IT-SICHERHEIT IM HOMEOFFICE

DAMIT STATT DES **CORONAVIRUS** NICHT EIN **COMPUTERVIRUS** ZUSCHLÄGT

Seit der Corona-Krise ist Homeoffice en vogue. Viele Arbeitnehmer arbeiten zum Schutz vor einer Ansteckung von zu Hause aus. Doch die virtuelle Zusammenarbeit mit den Kollegen bietet Einfallstore für Cyberkriminelle. Worauf Unternehmen achten müssen, damit IT-Sicherheit auch im Homeoffice gelingt.

▸ Das neuartige Coronavirus hat nicht nur das soziale Leben beeinflusst, sondern ist auch wirtschaftlich und rechtlich eine große Herausforderung. Um die Ausbreitung des Virus möglichst schnell einzudämmen und das Gesundheitssystem nicht übermäßig zu belasten, hatte die Bundesregierung Unternehmen dazu geraten, ihren Mitarbeitern Arbeit im Homeoffice zu ermöglichen, denn schließlich sollten die sozialen Kontakte auf ein Mindestmaß beschränkt sein. Auch wenn es „keinen gesetzlichen Rechtsanspruch auf mobiles Arbeiten“ gibt, wie Michaela Rassat, Juristin bei der Ergo Rechtsschutz Leistungs-GmbH, betont, setzten viele Unternehmen die Empfehlung der Bundesregierung um: Nie zuvor arbeiteten so viele Menschen gleichzeitig vom Homeoffice aus und werden das auch auf absehbare Zeit tun.

Manche Tätigkeiten, beispielsweise in der Produktion, lassen das Arbeiten in den eigenen vier Wänden nicht zu. „Außerdem ist es auch so, dass Arbeitgeber ihre Mitarbeiter nicht einfach zum mobilen Arbeiten verpflichten dürfen“, sagt Unternehmensjuristin Rassat. „Außer es besteht eine entsprechende Absprache im Arbeitsvertrag, an die sich der Mitarbeiter dann natürlich halten muss. Auch eine Betriebsvereinbarung kann die Arbeit von zu Hause vorsehen.“ Möglich sei auch eine Zusatzvereinbarung zum Arbeitsvertrag. Schließlich dürfte auch den Mitarbeitern aus Eigeninteresse daran gelegen sein, von zu Hause aus arbeiten zu dürfen. Denn solange es noch keinen Impfstoff gegen die vom neuartigen Coronavirus ausgelöste Krankheit Covid-19 gibt, ist ein Ansteckungsrisiko latent immer vorhanden.

Doch während die Unternehmen die Zusammenarbeit unter den Kollegen neu organisieren, setzen Cyberkriminelle ihre Arbeit wie gewohnt fort – und setzen dabei darauf, dass Mitarbeiter im Homeoffice weniger gut geschützt sind als im normalen Firmennetzwerk. Dabei sind die Unternehmen sich durchaus der Gefahren bewusst, die im Cyberspace lauern: Einer Studie des Digitalverbands Bitkom zufolge hat für gut acht von zehn befragten Unternehmen (84 Prozent) die Anzahl der Cyberattacken in den vergangenen zwei Jahren zugenommen, für mehr als ein Drittel (37 Prozent) sogar stark. 82 Prozent der befragten Firmen gehen davon aus, dass die Anzahl der Cyberattacken in den nächsten zwei Jahren weiter zunehmen wird. Und wegen ihrer Wirtschafts- und Innovationsstärke gelten deutsche Unternehmen – vor allem aus technikintensiven Branchen wie Chemie, Pharmazeutik, Finanzen oder Automotive – als besonders attraktives Ziel für Hacker.

UNTERNEHMEN KÖNNEN IT-SICHERHEIT IM HOMEOFFICE NICHT KONTROLLIEREN

Deshalb haben die Unternehmen zuletzt verstärkt in die IT-Sicherheit investiert. Laut Berechnungen des Marktforschungsunternehmens IDC im Auftrag des Digitalverbands Bitkom legten die Umsätze mit Sicherheitslösungen im vergangenen Jahr um 9 Prozent auf 4,4 Milliarden Euro zu. Der mit Abstand größte Teil der Ausgaben entfällt auf Dienstleistungen für digitale Sicherheit. In diesem Segment wurden im vergangenen Jahr 2,2 Milliarden Euro ausgegeben. Aber auch IT-Sicherheits-Software wie beispielsweise Virenscanner oder standardisierte Firewalls wurden flächendeckend angeschafft – hier lagen die Ausgaben bei 1,3 Milliarden Euro. So verfügen nun mittlerweile fast alle Betriebe für ihre Firmennetzwerke über die gängigen Schutzmaßnahmen wie professionelle Firewalls und Virenscanner und gewährleisten über interne Richtlinien auch die Nutzung sicherer Passwörter. Doch wie es um die IT-Sicherheit des heimischen Computers und des privaten WLAN-Netzwerks der Mitarbeiter bestellt ist, können die Unternehmen nicht kontrollieren.

