ISX2024

IT-Security Conference

isxconference.de | #isxcon #isxconference

VOGEL IT AKADEMIE

PASSION4IT

PASSION4IT GMBH
ÜBER UNS

Danke das wir uns vorstellen dürfen!

HAUSBERG. K2. MOUNT EVEREST. JEDE ERFOLGREICHE EXPEDITION FOLGT DEN GLEICHEN GRUNDSÄTZEN.

WIR SIND DIGITALE BERGFÜHRER

Für deine IT-Vorhaben hast du mit PASSION4IT deinen Bergführer gefunden. Erfahre mehr, wie du durch digitalisierte Prozesse dein Business in ungeahnte Höhen bringen kannst!!

Ob Klettersteigpremiere oder die persönliche Erstbesteigung eines der Seven Summits: Steht man allein am Fuß des Berges, lässt der Blick nach oben unweigerlich Zweifel am Gelingen des Unterfangens aufkommen.

Was aber, wenn genau in dieser Situation ein erfahrener Bergführer dir beruhigend die Hand auf die Schulter legt? Mit dir dein Vorhaben minutiös plant, dich auf alle Eventualitäten vorbereitet? Und am Tag X als dein Seilgefährte voraus steigt?

ZAHLEN, DATEN, FAKTEN

2019
Gegründet

8
Digitale Bergführer

70+
Kunden D-A-CH

3,8
Millionen € Umsatz

1%
Vom Umsatz an den Umweltschutz

IMMER WEITER. IMMER BESSER.

Eat. Sleep. Climb. Repeat.

ÜBERZEUGUNG. VERTRAUEN. STOLZ.

PASSION4IT

Diese Kunden vertrauen uns!


PASSION4IT
VON DER TRÜGERISCHEN SICHERHEIT
ZUR GEMESSENEN SICHERHEIT
WIE EIN CYBER-SECURITY-CHECK EURE
ORGANISATION ALS KMU STÄRKT
FLORIAN LAUMER – PASSION4IT – PROJEKTLEITER UND BERATER
ANDREAS KUGEL - STADT VIECHTACH - IT-LEITER

Cyber-Security-Checks (auch für NIS2):

- Planungssicherheit
- effiziente Budgetierung
- gezielte Investitionen

Gap-Analyse:

- Die Kluft zwischen dem aktuellen Sicherheitsniveau und Best Practices

Die Bedeutung der Dokumentation:

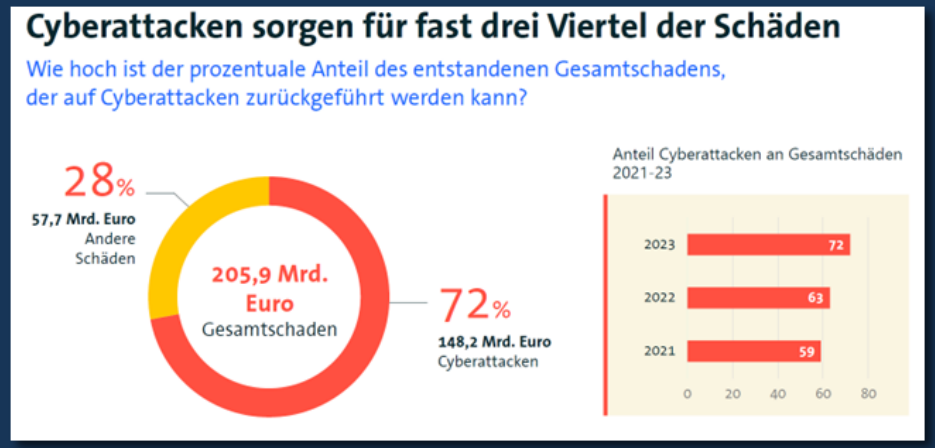
- vor, während und nach einem Angriff!

