

CYBERSECURITY – Die Homeoffice-Pflicht wurde vom Bundesrat aufgehoben, es gilt nun noch landesweit eine Homeoffice-Empfehlung. Eines ist für Experten wie Chris Eckert jedoch ganz klar. Wenn es um die Herausforderungen bei der IT-Sicherheit im Zusammenhang mit der Schwachstelle Mensch geht, so gilt:

«Die Gefahren werden nicht weniger»

Seit vielen Monaten arbeitet ein beachtlicher Teil der Angestellten verschiedenster Branchen wenn immer möglich von zu Hause aus. Der zu Beginn der Pandemie verordnete Umzug ins Homeoffice wurde in den meisten Fällen schnell und pragmatisch organisiert und umgesetzt. Selbst überzeugte Skeptiker der Arbeit von zu Hause aus – egal ob Arbeitnehmende oder Arbeitgebende – konnten im Laufe der Zeit einige Vorteile der Telearbeit nicht von der Hand weisen. Wie meistens in solchen krisenähnlichen Situationen wurde seitens der Arbeitgebenden vor allem Wert gelegt auf den möglichst zeitnahen Erhalt der Produktivität.

Nun hat uns die Realität wieder vollständig eingeholt, sofern sie überhaupt weg war. Das teilweise Weglassen der einfachsten Cybersecurity-Massnahmen oder schlicht das Ignorieren von möglichen Risiken in der Informationssicherheit rächt sich zusehends. Seit Pandemiebeginn hat sich die Zahl der Cyberangriffe stetig und rasant erhöht. Ein Ende ist nicht abzusehen, im Gegenteil: Hacker stehlen auf perfide Weise Daten, sehr gezielte Phishing-Attacken werden immer ausgeklügelter, «CEO-Fraud» hat kaum an Aktualität eingebüsst und Cyber-Erpressungen und Sabotage

mit Lösegeldforderungen werden immer zahlreicher und schlagen selbst bei Kleinstfirmen auf.

«SEIT PANDEMIEBEGINN HAT SICH DIE ZAHL DER CYBERANGRIFFE STETIG UND RASANT ERHÖHT.»

Vor nicht allzu langer Zeit versuchten Kriminelle zum Beispiel die Firewall der Unternehmen zu durchbrechen und dadurch Zugriff auf die Netzwerke zu erhalten. Die moderne Technik und Digitalisierung sind nicht mehr nur das alleinige und leicht überwindbare Ziel für Cyberattacken. Die Schwachstelle Mensch als unsicherer Faktor gerät zunehmend in den Fokus. Bereits heute gehen mehr als 50 Prozent solcher Angriffe auf das Konto des sogenannten «human risk».

Unbedingt (weiterhin) beachten

Wenn also 50 Prozent der erfolgreichen Angriffe auf Unternehmen auf die Schwachstelle Mensch – also wir alle als User – zurückzuführen sind, dann ist wohl unser bisheriges Verhalten näher und kritisch zu hinterfragen. Die folgende Aufzählung ist nicht abschliessend, soll Sie als Benutzer, Teilnehmer an Online-sessions, als Chef, aber auch als Privatperson animieren, sich nachhaltige Gedanken über das Schützenswerte in Ihrem Alltag und beim Homeoffice zu machen:

– Software auf sämtlichen Geräten (Smartphone, Pad, Laptop, Desktop, Scanner, Drucker) aktuell halten. Insbesondere die Sicherheitsupdates der Betriebssysteme und Antivirensoftware konsequent durchführen.



Gerade im Homeoffice gilt: Höchste Priorität der Informationssicherheit.

