16. Fachthemen-Forum von SuCoNetwork e.V.

Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten?

Dr. Brita Hohlmann, SuCoNetwork e.V.

2. November 2026

Die 10 wichtigsten Punkte:

1. Cyber Resilience erhält die Handlungsfähigkeit

Kurzbeschreibung: Cyber Resilience umfasst die Vorbereitung auf erfolgreiche Cyberangriffe. Im Forum stand das Zusammenspiel von IT, Fachbereichen und Geschäftsführung im Mittelpunkt, damit Organisationen Schäden begrenzen und ihren Betrieb kontrolliert wiederherstellen können.

Kernaussage: Bereiten Sie neben Prävention und technischer Abwehr auch die gemeinsame Bewältigung eines Angriffs vor.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – widerstandsfähige betriebliche Abläufe

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

2. Kleine Unternehmen sind bevorzugt angreifbar

Kurzbeschreibung: Automatisierte Angriffe suchen nach verwundbaren technischen Konstellationen. Die Referentin verglich das mit Schleppnetzfischen: Gerade kleinere Unternehmen können betroffen sein, ohne zuvor als besonders interessantes Einzelziel ausgewählt worden zu sein.

Kernaussage: Bewerten Sie die eigene Angriffsfläche anhand der eingesetzten Technik und ihrer Erreichbarkeit.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – Widerstandsfähigkeit kleinerer Unternehmen

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

3. Die gesamte Angriffsfläche im Blick behalten

Kurzbeschreibung: Zur unternehmensspezifischen Angriffsfläche zählen laut Folien auch Cloud-Dienste, ausgelagerte Systeme und über Datenaustausch verbundene Anwendungen. In der

Diskussion wurde davor gewarnt, durch externe Anbieter automatisch vollständige Sicherheit zu erwarten.

Kernaussage: Beziehen Sie externe Dienste und Schnittstellen in die Vorbereitung Ihres Krisenszenarios ein.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – verlässliche vernetzte Systeme

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

4. Sichere Kommunikationswege vorab vorbereiten

Kurzbeschreibung: Wenn Benutzerkonten gesperrt werden oder die gewohnte Kommunikationsplattform ausfällt, braucht die Organisation einen vorbereiteten Austauschweg. Der Vortrag fordert, nicht kompromittierte Kommunikation innerhalb des Unternehmens sowie mit Kunden und Lieferanten mitzudenken.

Kernaussage: Klären Sie vorab, wer über welche alternativen Kanäle erreichbar sein muss.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – Kommunikation im Krisenfall

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

5. Entscheidungen und Zuständigkeiten rechtzeitig klären

Kurzbeschreibung: Über Abschaltungen, interne Informationen und Behördenkommunikation sollte im Angriff nicht erst organisatorisch verhandelt werden. Die Folien nennen klare Entscheidungsbefugnisse und einen besetzten Krisenstab als Grundlagen einer koordinierten Reaktion.

Kernaussage: Ordnen Sie kritische Entscheidungen und Kommunikationsaufgaben vorab konkreten Rollen zu.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – koordinierte Reaktion auf Störungen

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

6. Einen tragfähigen Minimalbetrieb vereinbaren

Kurzbeschreibung: IT und Fachbereiche müssen gemeinsam klären, welche Leistungen bei einem längeren Ausfall möglich bleiben. Der Vortrag verbindet die technische Priorisierung mit der Frage, wie lange ein Minimalbetrieb operativ und finanziell durchhaltbar ist.

Kernaussage: Fragen Sie auch, auf welche Systeme Ihre Organisation gegebenenfalls wochenlang verzichten könnte.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – betriebliche Kontinuität

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

7. Die Wiederherstellung einzelner Backups üben

Kurzbeschreibung: Eine kontrollierte Teilübung zeigt, ob sich ein einzelnes System oder eine Anwendung aus einem Backup wiederherstellen lässt. Die Referentin empfiehlt dafür eine geschützte Umgebung und einen bewusst überschaubaren Einstieg.

Kernaussage: Prüfen Sie die Nutzbarkeit einer Sicherung durch eine kontrollierte Wiederherstellung.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – erprobte Wiederherstellbarkeit

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

8. Den Wiederanlauf fachlich freigeben

Kurzbeschreibung: Wiederhergestellte Anwendungen müssen mit passenden Datenständen zusammenarbeiten. Vortrag und Folien beschreiben den Wiederanlauf als Folge einzelner Inbetriebnahmen, bei denen technische Wiederherstellung, Prüfung der Daten und fachliche Freigabe aufeinander abgestimmt werden müssen.

Kernaussage: Legen Sie fest, wer eine wiederhergestellte Anwendung nach der Prüfung fachlich freigibt.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – verlässlicher Wiederanlauf

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

9. Geschäftsführungen über passende Netzwerke erreichen

Kurzbeschreibung: In der Diskussion wurde angeregt, Geschäftsführungen über IHKs und Industrieverbände anzusprechen. Der Hintergrund: Technisches Risikobewusstsein in der IT führt nach den geschilderten Erfahrungen nicht automatisch zu Aufmerksamkeit und Entscheidungen auf Leitungsebene.

Kernaussage: Diskussionsimpuls: Wählen Sie für die Ansprache von Geschäftsführungen auch deren vertraute berufliche Netzwerke.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – Wissen für widerstandsfähige Organisationen

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting

10. Mit einem konkreten Angriffsszenario beginnen

Kurzbeschreibung: Ein gemeinsam durchgespieltes Angriffsszenario übersetzt abstrakte Risiken in konkrete Fragen zu Erkennung, Kommunikation und Wiederanlauf. Der vorgestellte Coaching-Ansatz

beginnt beim vorhandenen Zustand und entwickelt daraus schrittweise Maßnahmen mit den beteiligten Teams.

Kernaussage: Wählen Sie ein Szenario aus und halten Sie daraus entstehende Maßnahmen und Rollenbedarfe fest.

SDG-Bezug: SDG 9 Industrie, Innovation und Infrastruktur – schrittweiser Aufbau von Resilienz

Zitat: „Man muss es durchdenken, man muss es durchsprechen." – Dr. Brita Hohlmann

Quelle: Cyber Resilience – Wie können sich Unternehmen gezielt auf eintretende Cyberangriffe vorbereiten? · 02.11.2026 · Dr. Brita Hohlmann, Dr. Hohlmann Management Consulting