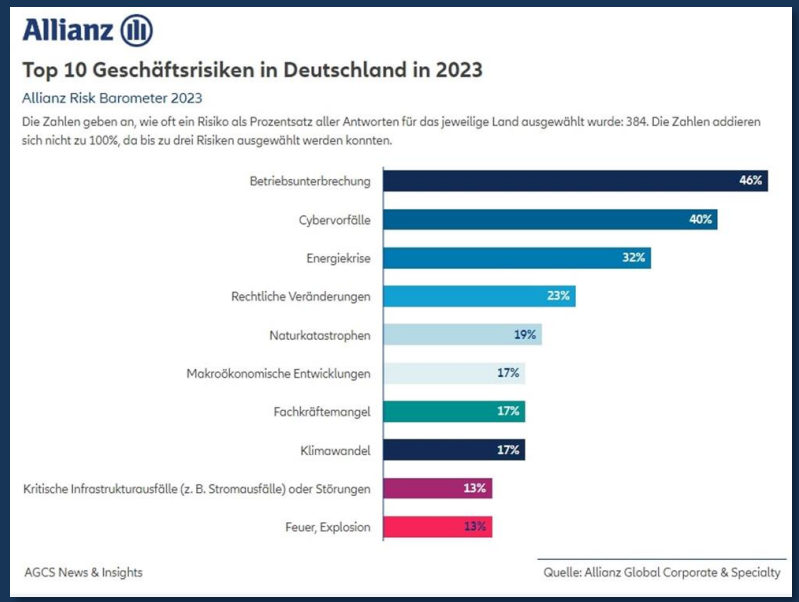
AUSGANGSSITUATION

EIN CYBER SECURITY CHECK MUSSTE UMGEHEND HER!

- IT in einem „unbekannten“ Cyber Security Status übernommen
- Mangelhafte Cyber Security Dokumentationen und Maßnahmen
- Hohe Verantwortung und Ausgangsituation

- Betriebsunterbrechung
- Wiederherstellungskosten
- Reputationsverlust
- Datenschutzverletzungen
- Vertrauensverlust


Cyberattacken sorgen für fast drei Viertel der Schäden
Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?
28%
57,7 Mrd. Euro
Andere Schäden
205,9 Mrd. Euro
Gesamtschaden
72%
148,2 Mrd. Euro
Cyberattacken
Anteil Cyberattacken an Gesamtschäden 2021-23
2023
72
2022
63
2021
59
0
20
40
60
80


Allianz
Top 10 Geschäftsrisiken in Deutschland in 2023
Allianz Risk Barometer 2023
Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 384. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.
Betriebsunterbrechung 46%
Cybervorfälle 40%
Energiekrise 32%
Rechtliche Veränderungen 23%
Naturkatastrophen 19%
Makroökonomische Entwicklungen 17%
Fachkräftemangel 17%
Klimawandel 17%
Kritische Infrastrukturausfälle (z. B. Stromausfälle) oder Störungen 13%
Feuer, Explosion 13%
AGCS News & Insights
Quelle: Allianz Global Corporate & Specialty

Mehrheit der Unternehmen verschweigt IT-Sicherheitsvorfälle

Redaktion / rh, 5.11.2023, 10:31 Uhr

TÜV-Verband: 82 Prozent der deutschen Unternehmen, die in den vergangenen 12 Monaten IT-Sicherheitsvorfall zu verzeichnen hatten, hielten diesen geheim.