So würden am heimischen Rechner oftmals weniger sichere Passwörter benutzt – und in Zeiten der ausschließlich virtuellen Zusammenarbeit mit den Kollegen seien die Menschen auch anfälliger für sogenannte Phishing-Attacken, warnt Claudia von Pawel, als Underwriting Manager Small Business verantwortlich für die Business Academy des Spezialversicherers Hiscox. So erschleichen sich Hacker beispielsweise mit Anrufen oder persönlichen Mails das Vertrauen der Menschen, um damit an deren Passwörter oder andere sensible Daten zu kommen. „Daher ist es wichtig, dass sich das Grundwissen darüber verbreitet, wie jeder Einzelne selbst für ein sicheres, digitales Arbeiten sorgen kann“, so von Pawel, denn sonst legt statt des Coronavirus ein Computervirus das Unternehmen lahm.

STARKE PASSWÖRTER SETZEN, PHISHING-ATTACKEN VORBEUGEN

„Viele, die von zu Hause aus arbeiten, meinen, allein durch den Zugang zum Firmennetzwerk per VPN sei ein rundum sicheres digitales Arbeiten möglich“, so von Pawel. Die Abkürzung VPN steht für „virtuelles privates Netzwerk“ und ermöglicht eine gesicherte Datenübertragung zwischen dem Firmenserver und dem Computer des Mitarbeiters. Ein VPN kann man sich wie einen Tunnel vorstellen, der die Informationen auf ihrem Weg vom Homeoffice-Mitarbeiter zum Server vor äußeren Angriffen schützt. Dabei wird ein kleines Netzwerk innerhalb des Internets geschaffen, zu dem nur Berechtigte Zugang haben. Um den Mitarbeitern im Homeoffice den VPN-Zugriff auf das Firmennetzwerk zu ermöglichen, muss auf dem Server des Unternehmens eine Hardware- oder

MICHAELA RASSAT,
Juristin, Ergo Rechtsschutz Leistungs-GmbH

ALEXANDER LEISTER,
Rechtsanwalt, CMS Deutschland

Softwarelösung etabliert werden, mit der der User Kontakt aufnimmt. Der Nutzer selbst benötigt, je nach Technologie, eine besondere Software, um sich einzuwählen. Aber eine sichere technische Infrastruktur allein genüge nicht, meint von Pawel. Vielmehr müsse jeder Einzelne auch bestimmte Verhaltensweisen beachten. Indem man konsequent starke Passwörter setzt und managt oder sich das Wissen aneignet, um selbst sehr professionell gemachte Phishing-Attacken oder telefonisch durchgeführte Hacking-Versuche zu vereiteln, kann jeder dazu beitragen, Cyberangriffe zu vereiteln und die ohnehin von den Auswirkungen der Corona-Krise gebeutelten Betriebe davor zu schützen, nun auch noch Opfer eines Hackerangriffs zu werden.

Unternehmen sind in der Pflicht, ihre Mitarbeiter bestmöglich vor den Gefahren in der digitalen Sphäre zu schützen – und das sollten sie schon aus Eigeninteresse tun: „Damit Unternehmen Schutz für ihre vertraulichen Informationen, wie Kundenlisten, Innovationsideen und Vertriebsstrategien, als Geschäftsgeheimnisse genießen, müssen sie sogenannte angemessene Geheimhaltungsmaßnahmen ergreifen“, sagt Alexander Leister, Rechtsanwalt bei der Wirtschaftskanzlei CMS Deutschland. „Ansonsten gelten die vertraulichen Informationen nicht als Geschäftsgeheimnisse. Dann bestünde kein Schutz gegenüber Datendieben und Betriebsspionen.“ Da bei der Arbeit das Risiko für die vertraulichen Informationen eines Unternehmens erhöht ist, „müssen Unternehmen ihren Mitarbeitern erhöhte Sorgfaltspflichten als angemessene Geheimhaltungsmaßnahmen auferlegen“, so Leister. „Dazu gehören zum Beispiel die Benutzung eines aktuellen Virenscanners, die sichere Verwahrung von Dokumenten und das Ausloggen beim Verlassen des Computers.“ Die erhöhten Sorgfaltspflichten sollten in einer eigenständigen Homeoffice-Vereinbarung konkret geregelt werden.