Bild: 123RF

- Geschäftliche und private Nutzung der Devices (IT- und Elektronik-Geräte) nicht vermischen. Der private PC oder Laptop birgt in der Regel grössere Sicherheitslücken, da oft eine Vielzahl von privaten Apps und Accounts mit einem permanenten Login versehen sind. Ausserdem benutzen wir Menschen den Geschäfts-PC meist etwas respektvoller und zurückhaltender als ein privates Gerät.
- Bei längeren Pausen oder Unterbrüchen wird das Abmelden von den Systemen/Zusammenklappen der Laptops empfohlen. Bei längerer Abwesenheit die Systeme herunterfahren, die mobilen Geräte nicht offensichtlich herumstehen lassen, sondern wegpacken und bestenfalls einschliessen.
- Das Heimnetzwerk sollte über gesicherte Verbindungen verfügen: Der Internetzugang zu Hause mit min-

destens WPA2 absichern, für die Kommunikation mit dem Firmennetzwerk wird ein VPN (Virtual Private Network) empfohlen.

- Die Webcam abdecken, wenn diese nicht verwendet wird. Dies scheint banal, aber es ist ein guter Schutz gegen sogenannte «Lauschangriffe».

• Besondere Vorsicht ist geboten bei auffälligen E-Mails (Phishing-Mails, CEO-Fraud, Paketankündigungen etc.) oder Dateianhängen, insbesondere von unbekanntem Absender.

- Im Homeoffice wenn möglich die sprachgesteuerten Geräte ausschalten.
- Geschäftliche Unterlagen (Akten, Dokumente, Datenträger) zu Hause nicht herumliegen lassen (Clean Desk Policy). Familienmitglieder, Mitbewohner und Besucher sind Dritte und haben kein Anrecht auf

UNTERNEHMENSCHUTZ

Neuer Lehrgang

Zugeschnitten auf den umfassenden Unternehmensschutz für KMU in der Schweiz wurde ein neuer Lehrgang erschaffen. Der CAS «Business Protection» an der Hochschule für Wirtschaft HWZ in Zürich startet am 18. Februar 2022 und dauert berufsbegleitend 18 Tage. Es sind noch Studienplätze frei:



einen Zugang zu geschäftlichen Daten und Informationen. Nicht mehr benötigte Aktenstücke sind nicht einfach im Kehrort oder Altpapier zu entsorgen, sondern im Aktenvernichter.

- Führen Sie geschäftliche Telefongespräche oder Onlinesitzungen von daheim und unterwegs in einer normalen, zurückhaltenden Tonlage. Das Besprochene ist in den meisten Fällen weder für Nachbarn noch Fremde bestimmt.

• Vermeiden Sie zur Kommunikation und zum Austausch von geschäftlichen Informationen unter Mitarbeitenden die kaum sicheren Kommunikationskanäle wie Whatsapp und dergleichen. Bevorzugen Sie verschlüsselte und datenschutzfreundliche Lösungen wie beispielsweise Threema.

- Die Prämissen Vertraulichkeit, Datenschutz und Compliance gelten insbesondere beim Homeoffice.

Chris Eckert

DER AUTOR

Autor **Chris Eckert** ist Founding Partner der Swiss Business Protection AG und verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich und der Bundeskriminalpolizei.

www.swissbp.ch

VERSICHERUNGSRATGEBER – Selbstfahrende Arbeitsmaschinen dürfen auf dem Werkareal ohne Immatrikulation und Kontrollschild eingesetzt werden. Doch wer haftet, wenn dort ein Unfall passiert?

Mit dem Mäher auf dem Werkareal unterwegs ...

O.B. aus G.: «Ein Mitarbeiter unseres Gartenbaubetriebes hat mit unserem Balkenmäher ein auf dem Betriebsareal abgestelltes Fahrzeug eines anderen Mitarbeiters beschädigt. Bekanntlich gilt eine Mähmaschine als selbstfahrende Arbeitsmaschine, welche keiner strassenverkehrsrechtlichen Immatrikulationspflicht unterliegt und ohne Kontrollschild auf dem Werkareal eingesetzt werden darf. Es besteht also kein Motorfahrzeughaftpflichtschutz. Unser Gartenbauer hat den Fall unverzüglich seiner Privathaftpflichtversicherung gemeldet. Diese hat nun den Schaden abgelehnt, da für gewerbliche Tätigkeiten keine Deckung bestehe. Wie muss ich mich verhalten, denn der geschädigte Mitarbeiter erwartet verständlicherweise eine volle Schadenübernahme von unserer Gartenbau-firma.»

