economiesuisse

Gefahren für KMU: digitale Effizienzsteigerung im Cyberraum

Die Nutzung digitaler Hilfsmittel ist für viele unserer Unternehmen von grundlegender Bedeutung für die Entwicklung ihrer Geschäftsmodelle. Nicht vergessen werden darf dabei die Cybersicherheit. Nachlässigkeiten in diesem Bereich können schwerwiegende Folgen für das Unternehmen und die Geschäftspartner haben.

Wer beim Begriff «Digitalisierung der Wirtschaft» nur an technologiegetriebene Grossunternehmen oder dynamische Start-ups aus dem Crypto Valley denkt, übersieht, dass heute alle Unternehmen in der einen oder anderen Art den digitalen Fortschritt für ihre Zwecke nutzen. Zahlreiche Erleichterungen, welche die neuen Technologien bieten, sind gerade auch aus dem Alltag der hiesigen KMU – sei es die Schreinerei, die Velowerkstatt oder das Treuhandbüro – nicht mehr wegzudenken.

Dies betrifft nicht nur den PC für die Buchhaltung oder die Textverarbeitung. Baupläne werden elektronisch erstellt und versandt, der Aussendienstmitarbeitende erfasst die Bestellung gleich vor Ort auf seinem Tablet, der Einkauf der Rohstoffe erfolgt über eine Plattform und das Analysegerät im Labor lädt die Updates direkt aus dem Internet. Andere Unternehmer setzen voll auf digitale Werkzeuge. Nomadisches Arbeiten oder additive Fertigung sind hier die Stichworte.

Schaut man einige der jüngeren Umfragen an, kommt der Eindruck auf, dass viele Unternehmen in unserem Land davon ausgehen, dass sie mit der Digitalisierung

nichts am Hut haben. Darauf angesprochen, sagen diese Unternehmen, dass die technologische Entwicklung sie nicht direkt betrifft. Wie erklärt sich dieser anscheinende Widerspruch? Viele Nutzungen der modernen Technik haben sich langsam in den Alltag unserer KMU geschlichen und waren dabei nicht Teil einer gezielten Digitalisierungsstrategie.

Somit waren bei Weitem nicht alle Entwicklungen die Folge eines bewussten Entscheides und geschahen oftmals nebenbei: zum Beispiel der Wechsel auf ein neues Telefon oder auf eine digitale Dokumentenverwaltung, oder die regelmässige Nutzung des Internets. Vernetzte elektronische Hilfsmittel gehören gerade auch bei unseren KMU heute derart zum Alltag, dass sie oft gar nicht mehr als solche wahrgenommen werden. Und genau hier liegt aus Sicht der Cybersicherheit die grösste Gefahr.

Neue technologische Möglichkeiten, neue Formen der Kriminalität

Die Digitalisierung und die damit verbundene Vernetzung der Systeme (viele Werkzeuge, Überwachungskameras oder Küchengeräte sind bereits heute mit dem Internet verbunden) führen dazu, dass wir auf einer ganz neuen Ebene verwundbar werden. Denn gerade auch im digitalen Raum tummeln sich Leute oder Organisationen mit kriminellen Machenschaften. Angriffe können von überall auf der Welt aus anonym und mit wenig Aufwand direkt bei unseren Unternehmen durchgeführt werden. Cyberkriminelle kümmern sich nicht um Landesgrenzen.

Sie zieht es dorthin, wo sich leichte Beute machen lässt, also mit verhältnismässig geringem Aufwand viel zu holen ist. So nehmen spezialisierte Kriminelle gerade auch Schweizer KMU ins Visier. Dabei stehen diejenigen im Fokus, welche sich nicht mit Fragen rund um die Sicherheit auseinandersetzen und keine geeigneten Abwehrmassnahmen ergreifen.

Die Digitalisierung hat somit eine Kehrseite: neue Formen der Kriminalität. So können über das Internet Daten gestohlen oder abgeändert, Systeme beschädigt und Unternehmen erpresst werden. Damit tun sich neue Gefahren auf, welche in der analogen Welt noch nicht existierten. Eine Vielzahl der kriminellen Angriffe lässt sich aber verhindern. Ein Unternehmen muss sich dazu, wie auch in der physischen Welt, Gedanken machen, wie es sich vor der kriminellen Energie Dritter schützen kann. Wenn die Sicherheit vernachlässigt wird, werden technische Erleichterungen schnell zum existenzbedrohenden Risiko für ein KMU. Viele Anwender, Unternehmen wie auch Private, ignorieren heute mögliche Gefahren beim Einsatz neuer Technologien.