CLAUDIA VON PAWEL,
Underwriting Manager Small Business, Hiscox Deutschland

HAYE HÖSEL,
Geschäftsführer und Gründer, HUBIT Datenschutz GmbH & Co. KG

SECHS REGELN FÜR GUTE PASSWÖRTER

Ein gutes, sicheres Passwort zu finden, ist gar nicht so leicht. Die Verbraucherzentrale Baden-Württemberg hat sechs Regeln für gute Passwörter aufgestellt:

1. Ein Passwort sollte mindestens 10 Zeichen lang sein.
2. Es sollte aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z.B. § & ? * ! ?) bestehen und nicht in einem Wörterbuch zu finden sein oder mit dem Nutzer selbst oder der Familie im Zusammenhang stehen. Namen, Geburtsdaten, Telefonnummern oder Ähnliches sind also tabu.
3. Es sollte keine bloße Zahlenfolge (12345...), alphabethische Buchstabenfolge (abcdef...) oder eine Reihe benachbarter Tasten auf der Tastatur (qwertz...) darstellen.
4. Je sensibler ein Zugang ist (etwa beim Zugang zum Firmennetzwerk), umso mehr Sorgfalt sollte man bei der Auswahl eines starken Passworts walten lassen.
5. Nicht das gleiche Passwort für alle Portale nutzen, sondern mindestens für die wichtigsten und meist genutzten Dienste eigene Passwörter anlegen.
6. Wurde das Passwort von einem Anbieter übermittelt, sollte man es bei der ersten Anmeldung auf dem jeweiligen Portal ändern. Weitere Gründe zum Ändern des Codes wären, wenn der Online-Dienstleister einen dazu auffordert, große Datenlecks bekannt werden oder der Computer mit Schadsoftware infiziert worden ist.

DIE DS-GVO GILT AUCH IM HOMEOFFICE

Gerade in Sachen Datenschutz müssen Unternehmen und ihre Mitarbeiter bei der Arbeit im Homeoffice gut aufpassen, denn die Datenschutz-Grundverordnung (DS-GVO) gilt natürlich auch in Corona-Zeiten. Dies betreffe einerseits den Schutz persönlicher Daten von Kunden und Mitarbeitern, andererseits aber auch die Sicherheit von sensiblen Daten des Betriebs, betont Unternehmensjuristin Rassat. „Es muss sichergestellt sein, dass diese nicht nach außen dringen können." Hier sei neben technischen Lösungen vor allem die verstärkte Sensibilisierung der Mitarbeiter notwendig.
„Auch in der aktuellen Situation sollten Unternehmer ihre Mitarbeiter weiterhin für den Datenschutz sensibilisieren", betont auch Haye Hösel, Geschäftsführer und Gründer des Datenschutz- und IT-Sicherheitsspezialisten Hubit Datenschutz. „Was sich für viele Unternehmen bereits im Alltag als schwierig herausstellt, bedeutet in der aktuellen Situation eine noch größere Hürde." In jedem Fall müssten Unternehmer Regelungen treffen, wie Mitarbeiter im Homeoffice zu arbeiten haben. Diese sollten idealerweise in einer Richtlinie dokumentiert und direkt an die Mitarbeiter verschickt werden.
„Neben der Erfüllung der rechtlichen Anforderungen ist es für Unternehmen wichtig, bei ihren Mitarbeitern ein Bewusstsein für das erhöhte Risiko für vertrauliche Informationen bei der Homeoffice-Arbeit zu schaffen", bestätigt CMS-Anwalt Leister. „Dazu dienen beispielsweise praktische Leitfäden." Auf diese Weise könnten Risikolagen faktisch reduziert oder gar ausgeschlossen werden.
Für Unternehmen ist in Bezug auf den Datenschutz zunächst einmal relevant, ob ihre Mitarbeiter mit personenbezogenen Daten umgehen oder nicht", sagt Hösel. „Dies trifft jedoch auf nahezu jeden Arbeitsplatz zu, denn zu den personenbezogenen oder personenbeziehbaren Daten zählen nicht nur Namen, sondern beispielsweise auch Telefonnummern, E-Mail-Adressen, Kontodaten, Personalnummern oder IP-Adressen." Dementsprechend sollten Unternehmen auch in der aktuellen Ausnahmesituation ihre Mitarbeiter dazu anhalten, gewisse Maßnahmen zu befolgen. So gilt zunächst, dass das Arbeitszimmer abschließbar sein muss und Unterlagen in einem abschließbaren Schrank aufbewahrt werden müssen. „Auch Laptops, PCs sowie externe Datenträger wie zum Beispiel USB-Sticks gilt es zu verschlüsseln oder einzuschließen", so Hösel. Normalerweise sollen Arbeitnehmer im Homeoffice nicht ihre privaten Geräte nutzen. „In vielen Fällen möchten Arbeitgeber aus Sicherheitsgründen nicht, dass die Arbeit auf dem privaten Laptop erfolgt oder darauf wichtige Kunden- und Unternehmensdaten gespeichert werden", sagt Ergo-Juristin Rassat. Bei klassischen Telearbeitsplätzen übernehme daher normalerweise der Arbeitgeber die Ausstattung mit Dienstgeräten. „In Zeiten von Corona ist dies aber oft auf die Schnelle nicht möglich", so Rassat. In solchen Fällen seien genaue Absprachen und klare Vereinbarungen erforderlich, um Missverständnissen vorzubeugen.

