KFV
Kuratorium für Verkehrssicherheit

KFV - Sicher Leben #23

Cybersicherheit als Chance

Cyberkriminalität und ihre Prävention bei kleinen und mittleren Unternehmen in Österreich

KFV (Kuratorium für Verkehrssicherheit)

KFV - Sicher Leben #23

Cybersicherheit als Chance

Cyberkriminalität und ihre Prävention bei kleinen und mittleren Unternehmen in Österreich

KFV - Sicher Leben. Band #23. Cybersicherheit als Chance. Wien, 2020

Medieninhaber und Herausgeber
KFV (Kuratorium für Verkehrssicherheit)

Autor
Dr. Georg Plattner

Mitarbeit
Mag.ª Monika Pilgerstorfer, Mag.ª Dagmar Lehner, Dr.in Claudia Riccabona-Zecha

Auftraggeber
Dr. Armin Kaltenegger

Gender-Hinweis
Zugunsten besserer Lesbarkeit findet entweder die männliche oder weibliche Form personenbezogener Begriffe Verwendung. Gemeint und angesprochen sind alle Geschlechter.

KFV
Kuratorium für Verkehrssicherheit

INHALTSVERZEICHNIS

1 EINLEITUNG 9

2 PROBLEMLAGE 13
2.1 Bedeutung der KMU für die österreichische Wirtschaft 13
2.2 Cyberkriminalität in Österreich 14
2.3 Cyberkriminalität als Bedrohung für Wirtschaftsunternehmen 15
2.4 Die besondere Anfälligkeit von KMU für Cyberkriminalität 16
2.5 Konformität mit Datenschutz als Herausforderung 16

3 METHODEN 23
3.1 Repräsentative Befragung kleiner und mittlerer Unternehmen 23
3.2 Qualitative Experteninterviews 24

4 ERGEBNISSE 29
4.1 Betroffenheit 29
4.2 Schaden 35
4.3 Risikoeinschätzung 38
4.4 Fokus: Informationspflicht bei Datendiebstahl - ein blinder Fleck? 40
4.5 Schutzmaßnahmen: Experten-Empfehlungen versus Unternehmensrealität 43

5 CONCLUSIO 51
5.1 Sicherheit als Chance sehen! 51
5.2 Präventionstipps 52
5.3 Politische Empfehlungen 54

6 TABELLENVERZEICHNIS 59

7 ABBILDUNGSVERZEICHNIS 63

8 LITERATURVERZEICHNIS 67

IMPRESSUM 70

1

1 EINLEITUNG 9

1 EINLEITUNG

Die Durchdringung aller Lebens- und Gesellschaftsbereiche durch digitale Innovationen und die globale Vernetzung durch das Internet führen seit Jahren auch zu einem rasanten Anstieg von Kriminalität im digitalen Raum. Auch in Österreich steigt die Zahl der Straftaten im Internet seit Jahren dramatisch an und stand im Jahr 2018 bei 19.627 Delikten, was eine Steigerung um beinahe 17 Prozent im Vergleich zum Vorjahr bedeutet (Bundeskriminalamt 2019, 42). Auch für Wirtschaftsunternehmen bedeutet dieses rasant wachsende Kriminalitätsfeld eine neue Herausforderung. Während sich große Unternehmen aufwendige Schutzmechanismen leisten können und ganze Abteilungen sich nur der Abschirmung der digitalen Infrastruktur widmen, ist dies für kleine und mittelständische Unternehmen (KMU)[1] oft aus praktischen und finanziellen Gründen nicht möglich. Dies wissen auch Kriminelle und machen sich diesen Umstand zunutze: Weltweit machen KMU fast 60 Prozent der von Cyberkriminalität betroffenen Unternehmen aus (Walker 2019).

Österreichs Wirtschaft ist stark durch KMU geprägt, über 99 Prozent der österreichischen Unternehmen werden als solche definiert (Bundesministerium für Digitalisierung und Wirtschaftsstandort 2019). Es ist daher davon auszugehen, dass diese Unternehmen auch vielfältige Erfahrungen mit Cyberkriminalität gemacht haben. Die hier vorliegende Studie hat es sich zum Ziel gesetzt, dieses Kriminalitätsfeld genauer zu durchleuchten. Es soll der momentane Gefährdungs- und Schadensstand untersucht werden, darüber hinaus sollen eine Einschätzung zukünftiger Trends sowie Tipps zur Vermeidung von Viktimisierung geboten werden. Das Kuratorium für Verkehrssicherheit ließ hierfür eine repräsentative Befragung von VertreterInnen kleiner und mittlerer Unternehmen in Österreich durch das Gallup Institut durchführen. Zusätzlich wurden vertiefende Interviews mit Experten im Bereich Cyberkriminalität und Wirtschaft geführt.

