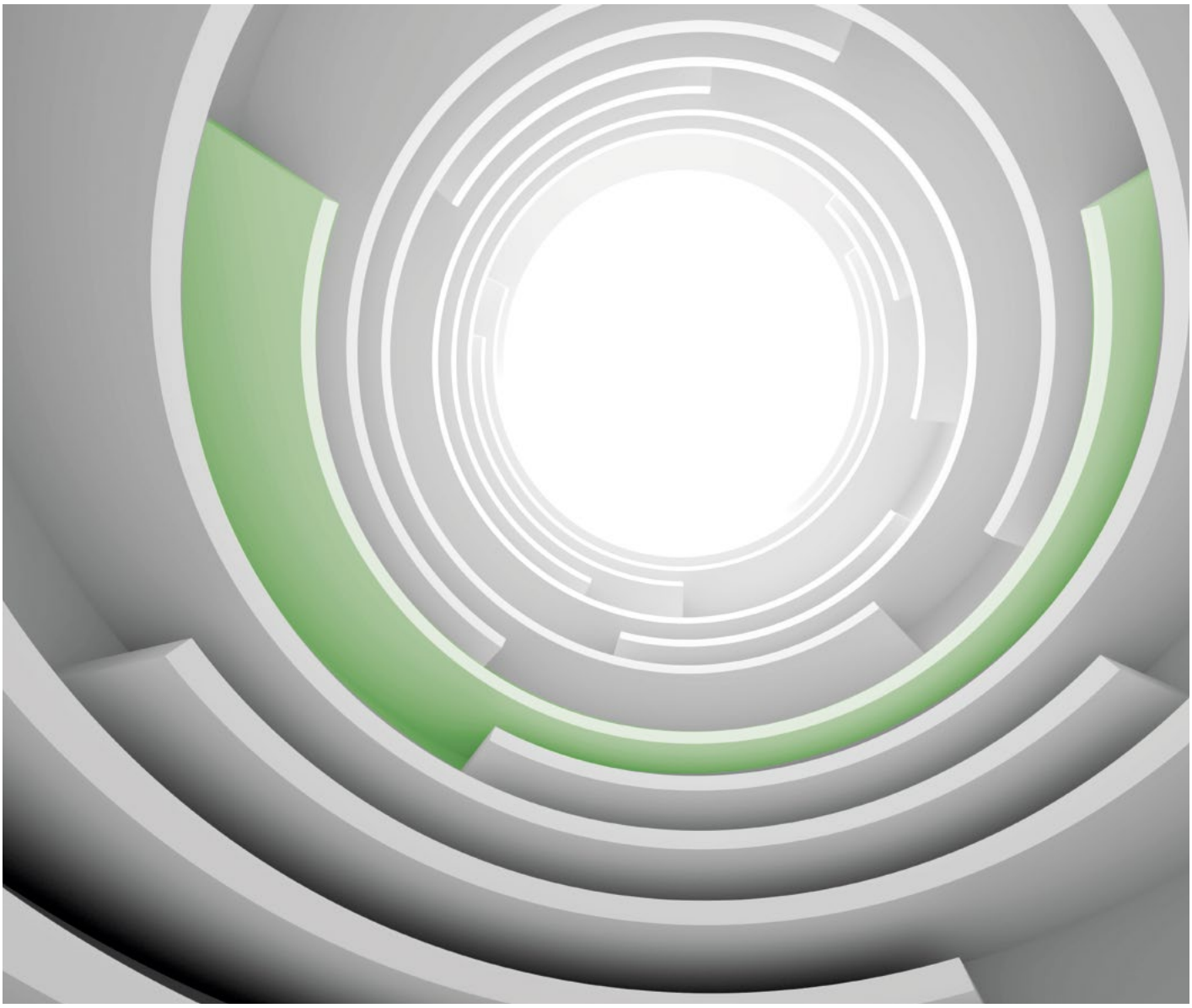
Deloitte.
Private



Operative Risiken im Mittelstand

Cyber Resilience: Stärkung der Responsefähigkeiten für den Ernstfall

Die Cyberbedrohungslage ist durch die russische Invasion in die Ukraine und die durch die westliche Staatengemeinschaft verabschiedeten Sanktionen massiv angestiegen, da sind sich alle Beobachter und das Bundesamt für Sicherheit in der Informationstechnik (BSI) einig. Unternehmen, staatliche Einrichtungen, Behörden und kritische Infrastruktur können mit hoher Wahrscheinlichkeit Ziele von verstärkten Cyberangriffen werden.

MAKING AN IMPACT THAT MATTERS since 1845

Was ist zu tun?

