IT-Services stehen zur Verfügung“. Polizeiliche Informationssysteme, Datenbanken, Register oder personenbezogene Daten von Bürgerinnen und Bürgern seien von dem Cyberangriff nicht betroffen gewesen.

Teilen

news ORF.at



EUROPÄISCHE FLUGHÄFEN

Cyberangriffe auf Check-in-Systeme gemeldet

Mehrere europäische Flughäfen haben am Samstag mit Problemen bei ihren Systemen für die Passagierabfertigung gekämpft. Der Flughafen Brüssel sprach von den Folgen eines Cyberangriffs. Betroffen waren auch der Airport London-Heathrow sowie die Flughäfen in Berlin und Dublin. Der Flughafen Wien-Schwechat war nicht betroffen.

20. September 2025, 9.22 Uhr (Update: 20. September 2025, 17.30 Uhr)

Teilen

Der Flughafen Wien verzeichnete keine derartigen Vorkommnisse, sagte Flughafensprecher Peter Kleemann Samstagfrüh. Auch die deutschen Flughäfen Frankfurt und Hamburg berichteten, nicht betroffen zu sein.

Der Betrieb laufe normal, es gebe keine Einschränkungen. Sowohl in Berlin als auch in Brüssel sei mit erheblichen Auswirkungen durch Verspätungen und Flugausfälle zu rechnen, hieß es von beiden Flughäfen.

picturedesk.com/Carsten Koall

Information Security

durch Zugehörigkeit zur kritischen Infrastruktur

- strategisch
- technisch
- organisatorisch

notwendig, auf dem aktuellsten Stand zu sein, um Anforderungen zu erfüllen

in der
SVD

Wie?

- CISO < - > Geschäftsführung
- überwachend
- strategische Mitsprache
- direkter Ansprechpartner

- PDCA → Plan - Do - Check - Act (Adjust)

Risk Management

Risk Management

Fokus?

- one size fits all?
- Auswahl der passenden Methodik
- wie viel verträgt das Unternehmen?
- unbequem bleiben durch IKS

bei SVD?

- ERM - Enterprise Risk Management
- interne Audits & Kontrollen
- Akzeptanz strikt nach potentieller Auswirkung
- 3rd Party??? (schwierig)
- verankert in unseren TOMs

Business Continuity Management

Business Continuity Management



Womit sollen wir beginnen?

Worauf wollen wir uns konzentrieren?

Objektivität vs. Subjektivität

Business Continuity Management

Wie schnell können wir wieder funktionsfähig sein?

Wie minimieren wir Datenverlust und Imageschäden?

Wie verhindern wir, dass aus kleinen Vorfällen große Krisen werden?

Business Continuity Management

organisatorisch/strategisch:

- ISO/IEC 22301
- durch die High Level Structure passend zu anderen ISO-Themen
- SV-weit ebenso zentral

operativ:

- BSI-Standard 200-4
- vom IT-Notfallmanagement ausgehend
- Reaktiv → Aufbau → Standard-BCMS

Krisenmanagement nicht vergessen

Business Continuity Management



Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/BSI_Standard_s/standard_200_4.pdf?__blob=publicationFile&v=8, Seite 52

Frage:
führen Normen/Standards und
Mgmt-Systeme tatsächlich zu

Resilienz

oder...

Resilienz

Vorsicht: provokative Frage!

Wenn das Rechenzentrum redundant ist, aber kein Mensch erreichbar oder willens - wie steht es um die Resilienz?

Resilienz

kulturell

organisatorisch

technologisch

personell

infrastrukturell

ökologisch

cyber/digital

Resilienz

technologisch

- Redundanz aller IT-Systeme
- Monitoring (mit validen Schwellwerten)
- Backup-Konzepte
- Patch-Management
- Failover-Systeme
- Lifecycle Management

Resilienz

infra- strukturell

- Stromversorgung
- physische Sicherheitsmaßnahmen
- Klima/Kühlung
- Schutz vor Feuer/Wasser/...
- regelmäßige Tests der Komponenten
- Standortwahl

Resilienz

ökologisch

- Energieeffizienz
- alternative Quellen
- Nachhaltigkeitsgedanken
- ESG-Berichtspflichten
- Wiederverwertung / -verwendung

Resilienz

organi- satorisch

- Krisenmanagement-Teams mit klar definierten Rollen und Eskalationswegen
- Regelmäßige Übungen und Tests
- Dokumentation aller Prozesse, Kontakte und Ressourcen
- Lieferantenmanagement

Praxis-Tipp:

Führen Sie Mindset-Trainings durch, um ein Bewusstsein für Resilienz auf **allen Ebenen** zu schaffen.