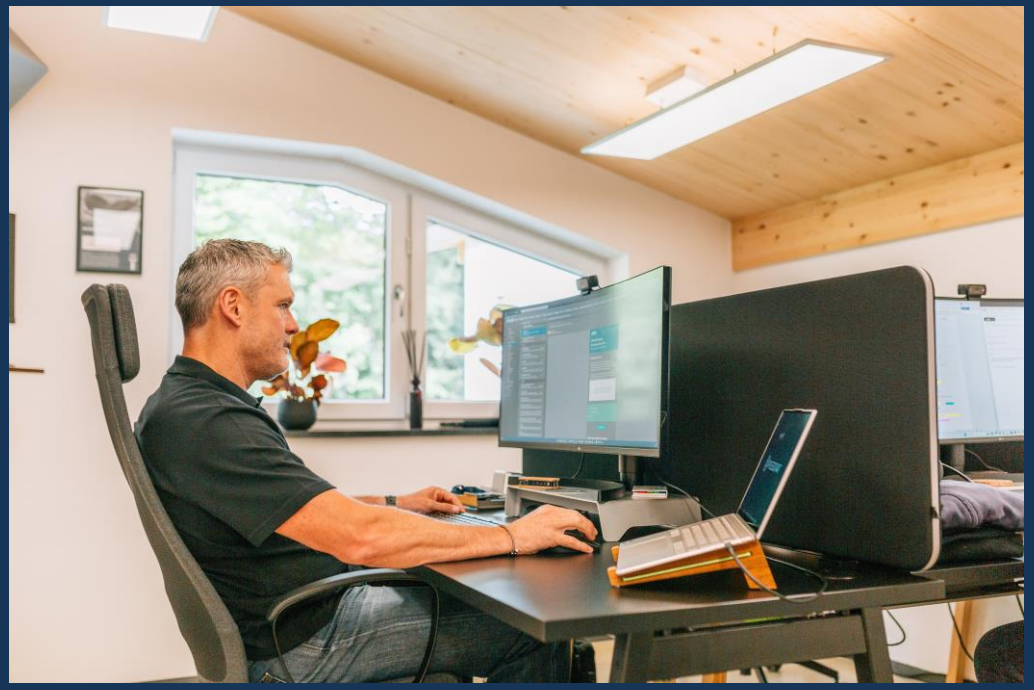
- Wie fange ich an?
- Was wurde bereits umgesetzt?
- Was muss noch erledigt werden?
- Welches Budget / Ressourcen wird benötigt?
- Wen benötige ich dazu?
- Wer koordiniert das ganze?

Ziel:

Aus der gefühlten Sicherheit eine messbare Sicherheit umsetzen.

Stuhlkreis?

Professionelle Methode?



VORGEHENSWEISE

PASSION4IT

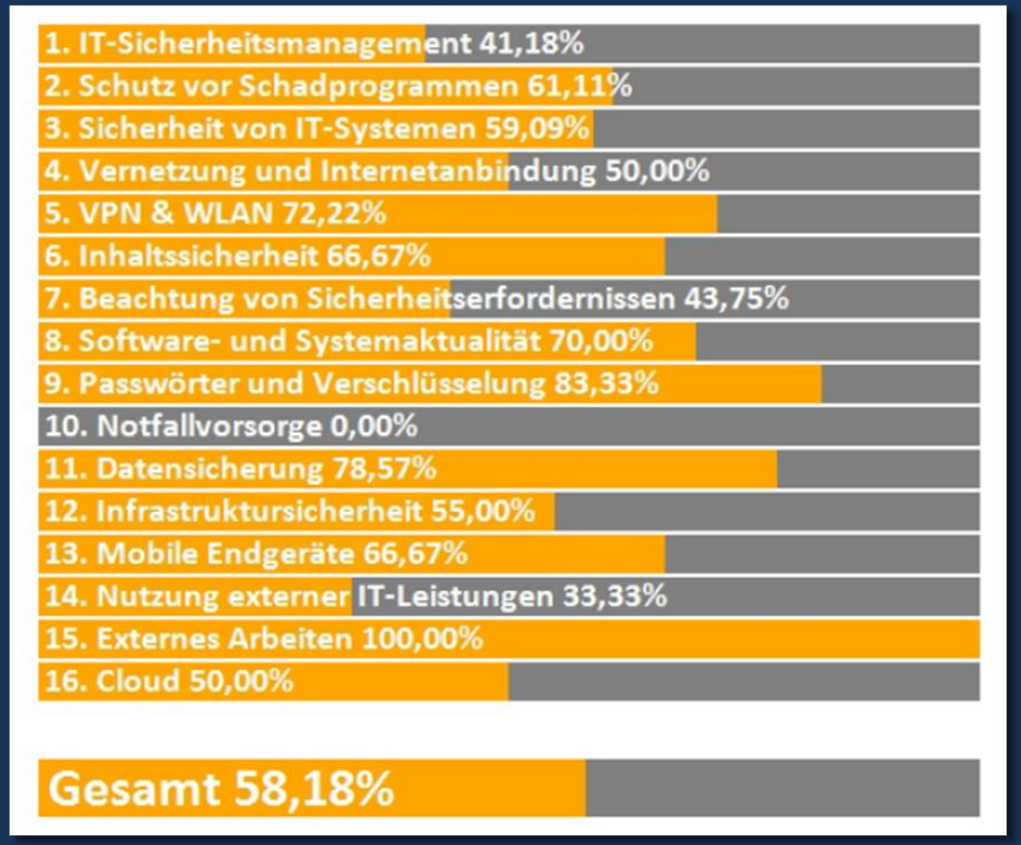
Regelmäßige Überprüfung und Optimierung
- Monitoring
- Audit
- Verbesserungsvorschläge