Die vorliegende Studie soll als Basis dienen, um den Zustand der Cybersicherheit bei KMU in Österreich darzustellen, Trends in puncto Schwächen und Stärken der Prozesse und Strukturen der Unternehmen aufzuzeigen sowie einen Überblick über Maßnahmen zur Prävention von Cyberangriffen zu bieten. Gleichzeitig soll sie auch für die Unternehmen selbst als Informationsquelle zur Optimierung der eigenen Cybersicherheit dienen.

Die zentrale Botschaft, die durch diese Studie transportiert werden soll, ist eine doppelte: Die handelnden Personen in Österreichs Unternehmen wissen mehrheitlich zu wenig über das Risiko von Cyberkriminalität, es besteht Verbesserungspotenzial in der Prävention. Gleichzeitig dient eine umfassende Cybersicherheits-Strategie auch bei kleinen und mittleren Unternehmen nicht nur dem eigenen Schutz, sondern ist ebenso Werbung nach außen: Ein sicheres Unternehmen ist ein gern gesehener Partner, und damit ist Cybersicherheit für Unternehmen eine große Chance, sich selbst als verlässlich und am Puls der Zeit auf dem Markt zu positionieren.

1 KMU werden in dieser Studie definiert als Unternehmen mit maximal 50 MitarbeiterInnen (kleine), sowie zwischen 50 und 250 MitarbeiterInnen (mittelständische). Diese Definition basiert auf Empfehlungen der EU-Kommission (Wirtschaftskammer Österreich 2019).

2

2 PROBLEMLAGE 13

2.1 Bedeutung der KMU für die österreichische Wirtschaft 13

2.2 Cyberkriminalität in Österreich 14

2.3 Cyberkriminalität als Bedrohung für Wirtschaftsunternehmen 15

2.4 Die besondere Anfälligkeit von KMU für Cyberkriminalität 16

2.5 Konformität mit Datenschutz als Herausforderung 16

2 PROBLEMLAGE

2.1 Bedeutung der KMU für die österreichische Wirtschaft

Österreichs Wirtschaft ist, wie die der anderen EU-Mitgliedsstaaten auch, von einem starken Übergewicht kleiner und mittlerer Unternehmen gekennzeichnet: „Die insgesamt rund 329.000 KMU der marktorientierten Wirtschaft stellen 99,6 Prozent der österreichischen Unternehmen. Sie beschäftigten im Erhebungsjahr 2016 rund zwei Millionen Menschen (68 Prozent der Arbeitsplätze) und erwirtschafteten 63 Prozent der Umsätze (455 Mrd. Euro) sowie 62 Prozent der Bruttowertschöpfung (123 Mrd. Euro)“ (Bundesministerium für Digitalisierung und Wirtschaftsstandort 2019). Die überwiegende Mehrzahl dieser Unternehmen (87 Prozent) hat weniger als zehn Beschäftigte. Kleine und mittlere Unternehmen spielen darüber hinaus auch eine wichtige Rolle in der Lehrlingsausbildung.
Die Mehrzahl der KMU ist in den Sparten Gewerbe und Handwerk, Handel sowie Information und Consulting tätig. Aufgeschlüsselt nach Umsatz ist der Handel die stärkste Sparte kleiner und mittlerer Unternehmen in Österreich (Wirtschaftskammer Österreich 2017, 36). In den Sparten Gewerbe und Handwerk, Information und Consulting sowie Handel beträgt der Anteil der Ein-Personen-Unternehmen (EPU) mehr als 50%. Die anteilig größte Zahl an Beschäftigten bei KMU findet sich in den Sektoren Bank und Versicherung sowie Industrie mit jeweils um die 40 Beschäftigten im Durchschnitt. Am geringsten ist diese Zahl bei Unternehmen, die im Informations- und Consulting-Bereich tätig sind (weniger als 5).

