MZO AG
Versicherung & Vorsorge

IT-Sicherheit in Ihrem KMU

Verschaffen Sie sich einen Überblick
und versichern Sie Ihre Daten

- Übersicht über die Cyber-Risiken
- Sicherheit im Betrieb
- Sicherheit durch Ihr Personal
- Sicherheit durch eine Versicherung

mit **Checkliste** für mehr IT-Sicherheit

www.mzo.ch

Wir haben den 360° Blick

Unser Beratungsansatz beleuchtet das Thema IT-Sicherheit aus drei Perspektiven

Vernetzte Geräte und Maschinen, Daten in der Cloud oder die digitale Kommunikation: Die Digitalisierung erhöht die Effizienz in den Betrieben, bringt aber auch neue Gefahren. **Cyberrisiken zählen heute zu den grössten und unberechenbarsten Gefahren für Unternehmen.** Ein Datenverlust, blockierte oder fehlgeleitete IT-Systeme, eine Lösegeldforderung oder hohe Wiederherstellungskosten können verheerend sein. Das Thema IT-Sicherheit in einem Betrieb muss deshalb Chefsache sein und gesamtheitlich angegangen werden.

Übersicht über die Cyber-Risiken

Die Digitalisierung (und damit die Gefahr von Cyber-Angriffen) umfasst alle Branchen. Je nach Betrieb sind die Risiken unterschiedlich gelagert. Verschaffen Sie sich einen Überblick über mögliche Gefahren, deren Risiken und Folgen.

Gefahren und Ursachen

Hackerangriff
DoS/DDos-Attacke, Brute-Force Attacke, Umgehung Firewall, Phishing etc.

Schadsoftware
Viren, Trojaner, Spyware, Ransomware

Verhalten Anwender
Anwendungsfehler, Ausnutzen des Verhaltens (Social Engineering), Sabotage durch Mitarbeitende

Bedienung Netzwerk
Fehlerhafte Bedienung des Computernetzwerks

Wartung
Mangelnder Unterhalt und Pflege des Computernetzwerks

Technisches Versagen
Headcrash Festplatte, Ausfall Computersystem ohne Cyber-Attacke

Diebstahl oder Sabotage
Diebstahl von Datenträgern (z.B. Laptop, Smartphone) oder mutwilige Beschädigung

Externe Schäden
Schäden beim IT-Dienstleister oder Cloud-Anbieter

Reduzieren Sie die potentiellen Gefahren durch Personalschulungen.

Risiko

Vertraulichkeit
Unbefugter Zugriff auf Systeme und Entwendung von Daten

Integrität
Datenlöschung oder schädigende Manipulation

Verfügbarkeit
Unterbruch und Blockade von Daten und Systemen

In allen drei Bereichen kann eine Erpressungssituation entstehen.

Minimieren Sie die Risiken durch geeignete Massnahmen im Betrieb.

Folgen

Finanzielle Auswirkungen
Forensikkosten, Entfernung von Schadsoftware, Wiederherstellung von Daten und Systemen, Kosten und Verluste beim Zahlungsverkehr, Telefonie, Warenverlust sowie Lösegelder

Betriebsunterbruch
Stillstand von Betrieb und Produktion, Mehrkosten

Datenschutzverletzungen
Veröffentlichung von vertraulichen Daten, evt. behördliche Verfahren

Reputationsrisiken
Krisenmanagement und Reputationsmassnahmen für Kundschaft und Öffentlichkeit

Verlagern Sie die Kosten eines Cyberangriffs auf eine Versicherung.

Sicherheit im Betrieb

IT Security Audit – Stresstest für Ihre IT

In den meisten Fällen ist man genau dort angreifbar, wo man es kaum vermutet. Bereits mit wenigen Massnahmen lässt sich jedoch die Sicherheit in Ihrem Betrieb erhöhen. Lesen Sie dazu auch auf der letzten Seite unsere Tipps zu den minimalen IT-Grundregeln.

> «Im Schnitt dauert es 200 Tage, bis ein Unternehmen merkt, dass es attackiert worden ist. In über 50% der Fälle führt eine Attacke zu einem Unterbruch von Geschäftsprozessen.»

Quelle: KPMG

Gemeinsam mit unserem Partner Weibel/IT AG bieten wir ein «IT Security Audit» an. Mit diesem Stresstest werden Schwachstellen aufgedeckt – bevor es ungebetene Gäste tun. Ein «IT Security Audit» ist eine systematische Risiko- und Schwachstellenanalyse. Sie erhalten einen schriftlichen Bericht inklusive Empfehlungen.

