DOSSIER
RISIKO & SICHERHEIT

Bild: Leonid Tit – Fotolia.com

Wie kann sich ein KMU gegen Gefahren aus dem Internet schützen? Das Verwenden internetfähiger Geräte und der Umgang mit dem Internet selbst haben sowohl im privaten Umfeld als auch im Geschäftsbetrieb von Unternehmen in den letzten Jahren exponentiell zugenommen. Der Gebrauch ist im Privat- und Geschäftsleben kaum noch wegzudenken. Zugenommen hat aber auch die Gefahr aus dem Web.

VON OLIVER KAMIN*

Vermehrt werden onlinegestützte Dienstleistungen (bspw. Auslagerung von Daten in eine Cloud, Verwenden von E-Shops externer Dienstleister oder Dienste für Online-Finanztransaktionen) in Anspruch genommen. Zusätzlich sind eine zunehmende Funktionsintegration der verwendeten Endgeräte (bspw. Smartphones oder Tablet-Computer, die eine Vielzahl von Features von damals getrennten Geräten in sich vereinen) und eine Konvergenz der Arbeits- und Lebensbereiche (bspw. Bring Your Own Device bzw. die Verwendung von privaten Endgeräten im Geschäftsbetrieb oder das Arbeiten von zu Hause aus im sog. Home Office) zu beobachten. Aus diesen Umständen erwachsen zahlreiche Gefahren, die nicht nur von der Hard- und Software, den Kommunikationskanälen oder von weiteren äusseren Einflüssen und Personen ausgehen, sondern insbesondere auch von innen, also den Geschäftsführenden bzw. Mitarbeitenden eines Unternehmens selbst hervorgerufen werden.

Die richtigen Massnahmen treffen. Um diese Gefahren abzuwehren, sind Unternehmen angehalten, ihre betriebliche Informationsverarbeitung sicher zu gestalten, um sie sowohl gegen potenzielle Angriffe krimineller Organisationen und Personen (bspw. Missbrauch/Verlust von Daten oder Manipulation der IT-Infrastruktur und -Anwen-

DR. OLIVER KAMIN ist Studiengangsleiter für Wirtschaftsinformatik und Business-/IT-Consulting an der Fernfachhochschule Schweiz.

www.ffhs.ch

Bild: rawpixel – Fotolia.com

Die Gefahren, die aus dem Internet drohen, sind vielfältig.

dungen) von aussen als auch von innen zu schützen. In diesem Zusammenhang wären folgende besonders wichtige externe Bedrohungen zu nennen, denen mit den entsprechend aufgeführten Massnahmen entgegengewirkt werden könnte:

> Auffälligkeiten durch stets aktuelle Konfiguration und regelmässige Überwachung der (Netzwerk-)Hardware identifizieren,
> Anvisieren von Schwachstellen entgegenwirken, indem ein Patch-Management-System für die betrieblichen Anwendungen bzw. der Netzwerk-Software unterhalten wird,
> Angriffen auf den bspw. eigenen (Web-)Server durch das regelmässige Überprüfen des Applikationscodes vorbeugen,
> Insiderattacken durch das Prinzip der doppelten Kontrolle erschweren, wobei jede wichtige Ressource (bspw. Zugangsdaten oder Speicherorte) redundant vorzuhalten ist,
> eventuell bösartigen HTML-Mailverkehr überwachen lassen, sodass verhindert wird, dass abgehende HTML-Anforderungen überhaupt bei bösartigen Webseiten ankommen,
> Datenverlust tragbarer Geräte (bspw. USB-Sticks) durch Bereitstellung eines vertrauenswürdigen Dienstes zur mobilen Datenablage vorbeugen,
> Strategie für den Ernstfall durch einen (externen) Sicherheitsexperten im Unternehmen implementieren.

Bequemlichkeit als Gefahrenquelle. Der aber gewichtigste Aspekt sollte in diesem Zusammenhang nicht unterschätzt werden: Das tägliche unbewusste bzw. unachtsame Handeln der Geschäftsführenden und der Mitarbeitenden selbst im Betriebsalltag aus Bequemlichkeit lässt oft wichtige Sicherheitsaspekte ausser Acht. Folgende interne Bedrohungen sollten in einem Unternehmen mit den entsprechend genannten Massnahmen angegangen werden:

> Verwenden mobiler Geräte oder Arbeitsplatzrechner mit einem Administrationskonto vermeiden, indem Mitarbeitenden nur Nutzerkonten mit eingeschränkten Rechten eingerichtet werden,
> ungeschütztem Zurücklassen der Arbeitsplatzrechner zuvorkommen, indem eine automatische Aktivierung des Sperrbildschirms nach gewisser Inaktivität erfolgt, auch wenn Mitarbeitende nur eine kurze Pause einlegen und das Büro verlassen,
> Anschlussmöglichkeiten von externen Geräten und Datenträgern an Arbeitsplatzrechnern unterbinden,
> Ignorieren von Warnhinweisen und Sicherheitsmechanismen verhindern, sodass bspw. das automatische Starten und Synchronisieren von Dateien oder das Speichern von Passwörtern nicht möglich sind,
> Nutzung von unsicheren Netzzugängen durch das bspw. Festsetzen von Richtlinien zur obligatorischen Verwendung von Verschlüsselungstechnologien vermeiden,
> unbedachtes privates Surfen der Mitarbeitenden auf bspw. Fanseiten, Online-Shops, sozialen Netzwerken oder gar illegalen Angeboten durch das Betreiben eines Filters unterbinden, sodass bspw. Bot-Clients, Trojaner, Spyware, Tracking-Software, Keylogger oder Spambots solcher Anbieter nicht auf die Arbeitsplatzrechner kommen,
> Versenden unverschlüsselter Nachrichten bzw. E-Mails mit sensiblen Daten vermeiden, indem Mail-Anwendungen standardmässig die Ausgangspost verschlüsseln und signieren,
> Bedienfehler aus Unwissenheit (bspw. das versehentliche Löschen von Dateien) durch Mitarbeiterschulungen minimieren.