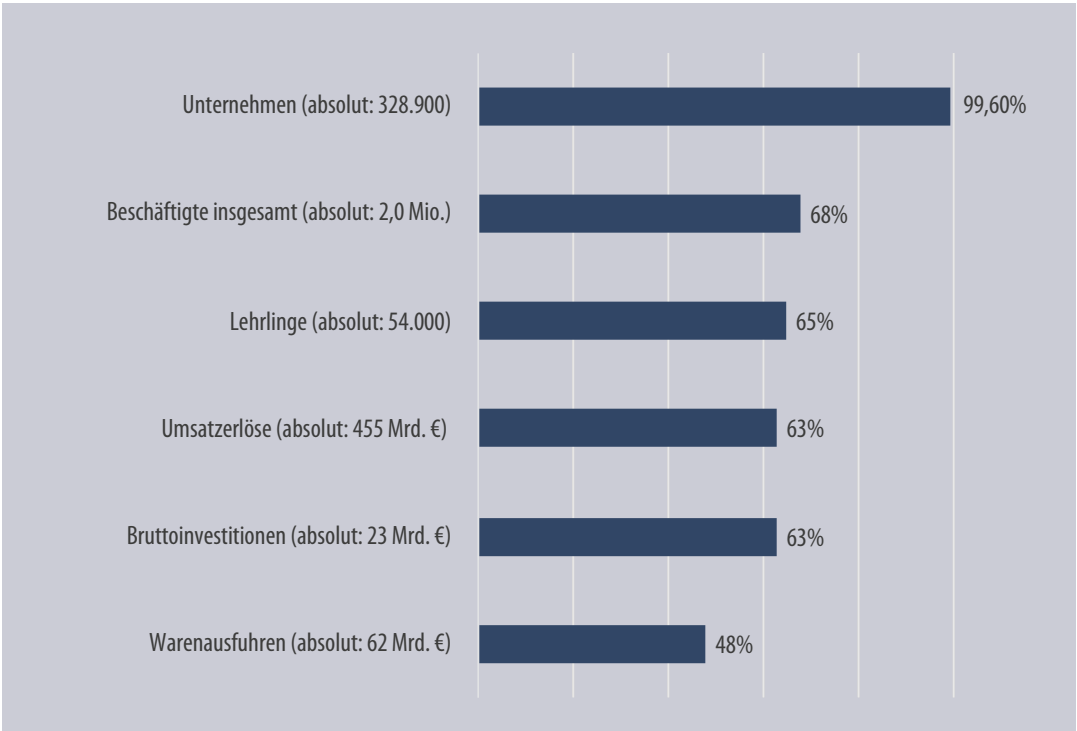

Abbildung 1: *Anteil der KMU an allen Unternehmen in Österreich.* *Quelle: BMDW 2019*

Anhand dieser Zahlen ist klar ersichtlich, welch hohen Wert KMU für den Wirtschaftsstandort Österreich besitzen und welch große Rolle sie auch gesamtgesellschaftlich spielen. Die KMU hatten außerdem großen Anteil an der sehr guten Krisenbewältigung der österreichischen Wirtschaft in den Jahren ab 2008 (Wirtschaftskammer Österreich 2017, 14).

Die Digitalisierung der heimischen KMU war bereits 2015 höher als im EU-Durchschnitt, jedoch weiterhin deutlich geringer als bei Großunternehmen (ebda., 18). Kleine und mittlere Unternehmen sind im digitalen Zeitalter angekommen und nutzen die Möglichkeiten, die sich dadurch bieten. Mit diesen Chancen einher gehen jedoch auch die Risiken, die in der digitalen Welt lauern. Damit ist es von besonderem Interesse, zu eruieren, inwiefern diese Unternehmen vom neuen und sich stetig weiter entwickelnden Phänomen der Cyberkriminalität betroffen sind. Darüber hinaus wird es im Zuge der fortschreitenden Digitalisierung auch immer wichtiger, den KMU unterstützende Werkzeuge in die Hand zu geben, die es ihnen ermöglichen, sicher durch die digitale Welt zu navigieren und sich angemessen vor Bedrohungen schützen zu können.

2.2 Cyberkriminalität in Österreich

Cyberkriminalität ist auch in Österreich ein in den letzten Jahren stark gewachsenes Kriminalitätsfeld. Die „Cyber Sicherheit Steuerungsgruppe“ der österreichischen Regierung stellte in ihrem aktuellen Bericht fest, dass Cybercrime-Delikte, „(…) im engeren Sinn (Straftaten, die an IT-Systemen oder Daten begangen werden, beispielsweise widerrechtlicher Zugriff auf ein Computersystem oder Datenbeschädigung) (…)“, im Vergleich zum Vorjahr rückläufig sind (Cyber Sicherheit Steuerungsgruppe 2019, 16). Dies betrifft die Zahlen für das Gesamtjahr 2019. Jedoch stiegen die Delikte „im engeren Sinn“ von 2017 auf 2018 um mehr als die Hälfte an (Cyber Sicherheit Steuerungsgruppe 2018, 15). Dies bedeutet, dass 2019 zum ersten Mal keine Steigerung im Bereich dieser Deliktform festgestellt werden konnte. Diese Zahlen fassen jedoch alle Arten von Cyberkriminalität zusammen, also sowohl im privaten als auch im wirtschaftlichen Bereich, und darüber hinaus auch nur jene, die der engen österreichischen Definition entsprechen:

Die österreichische Gesetzgebung unterscheidet nämlich in ihrer Klassifizierung zwischen Cybercrime „im engeren“ und „im weiteren“ Sinn. Ersteres bedeutet, wie im obigen Zitat bereits angedeutet, dass sowohl Tatinstrument als auch Angriffsziel IT-Systeme oder Daten sein müssen. Zur Bekämpfung dieser Art von Cyberkriminalität existiert im Bundeskriminalamt ein spezielles Kompetenzzentrum, das Cyber Crime Competence Center (C4), das als nationale und internationale Koordinierungs- und Meldestelle dient.

