



GEMEINSAME DATENUMGEBUNGEN (CDE) IN DER ÖFFENTLICHEN VERWALTUNG FÜR BIM-PROJEKTE

SICHERHEITS- UND SCHUTZKONZEPTE FÜR GEMEINSAME DATENUMGEBUNGEN

LTRDir'in Antje Grande

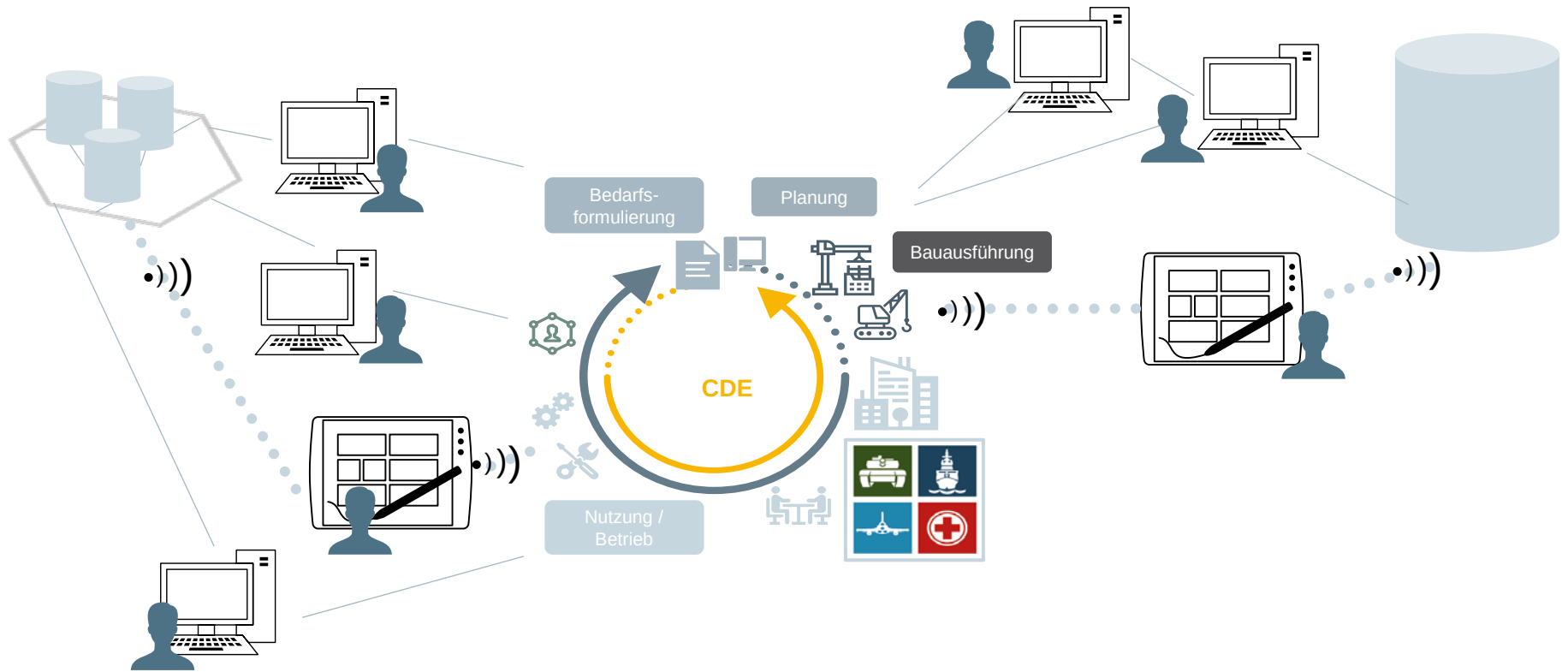
BAIUDBw Infra III 6 – Chief Information Security Officer Infrastruktur



