Herausforderungen der Schweizer Cyberdimension

Die digitale Transformation und der steigende Stellenwert des Homeoffice während Covid-19 erhöhen die Komplexität und die Herausforderungen in der Cyberdimension: Im Schweizer Cyberraum gibt es viel Nachholbedarf zur Sicherung von Infrastrukturen und Daten.

Marc K. Peter & Nicolas Mayencourt

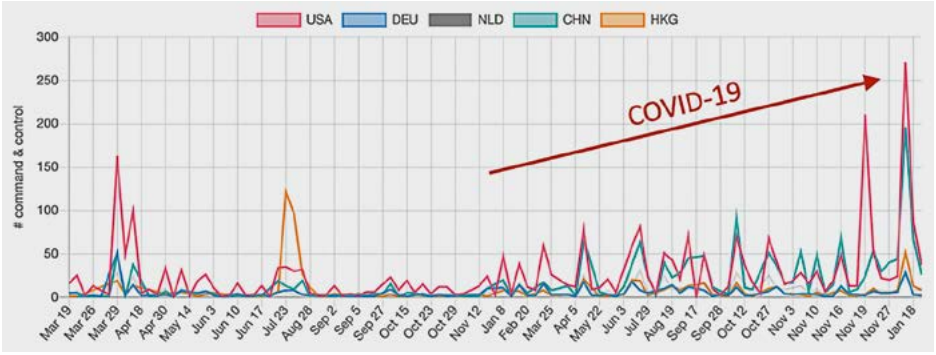

Abb. 1: Globale C2-Systeme März 2019 bis Januar 2021.

Die digitale Transformation ist ein Veränderungsprozess, welcher Wirtschaft, Gesellschaft und Politik nachhaltig verändert. In diesem Prozess, auch bekannt unter dem Begriff der vierten industriellen Revolution, steigt unsere Abhängigkeit von der IT und dem Internet. Die Cyberdimension durchdringt alle physischen Dimensionen und schafft so cyberphysische Systeme, durch welche unser Leben immer stärker von Computern dominiert, betrieben und kontrolliert wird. Neben der Abhängigkeit steigen auch die Risiken von Attacken auf die IT-Infrastruktur und Diebstahl sowie Verlust von Daten.

Die verschiedenen grossen Schweizer Studien der Hochschule für Wirtschaft FHNW zeigen eindrücklich den Stand der digitalen Transformation in der Schweiz. Als grosse Barrieren der Transformation werden seit mehreren Jahren die fehlende Zeit, das fehlende Wissen und der Mangel an ausgebildeten Mitarbeitenden beschrieben; zum grössten Risiko gehört die Cyber- und Datensicherheit. In der kurz vor Covid-19 publizierten Studie zur Transformation der Arbeitswelt in Schweizer Unternehmen wird zudem neu (bei einem Drittel der Befragten) die Überwachung am Arbeitsplatz durch die Arbeitgeberin und Staaten als Risiko genannt.

Covid-19 und das Homeoffice

Zusammen mit verschiedenen Forschungspartnern wurde 2020 in repräsentativen KMU-Studien der Stand zum Homeoffice und der Cybersicherheit zwischen der ersten und der zweiten Covid-19-Welle analysiert.

Im Umfeld der Workplace-Transformation wird vielfach der Begriff des Blended Working diskutiert (ein Arbeitsumfeld, in dem diverse Arbeitsformen und -plätze bereitgestellt werden), zu welchem auch das Homeoffice gehört. Im ersten durch Covid-19 resultierenden Lockdown im März/April 2020 hat sich die Zahl der Mitarbeitenden, welche von zu Hause aus arbeiteten, fast vervierfacht. Seitdem (vor der zweiten Welle) hat sich das Homeoffice etabliert und die Nutzung ist gegenüber dem Stand vor dem ersten Lockdown um über die Hälfte (um 60% von 10% auf 16%) angestiegen.

Bei den eingesetzten Kommunikationsmitteln dominiert E-Mail weiterhin (bei 84% der KMU), gefolgt von Telefon, WhatsApp und anderen Messengerdiensten sowie Online-Konferenztools. Interessanterweise nutzen über die Hälfte der Unternehmen Messengerdienste und knapp die Hälfte Online-Konferenztools wie Google Meet, Skype, Teams oder Zoom. Die Unternehmensdaten gelangen so vielfach ins Ausland bzw. werden von ausländischen Diensten gehostet. So eröffnen sich weitere Risiken für Angriffe sowie Datenverluste.

Ein Drittel (29%) der Schweizer KMU geht davon aus, dass künftig noch mehr Mitarbeitende von zu Hause aus arbeiten werden. Damit verbunden, rückt auch die Cybersicherheit verstärkt in den Fokus:

WICHTIGE VERHALTENSREGELN IM HOMEOFFICE

- Nutzen Sie eine VPN-Verbindung, damit die Daten zur Unternehmens-IT verschlüsselt übertragen werden.
- Kommunizieren Sie nur über Unternehmenskonten und nicht über private E-Mail-Konten oder Messengerdienste wie WhatsApp.
- Sperren Sie den Computer, auch wenn Sie sich nur kurz vom Arbeitsplatz entfernen.
- Lassen Sie keine vertraulichen Dokumente und Ausdrucke herumliegen.
- Telefonieren Sie nicht auf dem Balkon über Vertrauliches.
- Verschlüsseln Sie IT-Systeme, E-Mails und Datenträger (z.B. USB-Sticks).
- Installieren Sie für Ihre Familie zur Privatnutzung keine Software/keine Apps
- Halten Sie Software und Virenschutz aktuell.