Cybercrime im weiteren Sinne bedeutet, dass ein Täter IT-Systeme zur Tatverwirklichung nutzt, das Ziel jedoch kein IT-System ist. Während unter erstere Definition klassisches Hacking oder auch DDoS-Attacken fallen, fällt unter die zweite Definition die klassische Erpressung (Ransomware) oder Betrug (Phishing), indem ein IT-System genutzt wird, um eine originär „klassische“ Straftat zu begehen.

Die zwei am häufigsten auftretenden Formen von Cyberkriminalität in Österreich sind Cyberverbrechen „im weiteren Sinne“. Zum einen ist dies Ransomware, also Schadsoftware, die in IT-Systeme geschleust wird und die darin befindlichen Daten verschlüsselt. Die Täter machen sich daraufhin bemerkbar und erpressen ihre Opfer, indem klar gemacht wird, dass die Daten nur gegen Lösegeldzahlungen wieder freigegeben werden.

Phishing, die zweite massiv steigende Deliktform, ist der Versuch, Geheimdaten abzuziehen. Klassischerweise geschieht dies über eine E-Mail, in der die Adressaten aufgefordert werden, ihre Daten

auf einer Homepage einzugeben. Dabei wird vorgetäuscht, eine seriöse Institution (bspw. eine Bank) zu sein. Die Seite, die in der E-Mail verlinkt wird, ist meistens täuschend echt nachgebaut und wirkt seriös. Werden die Daten eingegeben, erhalten die Betrüger Zugriff auf das Bankkonto, den Datenserver oder ähnliches.

Diese beiden Delikte stiegen auch im Jahr 2018 stark an. Da sie verhältnismäßig leicht und ohne besondere Vorkenntnisse gesetzt werden können und durch ihren Massencharakter eine sehr große Zahl an potenziellen Opfern in sehr kurzer Zeit erreichen können, bieten sich diese Delikte Kriminellen besonders an.

2.3 Cyberkriminalität als Bedrohung für Wirtschaftsunternehmen

Die Trendanalyse der Cyber Sicherheit Steuerungsgruppe der österreichischen Regierung beschreibt in ihrem Bericht über Cyberkriminalität in Österreich lediglich eine geringe Rücklaufquote der Delikte bei Unternehmen. Dies stützt sich auf eine Befragung von „führenden privaten Unternehmen aus der Cyber Security Branche".

Einen klaren Rückgang verzeichnet die Analyse im Bereich von klassischen DDoS-Attacken. Bei dieser Art von Angriff nutzen Kriminelle die Kapazitätsbeschränkungen aus, die es in jedem Netzwerk gibt, wie z.B. auf den Servern, auf denen die Website eines Unternehmens gehostet wird. Für einen DDoS-Angriff werden mehrere Anfragen an die angegriffene Webressource gesendet, um ihre Kapazität zur Verarbeitung von Anfragen zu überlasten und so die Verfügbarkeit der Seite zu stören.

Zugenommen haben hingegen die Tatbestände Ransomware und Datendiebstahl, Phishing ist laut dieser Analyse auf Vorjahresniveau geblieben (Cyber Sicherheit Steuerungsgruppe 2019, 13). Verringert hat sich jedoch die Erfolgsquote der Phishing-Angriffe, d.h., es blieb öfter nur beim Versuch als in früheren Jahren. Dies führt die Steuerungsgruppe auf eine größere Sensibilisierung der Nutzenden zurück. Unternehmen (wie auch Privatpersonen) bewegen sich immer vorsichtiger im digitalen Raum und bringen E-Mails und anderen Kontaktaufforderungen immer größeres Misstrauen entgegen.

CEO Fraud trat ebenfalls auf, teilweise im Zusammenhang mit vorherigen tatsächlichen Hacking-Angriffen. Beim CEO-Betrug geben sich Täter als Geschäftsführer (CEO) des Unternehmens aus und veranlassen einen Mitarbeiter zur Überweisung eines größeren Geldbetrages ins Ausland. Auch hier findet eine Verschiebung der Ziele hin zu kleinen und mittleren Unternehmen statt, da die größeren Unternehmen immer besser geschützt sind. Dies betrifft nicht bzw. kaum Ein-Personen-Unternehmen oder solche mit sehr wenigen Mitarbeitern, da hier der Personenkreis zu klein ist, um eine erfolgreiche Imitation der Geschäftsführung zuzulassen.

