Sicher nur mit Zertifikat?

Warum zertifizierte Standards lediglich eine Basis für IT-Security sein können

In der digitalen Welt reichen einfache Sicherheitsmaßnahmen zum Schutz existenzieller Daten nicht mehr aus. Zwar versuchen verschiedene Standards und Regelwerke Hilfestellungen für Unternehmen zu bieten, doch Zertifizierungen alleine wiegen Organisationen oft in falscher Sicherheit.

Andreas Altena

Die digitale Transformation stellt jedes Unternehmen vor neue Herausforderungen. War es vor 35 Jahren noch sicher genug, vertrauliche Informationen im Safe wegzuschließen, sind heute die Bedingungen durch die Digitalisierung weitaus komplexer. Die mit der Digitalisierung einhergehenden Risiken sind für jeden leicht nachvollziehbar, der die Medien verfolgt. Schon seit vielen Jahren wird die digitale Infrastruktur unterschiedlichster Organisationen immer wieder angegriffen.

Wer kennt sie nicht, die Schadsoftware mit blumigen Namen wie „I-love-you“ bzw. „Loveletter“ aus dem Jahr 2000 (Ziel: Verbreitung und Passwortklau), „Stuxnet“ im Jahr 2010 (Ziel: Steuerung von Leittechnik in Kraftwerken) und seit 2014 Ransomware wie „Emotet“ (Ziel: Stilllegen der IT mit Lösegeldforderungen). Allein die Pressemeldungen der letzten vier Monate zeigen Angriffe und deren Folgen auf die digitale Infrastruktur, etwa der Hack der australischen Krankenversicherung Medibank, das Lahmlegen einer gesamten Kreisverwaltung in Rhein-Pfalz-Kreis oder das Datenleck des Autozulieferers Continental.

Das Vorgehen der Angreifer zeigt vor allem die Professionalität und das mittlerweile sehr erfolgreiche Geschäftsmodell, welches damit verbunden ist. Das belegen auf der einen Seite Zahlen der regelmäßig

durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Lageberichte zur Cybersicherheit, auf der anderen Seite die vom LKA NRW veröffentlichten Zahlen zu Schäden in der deutschen Wirtschaft in Höhe von 105 Milliarden Euro (Stand: 2020).

Um vergleichbare Risiken möglichst einzuschränken, reagieren die EU und auch Deutschland selbst mit behördlichen und gesetzlichen Auflagen. Nur um eine wesentliche Regelung zum Schutz der kritischen Infrastrukturen und Unternehmen darzustellen, entstand das seit Juli 2015 gültige und immer weiterentwickelte *IT-Sicherheitsgesetz (ITSiG)* sowie das *Gesetz des Bundesamts für Sicherheit in der Informationstechnik (BSI)* inklusive der zugehörigen Verordnungen. Dies ist ein sehr markantes Beispiel für nationale Gesetzgebungen, die in der Regel auf der europäischen Gesetzgebung basieren. Darüber hinaus haben die Europaabgeordneten am 10. November 2022 nun weitere Regeln verabschiedet, die von den EU-Ländern strengere Aufsichts- und Durchsetzungsmaßnahmen und die Harmonisierung von Sanktionen verlangen. Was all diese Gesetzgebungen gemeinsam haben, sind strengere IT-Sicherheitsanforderungen an Unternehmen, Verwaltungen und die kritische Infrastruktur. Auf diese Weise will der Gesetzgeber die Resilienz in Sachen Cybersicherheit europaweit stärken.

Weltweite Regelwerke und Standards

Daneben werden weltweit Regelwerke und Standards entwickelt, die internationale Best-Practices für Organisationen und Unternehmen mit unterschiedlichen Schwerpunkten zusammenfassen. Hierzu ein kurzer Überblick über die für Deutschland wesentlichen Regelwerke, die auch eine Zertifizierung erlauben.