BUNDESWEHR

CDE

ZENTRALE PLATTFORM FÜR DIE DIGITALE ZUSAMMENARBEIT

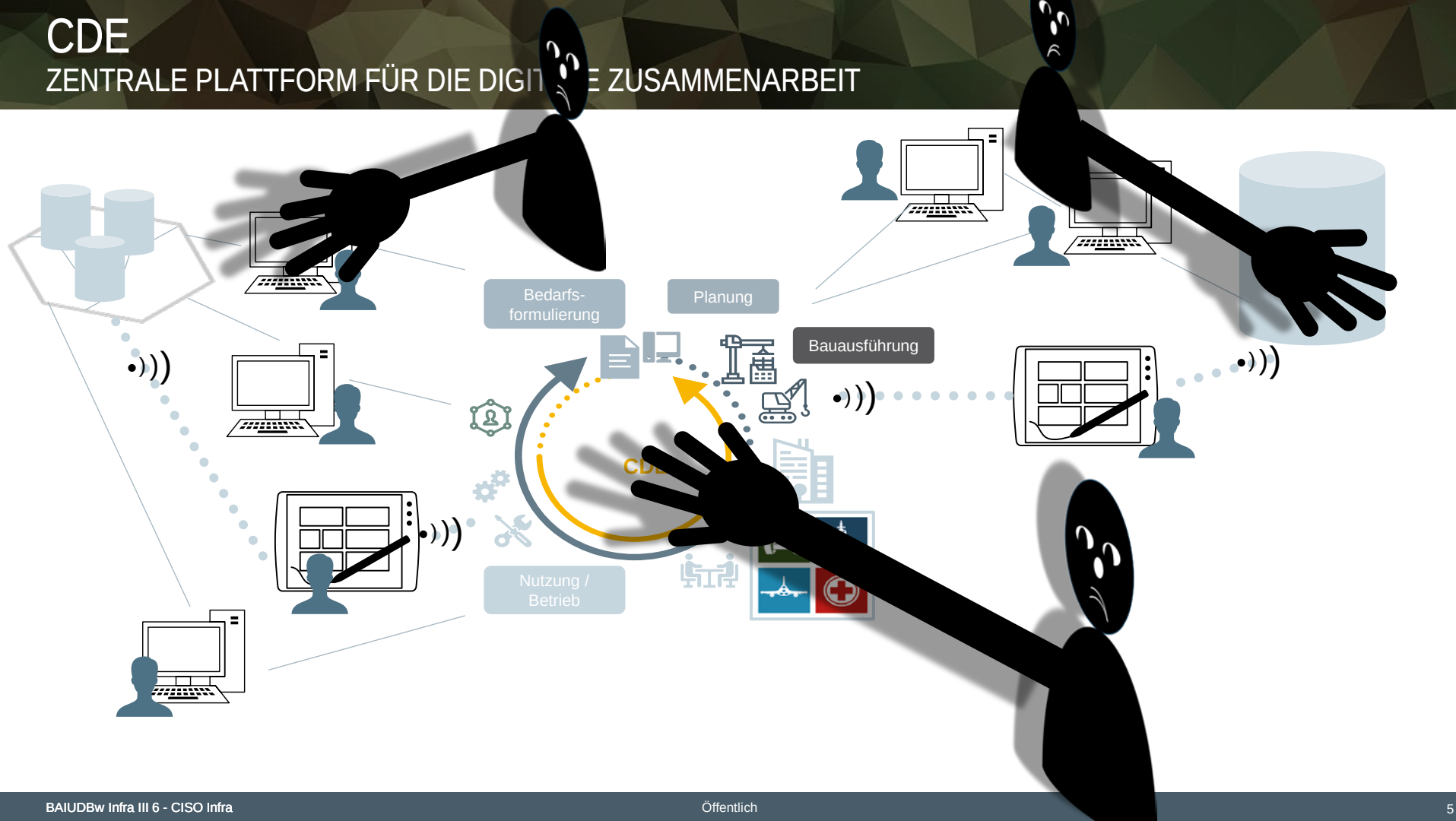


- Daten sind zentral, strukturiert und erläutert abgelegt
- Informationsmodelle erlauben die Ableitung weitergehender Informationen (z.B. Netzzusammenhänge)
- Datenstrukturen sind standardisiert und wiederholen sich

- Daten sind zentral, strukturiert und erläutert abgelegt
- Informationsmodelle erlauben die Ableitung weitergehender Informationen (z.B. Netzzusammenhänge)
- Datenstrukturen sind standardisiert und wiederholen sich
- Geringes Bewusstsein für digitale Bedrohung bei Beteiligten
- Einfache Verfügbarkeit digitaler Daten verleitet zum „Horten“ von Daten unabhängig von der Notwendigkeit

