ViCoCheck

Selfcheck ViCoTec: Ihr Ergebnis

Gesamtwertung

Ihre Punkte: 321 von erreichbaren 490

65%

Dieser Sicherheitscheck hilft Ihnen dabei, eine erste Einschätzung über den Sicherheitszustand Ihrer IT zu erhalten. Der Check ist aus über 30 Jahren Berufserfahrung und der DIN Spec 27076 Norm entstanden. Er stellt das absolute Minimum an Anforderungen für kleine Firmen zusammen (80% in der Bewertung reichen **NICHT** aus). Der Check ersetzt keine individuelle IT-Sicherheitsberatung.

Wir stellen Ihnen gerne für eine ganze Reihe an Punkten Vorlagen und Beispiele zur Verfügung. Einfach unter info@vicotec.de anfragen.

Herzliche Grüße - Ihr Team von ViCoTec und der Akademie für digitale Sicherheit

Dieser Bericht fasst von Nutzer eingegebene Daten zusammen. Daher können wir nicht jeden Fehler ausschließen. Auch können wir die Vollständigkeit nicht garantieren, da IT-Sicherheitsmaßnahmen immer individuell am Unternehmen auszurichten sind.
Alle Inhalte verstehen sich daher ohne jegliche Verpflichtung oder Garantien seitens der Autoren. Der Autor schließt jegliche Haftung für inhaltliche Mängel dieses Berichts aus.

Chef-Sache!

Frage	Antwort	Punkte
Wer ist bei Ihnen im Unternehmen der Hauptverantwortliche für die IT-Sicherheit? (Wenn Sie jetzt zögern, sind Sie es wahrscheinlich selbst.) Klare Verantwortung schafft Verbindlichkeit. Geschäftsführung trägt Gesamtverantwortung, kann aber IT-Leiter oder externen Dienstleister beauftragen. Ohne klare Zuständigkeit entstehen Sicherheitslücken.	Dienstleister	4/10
Richtlinien: Gibt es schriftliche, für alle Mitarbeiter verbindliche Richtlinien für die IT-Nutzung? (z.B. eine Passwort-Richtlinie, eine E-Mail-Richtlinie oder eine Richtlinie zur Nutzung von privaten Geräten). Schriftliche Richtlinien schaffen Klarheit für alle Mitarbeiter. Erstellen Sie einfache Regeln für Passwörter, E-Mail-Nutzung und private Geräte. Regelmäßig aktualisieren und kommunizieren.	Ja	10/10
Haben Sie eine Person benannt, die sich im Alltag um die IT kümmert? Hat diese Person dafür auch wirklich Zeit und das nötige Wissen? IT-Verantwortlicher braucht ausreichend Zeit und Fachwissen. Planen Sie mindestens 20% Arbeitszeit ein und ermöglichen Sie jährliche Weiterbildungen. Halbwertszeit von IT-Wissen beträgt nur 1,5 Jahre.	Teilweise	4/10
Haben Sie einen guten, aktuellen Überblick über die IT-Risiken in Ihrer Firma (existiert eine Risikoanalyse)? Risikoanalyse identifiziert Schwachstellen und Bedrohungen. Dokumentieren Sie IT-Risiken, bewerten Sie Eintrittswahrscheinlichkeit und Schäden. Aktualisieren Sie die Analyse jährlich.	Teilweise	4/10

Das digitale Fundament: Ihre IT-Infrastruktur

Stellen Sie sich Ihre IT wie Ihr Firmengebäude vor. Sie brauchen einen Bauplan, funktionierende Schlösser und eine Alarmanlage.

Frage	Antwort	Punkte
Haben Sie aktuelle eine Liste, die zeigt, welche Geräte (Computer, Server, Drucker) in Ihrem Netzwerk sind? (Dokumentation, Inventar) IT-Inventar verschafft Überblick über alle Geräte im Netzwerk. Erstellen Sie eine Liste mit Computern, Servern, Druckern inkl. IP-Adressen und Verantwortlichen. Monatlich aktualisieren.	Nein	0/10
Gibt es eine klare Regelung, wer in den Serverraum oder an die zentralen IT-Geräte darf? Physischer Zugang zu IT-Geräten muss kontrolliert werden. Serverraum abschließen, Zugangsberechtigungen dokumentieren. Nur autorisierte Personen dürfen an zentrale IT-Komponenten.	Ja	10/10
Gibt es eine Art "Alarmanlage" für Ihr Netzwerk? Also eine Software, die Alarm schlägt, wenn ungewöhnliche Dinge passieren? Netzwerk-Monitoring erkennt Angriffe und Anomalien frühzeitig. Installieren Sie Überwachungssoftware, die bei ungewöhnlichen Aktivitäten Alarm schlägt. Logs regelmäßig auswerten.	Teilweise	5/10
Haben Sie eine Firewall und wird diese regelmäßig gewartet und überwacht? Firewall schützt vor externen Angriffen. Konfiguration regelmäßig prüfen, Updates einspielen, Logs überwachen. Firewall-Regeln dokumentieren und bei Änderungen anpassen.	Teilweise	4/10