Dies bestätigt auch eine Untersuchung, welche die Hochschule Luzern hierzu zusammen mit dem KMU-Verband, dem Staatssekretariat für Wirtschaft (Seco), der Schweizer Kader-Organisation (SKO) und economiesuisse durchgeführt hat: Die hiesigen Unternehmen sind auf Bedrohungen im Cyberraum nicht ausreichend vorbereitet. 40 Prozent der befragten Firmen gaben an, sie seien kürzlich von digitalen Attacken wie Malware oder Phishing-Mails heimgesucht worden. Trotz der konkreten Gefahr können die Firmen nicht angemessen auf die Angriffe reagieren. Unter anderem, da es in vielen KMU an Wissen zum Umgang mit dem Thema Informationssicherheit fehlt.

Bewusstsein für Gefahren wächst, aber ...

Die Studie kommt zum Ergebnis, dass die Sensibilität für Cybersicherheit grundsätzlich gestiegen ist. «Digitalisierung, Robotik und Automatisierung» ist für die Führungscrews der Unternehmen das zweitwichtigste Thema – direkt nach der Effizienzsteigerung. Rund 78 Prozent der befragten KMU führen auch aus, dass Cybersicherheit in den letzten drei Jahren wichtiger geworden ist. Obwohl mittlerweile auch die KMU Fragen der Cybersicherheit breit diskutieren, besteht Handlungsbedarf. Die Studie hält nämlich auch fest, dass weniger als 50 Prozent der befragten Unternehmen ihre Sicherheitsmassnahmen in regelmässigen Abständen prüfen. Auch Leitfäden, wie mit Bedrohungen im Cyberraum umzugehen ist, kommen nur selten zum Einsatz. Das Gleiche gilt für Weiterbildungen. Es braucht somit Strategien, wie auf die zunehmenden Gefahren aus dem Internet zu reagieren ist.

Oft braucht es nur wenig, um die Sicherheit in einem Unternehmen markant zu verbessern. Durch den Fokus auf die Cybersicherheit in den betroffenen Unternehmen, aber auch bei den Geschäftspartnern, Lieferanten und Kunden, liessen sich Missbrauchsfälle massiv einschränken. Ein Sicherheitsrisiko kann nämlich zum eigentlichen Geschäftsverhinderer werden und das Unternehmen sogar als Ganzes, zusammen mit den Geschäftspartnern, in Gefahr bringen. Es gilt daher, dass Sicherheit und die damit verbundenen Kosten von Anfang an in den Business-Case einkalkuliert werden müssen. Das Ziel muss es sein, dass jedes Unternehmen – ob gross oder klein – ein angemessenes Sicherheitskonzept entwickeln kann, welches ausreichend Sicherheit bietet und gleichzeitig die operative Handlungsfähigkeit des Unternehmens aufrechterhält.

Die Verantwortung beginnt beim Einzelnen

Genauso wie wir selbst verantwortlich sind, unser Haus gegen Einbrüche zu sichern, ist auch primär jedes Unternehmen selbst verantwortlich, sich gegen die Bedrohungen im Cyberraum zu wappnen. Die Antwort auf diese Bedrohungen sind somit nicht staatlich vorgegebene Verhaltenspflichten. Im Gegenteil. Dezentrale und heterogene Systeme sind im Bereich der Cybersicherheit belastbarer als zentral ausgelegte Systeme. Insbesondere, wenn es darum geht, unerwarteten Herausforderungen und Krisen zu begegnen. Wo branchenspezifische Lösungen angezeigt sind, ist die Wirtschaft selbst gefordert. Sie kann durch Minimalstandards im Sinne von Empfehlungen die Cybersicherheit erheblich steigern.

Verständlich formulierte Leitlinien können dabei als Hilfestellung dienen. Solche Minimalstandards würden es auch ermöglichen, dass KMU vom Know-how der grossen Unternehmen profitieren und Asymmetrien im Cyberbereich zwischen den Branchen vermieden werden können. Der Staat leistet seinen Beitrag, indem er ebenfalls solche Sicherheitsstandards fördert und für eine ausgeglichene Handhabung in Bezug auf die internationale Gesetzgebung sorgt. Im Krisenfall, das heisst, wenn es zu einem breit angelegten Angriff kommen sollte, ist eine klare Zuordnung der Aufgaben zwischen Privatwirtschaft und Staat unabdingbar.

Der Staat soll daher mit geeigneten, anreizbasierten Mitteln dafür sorgen, dass Cybervorfälle gemeldet werden. Dies erhöht die Transparenz, mindert die Bedrohungslage und hilft, die Auswirkungen solcher Angriffe auf Dritte zu reduzieren. Bevölkerung, Unternehmen, Verwaltung und Politik müssen angemessen sensibilisiert werden, um das Verständnis für Cyberrisiken zu verbessern. Bei der Sicherheit im Cyberraum handelt es sich um eine klassische

Verbundsaufgabe. Alles ist vernetzt und die Systeme beeinflussen sich gegenseitig. Dies heisst auch, dass jeder seinen Teil dazu beitragen muss, die Sicherheit zu erhöhen. Der Ruf nach Staat hilft genauso wenig, wie die eigene technologische Verwundbarkeit zu ignorieren.

Dieser Artikel ist ursprünglich im IT business erschienen.