Shoobridge Business
IT Solutions

IT SICHERHEITS **CHECKLISTE**

für Geschäfts-
führer

Inklusive:

- 5 kritische Fragen zur IT-Sicherheit
- Erfolgsfaktoren für Ihre IT-Sicherheit

Shoobridge Business IT Solutions

- + 15 Jahre **Erfahrung** als IT-Dienstleister
- über **150** Kunden in der aktiven Betreuung
- Team aus 11 + **Experten** -Tendenz steigend
- **IT zum Festpreis** - auf Augenhöhe und direkt

Für wen ist diese Checkliste relevant?

Unsere PDF-Checkliste richtet sich an kleine und mittelständische Unternehmen ab 10 und bis zu 250 Mitarbeitenden. Die IT-Infrastruktur ist in der heutigen Zeit das Herzstück eines jeden Unternehmens. Ohne IT fehlen jegliche Mittel für Rechnungen, Bestellungen, Aufträge etc. Um den fortlaufenden Betrieb und somit das Überleben Ihres Unternehmens zu gewährleisten, muss IT-Sicherheit in Form eines KPI messbar gemacht werden. IT-Sicherheit ist nämlich keine einmalige Bestandsaufnahme, sondern ein iterativer Prozess, der im ständigen Wandel steht und kontinuierlich verbessert werden muss.

Was unsere Kunden sagen

100+ mittelständische Unternehmen vertrauen bereits auf unsere systematische IT-Sicherheitsprüfung

Christian Dagg
Inhaber und Geschäftsführer
DAGG.INVEST GmbH

Mit Shoobridge IT Solutions haben wir einen IT-Partner, der sich durch **Professionalität** und **strukturierte Arbeitsweisen** auszeichnet. Was uns besonders beeindruckt ist, wie sie standardisierte Lösungen für unsere **spezifischen Bedürfnisse** finden. Durch eine **sorgfältige Situationsanalyse** entwickeln sie maßgeschneiderte Leistungen, die perfekt zu unseren Anforderungen passen.

IT-Security als KPI: so machen wir es möglich

Als Geschäftsführer haben Sie sämtliche KPI´s im Kopf:

Krankenstand im Durchschnitt? Na logo.
Umsatz pro Mitarbeiter? Aber hallo.
Materialaufwand pro Monat? Selbstverständlich.
IT-Sicherheit? IT-Sicherheit was?

IT-Sicherheit ist die wichtigste Metrik für Unternehmen. Nochmal: Ohne eine fortlaufende IT-Infrastruktur ist das Überleben Ihres Unternehmens ständig in Gefahr. Das darf in 2025 nicht mehr sein!

Cyberangriffe erreichen täglich neue Rekordhoch. Der wirtschaftliche Schaden 2024 beläuft sich alleine in Deutschland auf 220.000.000.000 €. Richtig, 220 Milliarden Euro. Im Jahr 2023 waren es noch 200 Milliarden Euro.

Lassen wir uns das nochmal auf der Zunge zergehen. Cyberkriminelle verdienen inzwischen alleine in Deutschland fast mehr Geld als der internationale Drogenhandel.

Um Arbeitsplätze und Ihr Unternehmen für die nächsten Jahre abzusichern, ist IT-Sicherheit kein “nice-to-have” mehr. IT-Sicherheit ist ein “must-have”. Beispiele gefällig?

Cyber-Versicherungen kommen im Ernstfall nur für Schäden auf, wenn nachweislich dokumentiert ist, dass genügend Maßnahmen ergriffen werden, um die IT-Sicherheit Ihres Unternehmens zu härten. Dazu zählen unterschiedliche Policies, personenbezogene Zertifikate in Sachen Phishing-Sensibilisierung Ihrer Mitarbeiter, ein aktives Risikomanagement uvm.

Verantwortlich für diese Prozesse, Dokumentationen und Nachweise sind Sie als Geschäftsführer. Auch wenn Sie inhouse eine IT-Abteilung oder einen IT-Administrator eingestellt haben: Sie delegieren Aufgaben. Keine Verantwortung. Die tragen Sie ganz alleine.