International oder national

Eine mögliche und für Unternehmen wichtige Unterscheidung ist die Frage nach dem Bereich, in dem der Standard oder das Regelwerk Anwendung finden soll. Bei einer nationalen Gesetzgebung ist das relativ einfach, da diese Gültigkeit für alle deutschen Unternehmen hat.

Dafür gibt es in Deutschland das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) stetig weiterentwickelte *IT-Grundschutz-Kompendium*, welches zusammen mit den sogenannten *BSI-Standards* ein umfassendes Werk zur Informationssicherheit darstellt. Es bietet über seine sogenannten *IT-Grundschutz-Bausteine* einen sehr umfassenden Blick auf alle möglichen Sicherheitsaspekte inklusive Ihrer Gefährdungen und darüber hinaus auch konkrete Maßnahmen zu deren Minderung. Dies reicht thematisch von hilfreichen Sicherheitsanforderungen an Apps über industrielle IT bis hin zu einem *Informationssicherheitsmanagementsystem (ISMS)*. Beeindruckend ist dabei allein schon der Umfang des Gesamtwerks von mehreren tausend Seiten.

Als wesentlicher Nachteil könnte gelten, dass dieses Werk nur national anerkannt ist und einen hohen formalen Aufwand in der Praxis mit sich bringt. Dennoch ist der Nutzen unbestritten, denn es birgt einen großen Wissensschatz. Ist das Unternehmen auch international aktiv, schließt sich das *IT-Grundschutz-Kompendium* allerdings eher aus. Es sei denn, dass es hierzu explizite Kundenanforderungen gibt.

International lohnt sich eher der Blick auf die global anerkannte *ISO 27001*, die im Oktober 2022 in einer neuen Revision veröffentlicht wurde. Diese Norm macht Vorgaben zur Implementierung und den Betrieb eines ISMS im Unternehmen, ist dabei allerdings weniger konkret als das IT-Grundschutz-Kompendium. Das Ziel der ISO 27001 ist eher, den Rahmen vorzugeben (Was ist zu tun?) als konkrete Umsetzungsvorgaben (Wie ist es zu tun?) zu liefern. Unternehmen bleibt die Ausgestaltung in einer angemessenen Art und Weise selbst überlassen. Die größten Nachteile der ISO-Norm sind sicherlich:

- die Aktualität (die aktuelle Revision hat neun Jahre auf sich warten lassen) und
- der mögliche Rahmen der individuellen Ausgestaltung durch die Unternehmen (Zumindest wird es oft so empfunden).

Empfehlen kann man daher als Grundlage die ISO 27001, gepaart mit konkreten Umsetzungsvorschlägen des IT-Grundschutzkompendiums. Beide Regelwerke gehen von jährlichen Zertifizierungsinterval- »»

len durch unabhängig agierende dritte Parteien (Zertifizierungsgesellschaften) aus, was typisch für diese Verfahren ist.

Branchenspezifisch

Um dieser Bandbreite an Möglichkeiten entgegenzuwirken, haben sich daneben branchenspezifische Ausprägungen etabliert. Ein bekanntes Beispiel dafür ist *Tisax (Trusted Information Security Assessment Exchange)*, ein branchenspezifischer Rahmen für die Automobilindustrie. Dienstleister und Zulieferer der Automobilindustrie müssen in dreijährigem Abstand nachweisen, dass sie die hohen Anforderungen ihrer Kunden hinsichtlich der Informationssicherheit einhalten. Basis für diese unabhängig durchzuführenden Prüfungen ist ein vom Verband der Automobilindustrie (VDA) entwickelter Fragebogen zur Informationssicherheit *(ISA – Information Security Assessment)*. Dieser bezieht sich auf wesentliche Aspekte der internationalen Norm ISO 27001, erweitert um ein Reifegradmodell, und bietet konkrete Anforderungen. Eine Besonderheit bei diesem Standard ist, dass hier kein Zertifikat, sondern ein Label auf einer durch die *ENX-Association* bereitgestellten Plattform ausgestellt wird. Über diese Plattform können dazu erforderliche Informationen zwischen den Tisax-Teilnehmern gezielt ausgetauscht werden.

