board talk

fcs

Cyber Security

Issue #6 • 01/2022

Bei fast keinem Austausch unter Verwaltungsräten im letzten Jahr war «Cyber Security» nicht ein vieldiskutiertes Thema. Zu Recht! Zwar sind Verwaltungsräte meist nicht Experten auf diesem Gebiet, doch können und müssen sie bezüglich «Cyber Security» eine führende Rolle einnehmen.

1. Starker Anstieg von Vorfällen

2021 haben die Vorfälle wiederum stark zugenommen. Vorfälle sind u.a. Malware Angriffe (Ransomware und Spyware), Phishing Emails, Hacking, Defacing etc.

Globalisierung, Digitalisierung, Home Office, Cloud Computing sind einige der Ursachen. Eine andere ist schlicht die Tatsache, dass sich mit Ransom-Attacken gut Geld verdienen lässt. Es ist eine interessante Einkommensquelle verbrecherischer Organisationen. Diese operieren global in Jurisdiktionen, in denen auf dem Rechtsweg kaum gegen sie vorgegangen werden kann.

2. Wie sind Unternehmen gefordert?

Gegen Angriffe gibt es grundsätzlich zwei Strategien: Prävention und Reaktion. Ein Unternehmen muss beide verfolgen.

Einerseits soll die eigene Infrastruktur mit Hilfe von technischen Massnahmen vor Angriffen so gut wie möglich geschützt werden. I.d.R. mit geeigneter Software (Firewalls, Antiviren-Programme) sowie regelmässigen Aktualisierungen.

Auf prozessualer Ebene helfen u.a. eine gute Benutzeradministration sowie regelmässige Backups. Auch die Sensibilisierung der Mitarbeiter ist entscheidend (s. nachfolgend).

Aber es gibt keinen 100%igen Schutz! Deshalb braucht es einen Notfallplan. Bei erfolgtem Angriff muss sofort und richtig reagiert werden. Während viele Unternehmen schon einen relativ guten Schutz aufgebaut haben, tun sich viele schwer mit dem Notfallplan. Dabei ist dieser mindestens so wichtig. Nur bei Banken ist ein solcher eher schon Standard.

Im Bedarfsfall muss sofort klar sein, wer was zu tun hat. Der Cybersecurity-Leitfaden des Bundes zeigt beispielhaft, was ein solcher Notfallplan für KMUs berücksichtigen müsste (über digitalswitzerland.com).

einige Fakten...

allein in der Woche 2/2022 gingen beim Schweizer NCSC 881 Meldungen ein, u.a. 169 Hinweise wegen Phishing (*ncsc.admin. ch*)

43% von Schweizer CEOs erachten Cyber Risiken als das grösste Hindernis für weiteres Wachstum (*pwc.ch*)

Siegfried, V-Zug, Comparis, Saurer, Kantonalbank Neuenburg, Zürich Versicherungen, Stadt St. Gallen, Waldhaus Flims, MCH Group, Bucher u.v.m. haben 2021 einen Cyber Angriff gemeldet (*konbriefing.com*)

vermutete 27% der weltweit angegriffenen Unternehmen zahlen das Lösegeld von durchschnittlich USD 1 Mio. (*crowdstrike.com*)

weltweite Ransomware Zahlungen werden in 10 Jahren jährlich rund CHF 250 Mia. betragen (*cybersecurityventures.com*)

«Es gibt nur zwei Arten von Firmen, die die schon gehackt wurden und die die es noch nicht wissen.» (*Urs Küderli, PwC Schweiz*)

3. Faktor Mensch

Der Mitarbeiter ist das wertvollste Asset jeder Unternehmung, aber auch das schwächste Glied bezüglich «Cyber Security». Erfahrungsgemäss dringen Angreifer meist über eine Türe ins Datennetzwerk einer Firma ein, welche ihnen mittels sog. Phishing Emails unwissentlich von einem Mitarbeiter geöffnet wurde. Es ist erstaunlich, wie professionell solche Emails mittlerweile sind; wie einfach diese zu erstellen sind; und wie viele Mitarbeiter bei Testläufen jeweils immer wieder darauf hereinfallen.

Ohne Einzelnen einen Vorwurf zu machen, muss einfach betont werden, dass es folgendes braucht: Sensibilisierung, Test, Sensibilisierung, Test, Sensibilisierung usw.

4. Aufgabe des Verwaltungsrates

Verwaltungsräte sind meist keine IT bzw. Cyber Security Experten. Das ist auch nicht nötig. Aber sie müssen dafür sorgen, dass diese Experten entweder in der Unternehmung vorhanden sind oder dass das notwendige Know-how extern beschafft wird.

Im Rahmen der Risikobeurteilung wird ein VR-Gremium kaum umhinkommen, Cyber-Risiken zu diskutieren und zu beurteilen. Empfehlenswert ist dabei die Teilnahme des internen Experten. Für Nicht-IT-Experten wie mich ist es nämlich schwierig, die Risiken richtig einzuschätzen, insbesondere unter Berücksichtigung der bestehenden internen Schutzmassnahmen.

Meine Erfahrungen haben gezeigt, dass technische und prozessuale Massnahmen das Cyber Risiko zwar erheblich reduzieren können; das Restrisiko verbleibt trotz hohen Kosten aber immer auf einem ungemütlichen Niveau.

Letztlich muss sich der Verwaltungsrat aber überzeugen, dass das Cyber Risiko angemessen überwacht und die notwendigen Massnahmen ergriffen werden.

Wenn ich für die laufende Amtsperiode zwei Empfehlungen mit auf den Weg geben darf, sind es folgende:

- **Sorgen Sie dafür, dass in der Schublade Ihrer Unternehmung ein Notfallplan liegt und dass dieser auch schon einmal 1:1 durchgespielt worden ist.**
- **Versichern Sie sich, dass alle Mitarbeiter Ihrer Unternehmung immer wieder und wieder sensibilisiert und getestet werden.**

fcs company gmbh • Seegartenstrasse 2, CH-8008 Zürich • www.fcscompany.ch
Hans-Peter Wyss • +41 (0)79 430 9975 • hwyss@fcscompany.ch