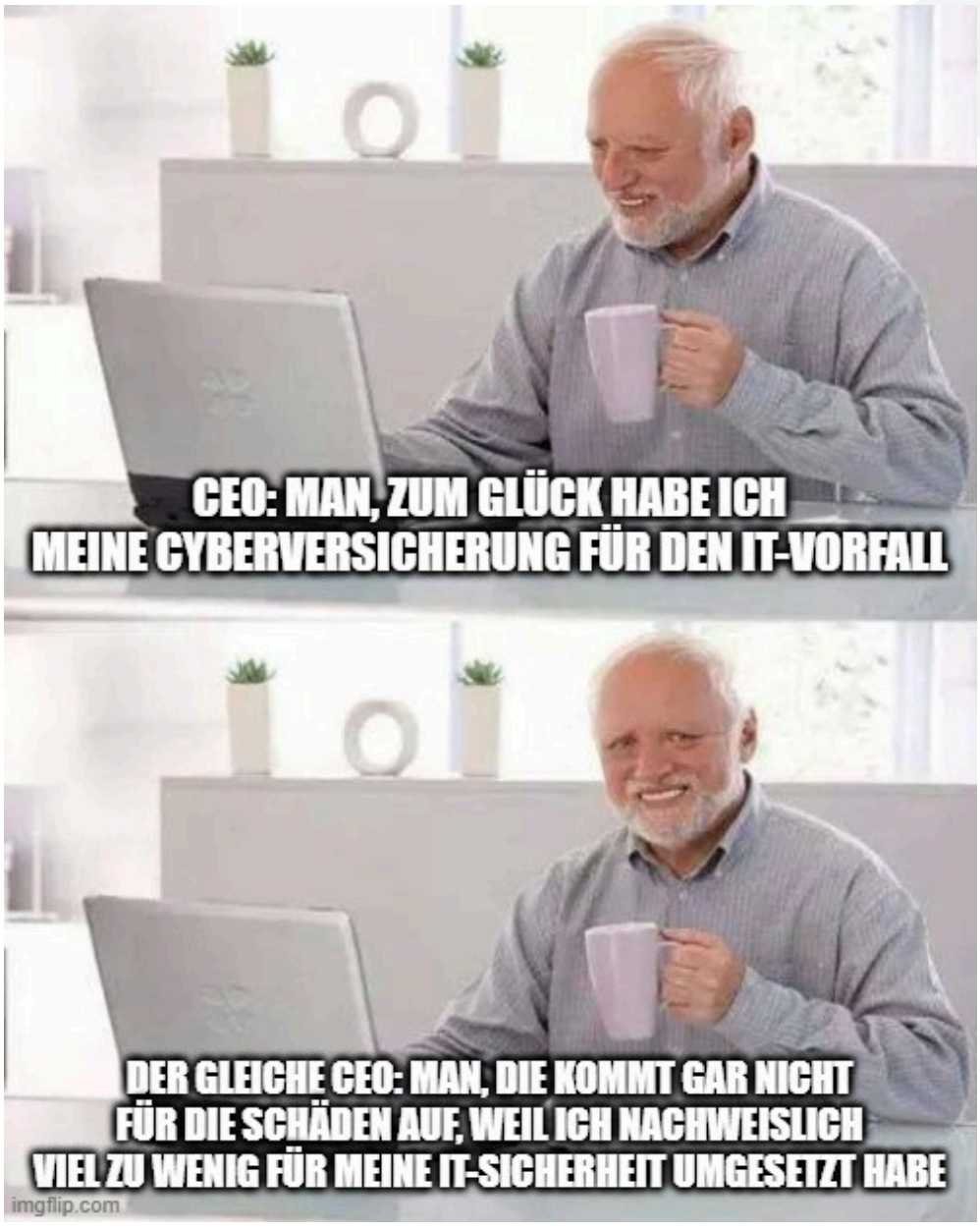
Wenn persönliche Enthaftung und eine im Schadensfall zahlende Versicherung ein Antrieb für Sie sind, lesen Sie unbedingt weiter…

