IFAKTOR
Systeme | Software | Service

DIE 4 SECURITY-VERSÄUMNISSE VIELER KMUS

Cyberkriminalität gefährdet zunehmend die Systeme und die Datenintegrität kleiner und mittlerer Unternehmen – denn gerade ihnen fehlt es häufig an Security-Expertise und IT-Manpower. Wie gut ist Ihr Unternehmen in Sachen IT-Sicherheit aufgestellt? **Machen Sie jetzt unseren Cyber-Sicherheits-Check speziell für KMUs.**

Die Hälfte aller Cyber-Attacken in Deutschland betrifft inzwischen KMUs. Einer der Gründe dafür: Die – heute oft organisierten – Cyberkriminellen haben sie als leichte Opfer identifiziert, da das Thema IT-Sicherheit in vielen KMUs immer noch nicht Chefsache ist. Große Sicherheitslücken gibt es speziell bei den Themen Backups, Rollen und Rechte, Notfallplan und Mitarbeitersensibilisierung. Wie gut ist Ihr Unternehmen gewappnet? Mit unserer IT-Security-Checkliste machen Sie eine schnelle Selbstdiagnose.

Sven Berghoff
Mitglied der Geschäftsleitung bei ifaktor

Liebe Geschäftsführerinnen, liebe Geschäftsführer,

wenn die kritische Bedeutung von Cyber Security für KMUs heute so oft beschworen wird, dann hat das einen handfesten Grund: Die Zahl der Angriffe steigt rasant und sie richten sich immer häufiger gegen KMUs. **Insgesamt waren in Deutschland 2020/21 etwa neun von zehn Unternehmen betroffen**, berichtet Bitkom – etwa die Hälfte von ihnen KMUs. Gesamtschaden für die deutsche Wirtschaft in diesem Zeitraum: 223 Milliarden Euro.

9 von 10 Unternehmen Ziel von Angriffen

Ein Grund dafür, dass zunehmend KMUs ins Visier organisierter Cyberkrimineller geraten, ist ihre Wehrlosigkeit. Denn gefährlich vernachlässigte Schutzvorkehrungen machen gerade kleinere und mittlere Unternehmen zu leichten Opfern. Das interne IT-Team ist oft mit dem Tagesgeschäft komplett ausgelastet, nicht ausreichend geschult oder – auch das gibt es leider – externe Dienstleister machen ihren Job schlecht, um es mal so klar zu sagen.

IT-Security muss Chefsache werden

Und obwohl IT-Security definitiv Chefsache sein sollte: Viele GFs vertrauen mehr oder weniger blind darauf, dass an dieser Front alles Notwendige getan wird. In der Mehrzahl der Fälle leider zu Unrecht. Das beginnt bei der fehlenden Sensibilisierung der Mitarbeiter. Denn zu den häufigsten Einfallstoren für Schadsoftware gehören Phishing-Mails, die vom Team nichtsahnend geöffnet werden. Auch ein zu sorgloser Umgang mit Zugriffsrechten bildet häufig eine offene Flanke, etwa für Ransomware. Das ist Schadsoftware, mit der Kriminelle Daten verschlüsseln und diese nur gegen hohe Lösegeldzahlungen wieder freigeben – bei KMUs die häufigste Methode von Angriffen. Und schließlich, wenn der GAU dann eingetreten ist, fehlt in vielen Unternehmen ein Notfallplan.

Es gibt die einschlägigen Sicherheitsvorkehrungen, die wir alle auch privat treffen sollten – dazu gehören Virenschutzprogramme und Firewalls, sichere Passwörter, regelmäßige Passwortwechsel und eine Zwei-Faktor-Identifizierung, wo immer es geht. In Unternehmen gehen die Anforderungen darüber natürlich weit hinaus. Auf Basis unserer täglichen Erfahrung haben wir vier Punkte ermittelt, bei denen es in der Praxis bei KMUs oft hapert. Die Checkliste, die wir daraus abgeleitet haben, hilft Ihnen bei der Selbstdiagnose: Ist Ihr Unternehmen ausreichend geschützt? Die Checkliste sollten Sie mit Ihrem eigenen IT-Team oder einem externen IT-Dienstleister sorgfältig durchgehen, um Handlungsbedarf zu erkennen.

DIE IT-SECURITY CHECKLISTE: 4 VERSÄUMNISSE VON KMUS

01

SCHLECHTE BACKUPS

Werden Ihre geschäftskritischen Daten regelmäßig extern gesichert?

Wo liegen die Schwächen?

