Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Keep calm and remember your *Meldewege*:

Erste Reaktion auf einen Cyber-Vorfall

Bonn, 04.09.2024

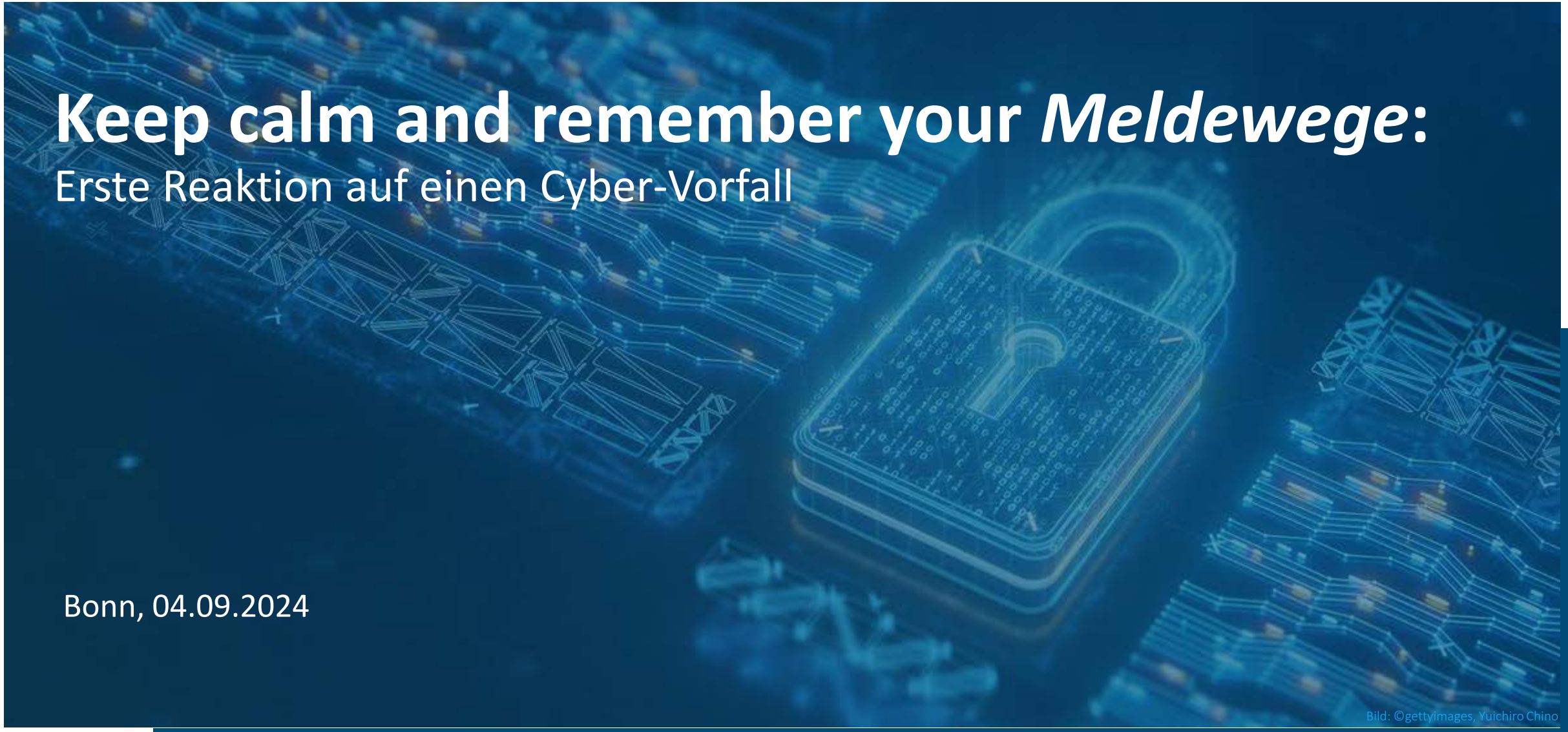


Bild: ©gettyimages, Yuichiro Chino

Wer bin ich?

Maike Vossen

B.A., B.Sc., M.A.