Maßnahmen planen
- Priorisierung
- Maßnahmenkatalog

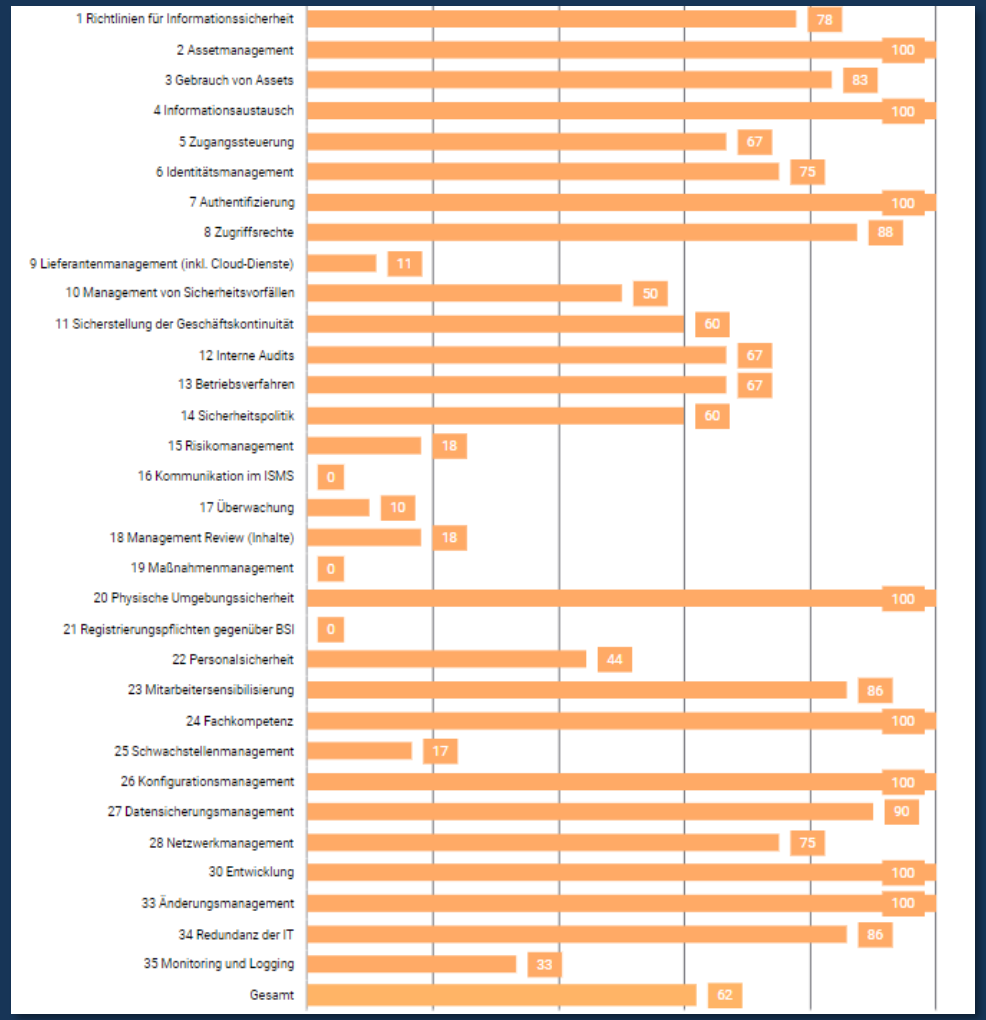
Maßnahmen umsetzen
- Implementierung
- Dokumentation
- Schulung

Lücken identifizieren
- Schwachstellenanalyse
- Risikoanalyse

Ist-Zustand ermitteln
- 16 Prüfkriterien / 128 Prüfpunkte
- Interview
- Dokumentsichtung
- Begehung



