Informationssicherheit ist eine tragende Säule

Wie ISO 27001 vor Cyberattacken schützen kann

Die steigende Zahl an Hackerangriffen ist eine Folge des Digitalisierungsschubs, der durch die Corona-Pandemie noch weiter Fahrt aufgenommen hat. Doch Unternehmen sind diesen Risiken nicht hilflos ausgeliefert. Gerade jetzt ist ein guter Moment, in die Informationssicherheit zu investieren und effizientere Schutzstrategien zu entwickeln. Wer sich ISO 27001-zertifizieren lässt, hat die Gewissheit, dass sensible Informationen nach den weltweit besten Standards geschützt sind.

Joyce van Luijn-Bonneveld

Cyberattacken und Datenleaks zählen zu den fünf wahrscheinlichsten Risiken für Unternehmen (Weltwirtschaftsforum, Global Risks Report 2018) Und sie betreffen alle Branchen und Firmengrößen. Selbst Betriebe mit professioneller IT-Abteilung, etwa Konzerne, öffentliche Einrichtungen, Krankenhäuser oder Flughäfen, sind von Cyberangriffen betroffen. So erbeuteten Cyberkriminelle Anfang Dezember bei einem Angriff auf die Europäische Arzneimittelbehörde EMA Zulassungsdaten für den Corona-Impfstoff der Pharmaunternehmen Biontech und Pfizer. Wenig später machte die Nachricht über einen großangelegten Hackerangriff auf die IT-Systeme der Funke-Mediengruppe Schlagzeilen. Erst nach Wochen erschienen alle Zeitungen wieder regulär.

Der weltweite Datenverlust in Firmen durch Diebstahl oder Fehler summiert sich auf über fünf Millionen Datensätze pro Tag. Dies fand das niederländische Unternehmen Gemalto in einer Studie heraus, die bereits vor der Pandemie erschien. Der Hintergrund: Schon seit Jahren werden die IT-Umgebungen immer komplexer und damit angreifbarer. Parallel dazu verfeinern und automatisieren Betrüger ihre Methoden. Corona hat diese Tendenz lediglich beschleunigt. Durch den verlängerten Lockdown werden gerade Home Offices zunehmend Opfer gezielter Phishing- oder Hackerangriffe. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt seit Beginn der Pandemie eine eindeutige Verschärfung der Sicherheitslage fest.

Häufiges Angriffsziel: Home Office

Seit Jahren erfreut sich das Home Office steigender Beliebtheit. Schon vor Covid-19 konnten laut einer Statista-Umfrage theoretisch 80 Prozent der deutschen Beschäftigten von Zuhause aus arbeiten. Auch ISO

27001, die weltweit führende Norm für Informationssicherheit, hatte sich bereits seit Längerem mit Kontrollen für mobile Geräte und Telearbeit auf das Arbeiten in den eigenen vier Wänden eingestellt. So sehr sich die meisten Beschäftigten ein Ende des Lockdowns wünschen, die Arbeit im Home Office hat auch ihr Gutes und könnte sich deshalb nach der Pandemie weiter etablieren. Der wichtigste Pluspunkt: Der Arbeitsweg entfällt, die Arbeitnehmer sparen Zeit und Nerven, die Umwelt wird geschont.

Doch auch nach Monaten der Pandemie entspricht die technische Ausstattung am heimischen Schreibtisch häufig nicht den Sicherheits- und Wartungsstandards des Arbeitgebers. Die Folge ist ein erheblicher Verlust der Informationssicherheit und Kontrolle. Oft nutzen die Beschäftigten ihr eigenes Equipment, auf das in der Regel auch Familie und Mitbewohner zugreifen können. Unterschätzt wird dabei auch das Risiko durch Unterlagen in Papierform, die oft unbeobachtet am Arbeitsplatz liegen bleiben oder ungeschreddert im Papierkorb landen.