Die Nachteile von Tisax zeigen sich bei den sogenannten Assessment-Levels, die den Umfang der Prüfung definieren. So kann beispielsweise eine reine Plausibilitätsprüfung bei Assessment-Level 2 durch den Prüfer schon ausreichend sein, um eine angemessene Umsetzung von Informationssicherheit zu bestätigen. Bei Assessment-Level 1 genügt sogar eine reine Selbstauskunft über den Fragebogen des VDA. Berücksichtigt man daneben noch die technischen Entwicklungen und Bedrohungen in der IT-Sicherheit allein innerhalb weniger Monate, erscheint der dreijährige Prüfungszyklus nicht angemessen.

Dennoch ist Tisax für die Branche wichtig, um das Thema Informationssicherheit zu etablieren. Tisax ist dadurch zum Defacto-Standard geworden und wird fortlaufend weiterentwickelt Eine Prüfung auf dem höchsten *Assessment-Level 3* lässt sich am ehesten mit einer ISO-27001-Zertifizierung vergleichen und wird in der Praxis immer häufiger von den Automobilherstellern (OEM) eingefordert.

Technologiespezifisch

Zu guter Letzt werfen wir einen Blick auf einen technologischen Standard, den *Kriterienkatalog C5 (Common Computing Compliance Criteria Catalogue)*. Dieser definiert die Mindestanforderungen an ein sicheres Cloud-Computing. Ein nicht unwichtiger Aspekt und damit wichtiger Faktor, berücksichtigt man die aktuellen Strategien vieler Organisationen, Anwendungen in die Cloud auszulagern. Auf der anderen Seite gehen immer mehr Hersteller von Software dazu über, ihre Softwareprodukte nur noch in einer Cloud als *SaaS-Angebot (Software as a Service)* und nicht mehr *On-Premise* (Selbst installierbar und auf eigenen IT-Infrastrukturen zu betreiben) anzubieten.

Somit richtet sich der Kriterienkatalog C5, welcher primär durch das BSI entwickelt und spezifiziert wurde, auf der einen Seite an professionelle Cloud-Anbieter, auf der anderen Seite an deren Prüfer und Kunden. Im Jahr 2016 erstmals veröffentlicht, gilt der Kriterienkatalog mittlerweile als ein Qualitätsmerkmal hinsichtlich eines sicheren Cloud-Betriebs in der Wirtschaft und somit als eine wichtige Orientierung sowie als Kriterium für die Auswahl eines Cloud-Anbieters.

Als zugrundeliegende Prüfungsmethodik bildet der *International Standard on Assurance Engagement 3000 (ISAE 3000)* den übergeordneten Rahmen, wodurch Prüfungen in Form einer Angemessenheits- oder einer Wirksamkeitsprüfung durchgeführt werden können und zu einem C5-Testat inklusive Bericht führen.

Als Nachteil kann auch hier der Abstand zwischen den Entwicklungen des Kriterienkataloges (aktualisiert 2019, veröffentlicht 2020) und dem technologischen Fortschritt betrachtet werden. Außerdem bietet nur eine Wirksamkeitsprüfung und die damit verbundene höhere Prüfungstiefe (Typ 2) eine verlässliche Aussagekraft im Bericht, da hier die Durchführung der Kontrollen über den gesamten Prüfungszeitraum (typischerweise sechs oder zwölf Monate) nachgewiesen wird.

Insgesamt überwiegen bei diesem Beispiel die Vorteile durch Rückgriffe auf etablierte Standards und die technologische Spezifizierung sowie auf die Nutzung etablierter Prüfmethodiken. Nicht ohne Grund hat sich dieser Standard auf dem Markt schnell als ein wichtiges Alleinstellungsmerkmal bei der Auswahl eines Cloud-Anbieters etabliert. Sowohl durch den potenziellen Kunden als auch in der Nutzung durch den Anbieter selbst.