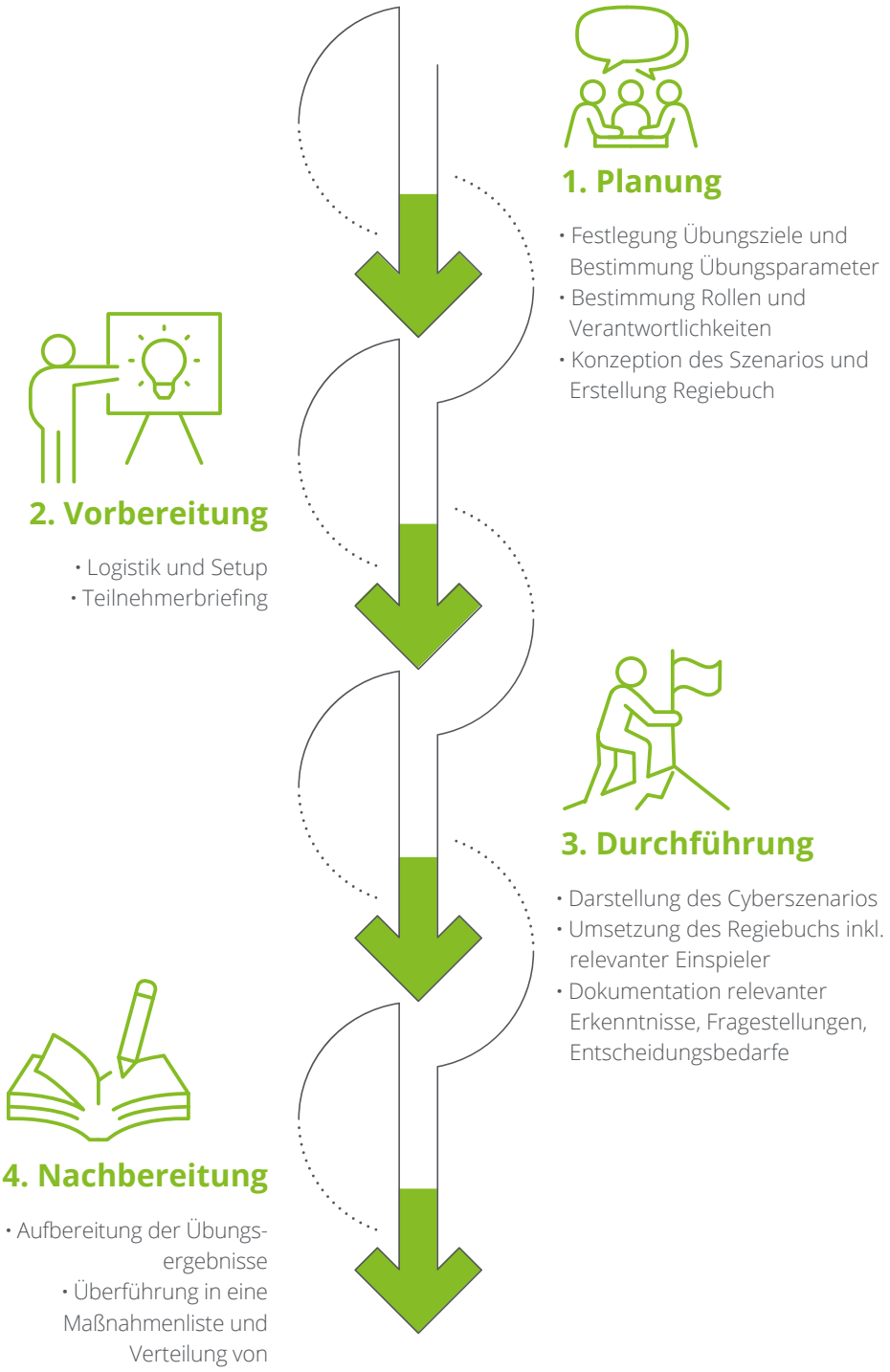
Die derzeit dringend empfohlenen Maßnahmen zur Erhöhung der IT-Sicherheit sind auch eine Frage der Personalkapazität, des Zugriffs auf technische Fähigkeiten und der schnellen Verfügbarkeit – kurz der Responsefähigkeiten der Organisation.

- Unterscheidung zwischen präventiven Sicherheitsmaßnahmen und dem Umgang mit dem Ernstfall
- Responsefähigkeit zum schnellen Umgang mit akuten Cyberbedrohungen oder konkreten Angriffen (Cyber Incident Response)
- **Wichtiges Ziel:** Herstellung von Handlungssicherheit und Reaktionsfähigkeit im Cybervorfall
- **Wie?:** Simulieren Sie den Ernstfall in einer theoretischen Krisenübung gemeinsam mit Ihren kritischen Geschäftsbereichen.

