Text: Andreas Heer | Medien:Swisscom

Ein Beispiel von dreien: Das Backup läuft zwar, aber niemand hat die Wiederherstellung getestet. Um solche Fälle von trügerischer Sicherheit müssen sich Geschäftsführer kümmern. Erfahren Sie im Artikel, wo die Risiken liegen und wie Sie sie mildern.

Die meisten KMU unternehmen diverse Anstrengungen für Datenschutz und Datensicherheit. Doch unklare Zuständigkeiten und Verantwortlichkeiten unterlaufen den Schutz vor Datenverlust und Cyberattacken. Drei Beispiele – und Lösungsansätze.

Die Daten werden regelmässig im Backup gesichert, der IT-Partner spielt Updates ein und der Zugriff auf die Cloud-Datenablage ist mit verschiedenen Zugriffsrechten geregelt. Alles im grünen Bereich also? Schauen wir genauer hin und entlarven wir die Irrtümer, die die gut gemeinten Sicherheitsmassnahmen wieder zunichte machen. Die drei Beispiele haben etwas gemeinsam: Das Scheitern liegt nicht an der Technik, sondern an organisatorischen Fehleinschätzungen.

Ein genauer Blick lohnt sich, denn Geschäftsführer und Inhaberinnen sind von Gesetzes wegen verantwortlich für Datenschutz und Datensicherheit in ihrem KMU. Diese Verantwortung sowie das Risiko lassen sich nicht auslagern – weder an Mitarbeitende noch an IT-Dienstleister oder an eine Versicherung. Und das neue Datenschutzgesetz (nDSG), das am 1. September dieses Jahres in Kraft tritt, erhöht die Ansprüche an die Datensicherheit als Voraussetzung für den Datenschutz. Jetzt ist also ein guter Moment, um die getroffenen Massnahmen zu prüfen, zu hinterfragen – und zu verbessern. Dieser Artikel zeigt mögliche Probleme auf und liefert Lösungsansätze in Form einer Checkliste.

Irrtum 1: Dank Backup sind die Daten gesichert

In regelmässigen Abständen sichert das KMU seine wichtigen Geschäftsdaten – Office-Dokumente, die Datenbanken von CRM und ERP, Handbücher und was sonst noch an relevanten digitalen Informationen anfällt. Doch im Notfall muss sichergestellt sein, dass die Daten auch wiederhergestellt werden können. Und Cyberkriminelle dürfen bei einem erfolgreichen Angriff keinen Zugriff auf die Backups erhalten, weil sie diese sonst verschlüsseln und unbrauchbar machen oder veröffentlichen können.

Überdenken Sie Ihre Backup-Strategie, falls eine dieser Aussagen auf Sie zutrifft:

- Die Sicherung ist permanent von einem PC aus zugänglich, weil sie auf einer externen Festplatte oder in einem Netzwerkspeicher liegt.
- Die Sicherung ist unverschlüsselt.
- Es gibt keine Prüfung, ob die Wiederherstellung funktioniert und ob die Backup-Medien verfügbar und lesbar sind.

Irrtum 2: Zugriffsrechte und persönliche Konten schützen unsere Daten

Im Prinzip ist diese Aussage korrekt. Doch in der Realität schaut die Situation oftmals anders aus, indem beispielsweise alle auf alles Zugriff haben. Was vielleicht als Vertrauensbeweis in die Mitarbeitenden gedacht ist, erleichtert Cyberkriminellen die Arbeit ungemein.

Auch hier: Wenn eine der folgenden Aussagen auf Sie zutrifft, sollten Sie die Berechtigungen überprüfen:

- Alle Mitarbeitenden haben Zugriff auf die gesamte Dokumentenablage – mit wenigen Ausnahmen wie Buchhaltung und HR.
- Wenn Mitarbeitende das Unternehmen verlassen, bleiben die Konten eine Zeit lang aktiv.
- Für gewisse Cloud-Dienste oder das Intranet nutzen mehrere Mitarbeitende dasselbe Konto und Passwort.

Irrtum 3: Wir spielen regelmässig Updates ein

Das Problem liegt in der Definition von «regelmässig»: Spielen Sie Sicherheits-Updates sofort nach Erscheinen ein, oder gibt es fixe Zeitintervalle, in denen Ihr KMU selbst oder der IT-Partner Arbeitsstationen und Server aktualisiert? Bei schwerwiegenden Sicherheitslücken in Windows und in Office-Anwendungen (Microsoft 365) verschaffen Sie Cyberkriminellen mit verzögerten Updates ein – hoch willkommenes – Zeitfenster, um die Lücke auszunutzen.