ISO 27001 – Mutter der IT-Security-Standards

Alle hier genannten Standards, Normen, Gesetzgebungen oder Kriterienkataloge ziehen die ISO 27001 als Basis heran. In den Unterlagen der unterschiedlichen Regelwerke werden Sie daher in der Regel Referenzen oder auch Kreuzreferenztabellen finden, weshalb diese ISO-Norm als Mutter der hier dargestellten Anforderungen bezeichnet werden könnte. Wirft man einen weiteren Blick auf die gesamte 27000-Normenfamilie, können weitere Schätze gehoben werden.

So ist ISO 27002 ein hervorragendes Nachschlagewerk, um die unterschiedlichsten Lösungsansätze für die grob definierten Mindestanforderungen zu finden. Damit ist sie auch eine geeignete Basis, um eine individuelle Lösung für die eigene Organisation zu implementieren. Weitere Normen in der Familie beschreiben unter anderem die Umsetzung eines geeigneten Risikomanagements, welches die Basis für jedes präventive Vorgehen in der Informationssicherheit methodisch überhaupt erst ermöglicht. Daneben finden sich weitere Normen, die zum Beispiel Datenschutzanforderungen, technologische und branchenspezifische Anforderungen im Umfeld der Informationssicherheit beschreiben. Allerdings stellt nur ISO 27001 eine geeignete Basis für eine anerkannte, sprich akkreditierte, Zertifizierungsgrundlage bereit.

Der Vorteil der 27000-Normenfamilie liegt somit klar in deren Vielfältigkeit und uneingeschränkten Akzeptanz. Einen weiteren Vorteil bietet die Möglichkeit der individuellen und damit angemessenen Ausgestaltung im eigenen Unternehmen. Manch einer wird diese Flexibilität allerdings auch eher als Nachteil einschätzen, da es wenig konkrete Beschreibungen zur Umsetzung gibt und es daher aufwendig sein kann die individuell beste Lösung für das eigene Unternehmen zu finden. Sicher ist, dass gerade diese Flexibilität mit der gleichzeitig be-

stehenden Komplexität in den Anforderungen der Informationssicherheit zu der Ausgestaltung weiterer Standards geführt haben. Mit allen Vorteilen und Nachteilen, die dann wieder gesehen werden können.

Praxiserfahrungen mit den Zertifizierungen

Leider laufen nicht nur die ISO-27001-Zertifikate Gefahr an Wertigkeit zu verlieren. In der Praxis sehen wir oft Schwächen in der Umsetzung und eine damit einhergehende Verringerung des Sicherheitsniveaus auf Seite der Organisationen. Und teilweise wird diese Entwicklung durch die Zertifizierungsgesellschaften befeuert. Woran machen wir das fest?

Sicherheitsbeauftragte verschiedener Unternehmen berichten von eindeutig identifizierten Schwächen in den Audits, die aber nicht zu formulierten Abweichungen durch die Auditoren in den Zertifizierungsverfahren führen. Die Folgen fehlender Argumentationsgrundlagen für die Sicherheitsbeauftragten gegenüber ihrem Management sind klar: Dringende Präventivmaßnahmen werden vernachlässigt. Das schadet der Informationssicherheit des Unternehmens, liegt aber definitiv nicht an der ISO 27001 oder an den anderen Regelwerken. Denn diese haben mittlerweile einen teils sehr hohen Reifegrad erreicht. Vielmehr sollte die beschriebene Auditpraxis als Warnung verstanden werden, dass sich kein Unternehmen auf den erworbenen Zertifikaten ausruhen sollte!

Auswahlkriterien für Unternehmen

Entscheidend für Unternehmen, unabhängig von den hier dargestellten Regelwerken und der Kritik, gibt es zwei wesentliche Fragestellungen zum Umgang mit dem Thema Informationssicherheit:

- **Woher kommen die Anforderungen?** Sind es gesetzliche oder behördliche Anforderungen, die es umzusetzen gilt (z.B. Digitalrecht, DSGVO oder IT-Sicherheitsgesetz)? Oder sind es kundenspezifische Forderungen, die zwingend in das Compliance Management des Unternehmens implementiert werden müssen?
- **Was soll damit erreicht werden?** Gilt es eine Rechtskonformität, Haftungsreduktion oder die Erfüllung von Kundenanforderungen sicherzustellen? Bedeutend kann alleine der präventive Umgang mit dem Thema für den Fortbestands des Unternehmens sein.

