QUANSATECH IT

PRIORITÄTENCHECK FÜR UNTERNEHMEN

IT-Sicherheit im Unternehmen: das Wichtigste zuerst klären

Eine verständliche Arbeitsunterlage für Geschäftsführung und interne Ansprechpartner. Markieren Sie, was geklärt ist. Offene Punkte werden anschließend nach Geschäftsauswirkung und Dringlichkeit geordnet.

Wichtig: Dieser Check ersetzt keine technische Sicherheitsprüfung. Er hilft, die richtigen Fragen zu stellen, bevor weitere Produkte gekauft oder bestehende Systeme vorschnell umgebaut werden.

1. Kritische Geschäftsabläufe

Zuerst wird geklärt, was für den Betrieb wirklich weiterlaufen oder rasch wiederhergestellt werden muss.

- [ ] Die wichtigsten Abläufe sind benannt, zum Beispiel Auftrag, Produktion, Termin, Kommunikation oder Abrechnung.
- [ ] Für jeden kritischen Ablauf ist bekannt, wie lange ein Ausfall tragbar wäre.
- [ ] Abhängigkeiten von Internet, E-Mail, Servern, Cloud-Diensten und Fachsoftware sind grob erfasst.
- [ ] Es ist geklärt, welche Daten und Systeme in welcher Reihenfolge benötigt werden.
- [ ] Eine einfache Zwischenlösung für den Notbetrieb ist soweit sinnvoll vorbereitet.

2. Konten, Rechte und externe Zugänge

Ein gestohlenes oder vergessenes Schlüsselkonto kann mehr Schaden verursachen als ein einzelnes defektes Gerät.

- [ ] Unternehmenseigene Administrator- und Notfallkonten sind bekannt und sicher dokumentiert.
- [ ] Mehrstufige Anmeldung (MFA) schützt zentrale Konten und Fernzugänge.
- [ ] Mitarbeitende besitzen nur die Rechte, die sie für ihre Aufgabe wirklich benötigen.
- [ ] Austritte, Rollenwechsel, alte Konten und gemeinsame Benutzer werden nachvollziehbar bearbeitet.
- [ ] Zugänge von Dienstleistern und Softwarepartnern sind begrenzt und können entzogen werden.

3. Sicherung und Wiederherstellung

Eine vorhandene Sicherung ist erst dann belastbar, wenn Umfang, Schutz und Wiederherstellungsweg geklärt sind.

- [ ] Es ist bekannt, welche wichtigen Daten und Systeme tatsächlich gesichert werden.
- [ ] Mindestens eine Sicherung ist sinnvoll getrennt und vor unberechtigtem Löschen geschützt.
- [ ] Fehler, abgebrochene Sicherungen und zu wenig Speicherplatz werden bemerkt.
- [ ] Eine Wiederherstellung wurde für wichtige Daten oder Systeme praktisch getestet.
- [ ] Verantwortliche, Reihenfolge und benötigte Zugänge für den Wiederanlauf sind dokumentiert.

Die drei wichtigsten offenen Punkte

QUANSATECH IT

BETRIEB UND REAKTION

Schutz im Alltag wirksam halten

Sicherheitsmaßnahmen müssen auch bei Urlaub, Personalwechsel und Zeitdruck funktionieren. Deshalb gehören Wartung, Erkennung und klare Entscheidungen zum selben Sicherheitsstand.

4. Updates und alte Systeme

Nicht jedes Update ist gleich dringend. Entscheidend sind Angriffsweg, Geschäftsrisiko und ein sicherer Wartungsablauf.

- [ ] Internet-erreichbare Systeme, Firewalls, VPN und kritische Schwachstellen werden besonders zeitnah beurteilt.
- [ ] Betriebssysteme, Geräte und Fachsoftware ohne Hersteller-Support sind bekannt.
- [ ] Für Sicherheitsupdates gibt es Verantwortliche, Wartungsfenster und eine Kontrolle des Ergebnisses.
- [ ] Bei alter Software sind Zwischenmaßnahmen und ein realistischer Migrationsweg festgelegt.

5. Meldungen und Reaktion

Ein Alarm hilft nur, wenn klar ist, wer ihn bewertet und welche nächste Handlung erlaubt ist.

- [ ] Wichtige Sicherheitsmeldungen und auffällige Anmeldungen erreichen eine zuständige Person.
- [ ] Notfallkontakte und wichtige Unterlagen sind auch ohne funktionierende Firmen-IT erreichbar.
- [ ] Es ist geklärt, wer Systeme trennen, Konten sperren oder externe Hilfe anfordern darf.
- [ ] Nach einem Vorfall werden Ursache, Maßnahmen und offene Risiken nachvollziehbar dokumentiert.

6. Offene Punkte richtig einordnen

Nicht alles muss gleichzeitig umgesetzt werden. Jeder offene Punkt erhält eine verantwortliche Person, einen realistischen Termin und ein prüfbares Ergebnis.

A - sofort klären	B - zeitnah planen	C - geordnet verbessern
Fehlender Schutz für zentrale Zugänge, unklare Sicherung oder keine realistische Wiederherstellung bei einem kritischen Ausfall.	Hohes Betriebsrisiko mit vorhandener Zwischenlösung. Verantwortung, Termin und erwartetes Ergebnis festlegen.	Dokumentation, Komfort und zusätzliche Schutzebenen, nachdem die kritischen Grundlagen belastbar sind.

Sicherheitsstand unverbindlich einordnen

Quansatech prüft den vorhandenen Stand und ordnet die nächsten Schritte ohne unnötigen Komplettumbau.
Kerngebiet Oberösterreich.
+43 720 895056 | **office@quansatech.at**
www.quansatech.at/it-sicherheit-oberoesterreich/