BASIS: BSI-Grundschutz / ISO27001 auf KMU-Anforderungen

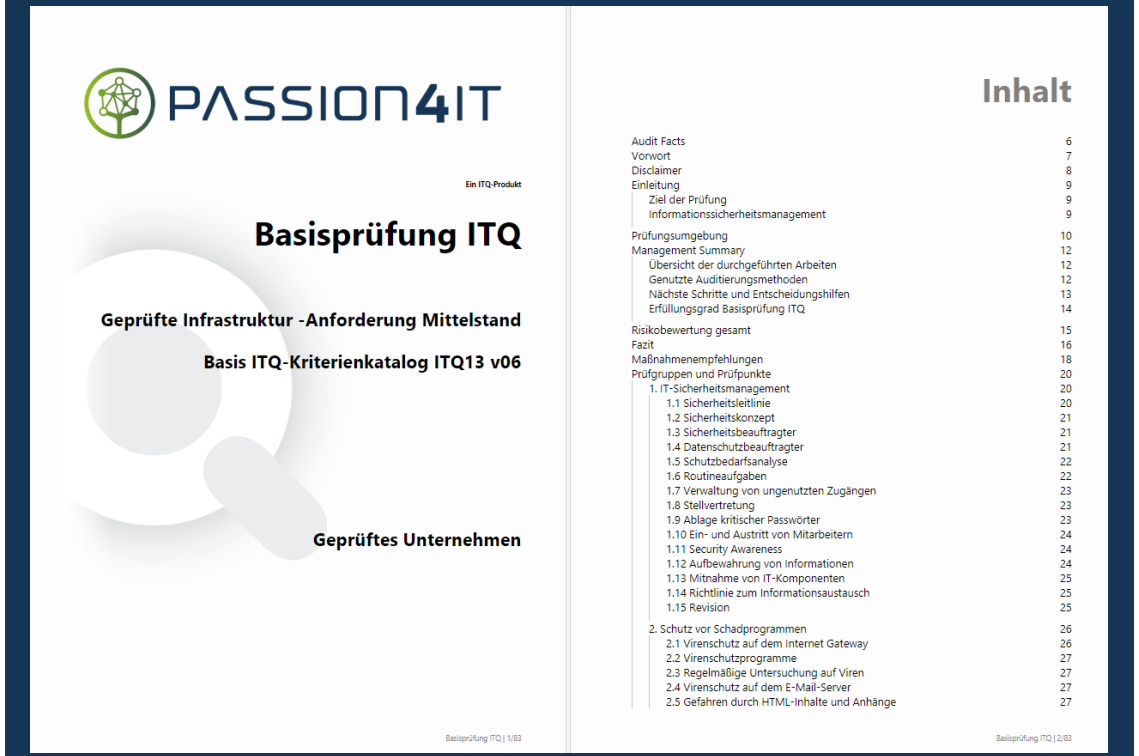


Ebenfalls 260 Prüfpunkte basierend auf den aktuellen NIS2 Anforderungen

#NIS2EinfachGemacht

Probleme mit **hohem Risikograd** sind rot gekennzeichnet.
Probleme mit **mittlerem Risikograd** orange.
Probleme ohne Farbkodierung weisen einen **niedrigeren Risikograd** auf.

Kennung	Maßnahmenempfehlung	Prüfpunkt
A02	Erstellen eines Sicherheitskonzeptes	1.2
A03	Übersicht der gesetzlichen Anforderungen	1.3
A04	Ernennen eines IT-Sicherheitsbeauftragten	1.4
A07	Durchführen einer Schutzbedarfsanalyse	1.7
A10	Stellvertretungsregelungen definieren	1.10
A11	Passworthinterlegung regeln	1.11
A14	Bereitstellen von verschließbaren Behältnissen	1.14
A17	Erstellen einer Richtlinie zum Informationsaustausch	1.17
A18	Jährliche Revision des Sicherheitsstatus	1.18
B04	Dedizierter Virenschutz für E-Mail Server	2.4
B07	Handlungsanweisung zur Verhaltensweise bei Virenbefall	2.7
B08	Routineaufgabe zur regelmäßigen Überprüfung der Virenschutzprogramme	2.8
C10	Systemdokumentationen erstellen oder aktualisieren	3.10
D07	Netzwerk-Topologieplan erstellen	4.7
D08	Erstellen einer Sicherheitsrichtlinie für Router und Switches	4.8
E06	Erstellen einer WLAN-Sicherheitsrichtlinie	5.6
F03	Erstellung einer E-Mail-Richtlinie	6.3