Bundesamt für Sicherheit in der Informationstechnik

Referat C 21 – CERT-Bund, Grundsatz und Warn- und Informationsdienst WID

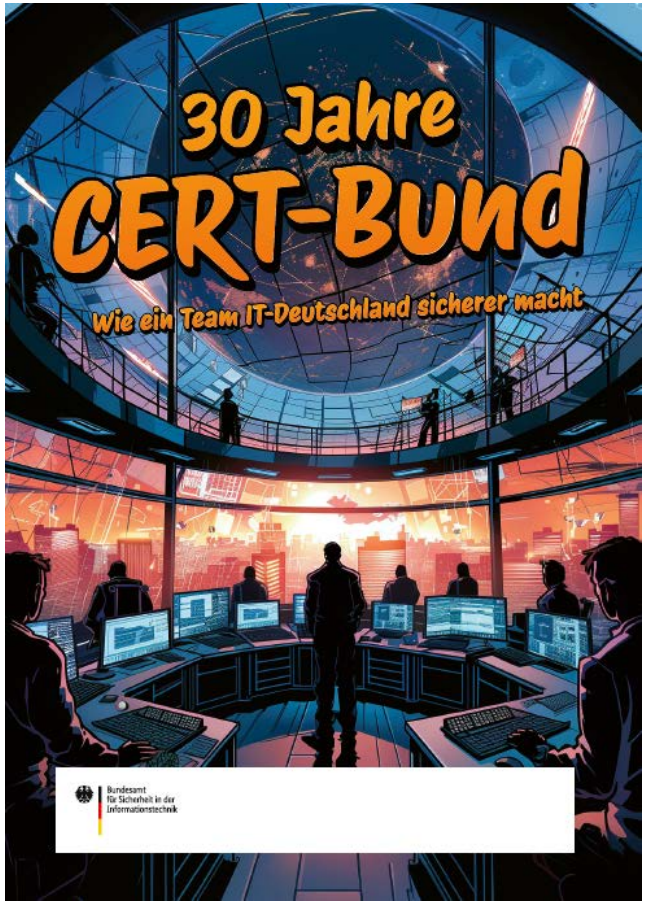
maike.vossen@bsi.bund.de

www.bsi.bund.de

@bsi_bund @certbund

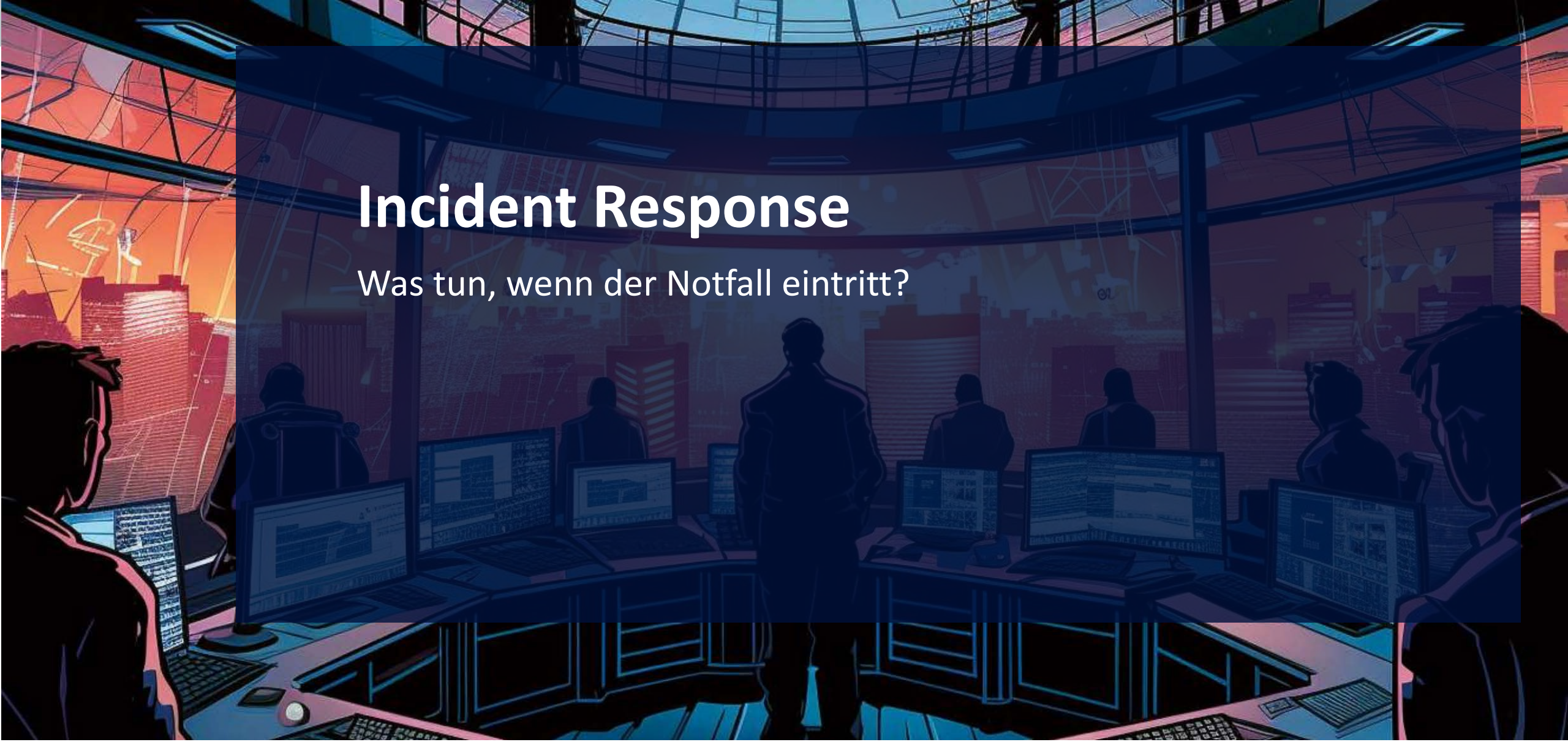
Was macht CERT-Bund eigentlich?