Bei digitalen Daten ist es besonders wichtig, die Passwörter im Blick zu behalten. Anders als in der Firma sind sie zuhause meist einfach, werden kaum verändert und es gibt keine Passwortmanager. Auch Anti-Malware- und Antivirus-Programme sind häufig unzureichend oder werden nur selten aktualisiert. Für Cyberkriminelle, die Phishing-Mails mit Bezug zu Covid-19 versenden, ist das Home Office daher das perfekte Ziel.

ISO 27001: weltweit beste Praxis in Sachen Sicherheit

Für Unternehmen, die noch nicht ISO 27001-zertifiziert sind, wäre jetzt der ideale Moment, ihre Sicherheitsstrategie zu überprüfen. Das Informationssicherheitsmanagementsystem (kurz: ISMS) gemäß ISO 27001 stellt sicher, dass es im Unternehmen angemessene Kontrollen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gibt. Wer sich für ISO 27001 entscheidet, hat die Gewissheit, dass Sicherheitsprobleme gemäß der besten Praxis behandelt werden. Ein weiterer positiver Effekt: Unternehmen und Organisationen können ihren Kunden und Lieferanten zeigen, dass sie die Informationssicherheit verstehen und ernst nehmen.

Mit einer ISO 27001-Zertifizierung durch Lloyd's Register konnte Dormakaba, ein Anbieter für sicheren Zutritt zu Gebäuden und Räumen, die Beziehungen zu seiner Klientel weiter festigen und Neukunden hinzugewinnen. Für den international agierenden Hersteller war die interne Informationssicherheit nach eigenen Aussagen geschäftsentscheidend. Zum Kundenkreis gehören Banken und Versicherungen, die großen Wert darauf legen, möglichst viel Kontrolle über ihren digitalen Fußabdruck zu behalten. Viele Großkunden des 15 000 Mitarbeiter umfassenden Unternehmens machen daher eine Ausrichtung nach ISO 27001 für ihre Lieferanten zur Bedingung. Unterstützung durch das Management ist das A und O.

Ein nicht zu unterschätzender Erfolgsfaktor bei der ISO 27001-Zertifizierung ›››

So schützen Arbeitnehmer Ihr Home Office

- Beantworten Sie keine Phishing-Mails und klicken Sie keine Links an, wenn Sie den Absender der Mail nicht kennen. Auch wenn sich jemand als Vertrauensperson ausgibt: Geben Sie auf keinen Fall Ihr Passwort heraus!
- Lassen Sie wichtige Unterlagen auch zuhause niemals offen herumliegen. Auch sollten vertrauliche Informationen nach Möglichkeit nicht ausgedruckt werden. Falls doch, sollten Sie sie nicht in den Papierkorb, sondern gleich in den Schredder entsorgen.
- Achten Sie immer darauf, dass Ihr Bildschirm beim Verlassen des Schreibtisches gesperrt ist und kein anderer Zugriff darauf hat.
- Verwenden Sie starke, komplexe Passwörter (am besten mit einem Passwortmanager) und ändern Sie diese regelmäßig.
- Arbeiten Sie stets mit sicherem, passwortgeschütztem WLAN.
- Nutzen Sie, eine Zwei-Faktor-Authentisierung, die zum Beispiel PIN und Fingerabdruck kombiniert.

Tipps für Arbeitgeber und Teamleiter

- Vergeben Sie Administratorenrechte nach dem Grundsatz „Kenntnis notwendig" – sie sollten, soweit es irgend möglich ist, beschränkt werden.
- Nutzen Sie eine „Risk Map", um potenzielle Risiken genau auszuarbeiten.
- Für die Arbeit zuhause ist es wichtig, umfassende Richtlinien zu entwickeln.
- Führen Sie mit Ihren Mitarbeitern und Mitarbeiterinnen mindestens alle drei Monate einen Funktions-Check durch.
- Und auch dies ist wichtig: Gleichen Sie Ihre ISO 27001-Sicherheitskontrollen zwischen Unternehmens-Arbeitsplatz und Home Office ab.

ist der Rückhalt durch das Management. Idealerweise versteht die Geschäftsführung die Gründe für die Implementierung und unterstützt diese umfassend – auch mit angemessenen Ressourcen und Zeit.

