Selbst-Check: Wo steht meine Organisation?

So funktioniert der Selbstcheck:

- Setzen Sie bei jeder Frage, die Sie mit Ja beantworten können, ein Häkchen.
- Jede Frage, die sie mit Nein beantworten und daher nicht abhaken können, zeigt akuten Handlungsbedarf auf.
- Am Ende ergibt sich eine Einschätzung des aktuellen Stands.

1. Strategische Vorbereitung

1.1 Grundlagen

- ☐ Gibt es ein dokumentiertes Konzept für die Kommunikation in einer Cyberkrise?
- ☐ Ist klar definiert, wer kommuniziert und wer nicht?
- ☐ Werden die Kommunikationsstrategien regelmäßig überprüft und angepasst?

1.2 Verantwortlichkeiten

- ☐ Gibt es ein Krisenkommunikationsteam, das jederzeit einsatzbereit ist?
- ☐ Wissen alle relevanten Personen, welche Rolle sie im Ernstfall haben?
- ☐ Sind die Eskalationswege für Cybervorfälle eindeutig definiert?

2. Früherkennung und erste Kommunikation

2.1 Schnelle Reaktion

- ☐ Gibt es ein internes Meldesystem, um Vorfälle sofort zu kommunizieren?
- ☐ Sind Prozesse definiert, um innerhalb der ersten Stunde handlungsfähig zu sein?
- ☐ Wird bereits in der Frühphase einer Cyberkrise aktiv kommuniziert?

2.2 Interne Koordination

- ☐ Ist sichergestellt, dass alle internen Stakeholder (IT, Legal, PR, Vorstand) schnell zusammenkommen?
- ☐ Gibt es eine sichere Kommunikationsplattform für den Notfall?
- ☐ Werden alle Ebenen der Organisation (von der IT-Abteilung bis zur Geschäftsführung) sofort informiert?

3. Interne Kommunikation und Krisenmanagement

3.1 Mitarbeiterinnen und Mitarbeiter als erste Verteidigungslinie

- ☐ Wissen alle Mitarbeiterinnen und Mitarbeiter, wie sie sich bei einer Cyberkrise verhalten sollen?
- ☐ Gibt es einen vorbereiteten Kommunikationsplan für interne Updates?
- ☐ Wird regelmäßig in Schulungen und Sensibilisierung investiert?

3.2 Transparenz und Vertrauen

- ☐ Wird intern schnell und regelmäßig über den Status der Krise informiert?
- ☐ Gibt es eine Strategie, um Gerüchten und Fehlinformationen vorzubeugen?
- ☐ Sind Führungskräfte darauf vorbereitet, Mitarbeiterinnen und Mitarbeiter zu beruhigen und zu führen?

4. Externe Kommunikation und Reputationsschutz

4.1 Kommunikation mit Medien, Kunden und Öffentlichkeit

- ☐ Gibt es vorbereitete Krisenstatements und FAQs für verschiedene Szenarien?
- ☐ Wird vermieden, dass zu lange geschwiegen oder verharmlost wird?
- ☐ Existiert eine Social-Media-Strategie für Cyberkrisen?

4.2 Umgang mit kritischen Anfragen

- ☐ Sind Pressesprecher und Kommunikationsverantwortliche mediengeschult?
- ☐ Gibt es einen Plan für den Fall fehlerhafter Berichterstattung?
- ☐ Ist definiert, welche Kanäle im Krisenfall aktiv genutzt werden?

4.3 Krisenkommunikation und Rechtsabteilung

- ☐ Wird die externe Kommunikation mit Rechts- und Datenschutzexperten abgestimmt?
- ☐ Gibt es vorbereitete Maßnahmen, um sich vor Haftungsrisiken zu schützen?
- ☐ Ist klar, wann und wie betroffene Kunden informiert werden müssen (Meldepflichten)?

5. Kommunikation mit Angreifern?

Falls eine Erpressung bzw. ein Ransomware-Angriff vorliegt:

- ☐ Gibt es eine klare Entscheidung, ob mit Angreifern kommuniziert wird oder nicht?
- ☐ Wurden mögliche Verhandlungsszenarien vorab analysiert?
- ☐ Ist ein Plan vorhanden, um externe Berater oder Behörden rechtzeitig einzubinden?

6. Nachbereitung und Lessons Learned

- ☐ Wird die gesamte Krisenkommunikation nach der Krise analysiert?
- ☐ Gibt es Prozesse, um aus Fehlern zu lernen und die Kommunikation weiterzuentwickeln?
- ☐ Werden Mitarbeiterinnen und Mitarbeiter und Führungskräfte nach einer Cyberkrise aktiv eingebunden, um Verbesserungsvorschläge zu sammeln?

Ergebnis: Wo steht meine Organisation?

Mehr als 80 Prozent Ja-Antworten: Sehr gut! Die Organisation ist stark aufgestellt.

50–79 Prozent Ja-Antworten: Sie haben eine solide Basis, es gibt aber noch einige Lücken. Diese sollten zeitnah geschlossen werden.

Weniger als 50 Prozent Ja-Antworten: Hohes Risiko! Die Cyberkrisenkommunikation ist nicht ausreichend vorbereitet.

Nächster Schritt:

Alle Nein-Antworten sind eine To-do-Liste:

Schritt 1: Erstellen Sie eine Prioritätenliste und entwickeln Sie einen konkreten Plan zur Verbesserung.

Schritt 2: Wiederholen Sie den Test regelmäßig, um den Fortschritt zu überprüfen.

Mehr Informationen zu Hintergründen und zur Anwendung finden Sie im Buch:

Kommunikation in der Cyberkrise: Sprach- und handlungsfähig im IT-Ernstfall

Isabelle Ewald, Alexander Schinner

ISBN-10: 3960092679
ISBN-13: 978-3960092674