Die Benefits unserer Checkliste (und Audits)

- unsere Checkliste hinterfragt genau die Dinge, die Sie als CEO oder IT-Leiter hinsichtlich Ihrer IT-Sicherheit wissen müssen (und viele IT-Dienstleister gar nicht auf dem Schirm haben oder abbilden können)

- die Checkliste gibt Ihnen einen ersten Aufschluss über den aktuellen Zustand Ihrer IT-Sicherheit. Eine Momentaufnahme reicht jedoch nicht aus. IT-Sicherheit ist ein fortlaufender Prozess. (dafür gibt es unserer Basisprüfung aus 124 Prüffragen in über 16 Prüfbereichen gemäß BSI-Grundschutz)

- wir haben 3 zertifizierte Auditoren im Unternehmen und auditieren unsere Kunden regelmäßig (inklusive Prüfsiegel)



Frage #1:
Cyber Versicherungen fordern klare Nachweise in puncto Mitarbeitersensibilisierung und IT-Sicherheitsmaßnahmen: Haben Sie solche?

Risiko bei Nichterfüllung:

Im Schadensfall bleiben Sie vollkommen alleine auf den Kosten sitzen.

Unter Umständen kann Geschäftsführern Fahrlässigkeit vorgeworfen werden, weil aktiv nichts zur Stabilisierung der IT-Sicherheit unternommen wurde.

Unsere Empfehlung:

Lesen Sie sich die Anforderungen Ihrer Cyber Versicherung nochmal durch und prüfen Sie, ob Sie alle Kriterien erfüllen, um im Ernstfall Unterstützung zu erhalten.

Bei fast allen Versicherungen zählen dazu z.B. Nachweise zur Phishing und E-Mail-Sensibilisierung der Mitarbeiter, aktuelle Virenschutzsoftware auf allen Clients, Servern und Cloudumgebungen.

Wir bieten unseren Kunden Phishing-Simulationen und E-Learning-Plattformen für Ihre Mitarbeiter an. Bei erfolgreichem Abschluss erhält jeder Mitarbeiter ein persönliches Zertifikat.

Das beste daran? Der Spaß kostet Sie gerade einmal einen Cappuccino pro Mitarbeiter pro Monat.

Frage #2:
Gibt es eine Informationssicherheitsleitlinie?

Risiko bei Nichterfüllung:

Rechtliche Risiken für den CEO:

- Mögliche strafrechtliche Konsequenzen bei grober Fahrlässigkeit, besonders wenn sensible Kundendaten betroffen sind
- Bußgelder nach DSGVO können persönlich zugerechnet werden

Geschäftliche Risiken:

- Erhöhtes Risiko von Datenlecks und Cyberangriffen durch fehlende Standards
- Reputationsschäden bei Sicherheitsvorfällen
- Möglicher Verlust von Geschäftspartnern, die Sicherheitsnachweise fordern
- Höhere Versicherungsprämien oder Deckungsausschlüsse

Organisatorische Risiken:

- Unklare Verantwortlichkeiten bei Sicherheitsvorfällen
- Ineffiziente oder falsche Reaktionen im Krisenfall
- Inkonsistente Sicherheitsmaßnahmen in verschiedenen Abteilungen

Unsere Empfehlung:

Stellen Sie sicher, dass es eine dokumentierte Informationssicherheitslinie gibt.

Einen Musterbericht haben wir Ihnen hier zusammengestellt:

Zum Musterbericht

Frage #3:
Wird regelmäßig getestet, ob die gesicherten Daten problemlos zurückgespielt werden können und die Dauer der Wieder-herstellungszeit angemessen ist?

Risiko bei Nichterfüllung:

IT-Dienstleister erkennen in automatischen systemischen Tests, ob Backupdaten korrekt gespeichert wurden.

Wurde ein Backup Ihrer Infrastruktur jemals für den Ernstfall getestet und wirklich vollständig aufgespielt?