Sie kennen es bereits: Wenn eine der folgenden Aussagen auf Sie zutrifft, sollten Sie die Update-Strategie hinterfragen:

- Wir (oder der IT-Partner) installieren Updates in definierten Zeitabständen.
- Wir haben Systeme in Betrieb, für die es keine Sicherheits-Updates mehr gibt.

- Gewisse Systeme können wir nicht aktualisieren, weil die Software, die darauf läuft, zu alt für neuere Betriebssysteme ist.

Testen Sie Ihre IT-Sicherheit

Über 30 Prozent aller Schweizer KMU wurden bereits Opfer eines Cyberangriffs. Wie gut sind Sie geschützt? Mit unserem IT-Security-Check prüfen Sie das Sicherheitsniveau Ihres Unternehmens und erfahren, welche Massnahmen Sie ergreifen könnten.

Zum Security-Check

Checkliste: Fragen an den IT-Partner zur Stärkung der IT-Sicherheit

Solche Sicherheitsprobleme sind meist keine Absicht. Sondern sie entstehen aufgrund unklarer Verantwortlichkeiten zwischen KMU und IT-Partner, mangelhafter Dokumentation oder Kostendruck bei IT-Dienstleistungen. Zeitnahe Updates beispielsweise bedingen häufigere Einsätze der IT-Fachleute oder des IT-Partners. Und gerade Updates sind ein gutes Beispiel dafür: IT-Sicherheit ist ein kontinuierlicher Prozess, den es laufend zu hinterfragen und anzupassen gilt.

Es lohnt sich, bei IT-Sicherheit näher hinzuschauen und Klarheit zu schaffen. Die Transparenz über Aufgaben und Verantwortlichkeiten zeigt Ihnen, wo Ihr KMU steht. Mit den passenden Sicherheitsmassnahmen reduzieren Sie die Risiken eines Cyberangriffs und den damit verbundenen Reputationsschaden sowie Betriebsausfälle. Ein ausgearbeiteter und kommunizierter Notfallplan senkt die Auswirkungen eines potenziellen Angriffs.

Diese Checkliste fasst wichtige Punkte zusammen, die Sie zusammen mit Ihrem IT-Partner diskutieren können, um zusammen die IT-Sicherheit zu professionalisieren:

1. **Geschäftskritische Daten und Applikationen:** Was benötigen Sie zwingend, um den Betrieb zu gewährleisten? Dies gibt Ihnen einen Hinweis auf die Priorisierung von IT-Sicherheitsmassnahmen.
2. **Leistungsbeschrieb der Serviceverträge:** Welche Aufgaben und Verantwortlichkeiten sind darin geregelt? Sind beispielsweise die Verschlüsselung von Backups festgehalten, das Update-Intervall, das Benutzermanagement oder die Reaktionszeit bei einem Ausfall?
3. **Dokumentation:** Gibt es eine standardisierte Checkliste für Wartungsarbeiten? Werden die erledigten Aufgaben protokolliert?

Haben Sie als Geschäftsführer dank der Dokumentation Transparenz über den aktuellen Zustand Ihrer IT?

4. **Security-Assessment:** Müssen Sie Klarheit schaffen über den aktuellen Stand Ihrer IT-Sicherheit? Mit einem Assessment erhalten Sie eine detaillierte Zustandsbeschreibung Ihrer Infrastruktur und können allfällige Optimierungs-Massnahmen auf Faktenbasis planen.
5. **Zusatzaufwände:** Wie werden zusätzliche Leistungen geregelt und verrechnet? Darunter fällt beispielsweise der ungeplante Austausch von Hardware oder die Anpassung von Firewall-Regeln ausserhalb der vereinbarten Wartung.
6. **Notfallplan:** Und zum guten und wichtigen Schluss: Funktionieren die Notfallmassnahmen bei einem Datenverlust oder Cyberangriff? Dazu gehört, dass präventive Sicherheitsmassnahmen wie ein Backup oder der Ausfall redundanter Netzwerkkomponenten getestet werden, bevor etwas passiert.

Die regelmässige Überprüfung und Anpassung von IT-Sicherheitsmassnahmen senkt das Risiko vor Datenverlust und erfolgreichen Cyberangriffen und damit auch das Risiko vor Betriebsausfällen. Zudem ist IT-Sicherheit ein zentraler Bestandteil der Vorgaben im neuen Datenschutzgesetz, das die Geschäftsleitung in die Verantwortung und Fürsorgepflicht gegenüber ihren Mitarbeitenden nimmt. Das nDSG sieht bei Verstössen eine persönliche Haftung und entsprechende Bussen vor. Mit einer erhöhten IT-Sicherheit verringern Sie das Risiko solcher Vorfälle und schützen damit sich selbst und Ihre Mitarbeitenden.