KMU sollten die Gefahr von Cyberattacken ernst nehmen

Roger Peduzzi, ICR Informatik AG

Mehr als ein Drittel der Schweizer KMU ist von Cyberattacken betroffen. Doch vielen ist nicht bewusst, was eine solche Attacke bedeutet. Das sollte sich ändern, indem zumindest gewisse Grundsätze befolgt und bewusste Entscheide getroffen werden.

Im September 2017 befragte das Markt- und Sozialforschungsinstitut gfs-zürich in einer repräsentativen Umfrage 300 CEOs von Schweizer KMU zum Thema Cyberrisiken[1]. Die nach wissenschaftlichen Methoden erfolgte Auswahl der KMU erlaubt es, die Resultate auf die Gesamtheit der Schweizer KMU (2015: 580 000) zu übertragen.

Die wichtigsten Ergebnisse im Überblick

- Die IT muss kontinuierlich funktionieren: Rund 62 Prozent der Befragten bewerten das kontinuierliche Funktionieren der IT als sehr wichtig für ihren Betrieb.
- Mehr als ein Drittel der KMU ist von Cyberattacken betroffen: Auf Basis der 300 befragten KMU kann die Anzahl der schweizweit von Erpressung betroffenen Firmen auf 23 000 (4 Prozent) geschätzt werden. Ungefähr 209 000 Unternehmen (36 Prozent) dürften von Malware wie Viren oder Trojanern betroffen gewesen sein.
- Das Risiko von Cyberangriffen wird stark unterschätzt: Das Risiko, Opfer eines Cyberangriffs zu werden, wird als tief eingeschätzt. Einen Tag lang ausser Gefecht gesetzt oder gar in der Existenz gefährdet zu werden, empfinden nur 10 Prozent bzw. 4 Prozent als grosse oder sehr grosse Gefahr. Über die Hälfte der befragten Geschäftsführer/-innen (56 Prozent) fühlen sich gut bis sehr gut vor Cyberangriffen geschützt.
- Der Schutz vor Cyberangriffen ist ungenügend: Nur 60 Prozent der Befragten geben an, Grundschutzmassnahmen wie Malware-Schutz, Firewall, Patch-Management und Back-up ganz umgesetzt zu haben. Systeme zur Erkennung von Cybervorfällen wurden nur von jedem fünften Unternehmen vollständig eingeführt, Prozesse zur Behandlung von Cybervorfällen nur von 18 Prozent der befragten Unternehmen, Mitarbeiterschulungen zum sicheren Gebrauch von IT lediglich von 15 Prozent.

Auch KMU sind von IT abhängig

Die allermeisten KMU sind heute auf eine funktionierende IT angewiesen. Aber gerade von den kleinen Unternehmen wird das Thema IT oft als nicht strategisch betrachtet und in der Folge halten sie die Ausgaben in diesem Bereich möglichst tief. Aufgrund dessen und wegen des fehlenden internen Know-hows sind sie dadurch besonders anfällig für Cyberangriffe. Die Resultate dieser Umfrage zeigen deutlich, dass Handlungsbedarf besteht. Die Schweizer KMU sind wichtig für die Schweizer Wirtschaft. Im Bereich der Finanzwirtschaft, wo viele vertrauliche Daten vorhanden sind und der Datenschutz zentral ist, ist es umso wichtiger, sich effizient gegen Cyberattacken zu schützen.

Nur die «Spitze des Eisbergs» wird bekannt

Aufgrund vieler Pressemeldungen ist das Szenario des Cyberangriffs mit folgendem Muster bekannt: Angreifer verschaffen sich Zugriff auf Computer und Server, verschlüsseln die darauf liegenden Dateien und fordern für die Entschlüsselung Lösegeld in Form einer Bitcoin-Überweisung. Und doch ist dies nur die Spitze des Eisbergs. Die meisten Angriffe erfolgen ohne das Wissen der Öffentlichkeit – und die Angriffsformen sind sehr unterschiedlich. Es können beispielsweise Trojaner über E-Mail-Anhänge, Internetseiten oder USB-Sticks eingeschleust werden oder Schwachstellen oder Sicherheitslücken des Betriebssystems, der Firewall oder weiterer sicherheitsrelevanter Systemkomponenten ausgenutzt werden. Auch eine ungenügende Trennung der Netzwerkzonen öffnet Angreifern Tor und Tür für Zugriffe auf die Server, und ein ungenügender Passwortschutz erleichtert den Zugriff auf PCs und Server und ermöglicht Missbrauch in unterschiedlichen Formen.