Kann Ihnen Ihr IT-Dienstleister mitteilen, wie lange Sie bräuchten, um mit dem Backup wieder im Tagesgeschäft arbeiten zu können?

Unsere Empfehlung:

Fragen Sie explizit nach, wann Ihr Backup in einer Live-Umgebung das letzte Mal getestet wurde und wie lange der Wiederherstellungsprozess dauert.

Denn eines ist gewiss: Im Ernstfall muss Ihr Backup funktionieren, damit Sie binnen weniger Stunden wieder einsatzfähig sind.

Jede Stunde ohne laufende Systeme ist ein wirtschaftlicher Totalschaden.

Wenn Ihnen die Frage nicht sachgemäß beantwortet werden kann, lassen Sie uns darüber sprechen, wie wir unsere Backup-Lösungen in Ihrem Unternehmen integrieren können.

Frage #4:
Besteht in einem Notfall die Zugriffsmöglichkeit auf alle relevanten Passwörter und werden diese aktuell gehalten?

Risiko bei Nichterfüllung:

- Systemausfälle können nicht schnell behoben werden, da unklar ist, wer Zugriff hat
- Verzögerte Reaktionszeiten bei kritischen Vorfällen
- Reputationsschäden bei Kunden
- Umsatzeinbußen durch längere Ausfallzeiten
- Verletzung der Sorgfaltspflicht der Geschäftsführung
- Haftungsrisiken bei Datenschutzvorfällen

Unsere Empfehlung:

Kurzfristig:

- Sofortige Dokumentation aller bestehenden Admin-Zugänge
- Einrichtung eines Notfall-Kontaktplans
- Hinterlegung von Notfallzugängen in einem versiegelten Umschlag beim Geschäftsführer

Mittelfristig:

- Implementierung eines Privileged Access Management (PAM) Systems
- Einführung eines dokumentierten Prozesses für Notfallzugriffe
- Regelmäßige Tests der Notfallprozeduren
- Schulung der Mitarbeiter zu Notfallprozessen

Langfristig:

- Integration in ein umfassendes Business Continuity Management
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsberechtigungen
- Aufbau redundanter Systeme für kritische Infrastrukturen
- Etablierung eines Information Security Management Systems (ISMS)

Frage #5:
Gibt es in Ihrem Unternehmen eine dokumentierte Bewertung, welche Ressourcen für Ihre Kernprozesse essentiell sind und wie kritisch deren Ausfall wäre?

Risiko bei Nichterfüllung:

- Übersehen von kritischen Abhängigkeiten
- Fehleinschätzung bei Investitionsentscheidungen
- Unnötige Downtime durch falsche Priorisierung
- Unzureichender Schutz kritischer Assets
- Überinvestitionen in unkritische Systeme
- Unterinvestitionen bei kritischen Systemen

Unsere Empfehlung:

Sofortmaßnahmen:

- Schnellbewertung der wichtigsten IT-Systeme
- Dokumentation bekannter Abhängigkeiten
- Priorisierung der kritischsten Geschäftsprozesse

Kurzfristige Maßnahmen (1-3 Monate):

- Durchführung einer strukturierten Schutzbedarfsanalyse
- Erstellung einer Prozesslandkarte mit Abhängigkeiten
- Bewertung der Kritikalität nach:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

Mittelfristige Maßnahmen (3-6 Monate):

- Implementierung von Schutzmaßnahmen entsprechend der Kritikalität
- Entwicklung von Notfallplänen für kritische Prozesse
- Regelmäßige Überprüfung und Aktualisierung

Langfristige Maßnahmen:

- Integration in das Risikomanagement
- Aufbau eines kontinuierlichen Verbesserungsprozesses
- Regelmäßige Audits der Schutzbedarfsanalyse
- Anpassung an veränderte Geschäftsprozesse

So läuft eine Basisprüfung bei uns ab

Vorbereitung & Planung:
Effiziente Abstimmung aller Details für einen reibungslosen Ablauf. Unser erstes Audit dauert i.d.R. vier Stunden und wird im besten Fall vor Ort durchgeführt. Dabei ist die Anwesenheit des Geschäftsführers und/oder IT-Leiters verpflichtend. Deshalb klären wir im Vorfeld alle wichtigen Details und finden einen passenden Tag.