CDE

ZENTRALE PLATTFORM FÜR DIE DIGITALE ZUSAMMENARBEIT



Verschlüsseln von Systemen mit Lösegeldforderung (Ransomware-Angriff)

Technisch

- Erfolgsfaktoren: fehlende technische Absicherung (keine Intrusion-Detection und / oder Intrusion-Prevention)
- Gesamtes Firmennetz betroffen
- Abfluss aller erreichbaren Informationen
- Infiltration kann Wochen bis Monate vor der Verschlüsselung erfolgt sein.

Reaktion

- Zurückhaltende Außenkommunikation der Betroffenen
- In der Regel wird Strafanzeige erstattet
- Fokus liegt auf Wiederherstellung der Geschäftsfähigkeit der Firma
- Hohes Bewusstsein für Risiko des Informationsabflusses

Phishing aus infiltriertem E-Mail-Account (**Mail-Spoofing**)

Technisch

- Infiltrierung von E-Mail-Accounts erfolgt häufig bei aus dem öffentlichen Netz zugänglichen E-Mail-Accounts
- Erfolgsfaktoren: (extrem) schwache Nutzer-Passwort-Kombinationen tlw. in Verbindung mit Social Engineering
- Häufig sind nur einzelne E-Mail-Accounts betroffen, nicht das eigentliche Firmennetz