PASSION4IT

Ein ITQ-Produkt

Basisprüfung ITQ

Geprüfte Infrastruktur -Anforderung Mittelstand

Basis ITQ-Kriterienkatalog ITQ13 v06

Geprüftes Unternehmen

Basisprüfung ITQ | 1/83

Inhalt

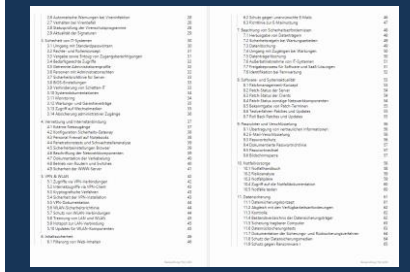
Audit Facts 6
Vorwort 7
Disclaimer 8
Einleitung 9
- Ziel der Prüfung 9
- Informationssicherheitsmanagement 9

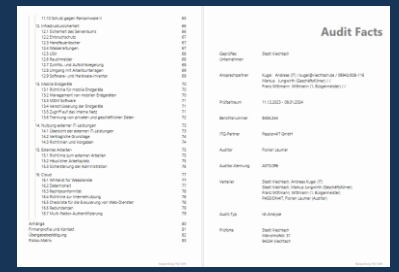
Prüfungsumgebung 10
Management Summary 12
- Übersicht der durchgeführten Arbeiten 12
- Genutzte Auditierungsmethoden 12
- Nächste Schritte und Entscheidungshilfen 13
- Erfüllungsgrad Basisprüfung ITQ 14

Risikobewertung gesamt 15
Fazit 16
Maßnahmenempfehlungen 18
Prüfgruppen und Prüfpunkte 20
1. IT-Sicherheitsmanagement 20
- 1.1 Sicherheitsleitlinie 20
- 1.2 Sicherheitskonzept 21
- 1.3 Sicherheitsbeauftragter 21
- 1.4 Datenschutzbeauftragter 21
- 1.5 Schutzbedarfsanalyse 22
- 1.6 Routineaufgaben 22
- 1.7 Verwaltung von ungenutzten Zugängen 23
- 1.8 Stellvertretung 23
- 1.9 Ablage kritischer Passwörter 23
- 1.10 Ein- und Austritt von Mitarbeitern 24
- 1.11 Security Awareness 24
- 1.12 Aufbewahrung von Informationen 24
- 1.13 Mitnahme von IT-Komponenten 25
- 1.14 Richtlinie zum Informationsaustausch 25
- 1.15 Revision 25

2. Schutz vor Schadprogrammen 26
- 2.1 Virenschutz auf dem Internet Gateway 26
- 2.2 Virenschutzprogramme 27
- 2.3 Regelmäßige Untersuchung auf Viren 27
- 2.4 Virenschutz auf dem E-Mail-Server 27
- 2.5 Gefahren durch HTML-Inhalte und Anhänge 27

Basisprüfung ITQ | 2/83





1.5 Schutzbedarfsanalyse

Risikoeinstufung OHNE GERING MITTEL HOCH **SEHR HOCH**

Ist-Zustand

Es bestehen keine Vorgaben der Leitungsebene in welchem Maße Prozesse, Systeme und Informationen zu schützen sind. Anforderungen an die IT, hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität von Informationen und Systemen, müssen klar dokumentiert und definiert werden. Andernfalls ist ein ordnungsgemäßer IT-Betrieb nicht möglich.

Bemerkung:
aktuell noch keine EInstufung

Maßnahmenempfehlung (A05)
Es muss eine Schutzbedarfsanalyse durchgeführt werden, die den Schutzbedarf der wichtigsten Ressourcen in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität einstuft. Das Ergebnis muss durch die Unternehmensleitung bestätigt werden und als Grundlage des Informationssicherheitsmanagements gelten. Berücksichtigt werden sollte hierbei nicht nur die Abhängigkeit von Anwendungen und IT-Systeme, sondern auch externer Dienstleister, Mitarbeitern und Räumlichkeiten.