Viele GFs gehen davon aus, dass es Backups gibt. Damit haben sie meistens recht, aber meine tägliche Erfahrung zeigt: Oft sind diese Backups schlecht umgesetzt, selbst, wenn externe IT-Dienstleister beauftragt wurden. Zudem werden viele Backups nicht gründlich getestet – was nicht funktioniert, zeigt sich erst, wenn es zu spät ist. Ein weiterer kritischer Punkt: Reicht die Datensicherung weit genug zurück?

Welche Gefahren drohen?

Sind, etwa bei einem Verschlüsselungs-Trojaner, alle Daten weg und es ist kein Back-up verfügbar, drohen hohe Lösegeldforderungen. Ein Wiederherstellen von Daten kann extrem zeitaufwendig sein und lange Systemausfälle können das Geschäft bis hin zur Pleite beeinträchtigen – **siehe den Fall des Fahrradherstellers Prophete**, der nach einem mehrwöchigen Betriebsstopp infolge eines Cyberangriffs im Dezember 2022 Insolvenz anmelden musste.

Ein weiterer häufiger Schwachpunkt: Werden Daten, etwa durch menschliche Fehler, versehentlich gelöscht und dies fällt erst Monate später auf, reicht das Backup in vielen Fällen nicht weit genug zurück. Beispiel: Bei Microsoft 365 werden Backups im Standard schon nach 30 Tagen gelöscht und die Daten sind dann für immer verloren. Für den Fall von Ereignissen wie Feuer- oder Wasserschäden ist es außerdem wichtig, dass Backups geografisch getrennt gespeichert sind.

Wo steht Ihr Unternehmen?

Je mehr Fragen Sie mit Ja beantworten können, desto sicherer ist Ihr Backup-System.

Ja	Nein	Weiß nicht	
☐	☐	☐	Verfügen Sie über ein separates, getrenntes Backup?
☐	☐	☐	Haben Sie eine Backup-Strategie, die festlegt, welche Daten wo und wie lange gesichert werden?
☐	☐	☐	Ist Ihr Backup geschützt vor Feuer- und Wasserschäden?
☐	☐	☐	Haben Sie evaluiert, ob ein Cloud-Backup für Sie sinnvoll ist?
☐	☐	☐	Ist die Backup-Frequenz für Ihr Business wirklich hoch genug?
☐	☐	☐	Verfügen Sie über ein redundantes System mit mehrfacher Datensicherung?
☐	☐	☐	Werden Ihre Backups mindestens einmal jährlich getestet?

02 FALSCH GESETZTE ZUGRIFFSRECHTE

Sind Adminrechte und Rollen so verteilt, dass menschliche Fehler weitestgehend ausgeschlossen sind?

Wo liegen die Schwächen?

Eine rollenbasierte Rechteverwaltung ist nach meiner Erfahrung in der Mehrzahl der KMUs gar nicht oder nur mangelhaft umgesetzt. Ganz häufig sehen wir, dass Mitarbeitende über Rechte verfügen, die sie in ihrer Rolle gar nicht benötigen – ein hochgefährlicher Zustand, wie die Praxis immer wieder zeigt. Aber ein Konzept, das Businessprozessen und Sicherheitsbedürfnissen gleichermaßen gerecht wird, kann auch in weniger großen Organisationen schon sehr komplex sein.

Welche Gefahren drohen?

Mangelhaft regulierte Admin- und Zugriffsrechte sind ein weit offenes Einfallstor für Cyberangriffe. Trojaner und andere Schadsoftware können durch unbedachtes Handeln von Teammitgliedern Zugriff auf das gesamte Firmennetzwerk und alle Daten bekommen. Gerade in Zeiten von mobilem Arbeiten und Home Office ist die Gefahr groß, denn Mitarbeitende laden heute vermehrt sensible Daten auf mobile Geräte. Geht ein Device verloren, wird es gestohlen oder mit Schadsoftware infiziert, kann schnell ein existenzgefährdendes Datendesaster drohen.

Wo steht Ihr Unternehmen?

Je mehr Fragen Sie mit Ja beantworten können, desto sicherer ist Ihre Rechte- und Rollenverwaltung.