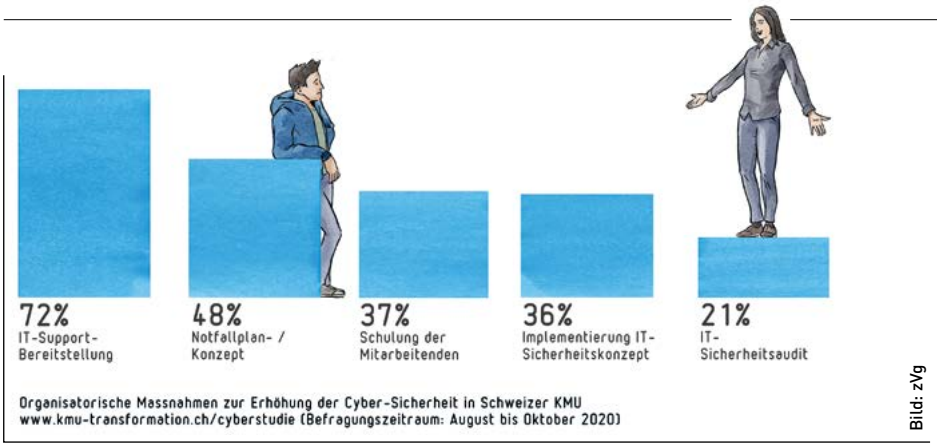

Bild: zVg

Abb. 2: Organisatorische Massnahmen zur Erhöhung der Cybersicherheit in Schweizer KMU im 2020.

WEITERE INFORMATIONEN

- Cyberstudie Schweizer KMU: www.cyberstudie.ch
- Studien zur digitalen Transformation: www.kmu-transformation.ch
- Schweizer Radarsystem CyObs: www.cyobs.ch
- Das Praxisbuch zur Cybersicherheit: www.it-sicherheit-kmu.ch
- Swiss Cyber Security Days: www.scsd.ch

Hier erachten zwei Drittel der Schweizer KMU das Thema als wichtig oder sehr wichtig. Je grösser das Unternehmen, umso höher wird das Thema Cybersicherheit gewichtet.

An den Swiss Cyber Security Days 2021 wurde eine Studie von Dreamlab Technologies präsentiert, welche den starken Anstieg von globalen Command-and-Control-(C2-)Infrastrukturen während der Pandemie zeigt (Abb. 1). Diese C2-Systeme werden dazu genutzt, um z.B. mit Phishing-E-Mails das Öffnen bzw. den Aufruf einer Webseite zu provozieren. Über die C2-Infrastruktur wird anschliessend Malware (trojanische Pferde) eingeschleust und die Computer so ausgespäht und kontrolliert.

Cybersicherheit in den KMU

Die Studie von 2020 zeigt, dass ein Viertel der Schweizer KMU bereits Opfer eines Cyberangriffs wurden, dessen Schadensbehebung mit erheblichem Aufwand verbunden war. Davon sahen ein Drittel einen finanziellen Schaden und je ein Zehntel einen Reputationsschaden oder den Verlust von Kundendaten. Demgegenüber steht noch immer das mangelnde Bewusstsein der Unternehmen, selbst Opfer eines Cyberangriffs zu werden: Nur gerade 11% schätzen das Risiko, durch einen Cyberangriff einen Tag ausser Gefecht gesetzt zu werden, als gross ein.

Wichtigste technische Massnahmen zur Erhöhung der Cybersicherheit sind gemäss Studienresultaten regelmässige Datensicherungen (Backups), der Einsatz von Antivirusprogrammen, regelmässige Software-Updates und der Einsatz von Firewalls. Jedoch besteht bei den organisatorischen Massnahmen noch viel Handlungsbedarf: Nur etwas mehr als ein Drittel der KMU schult regelmässig seine Mitarbeitenden, nur ein Fünftel führt IT-Sicherheitsaudits durch und nur ein Sechstel der KMU hat eine Cyberversicherung abgeschlossen (Abb. 2).

Der Schweizer Cyberspace

In der nun dritten Durchführung der Swiss Cyber Security Days wurden wieder die aktuellen Zahlen zum Stand der Nation, dem Schweizer Cyberraum, vorgestellt. Das Schweizer Cyberradarsystem CyObs analysierte die externe bzw. öffentlich zugängliche IT-Infrastruktur (Abb. 3) mit über 20 Millionen IP-Adressen und 2,3 Millionen .ch-Domains. Die Studie identifizierte über 100 000 publizierte und bekannte Verwundbarkeiten. Dazu zählen beispielsweise:

- 2900 Schwachstellen in E-Mail-Server-Software (exim_rce)
- 2400 direkt ansprechbare nicht mehr unterstützte Windows-Systeme (EOL)
- 837 verwundbare FortiOS-Installationen
- 400 direkt ansprechbare und verwundbare iLO-Kontrollsysteme
- 322 administrative Kontrollsysteme, welche mit Bluekeep infiziert sind
- 197 öffentlich zugängliche ungeschützte Datenbanken
- 118 Netzwerke, welche mit Eternalblue angegriffen werden könnten

Die verschiedenen Studien zeigen, dass die Themen der Digitalisierung, des Homeoffice und der Cybersicherheit im Umfeld von Covid-19 an Wichtigkeit gewonnen haben und die Schweiz noch viel leisten muss. Es ist an der Zeit, die Cyberdimension nicht nur als Risiko, sondern auch als Wettbewerbsvorteil für Wirtschaft, Gesellschaft und Politik wahrzunehmen und entsprechend zu investieren. ■

© Dreamlab Technologies AG

Abb. 3: Die externe Angriffsfläche des Schweizer Cyberspace (IP-Adressen und Domains) im Januar 2021.

MARC K. PETER
Professor an der FHNW im Bereich digitale Transformation
NICOLAS MAYENCOURT
CEO von Dreamlab und Programmdirektor der Swiss Cyber Security Days