ViCoTec
IT-SICHERHEIT & DATENSCHUTZ

Ole

IT-RISIKO-REPORT

Muster GmbH

DAS ERGEBNIS

›Es ist fast geschafft

67/100

Aktueller Stand
16.04.2024

Ole – IT-Risiko-Report

Dieser Report lässt Sie IT-Gefährdungen erkennen, Maßnahmen ergreifen und etabliert einen kontinuierlichen Verbesserungsprozess. Richtig umgesetzt bietet er Ihnen umfassenden Schutz vor IT- und Datenschutzgefahren, spart Ihnen langfristig Kosten, schränkt Haftungsrisiken ein und ist unkompliziert und direkt einsetzbar.

›Ein ganz großes Lob
Es sind aktuell keine Maßnahmen erforderlich.

›Es ist fast geschafft
Diese Empfehlungen sollten im Laufe der nächsten Monate umgesetzt werden.

›Auf dem Weg
Maßnahmen sollten zeitnah umgesetzt werden.

›Lassen Sie es uns jetzt anpacken
Maßnahmen müssen umgehend umgesetzt werden.

Bearbeitet:

Thorsten Brendel	17.04.2024

ViCoTec

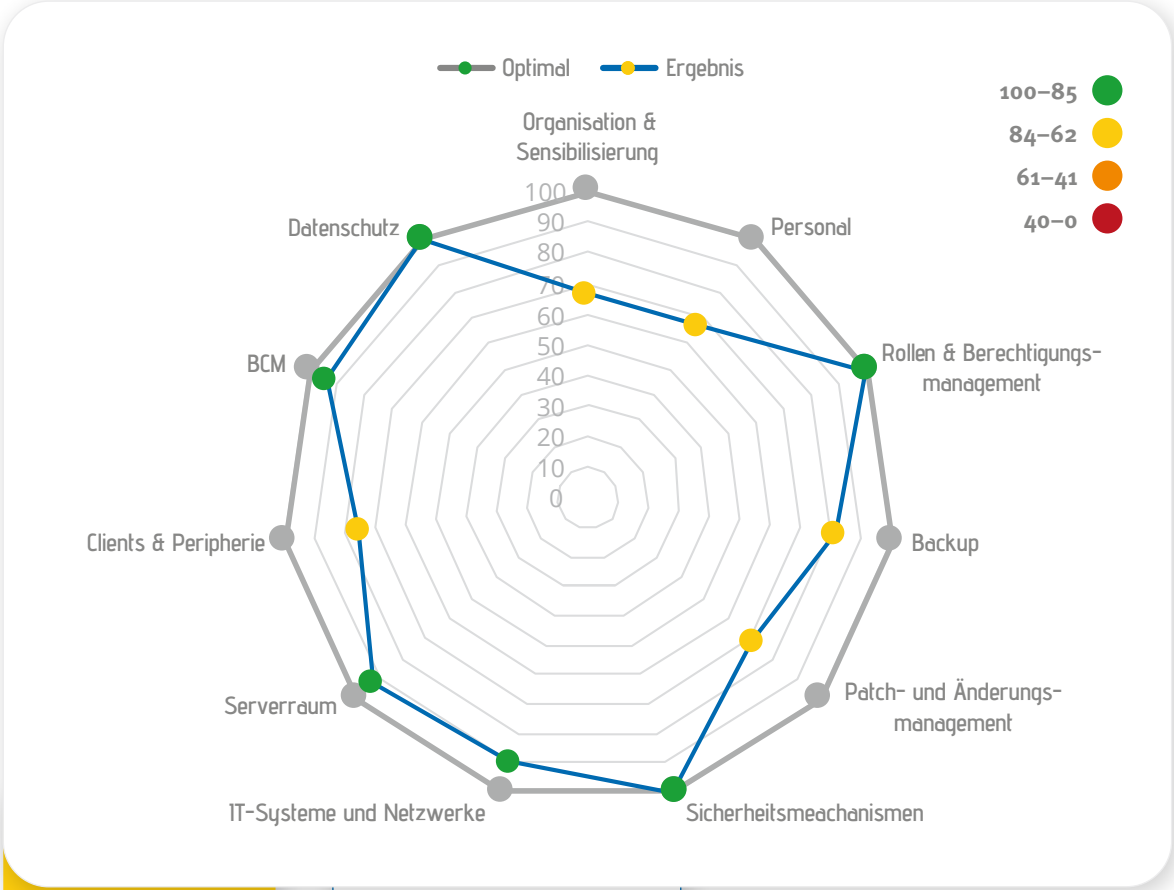
Geschäftsführungs-**bericht**

OLO

Der Bericht beleuchtet 11 Themenbereiche Ihrer IT und zeigt Ihnen die Gefährdungspotenziale.

ACHTUNG: Der Gesamtscore kann niemals höher sein als der schlechteste Einzelscore.

Das Ergebnis der **Risiko-Bewertung**



Aktueller Stand
16.04.2024
Version 1.0

Vorheriger Stand
-
Version -

OLK

›Es ist fast geschafft

67

Dringende Maßnahmen
IT-Sicherheit

1 Backup

Wie überprüfen Sie, ob die externe Datensicherung funktioniert hat und ob die Daten vollständig sind?

Erstellung und Sicherung von „auf Funktion geprüfte Datensicherungen“.

2 Organisation & Sensibilisierung

Wie stellen Sie sicher, dass alle Firmenangehörigen mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten identifizieren können?

Sicherer Umgang mit der IT durch alle Firmenangehörigen (bspw.: Erkennung von Phishing-Mails).
Jährliche Schulung der Mitarbeiter im Bereich Datenschutz und IT-Sicherheit.

3 Organisation & Sensibilisierung

Gibt es eine Leitlinie zur Informationssicherheit in Ihrem Unternehmen?

Implementierung einer Leitlinie zum Thema Informationssicherheit.

Dringende Maßnahme
Datenschutz

! Datenschutz

Keine dringenden Maßnahmen mit hoher Priorität erforderlich.

Veränderungen
seit dem letzten Report

Maßnahmen

	THEMENBEREICH	*LEITFRAGE*	HANDLUNGSEMPFEHLUNG/UMSETZUNGSHILFE
	HÖCHSTE PRIORITÄT DIE MASSNAHMEN DER HÖCHSTEN PRIORITÄT SOLLTEN SOFORT UMGESETZT WERDEN. DIE ZUGEHÖRIGEN GEFÄHRDUNGEN KÖNNEN EXISTENZBEDROHEND SEIN.		