	Vorfallart		Motivation
−	DDos	−	Monetär
+	Ransomware	+	Politisch
=	Phishing	=	Persönlich
−	CEO-Fraud/Fake Invoice/SCAM	−	Staatlich
=	Targeted Attack/ATP	=	Technisches Gebrechen
+	Datendiebstahl		
=	Botnet/C2		
=	Defacements		

Tabelle 1: *Trends bei Vorfallarten und Motivationen von Cyberkriminalität bei Unternehmen (bearbeitet durch Cyber Security Unternehmen)*
Quelle: Cyber Sicherheit Steuerungsgruppe 2019

2.4 Die besondere Anfälligkeit von KMU für Cyberkriminalität

Aufgeschlüsselt nach Unternehmensgröße ist in der Trendanalyse der Steuerungsgruppe klar ersichtlich, dass Ransomware und Phishing vor allem bei KMU als Delikt auftreten. Auch verschiedene Berichte weiterer Quellen betonen die besondere Anfälligkeit kleiner und mittlerer Unternehmen für Cyberkriminalität (Fearn 2019, Prosser 2019). Weltweit sind 58% der Unternehmen, die Opfer von Cyberattacken werden, kleine Unternehmen (Walker 2019).

Österreichische KMU nutzen im EU-Vergleich überdurchschnittlich häufig digitale Informations- und Kommunikationstechnologien. Beinahe jedes Unternehmen mit mindestens zehn Beschäftigten verfügt über einen Internetzugang, und 88 Prozent aller österreichischen KMU hatten bereits 2016 eine eigene Homepage (77% im EU-Durchschnitt). Fast 50 Prozent nutzten 2016 soziale Medien, mindestens 40 Prozent nutzen entweder Warenwirtschafts- bzw. Projektmanagement-Tools oder Software-Lösungen zur Kundenpflege (Wirtschaftskammer Österreich 2019, 8). Dies führt dazu, dass KMU in Österreich im digitalen Raum sehr präsent sind und somit für Täter ein attraktives Ziel abgeben.

Als Gründe für die besondere Anfälligkeit kleiner und mittlerer Betriebe werden vor allem mangelnde Ressourcen für Schutzmaßnahmen und fehlende Lösungskompetenz angeführt (Fearn 2019). Während größere Unternehmen in den vergangenen Jahren ihre Sicherheitsvorkehrungen sukzessive verbessert haben und auch bedeutende Ressourcen in die Cybersicherheit stecken, wird dieses Thema von kleinen und mittleren Unternehmen oft noch immer stiefmütterlich behandelt. Viele KMU unterschätzen laut bisher durchgeführter Studien aber auch schlicht und ergreifend das Risiko, dem sie ausgesetzt sind. Eine in Deutschland durchgeführte Studie zeigt, dass viele Unternehmen scheinbar davon ausgehen, dass das Risiko zwar allgemein sehr hoch ist, dies jedoch nicht für sie gilt (Sauermann 2019). Dies wissen auch Kriminelle und machen sich diesen Umstand zunutze.

Die Unterschätzung der Gefahren und die geringeren Ressourcen, um eine effektive Prävention für das eigene Unternehmen aufzubauen, führen dazu, dass die Gefahr, die für KMU von Cyberkriminellen ausgeht, weiter steigen wird.

Auch der Schaden, den diese Unternehmen erleiden, ist signifikant. Im Vereinigten Königreich ergab eine Studie, dass jede Attacke auf Unternehmen (10-49 MitarbeiterInnen) durchschnittlich Kosten von 65.000 £ nach sich zieht. Aufgerechnet würde das bedeuten, dass 80 Prozent sämtlicher durch Cyberkriminalität entstandener Schäden von dieser Unternehmenskategorie getragen werden (Prosser 2019).

All jene hier in aller Kürze präsentierten Gründe sprechen dafür, sich auch in Österreich intensiver mit der spezifischen Bedrohungslage für KMU durch Cyberkriminalität auseinanderzusetzen. Das KFV (Kuratorium für Verkehrssicherheit) bietet mit dieser Studie nun einen repräsentativen Überblick über den Status quo der Problematik und liefert wichtige Informationen für Unternehmen, Stakeholder und politische Entscheidungsträger. Darüber hinaus soll diese Studie aber auch eine Verbesserung der Prävention in den Unternehmen selbst ermöglichen.