Schutz auf allen Ebenen

Deshalb ist überall, wo IT eine zentrale Rolle spielt, der Informationssicherheit ein hoher Stellenwert einzuräumen. Unter Informationssicherheit wird der Schutz von digitalen wie auch nicht digitalen Systemen hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität der Daten verstanden. Massnahmen wie Installation von Antivirus- und Malware-Software, regelmässiges Einspielen von Updates und Patches, konsequentes Durchführen von Back-ups und

Restore-Tests sowie Sensibilisierung von Mitarbeitenden bieten einen gewissen Schutz. Doch um die Informationssicherheit wirklich gewährleisten zu können, muss mehr getan werden. Bewährt hat sich im deutschsprachigen Raum folgendes Vorgehen: Die Risiken und Bedrohungen werden oft anhand des IT-Grundschutzes (Katalog von Hunderten von Bedrohungsszenarien) erhoben. Dabei stellt man sich die Frage, ob die jeweilige Bedrohung für die jeweilige IT-Umgebung relevant ist oder nicht, und beurteilt die Wahrscheinlichkeit des Eintretens sowie die möglichen Auswirkungen. Sobald die Risiken bekannt sind, können technische und organisatorische Massnahmen zur Vermeidung oder Verminderung allfälliger Risiken getroffen werden. Wurde ein Risiko aufgrund der zu erwartenden Auswirkungen und der Eintrittswahrscheinlichkeit als relativ klein eingeschätzt und weitere Vorkehrungen für zu teuer und/oder für unverhältnismässig befunden, kann die Geschäftsleitung ein solches Risiko bewusst akzeptieren.

Auslagern bietet mehr Sicherheit

Wenn KMU die konsequente Umsetzung der Informationssicherheit als zu aufwendig einschätzen, dann kann das aus Expertensicht meist bestätigt werden. Es gibt aber eine Alternative, nämlich die konsequente Auslagerung von Daten und Applikationen zu Serviceprovidern. Dadurch werden auch die Aufgaben, die die Informationssicherheit betreffen, ausgelagert. Auf den Arbeitsplatzcomputern befinden sich als Folge keine relevanten oder sensiblen Daten mehr. Wenn ein PC ein Virus einfängt oder seine Festplatte durch einen Kryptotrojaner verschlüsselt wird, müssen die angegriffenen Computer nur neu aufgesetzt werden und sind danach sofort wieder einsatzfähig. Es gibt Serviceprovider, die auch das cloudbasierte Client-Management anbieten.

«Antivirus- und Malware-Software, regelmässige Updates und sensibilisierte Mitarbeitende genügen nicht. Wer sich vor Cyberangriffen schützen will, muss mehr unternehmen.»

So können die Inbetriebnahme neuer Arbeitsplatzcomputer sowie der Austausch von beschädigten oder kompromittierten PCs für das jeweilige KMU erheblich erleichtert werden. Natürlich müssen die Serviceprovider sorgfältig evaluiert werden. Serviceprovider sind oft nach ISO 27001 zertifiziert[2] oder werden von einem Wirtschaftsprüfer nach dem Kontrollregelwerk ISAE 3402[3] geprüft. Verfügt ein Serviceprovider über diese Qualitätsausweise, kann man davon ausgehen, dass die Informationssicherheit gewährleistet ist.

[1] Studie «Cyberrisiken in Schweizer KMUs» https://ictswitzerland.ch (Publikationen/Studien)
[2] ISO/IEC 27001 ist eine international anerkannte Norm zur Informationssicherheit
[3] ISAE 3402 ist ein international anerkannter Prüfungsstandard für interne Kontrollsysteme (IKS)

Zielorientiert, effizient und weitsichtig

FINIG und FIDLEG stellen neue Anforderungen an unabhängige Vermögensverwalter. Wer Probleme frühzeitig erkennt, hat Handlungsspielraum.

Als Prüfgesellschaft für Vermögensverwalter sind wir auf Ihre Anforderungen spezialisiert. Und stehen Ihnen bei den notwendigen Anpassungen und der Implementierung von entsprechenden Lösungen beratend zur Seite. Zielorientiert, effizient und weitsichtig.

Vergrössern Sie Ihren Handlungsspielraum und kontaktieren Sie uns per E-Mail info@swa-audit.ch oder per Telefon 055 415 54 70. Wir sind für Sie da – von KMU zu KMU.

Alle Informationen zu FIDLEG und FINIG auf www.swa-audit.ch

SWA Swiss Auditors AG
Bahnhofstrasse 3, 8808 Pfäffikon SZ
T 055 415 54 70, info@swa-audit.ch
www.swa-audit.ch