Ja	Nein	Weiß nicht	
☐	☐	☐	Sind Usern Ihrer IT-Systeme individuelle Benutzernamen, Kennwörter und Zugriffsrechte zugeteilt?
☐	☐	☐	Gibt es Zugriffsbeschränkungen und ist klar geregelt, welche Mitarbeitenden auf welche Daten zugreifen dürfen?
☐	☐	☐	Gibt es auch für Admins individuell und bedarfsgerecht zugeschnittene Zugriffsrechte?
☐	☐	☐	Ist klar geregelt, welche Rechte und Privilegien Anwenderprogramme und Benutzer innerhalb des Computersystems haben?
☐	☐	☐	Werden vertrauliche Daten und besonders gefährdete Devices wie Notebooks, Tablets oder Smartphones ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Aus der Praxis:

TROJANER-ANGRIFF AUF KÖLNER KMU

Zum Thema Verschlüsselungs-Trojaner möchte ich von einem aktuellen Vorfall aus meinem Arbeitsalltag berichten, wie er viele KMUs heute oder morgen betreffen könnte.

Ein Kölner Mittelständler engagierte uns vor einigen Monaten als IT-Dienstleister, weil er mit dem vorherigen Anbieter unzufrieden war: Systeme, Hardware und Software waren so veraltet, dass die IT zu einem echten Wachstumshindernis geworden war. Und, Sie ahnen es: Auch die IT-Sicherheit war extrem vernachlässigt worden, wie sich bald zeigte. Wunde Punkte waren hier zum Beispiel die Adminrechte der Mitarbeiter und mangelhafte Daten-Backups.

Neue, zeitgemäße Umgebung aufgesetzt

Wir bauten zunächst eine moderne IT-Umgebung auf. Das Benutzerrechte-System organisierten wir nach neusten Sicherheitsstandards um. Die Daten migrierten wir zu Microsoft 365 und richteten ein separiertes, externes Backup ein – für uns ein absolutes Muss, denn ein Backup auf dem selben System nutzt bei einem Angriff im Zweifelsfall gar nichts.

Totalausfall durch Verschlüsselungs-Trojaner

Unser Kundenunternehmen arbeitete unterdessen noch mit der alten Umgebung weiter. Soweit, so normal – bis der Kunde uns informierte, dass seine Telefonie ausgefallen war. Das erwies sich leider nur als die Spitze des Eisbergs, denn wir fanden in der alten Umgebung einen Verschlüsselungs-Trojaner, der zu diesem Zeitpunkt bereits ganze Arbeit geleistet hatte: Backups, Userdaten, Produktivdaten waren weg, die alte IT-Umgebung ein Totalausfall.

Cyberangriffe mit Folgen bis zur Insolvenz

Nur durch das extrem glückliche Timing kam der Kunde mit dem Schrecken davon, denn wir hatten die Daten ja bereits migriert und die neue Umgebung aufgesetzt. Das alte System schalteten wir komplett ab und zogen den Wechsel vor. Sogar die Telefonie über Microsoft Teams war sofort nutzbar. Unser Kunde entging so potenziell hohen Lösegeldforderungen und einem langwierigen System-Totalausfall – eine Situation, wie sie schon zu zahlreichen Insolvenzen geführt hat.

03 KEIN NOTFALLPLAN

Gibt es in Ihrem KMU klare Handlungsvorgaben für den Fall von IT-Ausfällen, Angriffen und sonstigen Schäden?

Wo liegen die Schwächen?

Ob Systemausfälle, Datenverlust, Malware oder Hackerangriffe: Die Panik ist naturgemäß erst einmal groß. Wie lange fallen welche IT-Strukturen aus? Wie lange lässt sich das durchhalten? Wie hoch fallen die Verluste aus? Je kritischer die betroffenen Businessprozesse sind, desto eher geraten Unternehmen hier in den existenzbedrohenden Bereich. Einen Riesenvorteil bringt ein zuvor festgelegter Notfallplan mit Sofortmaßnahmen und weiteren Handlungsanweisungen. Er muss von der ersten Sekunde an klarstellen, wer in welcher Situation was zu tun hat und welche Stellen zu informieren sind. Nur so können Ausfallzeiten minimiert und finanzielle und andere Schäden eingegrenzt werden. Wichtig dabei: Der Plan muss regelmäßig aktualisiert werden, da die Unternehmens-IT sich ja stetig weiterentwickelt.

Welche Gefahren drohen?

Schon kurze Systemausfälle können hohe Zusatzkosten und massive Umsatzeinbußen zur Folge haben, die schon viele Unternehmen in die Insolvenz gebracht haben. Wenn der Worst Case bereits eingetreten ist, ist es deutlich zu spät, sich Gedanken zu machen, wie man ihm begegnet. Chaos ist im Katastrophenfall ein Zustand, den sich kein Unternehmen leisten kann – erst recht kein KMU wie meins oder Ihres, die keine unermesslichen Ressourcen im Rücken haben.

Wo steht Ihr Unternehmen?