2.5 Konformität mit Datenschutz als Herausforderung

Die immer zentralere Rolle, die Daten und digitale Kommunikationswege in Gesellschaft und Wirtschaft einnehmen, stellt auch den Gesetzgeber vor große Herausforderungen. Um Sicherheit im digitalen Raum zu gewährleisten, hat die EU eine Vielzahl von Rechtsakten erlassen, die sich mit verschiedenen Aspekten der Cybersicherheit befassen.

Die größten Herausforderungen für KMU in der Umsetzung dieser Regelungen stellt die Datenschutz-Grundverordnung (DSGVO) zum Schutz personenbezogener Daten samt den entsprechenden nationalen Gesetzen dar.[2] Die DSGVO soll diesen Schutz sicherstellen, einheitliche Regeln für die Datenverarbeitung innerhalb der EU schaffen und einen starken und einheitlichen Vollzug sicherstellen. Gleichzeitig soll sie auch den freien Datenverkehr innerhalb der EU im Sinne des Europäischen Binnenmarktes sicherstellen. Sie war unmittelbar anwendbar und bedurfte somit grundsätzlich keines weiteren innerstaatlichen Umsetzungsaktes, es sei denn, um bestehende Gesetze mit der Verordnung in Einklang zu bringen.

Die DSGVO setzte die Mitgliedsstaaten der EU und die Unternehmen unter großen Anpassungs- und Umsetzungsdruck. So ergab eine EU-weite Studie ein Jahr nach Inkrafttreten der DSGVO, dass fast ein Drittel der europäischen Unternehmen die Datenschutz-Grundverordnung noch nicht umgesetzt haben. Viele Unternehmen gaben als Begründung hierfür an, nicht zu verstehen, wann sie welche Schritte zu setzen haben (Schmitz 2019). In Österreich zeigte eine Studie ein Jahr nach Einführung der DSGVO, dass diese bei sehr vielen KMU ins unternehmerische Bewusstsein gerückt ist: „2017 hatten nur 32 Prozent angegeben, von der DSGVO betroffen zu sein, dieser Wert ist 2018 auf 83 Prozent angestiegen (…)“ (APA OTS 2018). Gleichzeitig stellt allerdings deren Umsetzung die größte Herausforderung für die befragten KMU dar. Auch herrschte bei den befragten Unternehmen große Unsicherheit in Bezug auf die Grundverordnung, 43 Prozent brauchten laut eigener Aussage diesbezüglich Beratung. In einer weiteren Studie wurde festgestellt, dass die verschiedenen Maßnahmen ein Jahr nach der Einführung nur von maximal etwas mehr als 50 Prozent der Unternehmen gesetzt oder angepasst wurden. 10 Prozent der befragten Unternehmen hatten Mitte 2019 noch immer keinerlei Maßnahmen getroffen, um die DSGVO umzusetzen (APA OTS 2019).

Mit dem Inkrafttreten der DSGVO kam für die Unternehmen eine Vielzahl neuer Aufgaben im Bereich Datenschutz und Datensicherheit. Harald Wenisch (IT Security Experts Group der WKO) sieht hier bei UnternehmerInnen eine gewisse Überforderung, die durch die Vielzahl neuer Verordnungen, auch im nicht-digitalen Bereich, ausgelöst wird. Das Problem sei, dass Informationen über die Gründe und positiven Aspekte dieser Gesetzgebungen oft nur unzureichend für UnternehmerInnen aufbereitet würden. So sehen diese meist nur mehr Auflagen, die den Alltag zunehmend komplexer machen, nicht jedoch die positive Grundintention dieser Gesetze.

Im Folgenden soll in aller Kompaktheit gezeigt werden, welchen grundlegenden Fragen sich Unternehmen stellen müssen, um DSGVO-konform zu agieren. Das Kapitel 4.4 zeigt dann auch anhand der erhobenen Daten einen besonderen Aspekt der DSGVO, der direkten Bezug auf das Thema Cyberkriminalität nimmt, nämlich die Meldepflicht des Diebstahls personenbezogener Daten. Darüber hinaus bestehen folgende zentralen Pflichten für Unternehmen laut DSGVO:

- Zunächst benötigen Unternehmen grundsätzlich eine Rechtsgrundlage für die bestehenden Datenverarbeitungen. Darüber hinaus muss sichergestellt sein, dass nur tatsächlich benötigte Daten gespeichert werden, der Zweck der Datenverarbeitung ist klar zu formulieren.
- Außerdem ist sicherzustellen, dass alle Daten, die unter die DSGVO fallen, regelmäßig gelöscht werden, und zwar nach Erreichen des Zwecks, zu dem die Daten erhoben wurden, oder aber nach Ablauf gesetzlicher Fristen.
- Darüber hinaus müssen Unternehmen auch sicherstellen, dass die Sicherheit personenbezogener Daten gewährleistet ist. Hierzu müssen Unternehmen adäquate Schadensmanagement-Prozesse ent-