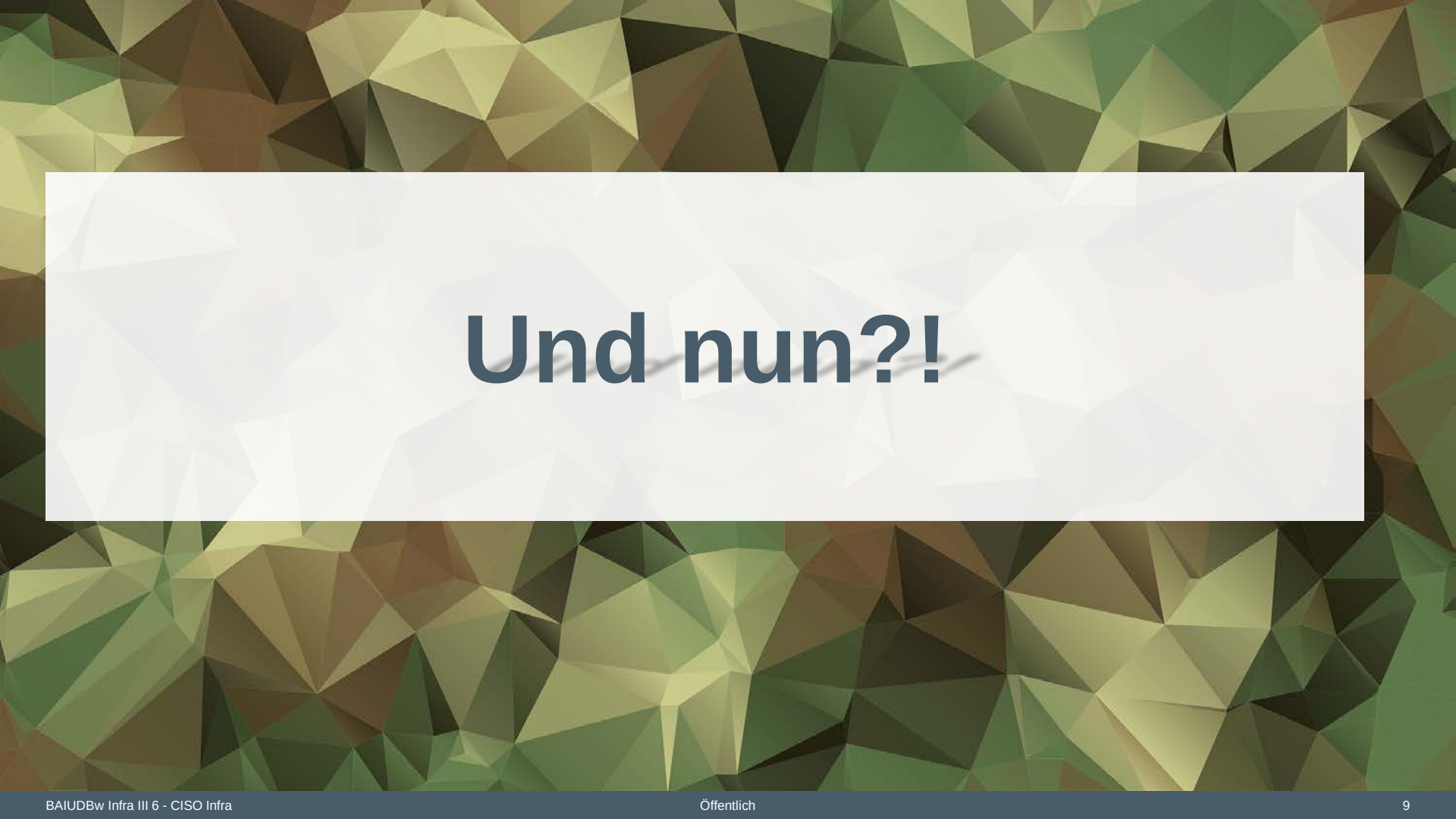
Reaktion

- Aufgrund der hohen Außenwirkung schnellere Reaktion des Betroffenen
- Häufig wird keine Strafanzeige erstattet
- Fokus liegt auf versandten Phishing-E-Mails
- Kein Bewusstsein für Risiko des Informationsabflusses aus dem E-Mail-Konto → *hier insbesondere Zugangsdaten zu Plattformen*

GEMEINSAMKEITEN DER ANGRIFFSARTEN

RANSOMWARE / MAIL-SPOOFING

- Das Hauptrisiko besteht im **Informationsabfluss**
- **Zugriff auf** die im infiltrierten System **gespeicherten Daten** besteht bei beiden Angriffsarten
- Bei Mail-Spoofing erhöht sich das Risiko eines Informationsabflusses dadurch, dass die Angreifer mit der **gestohlenen Identität** auftreten können.



Und nun?!

Projektgovernance

- **Klare Regeln** für die Projektarbeit und die Projektkommunikation inkl. Datenablage
- Festlegung und Einhaltung **Schutzbedarf** der Informationen
- Klare Festlegungen, welche Informationen vorüberwiegend und geführt werden → **Datensparsamkeit!**

Technischen Schutz etablieren

Awareness → **Bewusstsein** & **Kontrollen**

Was bedeutet das konkret? [1|3]

- Klären Sie zu Beginn des Projekts Sicherheitsfragen inkl. der konkreten Einstufung der Daten / Dokumente
 - ➔ für die Bundeswehr: Checkliste Sicherheit in Bauaufgaben
- Beachten Sie:

OFFEN ist nicht Öffentlich!

OFFEN ist Dienstgeheimnis / Geschäftsgeheimnis

- Jede **CDE** muss die **Mindestanforderungen des BSI für Cloud-Anwendungen** erfüllen

Was bedeutet das konkret? [2|3]

- Bei Einstufung der Datensache (VS-NfD^{*)}: CDE muss inklusive Clientrechner und dazugehöriger Verbindung VS-NfD-konform sein

Aktuell existiert keine CDE außerhalb von „Planerhaus“-Architekturen, die VS-NfD-konform ist!

^{*)} VS-NfD = Verschlusssache Nur für den Dienstgebrauch

Was bedeutet das konkret? [3|3]

Was also bei VS-NfD eingestuften Anteilen?

- **Inhaltlich:** Kein Unterschied zu offenen Maßnahmen
 - ➔ Informationsanforderungen gelten genauso
- **Organisatorisch und technisch:** Maßgaben zum Umgang mit VS-NfD einhalten (Merkblatt VS-NfD zur Verschlusssachenanweisung des Bundes)
 - **Bearbeitung** und **unverschlüsselte Ablage ausschließlich** in **VS-NfD freigegebenen Systemen**
 - **Austausch und Ablage** ausschließlich **verschlüsselt**

INFORMATIONSSICHERHEIT IN DER DIGITALEN ZUSAMMENARBEIT

WIE ES GELINGEN KANN



Vielen Dank für
Ihre Aufmerk-
samkeit!

Öffentlich