Kosten

ab **CHF 1'400.–**

Mandatskunden der MZO profitieren von 10% Rabatt. Dank dem Security Audit reduziert sich zudem die Prämie bei der Cyber-Versicherung.

Sicherheit durch Ihr Personal

Awareness Training – Plattform für Ihr Personal

Längst nicht alle Cyberattacken zeichnen sich durch raffinierte Angriffsstrategien aus. Noch immer hoch im Kurs stehen E-Mail-Angriffe mit infizierten Office-Dokumenten oder PDF. Der Schulung und Sensibilisierung des Personals ist deshalb höchste Aufmerksamkeit zu schenken.

> «Bei den meisten Angriffen kommen den Hackern vermeidbare Sicherheitslücken und unvorsichtiges menschliches Verhalten zugute.»

Quelle: Computerwoche.de

Die MZO AG bietet ein webbasiertes «Awareness Training» an. Auf der digitalen Plattform wird Ihr Team innerhalb eines Jahres durch verschiedene 10- bis 15-minütige Lektionen geführt, welche optimal neben dem Arbeitsalltag erledigt werden können. Damit fördern Sie das Wissen Ihrer Mitarbeitenden und tragen dazu bei, teure Cyberattacken zu vermeiden.

Kosten

CHF 70.–
pro Mitarbeiter:in / Jahr

Mandatskunden der MZO bezahlen nur CHF 60.–.

Sicherheit durch eine Versicherung

Versichern Sie Ihre Daten, solange Sie noch können

Eine Cyber-Versicherung ist ein Auffangnetz ähnlich einem Sicherheitsnetz, welches vor Steinschlag schützt. Längst nicht an jeder Hanglage ist ein solches Sicherheitsnetz notwendig.

Ob für Ihr Unternehmen ein solcher Schutz notwendig ist, stellen wir gemeinsam mit Ihnen fest. Folgendes Raster hilft Ihnen wie uns in der Entscheidungsfindung.

Daten

- Verarbeiten Sie vertrauliche Unternehmens-, Kunden- oder Personendaten?
- Ist Ihr Betrieb abhängig von der unmittelbaren Verfügbarkeit von digitalen Daten?
- Welche Folgen haben die Nicht-Verfügbarkeit (Verlust, Blockade, Manipulation) von Daten für Ihren Betrieb?
- Wie aufwändig ist eine Wiederherstellung der Daten?

Infrastruktur

- Welche Infrastruktur kann von einem Angriff betroffen sein (Maschinen, Server, EDV, Webseite, E-Payment)?
- Welche Folgen hat ein Ausfall der digitalen Infrastruktur für Ihren Betrieb?

Risikoeinschätzung

- Wie rasch hat ein Ausfall von Daten und Infrastruktur signifikanten Einfluss auf die Geschäftstätigkeit?
- Wie hoch ist der erwartete Umsatzausfall?
- Welche präventiven Massnahmen haben Sie im Betrieb bereits umgesetzt?

Ist nun der Entscheid für eine Cyberversicherung gefallen, so prüfen wir für Sie im Detail die Deckungen inklusive der versicherten Gefahren.

Vorsicht: In den AVB (Stichwort «Obliegenheiten») geben die Versicherungen vor, welche Vorgaben Sie hinsichtlich technischer und organisatorischer Massnahmen zu erfüllen haben.

Eigenschäden

- Daten- und System-wiederherstellung
- Maschinen und Produktion
- E-Banking und Kreditkarten
- Telefonhacking
- Social Engineering
- Lösegeld-Erpressung
- Betriebsunterbruch

Haftpflicht

- Ansprüche Dritter
- Datenschutz-Verletzungen
- Verletzung PCI-Standards

Dienstleistungen

- Rechtsschutz
- 24 Stunden- und 7 Tage-Erreichbarkeit
- Spezialisierte IT-Dienstleister (Forensik, Schadenbehebung)
- Freie Dienstleisterwahl (eigener IT-Dienstleister)
- Krisenmanagement (Datenschutz, Reputation, Erpressung)

Technische Versicherung

- Technische Schäden an Maschinen, Anlagen und EDV

Vertrauensschaden-versicherung

- Vermögensschäden infolge Diebstahl, Betrug oder Erpressung (z.B. fehlgeleitete Zahlungen aufgrund vorgespielter Identität)

Kosten

Preis wird individuell nach Bedürfnis und Gegebenheiten berechnet

Mit wenigen Massnahmen IT-Sicherheit erhöhen

Minimale IT-Grundregeln für jedes KMU

Check-Liste

Backup

Die wohl wichtigste Grundregel: Sichern Sie Ihre Daten!

