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

Zusammenfassung

Cyber Resilience bedeutet, nach einem erfolgreichen Cyberangriff handlungsfähig zu bleiben und den Betrieb kontrolliert wiederherzustellen. Im 16. Fachthemen-Forum von SuCoNetwork e.V. am 2. November 2026 erläuterte Dr. Brita Hohlmann, wie insbesondere kleinere und mittlere Organisationen ihre Teams darauf vorbereiten können. Ihr Schwerpunkt lag auf dem Zusammenspiel von IT, Fachbereichen und Geschäftsführung unter begrenzten personellen und finanziellen Ressourcen.

- Prävention, technische Verteidigung und Bewältigung erfüllen unterschiedliche Aufgaben. Der Vortrag stellte die organisatorische Vorbereitung auf den Fall in den Mittelpunkt, dass Schutzmaßnahmen einen Angriff nicht verhindern.
- Unternehmensspezifische Szenarien machen Abhängigkeiten sichtbar: Auch Cloud-Dienste, ausgelagerte Systeme und Schnittstellen gehören zur betrachteten Angriffsfläche. In der Diskussion wurde vor einem unkritischen Vertrauen in externe Anbieter gewarnt.
- Entscheidungsbefugnisse, Krisenstab und alternative Kommunikationswege sollten vorab geklärt werden. Fachbereiche bestimmen mit, welcher Minimalbetrieb möglich ist und wie lange er wirtschaftlich durchgehalten werden kann.
- Kontrollierte Wiederherstellungsübungen einzelner Backups können technische Lücken aufdecken. Der vollständige Wiederanlauf verlangt zusätzlich abgestimmte Datenstände und fachliche Freigaben.
- Für mehr Aufmerksamkeit im Management schlugen Teilnehmende IHKs und Industrieverbände als Zugänge vor. Die Referentin stellte ein mit S+P Lion entwickeltes Cyber Incident Response Coaching als schrittweisen Einstieg vor.

Für die Praxis folgt daraus: Ein gemeinsam durchgespieltes Angriffsszenario kann konkrete Verbesserungen anstoßen und damit die Widerstandsfähigkeit von Organisationen im Sinne von SDG 9 stärken.

Cyber Resilience wächst durch gemeinsam vorbereitete Reaktionen

Wer entscheidet über das Abschalten von Systemen, wenn ein Cyberangriff erkannt wird? Wie erreicht das Unternehmen seine Beschäftigten, wenn die gewohnte Kommunikation ausfällt? Solche Fragen standen im 16. Fachthemen-Forum von SuCoNetwork e.V. am 2. November 2026 im Mittelpunkt. Dr. Brita Hohlmann zeigte, wie Unternehmen ihre Handlungsfähigkeit nach einem erfolgreichen Angriff vorbereiten können. Der Bezug zu SDG 9, Industrie, Innovation und Infrastruktur, ist konkret: Widerstandsfähige digitale Abläufe helfen Organisationen, ihre Leistungen auch unter schwierigen Bedingungen aufrechtzuerhalten und wiederherzustellen.

Warum gerade kleine Unternehmen betroffen sind

Hohlmann richtete den Blick besonders auf Organisationen mit knappen IT-Ressourcen. Die IT betreut dort den laufenden Betrieb und übernimmt zugleich Sicherheitsaufgaben. Gewachsene Systemlandschaften, Lieferantenportale und Cloud-Dienste erhöhen die Zahl der Abhängigkeiten. Die Folien beziehen deshalb auch ausgelagerte Systeme und über Datenaustausch verbundene Anwendungen in die Angriffsfläche ein.

Zur Einordnung automatisierter Angriffe nutzte der Vortrag das Bild des Schleppnetzfischens: Gesucht werden verwundbare technische Konstellationen. Ein Unternehmen muss dafür nicht zuvor als besonders interessantes Einzelziel ausgewählt worden sein. KI beschleunige nach Einschätzung der Referentin die Ausnutzung veröffentlichter Schwachstellen. In der Diskussion wurde entsprechend die Vorstellung hinterfragt, kleinere Unternehmen seien wegen ihrer Größe oder ihres Geschäftsmodells automatisch wenig gefährdet. Das Gegenteil ist der Fall. Für die eigene Vorbereitung ist deshalb entscheidend, welche Systeme erreichbar sind und welche Abläufe von ihnen abhängen.

Bewältigung ergänzt Prävention und technische Abwehr

Der Vortrag unterscheidet drei Handlungsfelder: Prävention, Verteidigung und Bewältigung. Zur Prävention gehören beispielsweise Schulungen und ein Informationssicherheitsmanagementsystem, kurz ISMS. Technische Abwehr und Monitoring sollen Angriffe erkennen und begrenzen. Die Bewältigung setzt dort an, wo ein Angriff dennoch erfolgreich ist und das Unternehmen seine Abläufe unter Krisenbedingungen organisieren muss.

