Resilienz-Analyse

Standortbestimmung, Handlungspotenziale, Maßnahmen

Cyber-Angriffe stellen einen großen Risikofaktor für Unternehmen und Institutionen dar. Die Schäden sind vielfältig — von Informations- und Datenverlusten, über Arbeitsausfälle bis hin zu Reputationsverlusten. Es gilt, diese Risiken zu minimieren. Um Prozesse und Informationen zu schützen, ist es notwendig, die Informationssicherheit einer Bestandsanalyse zu unterziehen.

Dabei stehen folgende Fragen im Mittelpunkt:

- Wie gut ist Ihr Unternehmen/Ihre Institution geschützt?
- Ist Ihre Organisation IT-Security konform aufgestellt?

Die Resilienz-Analyse liefert Ihnen Antworten zu diesen und weiteren Fragen. Sie ist Nachweis im Falle des Eintritts, dass Sie alle notwendigen Maßnahmen zum Schutz Ihrer Organisation umgesetzt haben.

Nutzen Sie die Resilienz-Analyse für Ihre Standortbestimmung und um die richtigen, notwendigen Maßnahmen zu identifizieren sowie priorisiert umzusetzen!

Ziele & Ergebnis der Resilienz-Analyse

Mit der Resilienz-Analyse hat bzw. kennt Ihre Organisation:

+ ein **klares dokumentiertes Bild** über Fachverfahren, Prozesse und Abläufe
+ eine Zuordnung, welche IT-Unterstützung den Fachverfahren unterliegen
+ seine **verwaltungs-/geschäftskritischen Fachverfahren & Prozesse**
+ die Anforderungen an die **Service Level** der unterstützenden IT
+ eine Bewertung über die **IT-Resilienz**
+ eine Übersicht von möglichen **Verbesserungspotentialen**
+ Aussagen zur Vorgehensweise und IT-Unterstützung beim **Ausbau der Digitalisierung** von Fachverfahren
+ eine Bewertung zur Situation und ggf. Verbesserungspotentiale für das **Notfall- und Krisenmanagement**
+ Vorhaben und Projekte, die dem Organisationsverschulden entgegenwirken

Vorgehen und Ablauf der Resilienz-Analyse

01 Analyse der Prozesse und Verfahren: Analyse der Organisationsstruktur +++ Bestandsaufnahme der Prozesse +++ Prüfung der Dokumentation +++ Workshop mit den Fachverantwortlichen zum „Leben & Arbeiten im Prozess“

02 Zuordnung von IT zur Systemunterstützung von Verfahren: Erhalten Sie Antworten auf Fragen, wie: Welche Services und Anwendungen sind bestandsführend? +++ Wo und wie ist das Berechtigungsmanagement organisiert? +++ Unterliegen die Berechtigungen der Prozessanforderung? +++ Wie wichtig sind die Daten für den Geschäftsbetrieb?

03 Business Impact Analyse: Auswirkungen von Nichtverfügbarkeiten auf den Geschäfts- und Verwaltungsbetrieb +++ SLAs der Anwendungen u. Services +++ Auswirkungen einer Nichtverfügbarkeit +++ Ersatzszenarien zur Aufrechterhaltung des Geschäftsprozesses

04 Anforderungen an die unterstützende IT der Fachverfahren & Prozesse: Eindeutige Leistungsbeschreibung der IT-Anwendungen und Komponenten +++ Grundsätzliche Regelung zur Leistungserbringung +++ Jegliche Änderungen an der IT müssen prozessgeführt, genehmigt und getestet sein. +++ Definition in SLAs und Servicebeschreibungen

05 Adaption der Anforderungen & angewandte IT-Resilienz: ISO 27001-konforme Prüfung des Härtegrades von IT-Verbund und interagierenden Werten +++ Security Check +++ OSINT-Analyse +++ Penetration Tests +++ Aufzeigen von Verbesserungspotentialen

06 Analyse Business Continuity (BCM) und Krisenmanagement: Eindeutige Regelungen & Abläufe +++ Erreichbarkeiten +++ Notfallübungen +++ Handouts für Mitarbeitende +++ Service-Continuity-Pläne als dokumentierte Information

07 Maßnahmenempfehlung und Folgeschritte: Die Fülle an Details der Ergebnisse sind zu klassifizieren und zu priorisieren. Sie erhalten einen umfassenden Ergebnisbericht der auf Ihre Anforderungen in Bezug auf die Informations- und Cybersicherheit eingeht. +++ Setzen Sie nicht alles mit einmal um. +++ Fokussieren Sie sich auf die wichtigsten Themen. +++ Betreiben Sie eine echte Nachverfolgung der Feststellungen. +++ Denn resiliente Organisationen und Landschaften minimieren potenziellen Schaden.

Die Kosten für unsere Resilienz-Analyse starten bei 12.000 Euro. Die genauen Kosten für Ihre Resilienz-Analyse ermitteln wir gern individuell für Sie. Sprechen Sie uns an!

Ihr Kontakt: Wir beraten Sie gern. | Telefon +49 800 7000 585* | kontakt@gisa.de | www.gisa.de * kostenfrei im dt. Festnetz