Bewertung (23) Lesezeit 3 Minuten

Erstellt am 11.01.2019

IT-Sicherheit und Datenschutz: Diese Fehler sollten Kleinunternehmen vermeiden

Die IT-Sicherheit und der Datenschutz bereiten Kleinunternehmen aufgrund der Digitalen Transformation zunehmend Kopfzerbrechen. Wolfgang Sidler, Inhaber des IT-Beratungsunternehmens Sidler Information Security, zeigt die grössten Fehler auf, die Kleinunternehmer vermeiden sollten.

Fehler 1: Die Geschäftsleitung nimmt IT-Sicherheit und Datenschutz nicht Ernst

Machen Sie es besser, indem Sie als Inhaber oder Mitglied der Geschäftsleitung IT-Sicherheit und den Datenschutz vorleben und Weisungen erstellen wie zum Beispiel zum Umgang mit Passwörtern, mobilen Geräten, Informationen, E-Mail und Internet. Zeigen Sie, dass Ihnen persönlich das Thema IT-Sicherheit und Datenschutz wichtig ist, und sorgen Sie dafür, dass entsprechende Massnahmen eingeleitet und auch umgesetzt werden.

Fehler 2: Kostenlose Cloudlösungen verwenden

Kostenlose Clouds sind zwar praktisch und leicht zugänglich – jedoch kein Ort, an dem vertrauliche Dokumente wie Kundenverträge oder Listen mit Einkaufspreisen hochgeladen werden. Bedenken Sie, dass Ihre Daten bei kostenlosen Cloudlösungen in der Regel ausserhalb der Schweiz gespeichert werden und keinen genügenden Schutz bieten. Lassen Sie bei Cloudlösungen Vorsicht walten und setzen Sie im Minimum auf zertifizierte Clouddienste aus der Schweiz.

Fehler 3: Mitarbeiter sind zu wenig sensibilisiert

Eine der grössten Gefahren bei der IT-Sicherheit und beim Datenschutz sind fahrlässiger Datenverlust oder Datendiebstahl durch eigenes Fehlverhalten oder durch Fehlverhalten der Mitarbeiterinnen und Mitarbeiter. Wenn etwa ein Geschäfts-Notebook unbeaufsichtigt in einem externen Besprechungsraum liegenbleibt, Passwörter auf Post-it-Zetteln am Computer deponiert oder vertrauliche Dokumente in die kostenlose Dropbox gestellt werden, kann dies für das Unternehmen gravierende Folgen haben. Sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter für das Thema IT-Sicherheit und Datenschutz und schulen Sie sie. Es lohnt sich. Denn die aufwändigsten Firewalls und Security-Lösungen bringen nichts, wenn Mitarbeitende durch falsches Verhalten unerwünschte Übergriffe ermöglichen.

Das Thema IT-Sicherheit und Datenschutz ist zu existenziell, um es zu ignorieren. Packen Sie das Problem an und machen Sie Budget frei, um die Situation mit einem externen Berater in Ihrem Unternehmen zu klären und zu optimieren. Wählen Sie dabei einen pragmatischen Ansatz, indem Sie lieber einige wenige Massnahmen festlegen, diese dann aber auch umsetzen. Auf diese Weise vermeiden Sie, dass die IT-Sicherheit und der Datenschutz nicht zum Fass ohne Boden werden. Bei der Auswahl der Massnahmen empfiehlt es sich, das Zieldreieck Risiken, Benutzerfreundlichkeit und Kosten zu berücksichtigen.

Fehler 5: Kein Risikomanagement

Die Basis für jegliche Massnahme bei der IT-Sicherheit und Datenschutz ist ein effektives Risikomanagement. Machen Sie sich grundsätzlich einmal Gedanken darüber, welchen Risiken Ihr Unternehmen ausgesetzt ist und welches der Worst Case beim Eintreffen der grössten Risiken wäre. Stellen Sie sich dazu folgende Fragen:

- Welches sind in Bezug auf IT und Daten unsere Kronjuwelen, die geschützt werden müssen?
- Welche Bedrohungen und Gefahren bestehen gegenüber unseren Kronjuwelen?
- Welches sind die Risiken und Schwachstellen Ihrer IT-Infrastruktur?
- Welchen Schaden kann eine Sicherheitslücke für Ihr Unternehmen anrichten?

Planen Sie dann für jedes identifizierte Risiko Massnahmen, schätzen Sie die Kosten für die Umsetzung und bestimmen Sie Verantwortlichkeiten und Termine. Und seien Sie sich auch bewusst, dass eine 100-prozentige Sicherheit nicht möglich ist. Definieren Sie, welche Restrisiken Sie bewusst in Kauf nehmen und tragen können. Eine immer häufiger werdende Lösung sind Cybercrime-Versicherungen.

Fehler 6: Einmalprojekte statt Daueraufgabe

In Zeiten der digitalen Transformation verändert sich die Ausgangslage für die IT-Sicherheit und den Datenschutz immer schneller. Betrachten Sie IT-Sicherheit und Datenschutz als Daueraufgabe – nicht als ein Projekt mit einem Anfang und einem Ende. Und überprüfen Sie in regelmässigen Abständen, ob sich Ihre IT auf dem aktuellen Sicherheitsstand befindet.

Fehler 7: Mangelnde Benutzerberechtigungen

know-Prinzip). Überprüfen Sie jährlich die effektiven Benutzerberechtigungen und etablieren Sie einen wirksamen Mitarbeiter Ein- und Austritt-Prozess.

Fehler 8: Keine organisatorischen Begleitmassnahmen

Jede technische Massnahme zur IT-Sicherheit und zum Datenschutz zieht eine organisatorische Massnahme nach sich, vergleichbar mit einem Auto, das regelmässig einem Service unterzogen wird. Lässt man zum Beispiel eine Firewall installieren, muss diese immer auf dem neusten Stand gehalten werden. Definieren Sie dazu Aufgaben, Verantwortlichkeiten und Termine.

Gut zu wissen

Die im Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (DSGVO/GDPR) regelt europaweit, wie Unternehmen mit personenbezogenen Daten umgehen müssen. Die DSGVO gilt auch gegenüber Firmen mit Sitz in der Schweiz, die personenbezogene Daten von Internetnutzern in der EU auf ihren Webseiten erfassen (z.B. in Form von Cookies), um ihnen in der EU Waren oder Dienstleistungen anzubieten. Neu müssen die Unternehmen hierfür von den Betroffenen die Einwilligung direkt einholen oder darlegen, dass ihr Interesse auf Datenerhebung gegenüber dem Grundrecht der betroffenen Personen auf Datenschutz überwiegt.

Sicherheitsberater der 2009 gegründeten Sidler Information Security GmbH aus Hünenberg und berät KMU und grosse Unternehmen bei der IT-Sicherheit und Datenschutz. Er arbeitet zudem seit 2009 für den Datenschutzbeauftragten des Kantons Luzern und doziert an der Universität Luzern an der Fakultät Rechtwissenschaften. Zuvor war der Wirtschaftsinformatiker mit einem Master of Advanced Studies in Information Security bei verschiedenen Banken, Versicherungen und Unternehmen als Sicherheitsexperte tätig – auch international.

Bewertung (23)

Beitrag teilen

Das könnte Sie ebenfalls interessieren

Rücken Sie Ihre Kunden ins

Digitale Transformation in

Die Dos und Don'ts beim