Resilienz

kulturell

- Fehlerkultur
- Innovationskultur
- Motivation der Mitarbeitenden
- Incentives

Resilienz

personell

- Gesundheit der Mitarbeitenden
- Stressmanagement
- Führung in Ausnahmesituationen
- Gehör & Verständnis → Riesenaufgabe
- Highlander vs Musketiere
- Ausgewogenheit beachten

Resilienz

cyber / digital (1)

- **digitale Souveränität gegeben, wenn:**
- rechtssicher/DSGVO-konformer Betrieb (bspw. ohne Zugriff durch aus- ländische Behörden auf Daten)
- Wechselfähigkeit (kein Vendor-Lockin)
- Kontrolle gesichert (auch bei Ausfall, Sperrung oder Wechsel von Dienstleistern)
- Transparenz (durch einsehbaren Quellcode)
- und anpassbar und gestaltbar ist (durch Weiterentwicklung in der Community oder durch Dienstleister) *

*Quelle:

<https://www.zendis.de/media/pages/newsroom/publikationen/souveraenitaets-washing/751a2c5eb1-1755243871/zendis-whitepaper-souveraenitaets-washing.pdf>

Resilienz

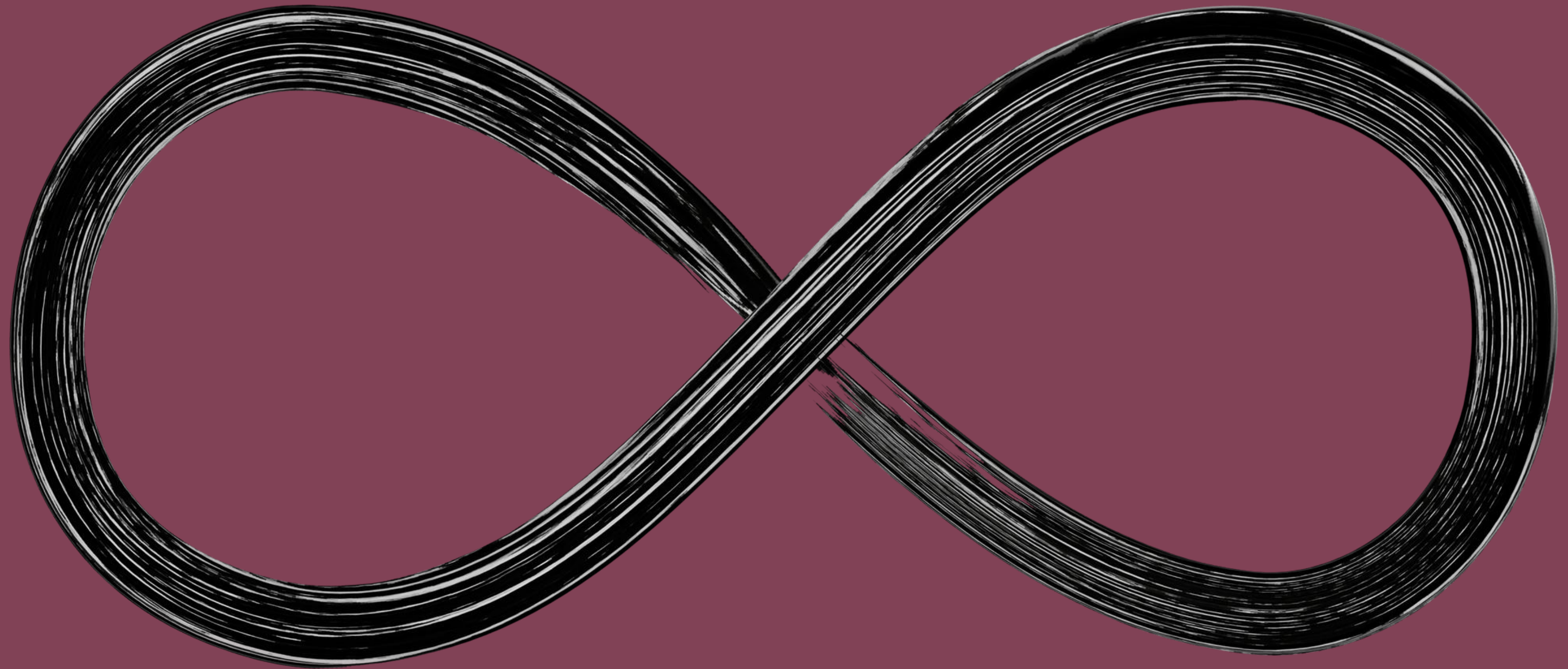
**cyber /
digital
(2)**

- Präventive Maßnahmen (wie Schwachstellen- und Attack Surface Management)
- Detektive Maßnahmen
- hoher Automatisierungsgrad
- korrektive Maßnahmen & Lessons Learned

*Quelle:

<https://www.zendis.de/media/pages/newsroom/publikationen/souveraenitaets-washing/751a2c5eb1-1755243871/zendis-whitepaper-souveraenitaets-washing.pdf>

Key Takeaways



Key Takeaways

Resilienz:

interdisziplinär

heterogen

ist mehr als das eigentliche Business



**Resilienz ist kein Zustand,
sondern ein Versprechen – das
wir täglich erneuern, um morgen
bestehen zu können.**

(Stefan Höller)

Vielen Dank!