2 http://data.europa.eu/eli/reg/2016/679/oj.

wickeln, insbesondere Zutrittskontrolle, Schutz vor unbefugter Systembenutzung, Weitergabekontrolle, Verschlüsselung von Datenträgern, Back-up-Strategie, Stromversorgung, Virenschutz, Firewall, Notfallpläne, Mitarbeitersensibilisierung und -schulung, …

- Datenschutz durch Technikgestaltung (Privacy by Design)
- Umsetzung technisch-organisatorischer Maßnahmen
- Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)
- datenschutzfreundliche Werkeinstellungen

Tipps für solche Schadensmanagement-Prozesse und Präventionsstrategien werden im Kapitel 5.2 dargestellt.

- Unternehmen müssen außerdem jederzeit nachweisen können, dass alle Datenverarbeitungen DSGVO-konform stattfinden. Dies betrifft z.B. die Dokumentation von Einwilligungserklärungen der Betroffenen, die Dokumentation von Sicherheitsmaßnahmen oder von Vereinbarungen mit Dienstleistern.
- Ein weiterer zentraler Punkt des Datenmanagement im Sinne der DSGVO ist die Informationspflicht gegenüber der Datenschutzbehörde. Hierunter fällt die umgehende Information bei Datenpannen (siehe Kapitel 4.4).
- Außerdem muss ein Verarbeitungsverzeichnis geführt werden, in dem laufend sämtliche Datenanwendungen im Unternehmen erfasst werden. Darüber hinaus muss die Erhebung besonderer Datenarten spezifisch ausgewiesen werden (Folgenabschätzung).
- Diese Vorkehrungen helfen, den Auskunftsrechten betroffener Personen gerecht werden zu können. Sollte eine Datenauskunft verlangt werden, hat diese innerhalb eines Monats zu erfolgen, inklusive der Überlieferung einer Kopie der verwendeten Daten.

3

3 METHODEN 23

3.1 Repräsentative Befragung kleiner und mittlerer Unternehmen 23

3.2 Qualitative Experteninterviews 24

3 METHODEN

3.1 Repräsentative Befragung kleiner und mittlerer Unternehmen

Als grundlegendes Datenmaterial wurde eine repräsentative Befragung von 500 kleinen und mittleren Unternehmen in Österreich beauftragt. Diese Befragung fand bereits zum zweiten Mal statt, was einen Vergleich mit dem Vorjahr (2018) ermöglichte. Sie wurde im September und Oktober 2019 durch das österreichische Gallup Institut durchgeführt.

Als Methode wurde das computerassistierte Telefoninterview gewählt. Der Fragebogen wurde bereits 2018 im Kuratorium für Verkehrssicherheit in Abstimmung mit dem Gallup Institut entwickelt und 2019 leicht adaptiert wiederverwendet. Das führt zu einer hohen Vergleichbarkeit auf Grund der gleichbleibenden Fragebogenstruktur.

Der Fragebogen bestand aus insgesamt 18 Fragen, die zum Ziel hatten, das Ausmaß von Cyberkriminalität betreffend österreichische KMU zu eruieren, die häufigsten Sicherheitsrisiken und Risikovermeidungsstrategien zu thematisieren sowie den Stand der Prävention in den Unternehmen selbst darzustellen.

Bei der Struktur der befragten KMU wurde darauf geachtet, eine 50:50-Aufteilung zwischen Unternehmen mit mehr als 50 MitarbeiterInnen und jenen mit weniger zu erreichen. Die weiteren Faktoren wurden nicht bereits in der Struktur vorgegeben und ergaben sich somit organisch. In Tabelle 2 ist die Struktur im Überblick dargestellt.

	Basis	In Prozent
Total	**500**	**100**
Funktion des/der Befragten		
IT	221	44
GF/InhaberIn	183	37
Andere	96	19
MitarbeiterInnen		
Keine/EPU	65	13
1-9	81	16
10-49	103	21
50+	251	50
Umsatz		
Bis 1 Mio. Euro	123	25
Bis 5 Mio. Euro	54	11
Bis 20 Mio. Euro	45	9
Über 20 Mio. Euro	40	8
K.A.	238	48