Sie haben noch keinen Notfallplan? **Finden Sie hier die Empfehlungen des BSI**. Falls Sie bereits einen Notfallplan erstellt haben, ist er umso sicherer, je mehr der folgenden Fragen Sie mit Ja beantworten können.

Ja	Nein	Weiß nicht	
☐	☐	☐	Haben Sie Ihren Notfallplan so abgelegt, dass Sie auch bei einem vollständigen Systemausfall Zugriff darauf haben?
☐	☐	☐	Wissen alle Mitarbeitenden, wie sie sich im Notfall zu verhalten haben?
☐	☐	☐	Haben Sie Ihre Business-Prozesse priorisiert – kritische Prozesse zuerst?
☐	☐	☐	Sind Passwörter für Notfälle sicher hinterlegt, mit einfachem Zugriff für schnellstmögliche Reaktionszeit?
☐	☐	☐	Ist Ihr Notfallplan aktuell auf Ihre IT abgestimmt, so wie sie heute besteht?

04 MITARBEITER SIND NICHT SENSIBILISIERT

Sind Ihre Mitarbeitenden bei Security-Themen ausreichend eingebunden und informiert?

Wo liegen die Schwächen?

Ich stelle immer wieder fest, dass die Bedeutung der Mitarbeitenden beim Thema Cyber Security enorm unterschätzt wird. Da gibt es Phishing-Mails, die kaum zu erkennen sind, wenn es seitens der Empfänger kein gesundes Grundmisstrauen gibt. Oder Angestellte, die bei mobilen Devices auf den Passwortschutz verzichten. Oder Social Engineering – eine Methode von Cyberkriminellen, Menschen so zu manipulieren, dass sie sensible Daten herausgeben. Sind Ihre Mitarbeitenden gegen solche Methoden ausreichend immunisiert? Security Awareness Trainings für Teams sind preiswert und überaus effektiv, wie Studien immer wieder belegen – aber in KMUs leider immer noch nicht Standard.

Welche Gefahren drohen?

Phishing-Mails sind die häufigsten Einfallstore für Malware in die Unternehmens-IT. Die wirtschaftlichen Schäden, die dadurch entstehen, sind enorm. Und gerade KMUs werden durch die hier oft unzureichende Aufklärung der Mitarbeitenden immer häufiger zu Angriffszielen. Versehentlicher Download von Malware, unfreiwillig preisgegebene Login-Daten, gestohlene mobile Devices ohne Passwortschutz … die Liste der Gefahren, die durch mangelnde Sensibilität der Mitarbeitenden entsteht, ist schier endlos.

Wo steht Ihr Unternehmen?

Je mehr Fragen Sie mit Ja beantworten können, desto besser ist es um die Security Awareness Ihrer Mitarbeitenden bestellt.

Ja	Nein	Weiß nicht	
☐	☐	☐	Lassen Sie regelmäßige Security Awareness Trainings durchführen?
☐	☐	☐	Lassen Sie regelmäßig Simulationen durchführen, um zu evaluieren, wie Ihre Mitarbeiter auf Phishing-Mails und andere Gefahren reagieren?
☐	☐	☐	Stellt Ihr Rollen- und Rechtesystem ein geringstmögliches Risiko sicher?

IHRE ERSTEN-SCHRITTE ZU MEHR IT-SICHERHEIT

Ich hoffe, dass der Cyber-Security-Check für einige Geschäftsführerinnen und Geschäftsführer ein Eye Opener ist. Denn ist die Gefahr erst einmal in ihrer ganzen Wucht erkannt, sind die ersten Schritte hin zu mehr IT-Sicherheit einfach, schnell und kostengünstig umsetzbar. Gehen Sie die IT-Checkliste mit Ihrem IT-Team, Ihrem externen IT-Dienstleister oder auch mit uns durch – wir beraten Sie gerne kostenlos und unverbindlich.

JETZT BERATUNGSGESPRÄCH BUCHEN

Ich freue mich auf das Gespräch mit Ihnen –
Ihr Sven Berghoff

Über ifaktor

Machen Sie Ihre IT zum Wachstumsfaktor: ifaktor ist Ihr strategischer IT-Dienstleister aus Köln. Ob als vollständige externe IT-Abteilung oder als Unterstützung Ihres IT-Teams: Wir sorgen für höchste IT-Sicherheit, reibungslosen Betrieb und eine innovative IT-Landschaft. Erwarten Sie passgenau abgestimmte IT-Lösungen, die Ihr Wachstum gezielt unterstützen.

www.ifaktor.de

IFAKTOR