Was soll - wie oft
- von wem
- wohin und
- wie lange

gesichert werden?

Beziehen Sie auch Ihre SaaS und Cloud-Dienste mit ein. Von wem können die Daten wieder hergestellt werden und wie lange dauert ein operativer Unterbruch bei einem Datenverlust?

Wenden Sie beim Backup die 3-2-1-Regel an:

- ☐ 3 Kopien aller kritischen Daten auf
- ☐ 2 unterschiedlichen Medien, davon sollte
- ☐ 1 offsite gelagert werden, sprich an einem anderen Standort als die Original-Daten.

Passwortrichtlinien

- ☐ Erstellen Sie eine interne Passwortrichtline mit Ihren Vorgaben.
- ☐ Für jedes Portal und für jedes Login ein eigenes Passwort verwenden.
- ☐ 2-Faktor-Authentifizierung sollte Standard sein.
- ☐ Passwörter unbedingt sicher aufbewahren.

Berechtigungskonzept

- ☐ Jeder Mitarbeitende (Rolle) sollte nur so viele Rechte haben, wie nötig.
- ☐ Vergeben Sie keine lokale Administratorenrechte.
- ☐ In einem Portal sollte die Rolle «Admin» immer mit einem separaten Benutzer gelöst werden.

Technische Schutzmassnahmen

- ☐ Aktueller Virenschutz, Spamfilter dazu evtl. eine Firewall. Je nach Branche sind weitere Massnahmen notwendig.
- ☐ Server und andere zentrale Infrastrukturkomponenten sollten vor physischem Zutritt und vor Überspannung geschützt werden.
- ☐ Updates und Patches zeitnah nach Veröffentlichung bei allen mit dem Internet verbundenen Geräten und Systemen installieren.

Mitarbeiter-Sensibilisierung

Häufigstes Einfallstor für Cyber-Attacken sind die Mitarbeitenden, welche durch gezielte Manipulation (Phishing-Mails, betrügerische Anrufe) dazu gebracht werden, Informationen preiszugeben oder Handlungen auszuführen.

- ☐ Regelmässige Thematisierung von Cyber-Gefahren und Datenschutz im Team.
- ☐ Awareness Training der MZO

IT-Verantwortlicher

- ☐ Bestimmen Sie einen internen IT-Verantwortlichen.
- ☐ Ziehen Sie in Ihre Überlegungen die Lieferanten und Verträge mit ein.
- ☐ Wer ist bei den Applikationen Ihr Ansprechpartner (1st Level / 2nd Level)?
- ☐ Was sind Ihre Sofortmassnahmen bei einem Cyber-Vorfall?

Denken Sie auch an folgende Themen

- ☐ Verschlüsselung besonders schützenswerter Daten gemäss neuem Datenschutzgesetz (in Kraft ab Sept. 2023).
- ☐ Wer ist Ihr Datenschutzverantwortlicher?
- ☐ Gesicherte und verschlüsselte E-Mails oder Kommunikationsverbindungen im Internet (VPN).
- ☐ Erfüllung der PCI-DSS Standards beim Angebot von Kredit-/Debitkarten-Zahlungen für Kunden.

Daten in der Cloud

Die Auslagerung von Daten in die Cloud ist keine Schadlosgarantie.

Die Datensicherheit bleibt in Ihrer Verantwortung und Cloud-Anbieter haften in der Regel nicht für Schäden. Zumal ein Angriff auf Cloud-Daten, zum Beispiel durch Social Engineering (Ausnutzung von Mitarbeitenden-Verhalten), weiter möglich ist.

Unser Tipp: Prüfen Sie unbedingt das Backup-Konzept des Cloud-anbieters.

Nutzungsbestimmungen von Microsoft365: «Sie sind für den Schutz der Sicherheit Ihrer Daten und Identitäten, lokalen Ressourcen und der von Ihnen gesteuerten Cloudkomponenten zuständig.»