Barracuda
Your journey, secured.

# Checkliste für Cyber-Resilienz

Die folgende Checkliste für Cyberresistenz stützt sich auf das Cybersicherheits-Framework des US National Institute of Standards and Technologies (NIST).

| ZIEL | STRATEGISCHE AUSRICHTUNG FÜR FÜHRUNGSKRÄFTE – WAS SIE WISSEN MÜSSEN | FORTSCHRITT |
|---|---|---|
| VORBEREITUNG | **Organisieren**<br>• Einhaltung der gesetzlichen Auflagen<br>Welche gesetzlichen Vorschriften und Compliance-Verpflichtungen haben Sie in jedem der Märkte, in denen Sie tätig sind? | ☐ |
| | • Einbindung und Zuständigkeit des Managements<br>Wer im Führungsteam muss an Entscheidungen zu Cyber-Resilienz und zu Risiken beteiligt sein? | ☐ |
| | • Cyberversicherung<br>Welche Art von Versicherung benötigen Sie und sind Sie bereit bzw. in der Lage, in diese zu investieren? | ☐ |
| | **Identifizieren**<br>• Asset-Management<br>Welche Assets haben Sie, wo befinden sie sich, wer hat Zugriff darauf? Was sind Ihre wichtigsten Ressourcen, um die Geschäftskontinuität und den Betrieb aufrechtzuerhalten? | ☐ |
| | • Risikomanagement und Strategie<br>Welches sind Ihre am stärksten gefährdeten Assets? Welchen Risiken sind diese ausgesetzt? Wie groß sind die möglichen Auswirkungen eines Angriffs hinsichtlich der Schäden, Störungen oder Verluste? | ☐ |
| STANDHALTEN | **Schützen**<br>• Sicherheitsprozesse, -richtlinien und -technologien<br>Wie können Sie Assets, Infrastruktur und Mitarbeiter im Rahmen Ihrer verfügbaren Ressourcen am besten schützen? | ☐ |
| | • Schulungen zum Thema Cybersicherheit<br>Wie schulen und unterstützen Sie Ihre Mitarbeiter? | ☐ |
| | • Wartung und Kontrolle – Patchen usw.<br>Sind die grundlegenden Sicherheitsmaßnahmen vorhanden? Patching, robuste Authentifizierung und Zugriffskontrollen (Multifaktor-Authentifizierung/Zero Trust) usw.? | ☐ |
| | **Erkennen**<br>• Technologien und Verfahren zur Erkennung<br>Können Ihre Sicherheitssysteme neue und neu aufgetretene Bedrohungen erkennen und blockieren? | ☐ |
| | • Security Operations Center<br>Ist Ihre Sicherheitsüberwachung zuverlässig und kontinuierlich? Können Sie den gesamten IT-Bereich rund um die Uhr überwachen und managen? Haben Sie Zugang zu den Tools, den Kompetenzen und dem Personal, um Warnsignale und Anomalien zu untersuchen? | ☐ |
| REAGIEREN | **Schadensbegrenzung**<br>• Planung und Reaktionsprozesse bei Vorfällen<br>Haben Sie einen Incident Response-Plan, der für das gesamte Unternehmen gilt? Wird dieser regelmäßig getestet und ist auf dem neuesten Stand? Wie können Sie Zwischenfälle eindämmen und neutralisieren? Welche Dauer der Ausfallzeiten können Ihre kritischen Systeme aushalten? Können Sie bei Bedarf auf manuelle Prozesse zurückgreifen? Falls Ihre Kunden ebenso davon betroffen sind, wie hoch ist der vereinbarte Servicelevel? Befindet sich Ihr System On-Premises oder in der Cloud? (Handelt es sich um ein Security-as-a-Service (SaaS) Unternehmen, ein Geschäftssystem usw.?) Wen müssen Sie im Hinblick auf die Compliance informieren und wann? | ☐ |
| | • Interne und externe Kommunikation | ☐ |
| | • Analyse von Vorfällen und Schadensbegrenzung | ☐ |
| WIEDERHERS-TELLUNG | **Wiederherstellen**<br>• Recovery-Planung<br>Haben Sie einen Geschäftskontinuitätsplan/Disaster Recovery Plan? Haben Sie bei Ihrem Cloud-Anbieter eine „Hohe Verfügbarkeit“ eingerichtet? Benötigen Sie Unterstützung durch Dritte, um alle Lücken aufzudecken und zu schließen? | ☐ |
| | • Interne und externe Kommunikation | ☐ |
| | • Verbesserungen<br>Welche Lektionen haben Sie gelernt? Welche Schritte unternehmen Sie/sollten Sie unternehmen, um Ihre Sicherheit zu erhöhen? | ☐ |