Veranstalter:

diruj | Deutsches Institut für Rechtsabteilungen & Unternehmensjuristen

Zertifizierungslehrgänge

Forensische Interviewtechnik

Kurs im Oktober in Frankfurt:
01.-02.10.20

Digital Legal Counsel

Kurs im November in Düsseldorf:
05.-06. und 11.-13.11.20

- Unter Berücksichtigung aktueller Hygieneregelungen
- Fortbildungsveranstaltungen mit Nachweis nach § 15 FAO

Jetzt beitragsfrei Mitglied werden!

© shutterstock.com/LightField Studios

Forensische Interviewtechnik

Zur Aufklärung krimineller Taten oder Vermeidung schmerzhafter Unternehmenssanktionen professionalisieren Unternehmen ihre internen Untersuchungen.
Je korrekter die Informationen aus Aussagen sind, desto besser und schneller führen die Ermittlungen zum Ziel.

Der Lehrgang bietet eine relevante, praxisorientierte Interviewtechnik sowie wissenschaftliche Erkenntnisse.

© shutterstock.com/Pressmaster

Digital Legal Counsel

Der fünftägige Lehrgang besteht aus einem rechtlichen Teil, der sich mit der Digitalisierung entlang der Wertschöpfungskette befasst und einem technischen Teil, der neben Erläuterungen von Begriffen wie „Smart Contracts" und „Blockchain" auch eine Einführung in Informatik und Programmiersprachen enthält.

Eine Auswahl an Referenten:

Henning Stuke
Kriminologe und Jurist
Trainer für forensische Interviewtechnik

Kristin Benedikt
Bereichsleiterin Internet, Bayerisches Landesamt für Datenschutzaufsicht

Dr. Thomas Beyer
Fachanwalt für Gewerblichen Rechtsschutz, KPMG Law Rechtsanwaltsgesellschaft mbH

Dr. Malte Grützmacher
Partner,
CMS Hasche Sigle

Dr. Marc Hilber LL.M.
Partner,
Oppenhoff & Partner

Martin Kilgus
Rechtsanwalt,
CMS Hasche Sigle

Detlef Klett
Partner,
Taylor Wessing

Dr. Friedrich Popp
Senior Associate,
Debevoise & Plimpton LLP

Erik Reischl
Anwendungsentwickler für Handelssysteme

Jetzt anmelden: www.diruj.de/fortbildungen

ARBEITS- UND PAUSENZEITEN IM HOMEOFFICE: VERTRAUENSSACHE

Für die täglich zulässige Höchststundenzahl und die Pausen gelten bei der Arbeit im Homeoffice grundsätzlich die gleichen Regelungen aus dem Arbeitszeitgesetz wie im Büro. „Häufig gilt laut Arbeitsvertrag beim mobilen Arbeiten die Vertrauensarbeitszeit. Das heißt, der Arbeitnehmer muss die vertraglich vereinbarte Arbeitszeit leisten, ohne dass der Vorgesetzte dies kontrolliert", erklärt Michaela Rassat, Unternehmensjuristin bei der Ergo Rechtsschutz Leistungs-GmbH. „Dabei ist es ratsam, sich an vorab vereinbarte Zeiten zu halten, damit die Kollegen wissen, wann sie den Mitarbeiter erreichen können." Arbeitnehmer, die zusätzlich zur Arbeit ihre Kinder betreuen müssen, sollten dies gegenüber dem Arbeitgeber ansprechen und nach Möglichkeit die Arbeitszeiten entsprechend anpassen. Um auch wirklich störungsfrei arbeiten zu können, raten Experten zu familieninternen Stundenplänen, in denen Eltern mit ihren Kindern die Spiel- und Arbeitszeiten festlegen.