Am Beispiel Dormakabas wird deutlich, wie entscheidend eine gute Planung und minutiöse Festlegung des Umfangs sind. Neben wesentlichen digitalen Unternehmensbereichen ließ der Hersteller auch seine zentrale Group IT zertifizieren. Auf diese Weise konnte Dormakaba das Gros der Maßnahmen selbst steuern und erreichte einen für eine Erstzertifizierung ungewöhnlich hohen Reifegrad. Verfügt ein Unternehmen über keine ISMS-Kompetenz im eigenen Hause, empfiehlt es sich jedoch, externe Dienstleister mit ins Boot zu holen.

Laut ISO-Norm müssen zunächst umfangreiche Managementprozesse definiert werden. Ein bereits vorhandenes Managementsystem nach ISO 9001:2015 ist hier sehr hilfreich. Schon in der Vergangenheit hatte der Hersteller Dormakaba ganze Fertigungsbereiche nach anderen ISO-Normen zertifizieren lassen. Ein Vorteil war zudem, dass rund die Hälfte der digitalen Entitäten Dormakabas bereits über integrierte Managementsysteme verfügten. Auf diese Weise hatte der Sicherheitstechnikkonzern einen deutlich geringeren Aufwand.

Basics, Remote Audits und gezielte Schulungen

Bei der Risikobewertung schätzt das Unternehmen vorab ein, wie viel Sicherheit in welchen Bereichen benötigt wird. Zu den vorbereitenden Basics zählt außerdem ein Plan zur Risikobehandlung, mit dem Maßnahmen und Verantwortlichkeiten priorisiert werden. Eine Investition, die sich für Dormakaba sehr gelohnt hat, waren die umfangreichen Schulungsprogramme für Mitarbeiter über die gesamte Unternehmensgruppe hinweg. Der Grund: Der Faktor Mensch spielt eine wichtige Rolle bei Cyberrisiken und deren Bekämpfung. Durch gezielte Schulungen können Fehler vermieden werden.

Dormakaba hatte die Implementierung zwar schon vor Covid-19 geplant, die Zertifizierung fiel dann aber exakt in die Pandemiezeit. Das Unternehmen konnte seinen Zeitplan dennoch ohne Probleme einhalten, da es schon seit Jahren zahlreiche interne Meetings per Video abgehalten hatte. Generell dürfen 50 bis 70 Prozent der Audits aus der Ferne stattfinden, sodass Dormakaba einen Teil seiner ISO 27001-Zertifizierung als Remote Audit durchführen konnte. Das Gros der Arbeitsplätze verfügte bereits über Notebooks mit Kamera. Zudem konnte die Begehung von Räumen ganz unkompliziert per Handy-Kamera erfolgen, die sich mühelos in die Microsoft Teams-Sitzungen integrieren ließen. Der Rundgang mit der Handy-Kamera ist ein gutes Beispiel dafür, dass es keine ausgereifte Video-Infrastruktur braucht, um sich während der Pandemie nach ISO 27001 zertifizieren zu lassen.

Fazit: Die seit Jahren steigenden Cyberrisken haben sich während der Pandemie noch einmal deutlich verstärkt. Für Unternehmen und Organisationen aller Größen wäre jetzt daher der beste Zeitpunkt, um sich dem Thema Informationssicherheit zu widmen. Die führende Norm ISO 27001 behandelt sensible Unternehmensdaten nach der weltweit besten Praxis, was sich auch positiv auf alle Geschäftsbeziehungen auswirkt. Damit die Zertifizierung gelingt, sind gute Planung und Rückendeckung durch das Management entscheidend. ■

INFORMATION & SERVICE

AUTORIN

Joyce van Luijn-Bonneveld ist Senior Lead Auditor, Information & Cyber Security bei Lloyd's Register. Sie verfügt über langjährige Führungserfahrung und arbeitet unter anderem als IT-Auditorin, Projekt- sowie Change-Managerin im Bereich IT-Infrastruktur. Seit über 30 Jahren ist sie zudem als IT-Line-Managerin, Trainerin und Coach tätig.

KONTAKT

Joyce van Luijn-Bonneveld
joyce.vanluijn@lr.org