Homeoffice & Unterwegs: Der mobile Arbeitsplatz

Frage	Antwort	Punkte
Gibt es klare und einfache Regeln für Mitarbeiter, die von zu Hause aus arbeiten? Weiß jeder, was er mit Firmendaten auf dem privaten Laptop tun darf und was nicht? Homeoffice-Richtlinien definieren sichere Arbeitsweise von zu Hause. Regeln für Firmendaten auf privaten Geräten, sichere Internetverbindung, Arbeitsplatz-Sicherheit festlegen.	nicht relevant	10/10
Sind alle mobilen Geräte (Firmenhandys, Laptops) mit einem sicheren Passwort geschützt? Mobile Geräte sind Diebstahl-gefährdet. Alle Firmenhandys und Laptops mit starken Passwörtern/PINs schützen. Bei Verlust sofortige Sperrung ermöglichen (Mobile Device Management).	Ja	10/10
Sind Festplatten von Laptops (mobilen Geräten) verschlüsselt (z.B. Bitlocker) Festplattenverschlüsselung schützt bei Geräteverlust. BitLocker (Windows-Festplattenverschlüsselung) oder FileVault (Mac) aktivieren. Verschlüsselungsschlüssel sicher verwahren und Wiederherstellungsverfahren testen.	Nein	0/10
Nutzen Ihre Mitarbeiter eine sichere "Tunnelverbindung" (VPN) o.ä. , wenn sie von außen auf Firmendaten zugreifen? VPN-Verbindung verschlüsselt Datenübertragung von extern. Alle Mitarbeiter müssen VPN nutzen, wenn sie von außen auf Firmendaten zugreifen. VPN-Software aktuell halten.	Ja	10/10

Physische Sicherheit: Schutz vor Diebstahl und Schaden

Frage	Antwort	Punkte
Stehen wichtige Geräte (Server) in einem verschlossenen Raum? Server gehören in verschlossene, klimatisierte Räume. Schutz vor Diebstahl, unbefugtem Zugriff und Umwelteinflüssen. Zutritt nur für autorisierte Personen, Zugangsprotokoll führen.	Ja	10/10
Sind Ihre Geräte bei Stromausfall, Überspannung oder Wasserschaden ausreichend geschützt? USV schützt vor Stromausfall, Überspannungsschutz vor Blitzschlag. Wichtige Geräte gegen Wasserschäden sichern. Regelmäßige Wartung der Schutzeinrichtungen durchführen.	Nein	0/10
Nutzen Sie auf ALLEN Geräten einen Virenschutz, der mindestens einmal am Tag aktualisiert wird? Virenschutz auf allen Geräten ist Grundschutz. Automatische Updates aktivieren, regelmäßige Vollscans durchführen. Virenschutz-Software zentral verwalten und überwachen	Ja	10/10
Sind alle Zugänge zu Systemen (Software und Hardware) mit einem sicheren und einzigartigen Passwort geschützt? Jedes System braucht einzigartige, starke Passwörter. Mindestens 12 Zeichen, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen. Passwort-Manager verwenden, regelmäßig ändern.	Ja	10/10
Sind alle wichtigen Zugänge (Administratoren, Buchhaltung, Konto, ..) zusätzlich mit einem zweiten Faktor geschützt? Zwei-Faktor-Authentifizierung (2FA) erhöht Sicherheit erheblich. Für alle kritischen Systeme aktivieren: E-Mail, Banking, Verwaltungszugänge. SMS, App oder Hardware-Token nutzen.	Nein	0/10
Werden auf allen Geräten mindestens monatlich aktuelle Softwareupdates (Patches) eingespielt? Software-Updates schließen Sicherheitslücken. Monatliche Patch-Zyklen einführen, kritische Updates sofort einspielen. Update-Management dokumentieren und überwachen.	Nein	0/10

Frage	Antwort	Punkte
Gibt es eine verantwortliche Person und eine Dokumentation für Virenschutz und Updatemanagement? Verantwortlichkeiten für IT-Sicherheit klar definieren. Eine Person für Virenschutz und Updates benennen, Vertretung festlegen. Dokumentation der Prozesse und Zuständigkeiten.	Ja	10/10

E-Mail: Das größte Einfallstor

90% aller Cyberangriffe beginnen mit einer einfachen E-Mail. Jede E-Mail ist wie ein Brief, der eine Bombe enthalten könnte.