1	Backup	*Wie überprüfen Sie, ob die externe Datensicherung funktioniert hat und ob die Daten vollständig sind?*	Erstellung und Sicherung von „auf Funktion geprüfte Datensicherungen“.
1	Organisation & Sensibilisierung	*Wie stellen Sie sicher, dass alle Firmenangehörigen mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten identifizieren können?*	Sicherer Umgang mit der IT durch alle Firmenangehörigen (bspw.: Erkennung von Phishing-Mails). Jährliche Schulung der Mitarbeiter im Bereich Datenschutz und IT-Sicherheit.
1	Organisation & Sensibilisierung	*Gibt es eine Leitlinie zur Informationssicherheit in Ihrem Unternehmen?*	Implementierung einer Leitlinie zum Thema Informationssicherheit.
1	IT-Systeme und Netzwerke	*Gibt es eine Risikoanalyse Ihrer zentralen Prozesse, der Hardware und der Software?*	Eine Risiko- und Chancenanalyse der aufgestellten Assets (Kronjuwelen) im Unternehmen um die einzelnen Risiken und Chancen zu bewerten.
	SEHR HOHE PRIORITÄT MASSNAHMEN VON SEHR HOHER PRIORITÄT SOLLTEN NACH 4–8 WOCHEN BEHOBEN WORDEN SEIN.		
2	Organisation & Sensibilisierung	*Angenommen, Sie hätten einen IT-Sicherheitsvorfall in Ihrem Unternehmen. Haben Sie klar geregelt, wie sich Beschäftigte verhalten und wem sie was und wann in welcher Form mitteilen müssen, damit der Vorfall zügig und fachgerecht bearbeitet werden kann? Falls ja, bitte erläutern Sie das näher.*	Erstellung eines dokumentierten Notfallplans, der allen Beschäftigten im Unternehmen zur Verfügung gestellt wird.
2	Organisation & Sensibilisierung	*Wer kümmert sich darum, dass Beschäftigte die Verhaltensweisen bei IT-Notfällen kennen und beachten?*	Im Rahmen der Sensibilisierungsmaßnahmen (Schulungen) wird der IT-Notfallplan besprochen und die zuständige verantwortliche Person vorgestellt.
2	Personal	*Gibt es einen geordneten Prozess zum Ausscheiden von Mitarbeitenden?*	Off-Boarding Prozess beim Ausscheiden von Mitarbeitenden . Checkliste auf Vollständigkeit überprüfen (bspw. BSI-Veröffentlichung „Ausscheiden von Mitarbeitenden – Checkliste“). Dies gilt gleichermaßen für interne wie externe Mitarbeitende.
2	BCM	*Existieren Definition von Sicherheitsvorfällen für die Mitarbeiter?*	Sensibilisierung der Mitarbeiter bezüglich der Einordnung von Sicherheitsvorfällen und die Früherkennung solcher.