Werden beide Fragestellungen betrachtet, geht es bei den möglichen Antworten vor allem um die Einhaltung von Compliance und um die Grundlage eines gesunden unternehmerischen Handels, unabhängig vom genutzten Standard. Spätestens bei den Herausforderungen der digitalen Transformation wird auch im Umfeld der Informationssicherheit eine weitere große Herausforderung schnell erkennbar: Eine sichere digitale Transformation kostet Geld.

Die Informationssicherheit ist dabei geprägt von präventiven Maßnahmen, die aus einem systematisch implementierten Risikomanagementprozess resultieren. Dennoch schaffen genau diese Investitionen in die Prävention eine direkte Resilienz in der digitalen Welt und fördern damit ebenso die Wettbewerbsfähigkeit heute und in Zukunft. Das Image eines Unternehmens ist ein hohes Gut und damit ebenso ein Wert, den es zu schützen gilt. Darüber hinaus werden die Kompetenzen der Mitarbeiter weiterentwickelt und damit die Sensibilität bei der Umsetzung angemessener und vor allem passenden Präventivmaßnahmen. Genau diese Investition zahlt sich am Ende aus.

Fazit

Informationssicherheit ist ein wesentlicher Baustein der digitalen Transformation. Einen angemessenen und zukunftsorientierten Schutz gibt es für Unternehmen erst, wenn diese zielgerichtet und schon beim Aufbau von Geschäftsprozessen eingeplant wird. Denn steht die Produktion oder das Geschäft erst einmal für einige Wochen still, werden sich die finanziellen Auswirkungen gegenüber den erforderlichen Investitionen in die Informationssicherheit mehr als relativieren. Dies wurde schon durch diverse Fälle im Lauf der letzten Jahre bestätigt. Nicht selten geht es schnell um die Existenz oder das Fortbestehen eines Unternehmens, wenn die digitale Infrastruktur zusammenbricht oder vertrauliche Informationen in die falschen Hände geraten. Auch die Auseinandersetzung mit der Aufrechterhaltung der Geschäftskontinuität wird daher einen wesentlichen Beitrag zur Unterstützung einer sicheren und resilienten digitalen Transformation leisten.

Klar ist auch: Es gibt keine hundertprozentige Sicherheit allein auf Basis einer Zertifizierung! Daher muss eine kritische Auseinandersetzung mit dem Thema und die Beteiligung aller involvierten Parteien erlaubt sein. Nur so ist eine sinnvolle Entwicklung zu gewährleisten, die wiederum allen zu Gute kommen kann. Bewusst sein sollte sich jeder vor allem über die fortlaufende Veränderung der Sicherheitslage und die damit einhergehende, andauernde Neubewertung des eigenen Sicherheitsniveaus in der digitalen Transformation. Dies liegt in der täglichen Verantwortung eines jeden Mitarbeiters im Unternehmen.

Eine Zertifizierung alleine kann das nicht leisten. Normen und Regelwerke sind hilfreiche Best-Practice-Werke. Sie unterstützen dabei, die Informationssicherheit präventiv und systematisch in einer Organisation zu etablieren. Am Ende entscheidet aber immer die richtige und damit individuell passende Nutzung in der Organisation über den Erfolg, unabhängig von einer Zertifizierung oder dem Regelwerk. ■

INFORMATION & SERVICE

AUTOR

Andreas Altena ist Geschäftsführer der Sollence GmbH, Krefeld. Als Berater, Trainer und DQS-Excellence-Auditor liegen seine Kernkompetenzen bei Organisationsentwicklung und integrierte Managementsysteme, Qualitäts-, Informationssicherheits-, Risiko und (IT-)Servicemanagement.

KONTAKT

Andreas Altena
a.altena@sollence.de