Frage	Antwort	Punkte
Trainieren Sie Ihre Mitarbeiter darin, gefälschte E-Mails (Phishing) zu erkennen? Wissen diese, worauf sie achten müssen, bevor sie klicken? Phishing-Schulungen sensibilisieren Mitarbeiter für E-Mail-Betrug. Regelmäßige Trainings durchführen, Phishing-Simulationen testen. Erkennungsmerkmale verdächtiger E-Mails vermitteln.	Ja	10/10
Haben Sie einen guten Spam-Filter, der gefährliche E-Mails automatisch aussortiert? Spam-Filter blockiert gefährliche E-Mails automatisch. Professionelle Lösung implementieren, regelmäßig konfigurieren. Quarantäne-Ordner überwachen, False-Positives vermeiden.	Ja	10/10
Wissen ALLE Mitarbeiter, was zu tun ist, wenn sie versehentlich auf einen verdächtigen Link geklickt haben oder der Rechner komische Dinge macht? Incident-Response-Plan für E-Mail-Sicherheitsvorfälle. Mitarbeiter wissen: Verdächtige E-Mail melden, betroffenen PC isolieren, IT-Verantwortlichen informieren. Schnelle Reaktion verhindert Schäden.	Nein	0/10

Ihre Mitarbeiter: Die menschliche Firewall

Ihre Mitarbeiter sind Ihre erste und wichtigste Verteidigungslinie. Ein unachtsamer Klick kann mehr Schaden anrichten als ein technischer Fehler.

Frage	Antwort	Punkte
Werden Ihre Mitarbeiter mindestens einmal im Jahr zur IT-Sicherheit geschult? Jährliche IT-Sicherheitsschulungen halten Wissen aktuell. Neue Bedrohungen, Unternehmensrichtlinien, praktische Übungen. Schulungsteilnahme dokumentieren, Verständnis prüfen.	Ja	10/10
Kennen Ihre Mitarbeiter die wichtigsten Tricks von Betrügern (z.B. der "Chef-Betrug" per E-Mail)? Social Engineering-Angriffe erkennen und abwehren. "Chef-Betrug", Telefonbetrug, gefälschte Rechnungen thematisieren. Mitarbeiter für Manipulation sensibilisieren, Verifikationsprozesse etablieren.	Ja	10/10
Nutzen alle Mitarbeiter sichere Passwörter und, wo es geht, eine zweite Absicherung (Zwei-Faktor-Authentifizierung)? Passwort-Sicherheit und 2FA für alle Mitarbeiter. Passwort-Manager bereitstellen, sichere Passwort-Erstellung schulen. Zwei-Faktor-Authentifizierung wo möglich aktivieren.	Ja	10/10
Gibt es eine Onboarding-Checkliste und eine Offboarding-Checkliste, damit Zugänge korrekt zugewiesen und wieder gesperrt werden. Strukturierte Mitarbeiter-Prozesse verhindern Sicherheitslücken. Onboarding: Zugänge einrichten, Schulungen. Offboarding: Alle Zugänge sperren, Geräte zurückgeben, Accounts löschen.	Ja	10/10
Arbeiten Mitarbeiter mit Administratorrechten an ihrem Arbeitsplatz? Admin-Rechte nur bei Bedarf vergeben. Separate Admin-Accounts für IT-Aufgaben, normale Benutzerkonten für tägliche Arbeit. Prinzip der minimalen Berechtigung anwenden.	Ja	10/10

Datensicherung: Ihr digitales Sicherheitsnetz

Wenn alle Stricke reißen und Ihre Daten verschlüsselt oder zerstört sind, ist das Backup Ihre einzige Rettung. Es ist die Versicherung für Ihr digitales Kapital.