Hohlmann betonte, dass umfassende Sicherheitsprojekte erhebliche interne Mitarbeit verlangen. Gerade bei knappen Ressourcen könne ein pragmatischer Einstieg über konkrete Szenarien helfen. Sie stellte dafür ein gemeinsam mit S+P Lion entwickeltes Cyber Incident Response Coaching vor. Es soll IT, Geschäftsführung und Fachbereiche auf ihr Zusammenspiel vorbereiten. Der Ansatz ergänzt bestehende Sicherheitsmaßnahmen. Die Folien beschreiben als Ziel eine koordinierte Reaktion, durch die Teams im laufenden Angriff auf vorbereitete Verantwortlichkeiten und Kommunikationswege zurückgreifen können.

Zuständigkeiten und Minimalbetrieb gemeinsam festlegen

Im Ernstfall braucht die IT klare Ansprechpartner und Entscheidungen. Wer darf Systeme abschalten? Wer informiert Beschäftigte, Kunden oder Lieferanten? Wer koordiniert die jeweils einschlägigen Meldungen an Behörden? Diese Aufgaben sollten vorab zugeordnet werden. Die konkreten Pflichten hängen von der Organisation und ihrem rechtlichen Umfeld ab; das Forum behandelte sie als Teil der individuellen Vorbereitung.

Auch die Kommunikation selbst gehört zum Szenario. Wenn Benutzerkonten gesperrt werden müssen oder die gewohnte Plattform nicht erreichbar ist, braucht das Team einen vorbereiteten, nicht kompromittierten Austauschweg. Die Geschäftsbereiche müssen zugleich klären, welche Leistungen im Minimalbetrieb möglich bleiben. Hohlmann schlug dafür eine ungewohnte Frage vor: Auf welche Systeme könnte man gegebenenfalls wochenlang verzichten? So werden Prioritäten und Abhängigkeiten greifbar. Dazu gehört die Frage, wie lange die Organisation diesen Zustand operativ und finanziell durchhalten kann. Ihre Aufforderung lautete: „Man muss es durchdenken, man muss es durchsprechen."

Wiederherstellung kontrolliert erproben

Ein vorhandenes Backup beantwortet noch nicht alle Fragen des Wiederanlaufs. Hohlmann empfahl kontrollierte Teilübungen: Ein einzelnes System oder eine Anwendung wird in einer geschützten Umgebung wiederhergestellt. Dabei lässt sich prüfen, ob benötigte Software und Zugänge verfügbar sind und die Sicherung tatsächlich nutzbar ist. Solche Übungen können überschaubar beginnen und konkrete Maßnahmen auslösen.

Die Folien beschreiben die vollständige Wiederherstellung als Folge vieler einzelner Inbetriebnahmen mit zunehmender Vernetzung der Datenflüsse. Dafür müssen Datenstände zusammenpassen und Anwendungen fachlich geprüft werden. Vorab ist deshalb auch festzulegen, wer eine wiederhergestellte Anwendung freigibt. Der Zeitbedarf betrifft das gesamte Unternehmen: Während die IT aufbaut und prüft, müssen Fachbereiche mit Einschränkungen arbeiten und die Geschäftsführung den weiteren Betrieb sichern.

Geschäftsführungen gezielt erreichen

Die Diskussion ergänzte den Vortrag um die Frage, wie das Thema im Management mehr Aufmerksamkeit bekommt. Teilnehmende berichteten, dass die IT die Gefahren häufig bereits sehe, während auf Leitungsebene die eigene Betroffenheit unterschätzt werde. Als mögliche Zugänge nannten sie IHKs und Industrieverbände. Das waren Vorschläge für die weitere Ansprache, keine bereits nachgewiesenen Kommunikationserfolge.

Ein weiterer Diskussionsbeitrag warnte vor trügerischer Sicherheit durch Hosting und Standardsoftware. Externe Dienste sollten daher in die eigene Betrachtung einbezogen werden. Als redaktioneller Praxistransfer lässt sich daraus ableiten, die Zusammenarbeit mit Anbietern im ausgewählten Krisenszenario ausdrücklich mit durchzuspielen.

Fazit

Cyber Resilience lässt sich vom vorhandenen Zustand aus schrittweise verbessern. „Es gibt für mich keinen schlimmen Zustand im Unternehmen", erklärte Hohlmann und plädierte dafür, mit den verfügbaren Möglichkeiten anzufangen. Ein sinnvoller erster Schritt ist, ein konkretes

Angriffsszenario gemeinsam zu besprechen und daraus Zuständigkeiten, Kommunikationswege und eine kontrollierte Teilübung abzuleiten. So wird erkennbar, was als Nächstes verbessert werden muss, damit die Organisation im Ernstfall handlungsfähig bleibt.