	THEMENBEREICH	*LEITFRAGE*	HANDLUNGSEMPFEHLUNG/UMSETZUNGSHILFE
	HOHE PRIORITÄT MASSNAHMEN VON HOHER PRIORITÄT SOLLTEN INNERHALB DER NÄCHSTEN MONATE UMGESETZT SEIN.		
3	Organisation & Sensibilisierung	*Wurden Regelungen zur sicheren Nutzung von IT-Systemen festgelegt?*	Regelungen können bspw. durch Richtlinien geregelt werden oder in Schulungen vermittelt werden.
3	Personal	*Werden die Mitarbeitenden für die Regelungen zur sicheren Nutzung von IT-Systemen sensibilisiert?*	Eine Sensibilisierung kann durch gezielte Mitarbeiterschulungen oder ViCoTeach erfolgen.
3	Backup	*Wie oft überprüfen Sie die externe Datensicherung?*	In regelmäßigen Abständen die Datensicherungen in einer Testumgebung einspielen und auf Funktion überprüfen. Prozess dokumentieren und in der Richtlinie zur Datensicherung definieren.
3	Clients & Peripherie	*Gibt es einen geordneten Prozess der Außerbetriebnahme von Clients?*	Dokumentierter Prozess für die Außerbetriebnahme eines Clients (z. B. lokaler Daten, Austragen des IT-Systems aus Verzeichnisdiensten und Datenbanken, Löschen der Daten auf dem IT-System durch Überschreiben, Löschen von Datensicherungsmedien, Entfernen sonstiger Informationen.
3	Multifunktionsgeräte	*Wird sichergestellt, dass der Zugriff auf Drucker und Multifunktionsgeräte nur durch berechtigte Personen erfolgt?*	Dies kann bspw. durch die Aufstellung an einem sicheren, zugangsgeschützten Ort erfolgen.

ViCoTec – Ihre Unternehmensberatung für IT-Sicherheit & Datenschutz für inhabergeführte Unternehmen in der Region Nordwesten.

Wir halten Ihnen den Rücken für den Weg in die digitale Zukunft frei.

ViCoTec IT-Sicherheit & Datenschutz
GmbH & Co. KG
Im Technologiepark 12
26129 Oldenburg

Tel: +49 441 24 92 65 20
info@vicotec.de

vicotec.de

ViCoTec
IT-SICHERHEIT & DATENSCHUTZ