Frage	Antwort	Punkte
Gibt es einen festen Plan, wie und wie oft Ihre wichtigsten Geschäftsdaten gesichert werden? Backup-Strategie sichert Geschäftskontinuität. 3-2-1-Regel: 3 Kopien, 2 verschiedene Medien, 1 extern. Automatisierte tägliche Backups wichtiger Daten, Backup-Plan dokumentieren.	Ja	10/10
Testen Sie regelmäßig, ob Ihre Daten rücksicherbar sind? Backup-Tests stellen Wiederherstellbarkeit sicher. Monatliche Restore-Tests durchführen, Wiederherstellungszeit messen. Backup-Integrität prüfen, Prozess dokumentieren.	Ja	10/10
Gibt es eine verantwortliche Person und eine Vertretung? Backup-Verantwortlichkeiten klar definieren. Hauptverantwortlichen und Vertretung benennen. Backup-Überwachung, Fehlerbehebung, Restore-Prozesse zuweisen.	Ja	10/10
Wie lange würde es dauern, bis Ihr Unternehmen nach einem kompletten Datenverlust wieder arbeitsfähig ist? Ein Tag? Eine Woche? Recovery Time Objective (RTO) definiert Ausfallzeiten. Kritische Systeme identifizieren, Wiederherstellungszeiten planen. Notfall-Hardware bereithalten, Prozesse testen.	Ja	10/10
Gibt es ein Backup, dass unveränderbar und gegen jeden Zugriff und Bedrohung (Brand, Wasser, Diebstahl) geschützt ist? Immutable Backups schützen vor Ransomware. Unveränderbare Backups auf separaten Systemen, Offline-Backups, geografisch getrennte Lagerung. Air-Gap-Prinzip anwenden.	Ja	10/10
Werden ALLE Backups sicher verwahrt (verschlossen, verschlüsselt, ...) Backup-Sicherheit verhindert Datenverlust. Verschlüsselung aller Backups, sichere Aufbewahrung, Zugangskontrollen. Backup-Medien vor physischen Bedrohungen schützen.	Ja	0/0

Klare Regeln: Wer darf was?

Ohne klare Zuständigkeiten und Regeln herrscht Chaos. Das gilt für die IT-Sicherheit genauso wie für die Buchhaltung.

Frage	Antwort	Punkte
Ist eindeutig festgelegt, welcher Mitarbeiter auf welche Daten zugreifen darf? (Gibt es ein Berechtigungskonzept) Berechtigungskonzept regelt Datenzugriff nach Rollen. Mitarbeiter erhalten nur benötigte Zugriffsrechte. Prinzip der minimalen Berechtigung, regelmäßige Überprüfung der Berechtigungen.	Nein	0/10
Wird das Berechtigungskonzept mind. jährlich geprüft? Jährliche Berechtigungsprüfung verhindert Rechte-Wildwuchs. Alle Benutzerkonten und Zugriffsrechte überprüfen, nicht mehr benötigte Rechte entziehen. Dokumentation der Änderungen.	Ja	10/10
Gibt es bei wichtigen IT-Änderungen ein Vier-Augen-Prinzip? Vier-Augen-Prinzip bei kritischen IT-Änderungen. Wichtige Konfigurationsänderungen von zwei Personen prüfen lassen. Change-Management-Prozess etablieren, Änderungen dokumentieren.	Ja	10/10
Haben Sie Verträge mit Ihren externen IT-Dienstleistern, die Vertraulichkeit und Sicherheitsstandards festlegen? Dienstleister-Verträge definieren Sicherheitsstandards. Vertraulichkeitsvereinbarungen, Sicherheitsanforderungen, Haftungsregelungen. Regelmäßige Überprüfung der Vertragserfüllung.	Nein	0/10

Datenschutz: Gesetz und Vertrauen

Frage	Antwort	Punkte
Wissen Sie, welche Kundendaten Sie wo speichern und wie sensibel diese sind? Datenklassifizierung identifiziert schützenswerte Informationen. Kundendaten, Geschäftsgeheimnisse, personenbezogene Daten kategorisieren. Schutzmaßnahmen entsprechend der Sensibilität anpassen.	Nein	0/10
Haben alle Mitarbeiter eine Verschwiegenheitserklärung unterschrieben? Verschwiegenheitserklärungen verpflichten Mitarbeiter zur Vertraulichkeit. Alle Mitarbeiter unterschreiben bei Einstellung. Regelmäßige Erinnerung an Vertraulichkeitspflichten.	Ja	10/10
Wissen die Mitarbeiter, was zu tun ist, wenn Daten gestohlen wurden oder abhandengekommen sind? Erkennen und Verhalten bei Datenpannen. Meldeprozesse an Aufsichtsbehörden, Betroffene informieren. 72-Stunden-Regel beachten, Schadensbegrenzung einleiten.	Ja	10/10
Werden Daten, die Sie nicht mehr brauchen, regelmäßig gelöscht? Datenlöschkonzept für nicht mehr benötigte Daten. Aufbewahrungsfristen definieren, automatische Löschung implementieren. Sichere Löschverfahren für sensible Daten anwenden.	Nein	0/10

Plan B: Was tun, wenn alles ausfällt?

