Sicherheit bei Änderungen an IT-Systemen

IT-Sicherheit. Änderungen an IT-Systemen sind heute nicht nur an der Tagesordnung, sondern schlichtweg notwendig, um den Betrieb auch in kleinen und mittleren Unternehmen zu gewährleisten. Dabei sind Change-Management-Prozesse und Risikobetrachtungen unabdingbar, um die IT-Security aufrecht zu erhalten.

IT-Sicherheit: Deutsche Unternehmen geraten durch ISO-Normen und die europäische Datenschutz-Grundverordnung (DS-GVO) zunehmend unter Handlungsdruck. (Bild: iStock.com/kynny)

Das Betriebssystem des Servers beim Galvanotechnik-Dienstleister wird von Windows 2012 auf Windows 2016 upgedated, der mittelständische Automobilzulieferer wechselt auf ein anderes E-Mail-System oder bei der Softwareschmiede wird das Regelwerk an der Firewall angepasst. Alle diese Beispiele aus der täglichen Betriebspraxis stellen kritische Punkte dar. Schließlich betreffen sie direkt die IT-Sicherheit in den Unternehmen und sollten daher einen Change-Management-Prozess auslösen. Konkret bedeutet das, dass die Vorgehensweise beschrieben, ein Testplan erarbeitet und ein Fall-Back-Plan erstellt werden muss. Außerdem muss der Change-Prozess im Nachgang mittels eines Reviews betrach-

tet werden. Ergänzend kommt noch eine Risiko- und Chancenbewertung dazu.

Das Ganze ist nicht wirklich neu. Schließlich ergeben sich bereits aus dem De-facto-Standard ITIL Empfehlungen für den Betrieb von IT-Systemen und Prozessen, die bei Änderungen an IT-Systemen angestoßen werden. Und wer nach ISO 27001 zertifiziert ist, muss sowieso bei jeder Änderung an IT-Systemen den Change-Management-Prozess in Gang setzen. Doch auch die ISO 9001 sowie die am 25. Mai 2018 in Kraft tretende europäische Datenschutz-Grundverordnung (DS-GVO) beinhalten die Anforderung einer Risiko- und Chancenbewertung als Vorgabe.

Qualitätsmanagement-Tools und Methoden unterstützen dabei, den Anforderungen an IT-Sicherheit durch Risikomanagement zu entsprechen.

Durch die gesetzlichen Anforderungen der DS-GVO, durch zwei ISO-Normen und zusätzlich aus den ITIL-Empfehlungen heraus haben Unternehmen jetzt also bis zu vier Argumente auf dem Tisch, die durchaus einen hohen Handlungsdruck auslösen und auf die Einführung professioneller Change-Management-Prozesse hinwirken.

Die Aufgabe für die Unternehmen liegt also darin, schnellstmöglich vom Bewusstsein, dass etwas gemacht werden muss – es ist schließlich bald eine gesetzliche Anforderung –, zu einer konkreten Umsetzung zu kommen. Und hier herrscht in vielen Betrieben leider heute noch wenig Klarheit im Hinblick auf eine ideale Herangehensweise. Dabei muss man die Welt nicht neu erfinden, gibt es doch durchaus bewährte Qualitätsmanagement-Tools und Methoden, die hervorragend dabei unterstützen, den Anforderungen an IT-Sicherheit durch Risikomanagement zu entsprechen.

Eine von zahlreichen Möglichkeiten, die Risikobewertung im Rahmen eines Change-Prozesses vorzunehmen, stellt die sogenannte FMEA-Methode, zu Deutsch „Fehlermöglichkeits- und Einfluss-Analyse", dar. Sie hat sich in der Praxis unter anderem deshalb sehr bewährt, weil man hier mit einer einzigen Methodik sowohl die Anforderungen an IT-Sicherheit gemäß der ISO 27001 sowie Qualitätsanforderungen aus der ISO 9001 und der DS-GVO abbilden kann.

Während der Weg zur Risikobewertung vielfach noch unklar ist, ist der Nutzen hingegen den meisten Unternehmenslenkern und IT-Verantwortlichen einleuchtend: Change Management führt schließlich dazu, dass Lücken aufgedeckt werden sowie anstehende Probleme erfasst und erkannt werden – und zwar, bevor man in eine Veränderung geht. Der Betrieb wird dadurch aufrecht gehalten, die IT-Sicherheit gewährleistet, und niemand wird in seiner Arbeit behindert – „Sicherstellung und Aufrechterhaltung des Betriebes im Unternehmen" lautet die Anforderung, die man damit erfüllt, im Normendeutsch.

Eine mögliche Konsequenz, um allen Kriterien gerecht zu werden, ist auch die Entwicklung eines integrierten Management-Systems (IMS), das normative wie gesetzliche Anforderungen in einem einzigen System abbildet. Spätestens dann sind wir bei einem echten Mehrwert fürs Unternehmen angelangt, weil ein IMS nicht nur die Informationssicherheit unterstützt, sondern auch an anderer Stelle Ressourcen bündelt, Synergien effektiv nutzt und so Zeit und Geld spart.

In der ISO 27001 werden viele Punkte im Bereich Informationssicherheit aufgegriffen, die auch in der neuen DS-GVO zum Tragen kommen. Vor deren Inkrafttreten stellen sich viele Unternehmen daher die Frage, ob es sich lohnt, im Zuge der DS-GVO-Aktivitäten gleich die ISO 27001-Zertifizierung mit anzugehen. Hier gibt es tatsächlich eine Schnittmenge: Wer sich nach ISO 27001 zertifizieren lässt, bedient neben den Normanforderungen automatisch rund 20 bis 30 Prozent der gesetzlichen Anforderungen aus der DS-GVO, die er ohnehin bis 25. Mai 2018 umsetzen muss. Der Aufwand für eine Neuzertifizierung nach ISO 27001 verringert sich also rein rechnerisch. Daher ist es durchaus eine Überlegung wert, sich diesen Synergieeffekt zwischen der ISO-Norm und der DS-GVO zunutze zu machen.

Change Management führt dazu, dass Lücken aufgedeckt und anstehende Probleme erkannt werden.

Ob mit oder ohne formale ISO 27001-Zertifizierung: Mit durchdachten Change-Management-Prozessen und dadurch, dass man im Vorfeld die geforderte Risikobetrachtung macht, wird IT-Sicherheit gewährleistet. Und das sollte jeder Organisation – unabhängig von normativen und gesetzlichen Regelungen – ein Anliegen sein. *Peter Miller / as*

Change Management

Rhein S.Q.M., www.qm-projects.de