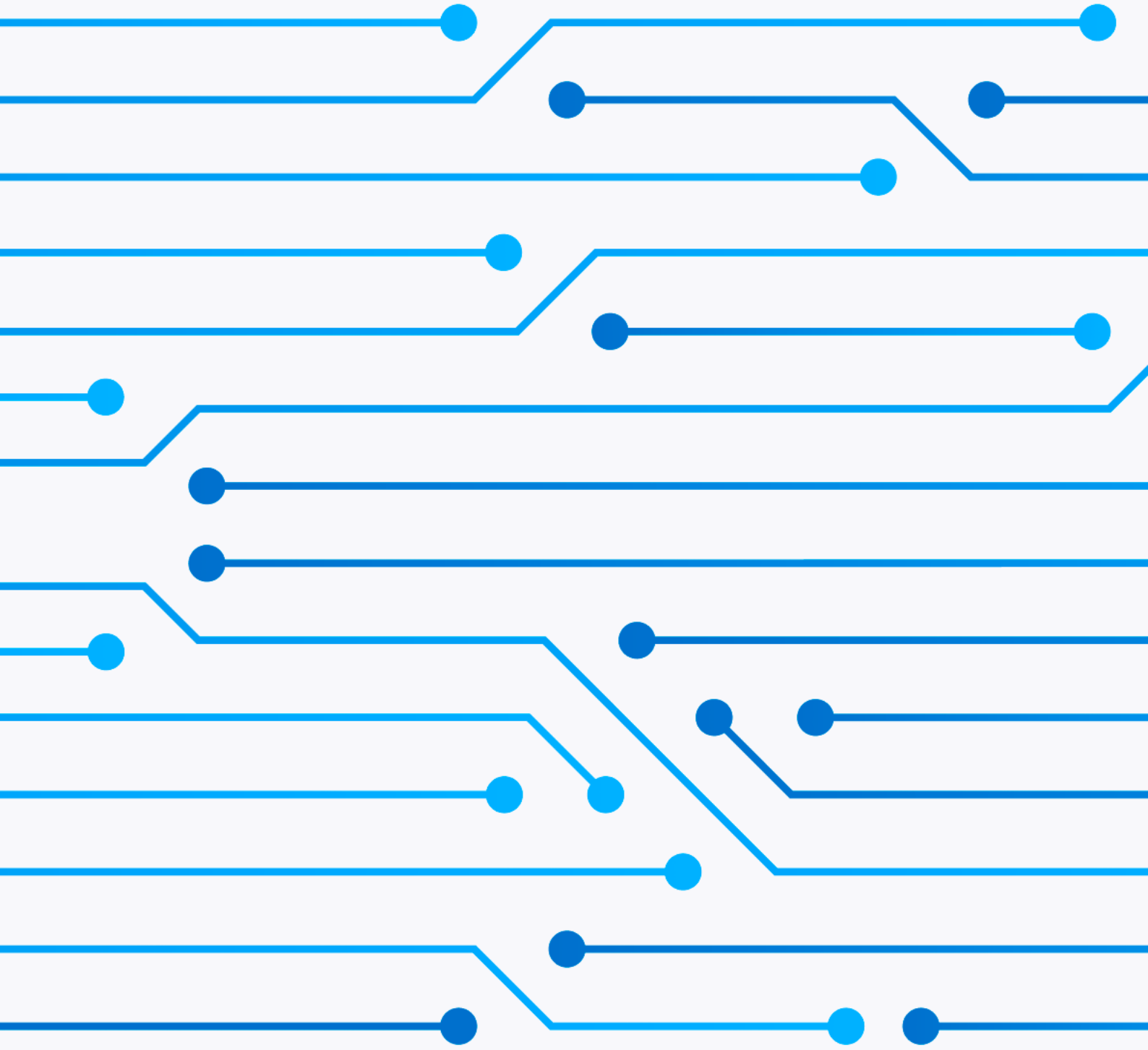
perseus.

Notfallplan für den Cybersicherheitsvorfall

Schritt für Schritt auf den Notfall vorbereiten und reagieren



Inhalt

Inhalt

Inhalt

Inhalt

01 | Einleitung

Jeder Notfall ist einzigartig und benötigt daher eine einzigartige Bewertung wie auch Vorgehensweise. Dieser Plan gibt ein grobes Gerüst vor und ist individuell für Ihr Unternehmen gestaltbar – unabhängig von bestimmter Hardware, Betriebssystemen, Protokollen oder Anwendungen.

1.1 Wozu dient der Plan?

Dieser Plan dient zur Vorbereitung auf den Notfall und als Handlungsorientierung im Notfall. Er soll das Notfallmanagement in Ihrem Unternehmen unterstützen: Notfälle definieren und beurteilen, Beteiligte identifizieren und Prozesse kreieren.
Der Notfallplan soll dabei unterstützen, weitere Schäden wie den Verlust von Betriebsgeheimnissen und Reputation zu vermeiden. Er soll dabei helfen, die Betriebsfähigkeit zu sichern oder wiederherzustellen und rechtliche Anforderungen zu erfüllen (IT-SicherheitsG, DSGVO).

1.2 Wie nutze ich diesen Plan?

Arbeiten Sie sich Schritt für Schritt durch unseren Plan. Wichtig ist, dass Sie im Vorfeld die Punkte unter „3. Vorbereitung auf den Notfall" bearbeiten. Dadurch wird der allgemein gehaltene Plan individuell an die Bedürfnisse Ihres Unternehmens angepasst. Auf diese Weise haben Sie eine erste Übersicht der wichtigen Informationen im Notfall.
Bitte beachten sie, dass wir keine Gewähr für Vollständigkeit, Aktualität und Richtigkeit des Planes übernehmen.

1.3 Exkurs: Wie lasse ich es erst gar nicht zu einem Notfall kommen?

Ebenso wichtig wie ein effektiver und verständlicher Notfallplan ist die Prävention. Indem Sie ein IT-Sicherheitskonzept mit verständlichen Richtlinien und regelmäßigen Übungen unternehmensweit etablieren, sorgen Sie dafür, dass ein Angriff auf Ihr Unternehmen so unwahrscheinlich wie möglich wird.

1.3.1 IT-Sicherheitsrichtlinien und IT-Sicherheitskonzept

Schaffen Sie ein umfassendes IT-Sicherheitskonzept für das gesamte Unternehmen (umfangreiche Informationen zum Thema „Notfallmanagement" finden Sie im BSI Standard 100-4). Etablieren Sie in diesem Rahmen verständliche Richtlinien zu Themen wie der Nutzung privater Endgeräte, dem Umgang mit E-Mails, Passwort-Sicherheit, Arbeitsplatzsicherheit, sicherem Surfen im Netz, Home Office, Sicherheits-Updates, Patch-Management, Firewall – eine erste Orientierung finden Sie und Ihre Mitarbeitenden in unserem Cybersicherheits-Training.

Hier ist Platz für Anmerkungen und um interne Richtlinien als Link o. ä. einzufügen.