Ein Notfallplan ist wie ein Feuerlöscher: Man hofft, ihn nie zu brauchen, aber wenn es brennt, rettet er Leben.

Frage	Antwort	Punkte
Gibt es einen einfachen, schriftlichen Plan, was im Falle eines kompletten IT-Ausfalls zu tun ist? Business Continuity Plan für IT-Ausfälle. Schriftlicher Notfallplan mit Kontakten, Prioritäten, Wiederherstellungsschritten. Alle Mitarbeiter kennen ihre Aufgaben im Notfall.	Ja	10/10
Kennen Ihre Mitarbeiter die wichtigsten Notfall-Kontakte (z.B. vom IT-Dienstleister), auch außerhalb der Geschäftszeiten? Notfall-Kontakte für schnelle Hilfe. 24/7-Hotlines von IT-Dienstleistern, interne Ansprechpartner, Eskalationswege. Kontaktliste aktuell halten, allen Mitarbeitern zugänglich machen.	Ja	10/10
Könnten Sie und Ihre Mitarbeiter im Notfall von einem anderen Ort aus weiterarbeiten? Alternative Arbeitsplätze für Geschäftskontinuität. Homeoffice-Möglichkeiten, Ausweichstandorte, mobile Arbeitsplätze. Notwendige IT-Ausstattung und Zugänge bereitstellen.	Ja	10/10

Der Ernstfall: Reaktion auf einen Angriff

Wenn ein Einbrecher im Haus ist, rufen Sie die Polizei und fangen nicht an, die Fenster zu putzen. Bei einem Cyberangriff ist schnelles und richtiges Handeln entscheidend.

Frage	Antwort	Punkte
Gibt es einen klaren Ablaufplan für den Fall eines Cyber-Angriffs? Cyber-Incident-Response-Plan für Angriffe. Sofortmaßnahmen, Eskalationswege, Kommunikation definieren. Incident-Response-Team benennen, externe Experten kontaktieren.	Nein	0/10
Können Sie feststellen, dass Sie angegriffen wurden? Angriffserkennung durch Monitoring und Logs. SIEM-Systeme, Anomalie-Erkennung, Mitarbeiter-Sensibilisierung. Verdächtige Aktivitäten schnell identifizieren und melden.	Ja	10/10
Können Sie betroffene Systeme schnell vom restlichen Netzwerk trennen, um eine Ausbreitung zu verhindern? Netzwerk-Segmentierung für Schadensbegrenzung. Betroffene Systeme schnell isolieren, Ausbreitung verhindern. Network Access Control, VLAN-Segmentierung implementieren.	Ja	10/10

Externe Partner: Die geteilte Verantwortung

Die Sicherheit Ihres Unternehmens hängt auch von der Sicherheit Ihrer IT-Dienstleister und Lieferanten ab. Eine schwache Stelle in der Kette gefährdet alle.

Frage	Antwort	Punkte
Stellen Sie sicher, dass Ihr externer IT-Dienstleister selbst sicher arbeitet? Vertrauen Sie blind oder prüfen Sie das? Lieferanten-Sicherheit prüfen und überwachen. IT-Dienstleister-Zertifizierungen, Sicherheitsaudits, Vertragsklauseln. Regelmäßige Bewertung der Sicherheitsstandards.	Nein	0/10
Wenn Sie Cloud-Dienste (z.B. für Backups oder Kundendaten) nutzen: Wissen Sie, wo diese Daten gespeichert werden und wie gut sie dort geschützt sind? Cloud-Security und Datenstandorte kennen. Anbieter-Zertifizierungen prüfen, Datenverarbeitung in EU, Verschlüsselung. Service Level Agreements für Sicherheit und Verfügbarkeit.	Nein	0/10
Könnte ein IT-Problem bei einem Ihrer wichtigen Lieferanten Ihren eigenen Betrieb lahmlegen? Lieferanten-Risikomanagement für kritische Abhängigkeiten. Single Points of Failure identifizieren, alternative Anbieter evaluieren. Business Impact Analysis für Lieferantenausfälle.	Nein	0/10