Durchführung der Prüfung:
Gemeinsam mit CEO und/oder IT-Leiter gehen wir den Prüfkatalog systematisch durch und schauen uns die Nachweise und Bedingungen (Serverraum, Absicherung etc.) vor Ort an.

Berichterstellung:
Detaillierte Aufbereitung aller Ergebnisse. Wir erstellen den ausführlichen Prüfbericht inkl. Auswertung, um die Ergebnisse im Nachgang mit Ihnen zu besprechen. Dafür benötigen wir i.d.R. 3 - 5 Werktage.

Ergebnispräsentation:
Persönliche Übergabe und Besprechung der nächsten Schritte. In einem ausführlichen Gespräch gehen wir die Gesamtauswertung durch und fokussieren uns auf die Risikobewertung. Für jeden Mangel wird eine klare Handlungsempfehlung definiert. Gemeinsam entwickeln wir eine Strategie zur Beseitigung der Risiken mit der höchsten Kritikalität.

Monatliches Jour-Fixe:
Jeden Monat finden Sie sich mit unserem Auditor zusammen (online oder vor Ort) und besprechen den aktuellen Zustand, aktuelle Kleinprojekte und zukünftige Ziele miteinander. Dieser engmaschige Austausch macht uns zu Ihrem IT-Security Sparringspartner und sorgt dafür, dass wir kontinuierlich an den von Ihnen gewünschten Risiken arbeiten und Ihre IT sicherer machen. Bei Bedarf schreiben wir Ihnen auch notwendige Dokumente wie ein IT-Notfallhandbuch, ein dokumentiertes Backupkonzept, eine Sicherheitsleitlinie usw.

*Wichtig: Wir auditieren auch unabhängig. Wenn Sie durch das Audit resultierende Sicherheitslücken mit Ihrem bisherigen IT-Dienstleister schließen möchten, ist das selbstverständlich möglich. Wir können auch nur die beratende und auditierende Instanz sein. (wobei unsere IT-Services zum Festpreis nur schwierig zu toppen sind)

Ihre nächsten Schritte

Vereinbaren Sie ein kostenloses Erstgespräch und lassen Sie uns darüber sprechen, wie wir Ihre IT-Sicherheit messbar machen und welche klaren Handlungsempfehlungen sich aus einem ersten Audit ergeben.

Eines vorweg: Nur, weil durch eine Auditierung Lücken und Mängel aufgedeckt werden, heißt das nicht, dass das ein negatives Bild auf Sie und/oder Ihre IT wirft. Man kann IT-Sicherheit auch auf die Spitze treiben und die Kuh durchs Dorf jagen. Das ist nicht das Ziel, das wir verfolgen.

Das Gegenteil ist der Fall.

Durch unsere regelmäßigen Auditierungen erhalten Sie eine stets aktuelle Risikobewertung, Dokumente und Nachweise wie z.B. einen IT-Notfallplan, ein dokumentiertes Backupkonzept, eine Richtlinie für mobiles Arbeiten und glasklare Handlungsempfehlungen für jede individuelle Schwachstelle.

Somit liegt es vollkommen in Ihrer Hand, die einzelnen Risiken abzuschätzen und zu entscheiden, ob Ihnen das Investment in Risiko X oder Y wert ist.

Für den Schadensfall sind Sie bestens gewappnet, denn unsere Audits und Maßnahmen können Sie problemlos der Cyber Versicherung vorlegen. Und mit jedem Stück aktiven Risikomanagement kommen Sie einer persönlichen Enthaftung immer näher.

Zum Erstgespräch

Folgen Sie uns auf LinkedIn.
Wir posten regelmäßig Content zum Thema IT-Sicherheit, Compliance und Co.

Kevin auf LinkedIn (Vertriebsleiter)

Neils auf LinkedIn (Geschäftsführer)

Kevin Kasper
Vertriebsleiter & Auditor