Management Summary

Übersicht der durchgeführten Arbeiten

Im Rahmen der Basisprüfung ITQ wurde durch unterschiedliche Auditmethoden, in der Prüfungsumgebung aus „Audits Facts", **der aktuelle Stand der Informationssicherheit** ermittelt.

Maßstab für die Bestimmung des Sicherheitsniveaus ist ein Anforderungskatalog, der von der ITQ für kleine und mittlere Unternehmen entwickelt wurde und insgesamt 124 Fragen umfasst, die 16 unterschiedlichen Prüfgruppen zugeordnet wurden. Die jeweiligen Ergebnisse der Prüffragen können dem Diagramm **„Erfüllungsgrad"** entnommen werden.

Es wurde für alle festgestellten Mängel oder Sicherheitslücken eine Liste mit **Maßnahmenempfehlungen** erstellt, nach deren Erledigung eine Risikobeseitigung oder -reduzierung auf einen angemessenen Grad sichergestellt ist. Der Empfehlungskatalog priorisiert zwar einzelne Maßnahmen, wenn der geprüfte Bereich ein erhöhtes Risiko für die Informationssicherheit ausweist, gleichwohl sollte die Reihenfolge nicht als verbindlich betrachtet werden.

Eine detaillierte Übersicht der **Prüfungsergebnisse zu den einzelnen Fragen** kann dem beigefügten Bericht entnommen werden. Inhaltlich werden der ermittelte IST-Zustand sowie die Folgen der Nichterfüllung beschrieben. Die ITQ hat zudem nach eigenem Ermessen eine erste **Risikoabschätzung** vorgenommen und das Ergebnis als Orientierungshilfe zu Verfügung gestellt.

Abschließend wird in einem **Fazit** eine Gesamtbewertung der unternehmerischen IT Infrastruktur vorgenommen und der Stand der Informationssicherheit auf Basis des Erfüllungsgrades bewertet.

DAS GROSSE MYSTERIUM DER IT-DOKUMENTATION:

EXISTIEREN SIE ODER HAT DER HUND SIE GEFRESSEN?

#Notfallplan

#Cyberversicherung

IT-INFRASTRUKTUR

Die Dokumentation deiner IT-Infrastruktur ist wie eine Schatzkarte – **ohne sie ist es schwer, den verborgenen Schatz zu finden oder den Weg zurück aus dem Labyrinth zu finden!“**

NOTFALLPLAN UND -KONZEPT

Ohne einen dokumentierten Notfallplan ist ein Cyberangriff wie ein Feueralarm ohne Feuerlöscher – **alle rennen herum, aber niemand weiß, was zu tun ist!**

VERFOLGUNG UND PROTOKOLLIERUNG VON ÄNDERUNGEN

Änderungen ohne Dokumentation sind wie ein Buch mit fehlenden Seiten – **plötzlich macht die Geschichte keinen Sinn mehr!**

#ZEROTRUST

SICHERHEITSRICHTLINIEN UND -VERFAHREN

Sicherheitsrichtlinien ohne Dokumentation sind wie Verkehrsregeln ohne Straßenschilder – **niemand weiß, wohin er fahren soll und Chaos it vorprogrammiert!**

#BACKUPKONZEPT

#CYBERVERSICHERUNG

Cyber Security ist keine einmalige Aufgabe, sondern muss als Prozess verstanden werden, indem kontinuierlich an der Verbesserung, Aufrechterhaltung und Kontrolle der Sicherheitsmaßnahmen gearbeitet wird.

#cybersecuritycheck

Florian Laumer
+49 151 11676 502
florian.laumer@passion4it.de

- ITQ-Auditor (Informationssicherheit)
- LEAD Digital Transformation Analyst (LEADing Practice)
- Certified SAFe 6 Agilist
- ICO ISMS Security Officer according to ISO/IEC 27001:2022
- CISM Cyber Security Experte

ICO-CERT International Certification Organization

SA SAFe 6

LEADing Practice Global University Alliance ((O))LEAD DIGITAL TRANSFORMATION ANALYST

Zertifizierter Auditor für IT-Sicherheit ITQ Institut für Technologiequalität

Terminvereinbarung zu einem Austausch
und unverbindlichen
16 Punkte Cyber-Security-Check light