Einfach und effektiv: das Szenario Cyberangriff üben – Table Top Exercise

- Eine sofort und mit geringem Aufwand umsetzbare sowie gleichzeitig hoch effektive Maßnahme für Entscheidungsträger ist die Durchführung einer Krisensimulation im Format der Table Top Exercise.
- Relevante Stakeholder – Unternehmensführung, IT-Leitung, CFO, Kommunikation, Legal & Compliance, die wichtigsten BU Leads – kommen für den theoretischen Durchlauf eines ausgewählten Cyberszenarios zusammen.
- Sinnvoller Zeithorizont 2–4 Stunden (Workshop-Charakter)
- Optimal ist ein einfaches Regiebuch, nach dem Step-by-Step die Entwicklungen und Auswirkungen eines Cyberangriffs durchgesprochen werden.

Abb. 1 – Umsetzung einer Krisenübung



Welcher Mehrwert entsteht?

- Sensibilisierung der teilnehmenden Stakeholder durch Betroffenheit/Auseinandersetzung mit der Frage „Wie weitermachen ohne IT?“

- Transparenz über zu treffende Entscheidungen (welche im Nachgang zur Übung nochmals angemessen analysiert und mit Optionen vorbereitet werden können), Beispiele:

1. **Response-Fähigkeit:** Welche Kompetenzen und Fähigkeiten werden wie schnell benötigt (IT-Incident Response, Verknüpfung mit Retainerkonzept, IT-Forensic, Notfallmanagement, Krisenmanagement, Kommunikation, Rechtssupport) und wie können diese beschafft werden – mittels interner Optionen oder externer Dienstleister?

2. **Business Impact:** Welche ökonomischen Auswirkungen hat ein Abschalten der IT/OT? Welcher Impact entsteht bei Ausfall/Nichtverfügbarkeit kritischer IT-Anwendungen? Ausweichmöglichkeiten und Geschäftsfortführungsplanungen bzw. Wiederanlaufplanungen nach einem Cyberangriff

3. **Compliance:** Welche Compliance-Auswirkungen können relevant sein? (Datenschutz, gesetzlich/regulatorischen Regelungen, Sanktionen (z.B. bei Lösegeldzahlungen an Hackergruppen russischen Ursprungs), Vertragspflichten gegenüber Kunden und Zulieferern, Arbeitsrecht etc.)

4. **Krisenkommunikation:** Welche Stakeholder müssen kommunikativ betreut werden? (Belegschaft, Dienstleister/Zulieferer, Kunden, Öffentlichkeit, Presse, Behörden)

5. **Umgang mit Straftatbestand:** Welche Aufgaben übernehmen (Ermittlungs-)Behörden (LKA, BKA, Datenschutzbeauftragte der Länder)? Welche Meldepflichten sind in welchen Fristen einzuhalten?

6. **Business Continuity Management:** Wie steht es um vorhandene Notfallpläne? Wie ist deren Wirksamkeit einzuschätzen? Ist die Fortführung der kritischen Geschäftsaktivitäten gewährleistet?

7. **Abschalten von IT/OT:** Wie funktioniert eine sofortige Umstellung von digitalisierten zu manuellen Geschäftsabläufen?

8. **Fortführung der Unternehmensführung:** Welche Aufgaben der Unternehmensleitung und der relevanten Entscheidungsträger des bisherigen Alltags müssen neu priorisiert und/oder delegiert werden?

9. **Cyberversicherung:** Welche Deckung ist mit dem Cyberversicherer vereinbart? Wie ist mit einer möglichen Kriegsausschlussklausel umzugehen?

Krisenstabsraum

- Informationssammlung
- Lagebewertung
- Definition von Maßnahmen
- Krisenbewältigung

Beobachter

Kommunikation und Interaktion via Mail

Übungssteuerung

- Steuerung der Einspieler
- Simulation der Außenwelt
- Reaktionen auf Rückfragen des Krisenstabs

Unser Angebot **Preis: Ab 20K€** **Dauer: 5 bis 10 Tage**

Kontakte

Ralph Noll
Partner
Lead Cyber Incident Response & Forensic
Tel: +49 211 8772 2285
rnoll@deloitte.de

Michael Mueller
Partner
Offering Lead Crisis & Resilience
Tel: +49 30 25468 5225
micmueller@deloitte.de

Dr. Christine Wolter
Partner
Tax & Legal | Leiterin Deloitte Private
Tel: +49 69 75695 7025
cwolter@deloitte.de

Deloitte.
Private

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeiterinnen und Mitarbeiter liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 11/2023