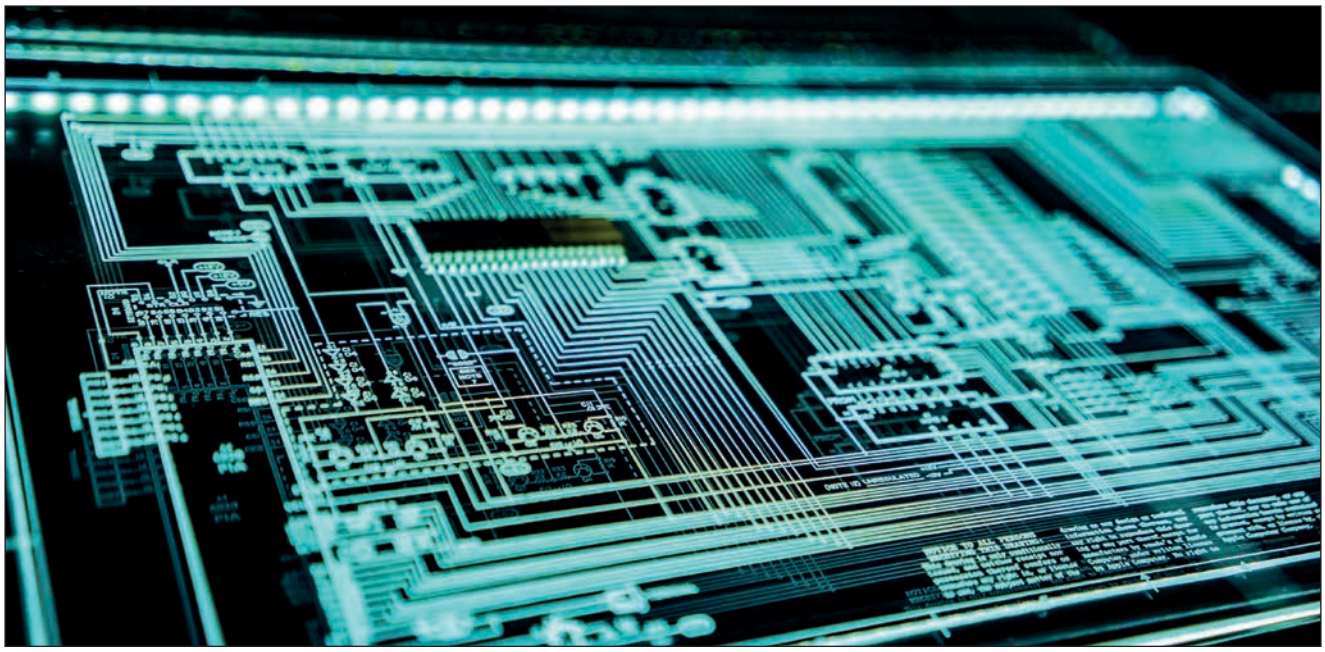

Wie sicher ist die eigene IT-Security?

Fallbeispiel Ein Security Audit ist eine der Möglichkeiten, mit denen Unternehmen ihre allgemeine Sicherheitslage testen und bewerten können. Ein Audit kann aber auch andere positive Effekt mit sich bringen, wie ein Beispiel eines Schweizer KMU zeigt.

Von Simon Wegmüller

Wer die Nachrichten rund ums Thema Cyber-Sicherheit auch nur am Rande verfolgt, sollte intuitiv verstehen, warum Audits wichtig sind. Neben den monetären Folgen eines Security Breach können Unternehmen dadurch auch schnell an Prestige und somit an Vertrauen seitens ihrer Kunden verlieren. Regelmässige Audits helfen dabei, diesem Risiko Herr zu werden und bringen zudem weitere positive Nebeneffekte mit sich. Im Normalfall folgt ein Audit einem festgelegten Prüfverfahren, etwa anhand einer Checkliste. Welcher Service respektive Anbiter dabei der richtige ist, hängt allerdings jeweils stark von den individuellen Umständen ab und ist in jedem Fall anhand Beratung durch einen Experten (IT-Auditor) abzuklären.