Sicherheitslücken durch Sensibilisierung schliessen. Zu erkennen ist, dass das Begegnen der internen Bedrohungen einer Sensibilisierung sowohl der Anwender als auch der Verantwortlichen im Unternehmen bedarf. Problem ist nämlich, dass Sicherheitsvorkehrungen nicht nur in der betrieblichen Informationsverarbeitung, sondern auch im Allgemeinen als diffus, unbequem und aufwendig angesehen werden. Nur ungern werden Arbeitskraft, Zeit und Geld in Dinge investiert, die für einen selbst nicht vollständig erfassbar sind, eher präventiv wirken, zumeist im Verborgenen ablaufen und nicht sofort zu quantitativ oder gar monetär messbaren Ergebnissen führen. Dies lässt sich mit dem vorsorglichen Abschluss einer Versicherung vergleichen: Man unterschätzt die Wahrscheinlichkeit, dass im eigenen Wirkungskreis ein Schadensfall eintritt, und verzichtet entweder auf einen Vertragsabschluss bzw. eine Sicherheitsvorkehrung oder nimmt sich dieses Themas nur halbherzig an (bspw. Wahl einer unzureichenden Variante). Kommt es dann zu einem Schadensfall, wo bspw. der Geschäftsbetrieb für einige Tage eingeschränkt ist oder stillsteht, da die betrieblichen Daten verloren, gestohlen, manipuliert oder zerstört wurden und nicht so ohne Weiteres rekonstruiert werden können, wird man sich (leider zu spät) des Schadensumfangs erst bewusst. Man würde nun gerne auf das bspw. fehlende Vollbackup des letzten Tages zurückgreifen wollen, oder man bereut es, entsprechende Sensibilisierungsmassnahmen nicht getroffen und Sicherheitslücken nicht vorher geschlossen zu haben.

In KMU fehlt oft das Risikobewusstsein. Grössere Unternehmen halten zumeist eigene mit qualifizierten Spezialisten be-

setzte IT-Abteilungen vor, um die Informationssicherheit sicherzustellen. Bei mittleren und kleinen Unternehmen ist dies oft nicht gegeben. Grund hierfür ist zum einen die oben genannte fehlende Sensibilität in der Geschäftsführung und bei den Mitarbeitenden bezüglich der potenziellen Gefahren einer unzureichenden Informationssicherheit des Unternehmens, da diese zumeist eher als Belastung und niederprioritär angesehen wird. Zum anderen sind oft in kleineren und mittleren Unternehmen mehrere betriebliche Funktionen auf eine Stelle bzw. Person vereint. So wird die Funktion der betrieblichen Informationsverarbeitung bzw. Informationssicherheit in kleinen Unternehmen oft von einem technikaffinen Mitarbeiter, der sonst hauptsächlich in einer anderen Funktion im Unternehmen tätig ist, nebenbei wahrgenommen.

Nicht nur regelmässig technisch schulen. Es ist zwingend erforderlich, dass sich sowohl Geschäftsinhaber als auch Mitarbeitende, die nicht hauptsächlich mit der Informationssicherheit im Arbeitsalltag und den wachsenden Risiken des Internets auseinandersetzen, weiterqualifizieren. Wichtige Wissensbestände zur Informationssicherheit sollten – für Mitarbeitende im Idealfall durch den Arbeitgeber gefördert – regelmässig durch entsprechende Aus- und Weiterbildungsmassnahmen vermittelt werden, um eine Sensibilisierung mit entsprechendem Kompetenzerwerb zur Abwehr der Gefahren (nicht nur) aus dem Internet zu gewährleisten. Diese Aus- und Weiterbildungen sollten jedoch nicht – wie häufig zu beobachten – auf hauptsächlich technischer Ebene ablaufen. Vielmehr müssten die technischen Aspekte mit soziologischen, ökonomischen, rechtlichen und anwenderorientierten Problemfeldern ganzheitlich im Sinne einer vernetzten Gesellschaft verknüpft und vermittelt werden. Ziel sollte es dabei sein, im Zuge eines (grenz-)überschreitenden Informationsaustausches zwischen Personen, Unternehmen und anderen Institutionen/Organisationen die wichtigsten und aktuellsten Gefahren bzw. Risiken zu verstehen und sich durch das Ergreifen geeigneter Massnahmen gegen externe und interne Bedrohungen zu schützen.

QUELLENNACHWEIS:

- Friedmann, K.: Die größten Risiken für die Datensicherheit, http://www.computerwoche.de/a/die-groessten-risiken-fuer-die-datensicherheit,1874650, Abruf am 26.9.2014
- Metzger, S.: Mit Hackern gegen Hacker, http://www.handelsblatt.com/unternehmen/it-medien/datensicherheit-mit-hackern-gegen-hacker/4448002.html, Abruf am 26.9.2014
- Watchguard: Top Ten Security Threats for SMEs, http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp.pdf, Abruf am 26.9.2014