- **C**omputer **E**mergency **R**esponse **Te**am des Bundes
- → Vorfallsbearbeitung
- Zielgruppe: Bundesverwaltung
- Aber auch in bestimmten Fällen: KRITIS, UBI, weitere Verwaltung



But wait, there is more!

- Veröffentlichung von Cybersicherheitswarnungen
- CERT-Bund Reports
- Coordinated Vulnerability Disclosure
- Threat Intelligence
- Technische und administrative Betreuung von Fachverfahren
- Nationale und internationale Netzwerke, Betreuung Nationales Cyber-Abwehrzentrum
- IT-Sicherheit von Großveranstaltungen
- […]



Incident Response

Was tun, wenn der Notfall eintritt?

Organisatorische Reaktion

- Ruhe bewahren und Kräfte einteilen!
- Melden und intern informieren → spätere Folie
- Einberufung Krisenstab
- Informationen sammeln und dokumentieren
- Externe Hilfe → spätere Folie
- Krisenkommunikation
- Business Continuity Management
- Nachbereitung

→ ACS Checkliste Organisatorisches

Technische Reaktion

- Privilegierte Nutzerkonten auf infizierten Systemen
- Gesamtes Netzwerk berücksichtigen
- Monitoring und Logging (Datenschutz beachten!)
- Integere Backups einspielbar? Backup-Daten aus anderen Quellen?

→ ACS Checkliste Technik

Meldestelle und Eskalationsstufen

- Einrichtung einer Meldestelle
- Definition von Eskalationsstufen
  - Beispiel BSI Standard 200-4: Grau (Normalbetrieb), Gelb (Störung), Orange (IT-Notfall), Rot (IT-Krise)
  - Checkliste für Meldestelle zur ersten Lagebewertung
  - Von der Eskalationsstufe abzuleitende Maßnahmen

Meldeketten

- Meldeketten sind abhängig von den Eskalationsstufen
- Spätestens ab einem IT-Notfall sollten diese mindestens folgende Glieder enthalten:
  - Geschäftsleitung
  - IT-Betrieb oder IT-Dienstleister
  - IT-Leitung
  - Informationssicherheitsbeauftragte (ISB)
  - Datenschutzbeauftragte
  - Pressestelle

Externe Meldepflichten und Adressaten

- Externe Meldepflichten ggf. stark individuell
- Ggf. Meldung von Datenschutzverstößen
- Ggf. Strafanzeige bei der ZAC
- Ggf. LfV
- Ggf. BSI oder Landes-CERT
- **Wichtig**: Kommunikation mit Kunden und Geschäftspartnern

Externe Hilfe

- **Wichtig**: Das BSI hat in den meisten Fällen keinen gesetzlichen Auftrag zur Vorfallsunterstützung bei Unternehmen
- Ggf. Landes-CERT (landesabhängig!)
- Allianz für Cybersicherheit
- BSI Liste der qualifizierten APT-Response-Dienstleister
- BSI Liste der zertifizierten Vorfalls-Experten
- Cyber-Sicherheitsnetzwerk

Einen Vorfall der ACS melden

- Hilft dem BSI bei der Erstellung eines verlässlichen und umfangreichen Lagebildes
- Aufschluss über neue Angriffsmethoden, Ziele und Schwachstellen
- Informationen werden vertraulich behandelt und nur anonymisiert geteilt
- Lageinformationen werden (je nach Einstufung) geteilt mit:
  - BMI
  - KRITIS und UBI
  - ACS
  - Verbünde VCV und CV
  - Nationales Cyber-Abwehrzentrum

Prävention

„Wir haben kein Maßnahmen-, sondern ein Umsetzungsproblem.“

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

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Maike Vossen
CERT-Bund

maike.vossen@bsi.bund.de
Tel. +49 (0) 228 9582 4157

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de