Mehrschichtigkeit

Oneconsult hat kürzlich ein Cyber Security Audit für einen seiner Kunden durchgeführt, um die Effektivität seiner Cyber-Defense-Kontrollen zu bewerten. Das Ziel war es, relevante Ergebnisse und Empfehlungen zu liefern, die die Cyber-Abwehr des Unternehmens stärken und gleichzeitig die Interessen des Unternehmens, seiner Kunden und anderer relevanter Stakeholder berücksichtigen.

Bei dem Unternehmen, das nicht namentlich genannt werden möchte und als Service Provider aktiv ist, sind rund 150 Mitarbeitende tätig, wovon rund 80 als Softwareentwickler und rund 30 im Bereich IT-Services arbeiten.

Der Audit erfolgte auch im Hinblick darauf, dass das Unternehmen seit 2011

> «Am wichtigsten ist es, jegliches Risiko für unsere Kunden zu minimieren. Die Sicherheit für sie steht immer im Zentrum.»
>
> **Andreas Müller (Name von der Redaktion geändert), Bereichsleiter IT Services und Mitglied der Geschäftsleitung, KMU in der Region Bern**

im grossen Stil Services via Rechenzentren anbietet, wobei ein hoher Sicherheitsstandard natürlich unerlässlich ist und auch von den Kunden verlangt wird. Aus diesem Grund liess sich das Unternehmen auch bereits gemäss ISO-27001 zertifizieren, was einen geregelten und sicheren Ablauf der durch die Rechenzentren gelieferten Dienstleistungen garantiert.

«Darüber hinaus verfügen wir über ein Gremium für Informationssicherheit, das aus diversen Rollen besteht – von Software-Entwicklern über Mitarbeitende im Bereich unserer Services bis hin zu Management-Positionen – indem wir auf einem strategischen Level Security-relevante Themen beraten und schlussendlich in die Firma einbringen», so Andreas Müller (Name von der Redaktion geändert), der als Bereichsleiter IT Services sowie als Mitglied der Geschäftsleitung einen tiefen Einblick in die inneren Vorgänge des Unternehmens besitzt.

Auswahl und Ausführung

Im Unternehmen wurden bereits, hauptsächlich spezifisch auf Anwendungsfälle, sporadisch Assessments und Risikoanalysen durchgeführt. Das in der Umgebung von Bern angesiedelte KMU hatte zudem bereits zuvor mit Oneconsult zu tun, wodurch die Wahl rasch auf den Anbieter von Security Audits fiel, da es bereits eine Geschäftsbeziehung gab und man sich gegenseitig vertraute.

Dass man sich dabei für einen kompletten Security Audit entschied, hat, so Müller, vor allem damit zu tun, dass das Unternehmen nicht nur etwa die Anwendungen, das heisst den Code, die Verknüpfungen untereinander und allfällige Sicherheitslücken, die auch Kunden des Unternehmens betreffen könnten, ganz genau überprüfen lassen wollte, sondern dass zugleich auch die dahinterliegende IT-Infrastruktur geprüft werden sollte. Es sollten also alle Aspekte rund um die IT und die Security der Unternehmung beleuchtet und einem prüfenden Blick unterzogen werden.

Auf eine längere und, so Müller, intensive Vorbereitungsphase beider Parteien, in der insbesondere eine genaue Dokumentierungen der Anwendungen und derer Funktion sowie auch der IT-Infrastruktur eine Rolle spielten, folgte ein rascher und sich in der Härte exponentiell steigernder Härtetest für das Berner Unternehmen. «Gesamthaft dauert der Prozess insgesamt sechs volle Arbeitstage, zum Teil mit zwei externen Beratern seitens Onconsult», erklärt Müller dazu, und fügt an: «Die Nacharbeiten dauern aber immer noch an.» So werden aktuell, resultierend aus den gewonnenen Einblicken durch den Audit, die Findings in die Systeme und Software implementiert. «Rund 80 Prozent haben wir bereits umgesetzt», so Müller. «Der ganze Prozess dauert mittlerweile rund 3 bis 4 Monate.»

