SELBSTEINSCHÄTZUNG IHRER CYBERRESILIENZ:

Bewerten Sie jede Frage auf einer Skala von 1 bis 5.
***1 = Stimme überhaupt nicht zu** und **5 = Stimme vollständig zu**.*
Addieren Sie am Ende die Punktzahlen, um Ihre Gesamtbewertung zu erhalten.

1. SICHERHEITSBEWUSSTSEIN:

Wie oft werden Ihre Mitarbeiter in Bezug auf aktuelle Cyberbedrohungen und Best Practices geschult?

☐ *Selten bis gar nicht* [1] | ☐ *Gelegentlich* [2] | ☐ *Durchschnittlich* [3] | ☐ *Häufig* [4] | ☐ *Regelmäßig und intensiv* [5]

.....

2. NOTFALLVORBEREITUNG:

Haben Sie einen gut dokumentierten Notfallwiederherstellungsplan für den Fall eines Cyberangriffs?

☐ *Nein, gar nicht* [1] | ☐ *Ja, aber er ist veraltet oder unvollständig* [2] | ☐ *Ja, aber er wurde vor langer Zeit erstellt* [3] | ☐ *Ja, er wurde vor Kurzem überarbeitet* [4] | ☐ *Ja, er ist aktuell und umfassend* [5]

.....

3. DATENVERSCHLÜSSELUNG:

Werden sensible Daten und Kommunikation innerhalb Ihres Unternehmens verschlüsselt?

☐ *Nie* [1] | ☐ *Selten* [2] | ☐ *Gelegentlich* [3] | ☐ *Häufig* [4] | ☐ *Immer* [5]

.....

4. NETZWERKSICHERHEIT:

Wie oft werden Sicherheitsüberprüfungen und Penetrationstests für Ihre Netzwerke und Systeme durchgeführt?

☐ *Nie* [1] | ☐ *Selten* [2] | ☐ *Jährlich* [3] | ☐ *Halbjährlich* [4] | ☐ *Vierteljährlich oder öfter* [5]

.....

5. REGELMÄSSIGE AKTUALISIERUNGEN:

Werden Software, Betriebssysteme und Sicherheitspatches regelmäßig und zeitnah aktualisiert?

☐ *Selten oder nie* [1] | ☐ *Gelegentlich* [2] | ☐ *Meistens* [3] | ☐ *Fast immer* [4] | ☐ *Immer* [5]

6. ZUGRIFFSKONTROLLE:

Verfügen Sie über strenge Zugriffskontrollen für Ihre IT-Ressourcen und Daten?

☐ Nein, gar nicht [1] | ☐ In begrenztem Umfang [2] | ☐ Teilweise [3] | ☐ Überwiegend [4] | ☐ Vollständig [5]

7. EXTERNE PARTNERSCHAFTEN:

Werden auch die Sicherheitspraktiken und -standards Ihrer externen Partner überprüft?

☐ Nie [1] | ☐ Selten [2] | ☐ Gelegentlich [3] | ☐ Meistens [4] | ☐ Immer [5]

8. INCIDENT RESPONSE:

Haben Sie klare Verfahren für den Umgang mit Cyberangriffen und Datenschutzverletzungen?

☐ Nein, nicht vorhanden [1] | ☐ Ja, aber sie sind nicht ausreichend [2] | ☐ Ja, teilweise [3] | ☐ Ja, gut etabliert [4] | ☐ Ja, sehr robust [5]

9. RISIKOBEWERTUNG:

Wird regelmäßig eine umfassende Bewertung Ihrer IT-Risiken durchgeführt?

☐ Nie [1] | ☐ Selten [2] | ☐ Gelegentlich [3] | ☐ Jährlich [4] | ☐ Mehrmals im Jahr [5]

10. MITARBEITERENGAGEMENT:

Sind Ihre Mitarbeiter aktiv in die Cyberresilienz-Strategie Ihres Unternehmens eingebunden?

☐ Nein, überhaupt nicht [1] | ☐ Wenige sind involviert [2] | ☐ Einige sind involviert [3] | ☐ Die meisten sind involviert [4] | ☐ Alle sind aktiv beteiligt [5]

IHRE PUNKTZAHL

INTERPRETATION DER PUNKTZAHL:

10-20 Punkte: *Niedrige Cyberresilienz, Verbesserungsbedarf*

21-30 Punkte: *Mittlere Cyberresilienz, einige gute Praktiken, aber Verbesserungspotenzial*

31-40 Punkte: *Gute Cyberresilienz, solide Praktiken und Vorbereitung*

41-50 Punkte: *Hohe Cyberresilienz, starke Sicherheitsmaßnahmen und Bereitschaft*

Wir helfen Ihnen, Ihre Cyberresilienz zu verbessern. Jetzt Kontakt aufnehmen mit netlogix IT-Services!