KOMMUNIKATION SOLLTE SICHER VERSCHLÜSSELT WERDEN

„Unter Berücksichtigung der aktuellen Umstände besteht die Möglichkeit, dass der Einsatz von Homeoffice gerechtfertigt ist, auch wenn ein DS-GVO-konformer Aktenvernichter fehlt oder der Familiendrucker genutzt wird", sagt Datenschutzexperte Hösel. „Für den Fall, dass ein privates Gerät zum Einsatz kommt, muss festgelegt werden, in welchem Umfang dies geschieht." Zudem muss sichergestellt sein, dass etwa das Betriebssystem und der Virenschutz auf dem aktuellsten Stand sind.

In jedem Fall sollte das elektronische Firmennetzwerk für Arbeitnehmer nur über ein sicheres Passwort zugänglich sein, ebenso wie die Kommunikation per E-Mail nur über den Server der Firma und damit verschlüsselt ablaufen darf. Neben der Nutzung von VPN-Verbindungen für den Zugang zum Firmennetzwerk betrifft das insbesondere auch die mobilen Geräte der Mitarbeiter: „Bei der Nutzung des Diensthandys sollten Mitarbeiter Messenger-Dienste wie WhatsApp, die laut DS-GVO als nicht datenschutzkonform gelten, meiden", rät Hösel. „Vielmehr sollten Unternehmen auf alternative Apps oder SMS setzen." Und wenn Videokonferenzen die herkömmlichen Meetings ersetzen, gilt es natürlich auch hier, für eine professionelle Verschlüsselung zu sorgen, damit keine vertraulichen Informationen nach außen dringen können. Regelmäßige Überprüfungen, Monitoring der Systeme und Aktualisierungen sind dabei elementar. Das Arbeiten in den eigenen vier Wänden ist aber neben den virtuellen auch mit ganz handfesten Risiken verbunden: „Beispielsweise wenn der Arbeitnehmer über ein Computerkabel stolpert oder ihm ein schwerer Ordner auf den Fuß fällt", sagt Ergo-Juristin Rassat. Bei solchen Arbeitsunfällen gilt grundsätzlich der Schutz der gesetzlichen Unfallversicherung, auch wenn diese während der Arbeit in den eigenen vier Wänden geschehen. Allerdings erstreckt sich der Schutz nur auf die Tätigkeiten, die im sachlichen Zusammenhang mit dem Beschäftigungsverhältnis stehen. Das bedeutet: „Unfälle am heimischen Schreibtisch, die anlässlich der Arbeitsverrichtung passieren, sind versichert", so Rassat. Das gelte auch für Dienstreisen oder Wege vom mobilen Arbeitsplatz zum Unternehmen, etwa um dringend benötigte Unterlagen abzuholen.

Verlässt der Mitarbeiter jedoch den heimischen Arbeitsplatz und betritt seinen privaten Bereich, etwa um sich einen Kaffee zu holen, erlischt der Versicherungsschutz und greift erst wieder beim erneuten Betreten des Arbeitsbereichs. „Bei einem Unfall auf dem Weg zur Toilette oder in die Küche besteht also kein gesetzlicher Unfallschutz, da diese Handlungen im Wesentlichen dem privaten Lebensbereich zuzuordnen sind", erklärt Rechtsexpertin Rassat. Grundsätzlich empfehlenswert für alle Heimarbeiter ist daher eine zusätzliche private Unfallversicherung. Denn nur dann ist man im Fall der Fälle vor kleinlichen Diskussionen gefeit, ob man sich noch im Arbeitsbereich oder vielleicht doch schon in der privaten Sphäre befunden hat. ■ *Harald Czycholl*

- Seit Beginn der Corona-Krise erlebt das Homeoffice einen Boom. Nie zuvor arbeiteten so viele Menschen gleichzeitig von zu Hause aus.
- Das bietet Cyberkriminellen Einfallstore, denn wie es um die IT-Sicherheit des heimischen PC-Arbeitsplatzes bestellt ist, können Unternehmen nicht kontrollieren.
- Wichtig ist eine gute technische Infrastruktur in Form eines VPN-Zugangs zum Firmennetzwerk und die Verwendung aktueller Sicherheitssoftware.
- Jeder Einzelne muss bestimmte Verhaltensweisen beachten: Wichtig ist die Verwendung sogenannter starker Passwörter und die Aneignung von Grundwissen zur Vermeidung von Phishing-Attacken.
- Die Kommunikation per E-Mail darf nur über den Server der Firma und damit verschlüsselt ablaufen.