Sehr geehrter Herr B: Der geschilderte Fall kommt immer wieder mal vor: Er stellt eine spannende versicherungsrechtliche Konstellation dar, die auf der Haftpflicht basiert. Ob eine Haftpflichtversicherung einen Schaden übernimmt, hängt primär von der Haftung selbst ab. Eine solche liegt



Fahrzeuge ohne Immatrikulationspflicht wie ein Balkenmäher sind in der Regel in der Betriebshaftpflicht mitversichert.

Bild: 123RF

vor, wenn beispielsweise ein Kausalhaftungs- (Geschäftsherrenhaftung, OR Art. 55, vgl. hienach) oder ein Verschuldenstatbestand (Verschuldenshaftung, OR Art. 41) erfüllt ist. Darüber hinaus bedarf es aber eines expliziten Versicherungsschutzes, der vertraglich vereinbart wurde, damit der Haft-

pflichtige für das Risiko seiner spezifisch betroffenen Tätigkeit einen Schutz beanspruchen kann.

Zuständig ist die Betriebshaftpflichtversicherung

Ihr Mitarbeiter hat fälschlicherweise seine eigene Haftpflichtversicherung angerufen. Im geschilderten Sach-

verhalt ist zwar von einer Fahrlässigkeit auszugehen, damit wäre die Verschuldenshaftung gegeben. Ihr Mitarbeiter agiert jedoch nicht als Privatperson. Deshalb hat die Privathaftpflichtversicherung zu Recht mitgeteilt, dass Ansprüche aus einer hauptberuflichen Erwerbstätigkeit vom Deckungsumfang ausgeschlossen sind. Für das geschilderte Ereignis ist einzig Ihre Betriebshaftpflichtversicherung zuständig.

Geschäftsherr haftet für das Verhalten seiner Mitarbeitenden

Ihr Betrieb haftet für das geschäftliche Verhalten Ihrer Mitarbeitenden, da Sie im Sinne von Art. 55 OR als Geschäftsherr für betriebliche Schäden haftbar sind, die Ihre Belegschaft in Ausübung der dienstlichen Verrichtungen gegenüber Dritten verursacht. Dies ist für Sie bedeutungsvoll, denn als Geschäftsherr müssen Sie Ihre Mitarbeiter deshalb sorgfältig auswählen, sie für ihre Aufgaben entsprechend instruieren und überwachen. Aus Art. 55 OR folgt, dass Sie verantwortlich sind für das, was Ihre Mitarbeitenden in ihren beruflichen Verrichtungen anstellen.

Vorausgesetzt, der geschädigte Mitarbeiter hat sein Fahrzeug berechtigtweise auf dem Areal abgestellt, ist Ihr Gartenbaubetrieb gegenüber Ihrem Mitarbeiter schadenersatzpflichtig. Sie haben aber zumindest die Berechtigung, einen Rückgriff auf den Schadensverursacher zu prüfen: Ihr Mitarbeiter kann grundsätzlich nach Massgabe seines Verschuldens zur Rechenschaft gezogen werden. Gemäss bisheriger Praxis müsste Ihr Mitarbeiter jedoch zumindest grobfahrlässig oder gar absichtlich gehandelt haben.

Sonderfall selbstfahrende Arbeitsmaschinen

Das Risiko von Fahrzeugen ohne Immatrikulationspflicht ist in der Regel in der Betriebshaftpflichtversicherung mitversichert, sofern solche ausschliesslich auf dem Betriebsareal zirkulieren. Dieser Schutz wird teilweise erweitert für den werkinernen Verkehr auf öffentlichen Strassen. Das zuständige Strassenverkehrsamt bewilligt dies namentlich, wenn sich ein Betriebsareal auf beide Seiten einer öffentlichen Durchgangsstrasse erstreckt.

laszlo.scheda@mobi.ch