Oneconsult hat genau zu diesem Zweck einen detaillierten Bericht für das Unternehmen erstellt, in dem die Findings einerseits aufgelistet werden, der aber auch schon teilweise konkrete Hinweise darauf gibt, wie man diese behebt. «Dies geschieht anhand der Kritikalität der Findings», so Müller. «Nun werden diese abgearbeitet, zumindest wo wir Bedarf sehen». Denn nicht immer müssten alle empfohlenen Massnahmen umgesetzt werden, erklärt Müller. Dies aus verschiedenen Gründen, etwa wenn es sich um spezielle Fachapplikationen handelt, bei denen der Nutzen nicht gegeben ist. Generell spielen Kosten-Nutzen-Rechnungen dabei eine Rolle. Eines betont der Leiter IT Services aber mehrfach: «Am wichtigsten ist es, jegliches Risiko für unsere Kunden zu minimieren. Die Sicherheit für sie steht immer im Zentrum.»

> «Was sicher aber eine Herausforderung war, ist das fachliche Verständnis der Tester für die einzelnen Applikationen.»
>
> **Andreas Müller (Name von der Redaktion geändert), Bereichsleiter IT Services und Mitglied der Geschäftsleitung, KMU in der Region Bern**

Ziel ist es, nachdem alle Umsetzungen vorgenommen wurden, dass noch einmal eine Nachüberprüfung seitens Oneconsult stattfindet, so dass man sicher ist, dass die Anpassungen korrekt gemacht wurden und sich dadurch keine neuen Sicherheitsrisiken aufgetan haben.

Zusammenarbeit

«Die Zusammenarbeit war sehr zielführend», zeigt sich Müller derweil von dem Dienstleister begeistert. «So wurde etwa auch ein High-Critical-Sicherheitsrisiko gefunden, was uns sofort kommuniziert wurde und es uns ermöglichte, diese Lücke sofort zu schliessen.» Der Bericht für die Nacharbeiten sei ebenfalls sehr seriös gestaltet, zudem habe sich das Unternehmen ans Budget gehalten.

«Was sicher aber eine Herausforderung war, gerade in einem solchen speziellen Fall, wo auch die Applikations-Sicherheit überprüft wurde und nicht nur die infrastrukturelle Sicherheit, die meist einfacher zu überprüfen ist, ist das fachliche Verständnis der Tester für die einzelnen Applikationen», verrät Müller. Unter Umständen kann das zum Beispiel zu Fehlinterpretationen seitens der Tester führen. «Hier hilft es sicher, wenn man im Vorhinein detailliert und gemeinsam anschaut, wieso einzelne Sachen so gemacht werden, so aufgebaut sind, wie sie es sind», so Müller.

Der CIO verrät zudem, dass ein Audit auch andere positive Nebeneffekte haben kann. «Wir profitieren aus diversen Aspekten des Audits. Wir hatten bei dieser Überprüfung zum Beispiel einen Fall, der einen Impact auf diverse Anwendungen hat, die von uns entwickelt worden sind – und zwar aus dem einfachen Grund, dass es den Leuten einfach nicht bewusst gewesen ist», so Müller.

Ausserdem sei auch der Schulungsaspekt wichtig, den die Mitarbeitenden durch den Audit-Prozess erfahren und der nicht zu unterschätzen sei. «Zudem ist es so, dass die eigene Mannschaft affiner wird, je mehr und je regelmässiger man solche Überprüfungen durchführt», führt Müller aus.

So würden heute etwa bereits im Vorfeld von Projekten teils ganz andere Überlegungen gemacht. «Fakt ist, wenn man ISO-Zertifizierungen richtig anwendet, und das gilt auch für die Learnings aus Assessments und Audits, profitiert man sowohl im Betrieb, in der Weiterentwicklung wie auch am Ende des Tages bei der Effizienz», so der Bereichsleiter IT Services. ■