Tabelle 2: *Struktur der befragten KMU* *Quelle: Gallup Institut 2019*

Branche		
Land- und Forstwirtschaft	8	2
Industrie/Produzierendes Gewerbe	135	27
Baugewerbe	68	14
Verkehr, Energie	32	6
Handel	144	29
Tourismus/Beherbergung/Gastronomie	37	7
Finanzdienstleistungen	5	1
Andere Dienstleistungen	71	14
Bundesland		
Wien	80	16
Niederösterreich, Burgenland	105	21
Steiermark, Kärnten	94	19
Oberösterreich, Salzburg	150	30
Tirol, Vorarlberg	71	14

Tabelle 2: *Struktur der befragten KMU* *Quelle: Gallup Institut 2019*

3.2 Qualitative Experteninterviews

Zusätzlich zu der repräsentativen Befragung von 500 KMU in Österreich wurden vier Tiefeninterviews mit Experten im Bereich Cybersecurity und Cyberkriminalität geführt. Die Gespräche fanden im Zeitraum September bis November 2019 statt. Als Methode wurde ein teilstrukturiertes Leitfadeninterview gewählt, um einen gemeinsamen Grundrahmen an Fragen festzulegen und gleichzeitig genug Spielraum für individuelle Themen zu lassen.

Der Zweck dieser Interviews war, die dokumentierte Selbstwahrnehmung der Unternehmen um eine vertiefende externe Sichtweise zu erweitern, um so ein möglichst umfassendes Lagebild zu schaffen. Die auf diese Weise gewonnenen Zusatzinformationen ergänzen daher die repräsentative Befragung um qualitatives Expertenwissen zum Thema. Durch die Kombination quantitativer und qualitativer Daten entsteht ein vielschichtiges und aussagekräftiges Gesamtbild der aktuellen Situation in Österreich.

Zwei der Befragten sind als Experten für Cybersicherheit bei Wirtschaftsverbänden tätig, ein Interviewpartner ist im Bundeskriminalamt im Bereich Cyberkriminalität tätig, und ein Befragter ist Geschäftsführer einer Cybersecurity-Firma. Mit dieser Kombination aus Dienstleistern, Interessenvertretern und Exekutive kann wiederum eine umfassende Menge an allgemeinen Informationen zum Themenkomplex Cyberkriminalität und im Besonderen betreffend kleine und mittlere Unternehmen und deren Erfahrungen mit diesem Thema erarbeitet werden.

Interviewpartner	Position
Michael Mörz	Cybercrime Competence Center (C⁴), Bundeskriminalamt
Harald Wenisch	Sprecher IT Security Experts Group der Wirtschaftskammer Österreich
Roland Sommer	Geschäftsführer, Plattform Industrie 4.0
Thomas Hoffmann	Geschäftsführer, Radar Cyber Security

Tabelle 3: *Liste Experteninterviews*

4

4 ERGEBNISSE 29

4.1 Betroffenheit 29

4.2 Schaden 35

4.3 Risikoeinschätzung 38

4.4 Fokus: Informationspflicht bei Datendiebstahl - ein blinder Fleck? 40

4.5 Schutzmaßnahmen: Experten-Empfehlungen versus Unternehmensrealität 43

4 ERGEBNISSE

4.1 Betroffenheit

Nahezu alle befragten Unternehmen benutzen Endgeräte zur digitalen Kommunikation. Im Vergleich zur Umfrage im Jahr 2018 gibt es jedoch leichte Rückgänge bei der Nutzung von Desktop-PCs (von 95 auf 93%), Laptops und Netbooks (von 86 auf 83%) sowie Tablets (von 59 auf 55%). Leicht erhöht hat sich lediglich die Nutzung von Smartphones (von 88 auf 89%).

Die befragten Unternehmen sind sich im Allgemeinen der Gefahren und verschiedenen Formen von Cyberkriminalität sehr bewusst (siehe Abbildung 2).

Im Detail betrachtet zeigt sich, dass Ein-Personen-Unternehmen allgemein ein geringeres Wissen über die verschiedenen Deliktformen aufweisen als die größeren KMU. Dies ist vor allem dadurch zu erklären, dass hier keine Personalreserve für die Auseinandersetzung mit diesen neuen Deliktformen besteht. Die Geschäftsführerin weiß möglicherweise allgemein über die Risiken im Internet Bescheid, wird sich aber kaum mit den spezifischen Risiken, die ihr in ihrer Rolle als Unternehmerin drohen, auseinandersetzen. Dies führt in weiterer Folge auch zu einer größeren Gefährdung, da sie auch weniger vorsichtig sind, was ihren Auftritt im digitalen Raum angeht. Darüber hinaus verwenden sie oft ihre private IT-Infrastruktur auch für das Geschäft, diese verfügt dann meistens auch lediglich über private Schutzmaßnahmen, die weniger umfangreich sind als jene, die für Unternehmen angeboten werden.

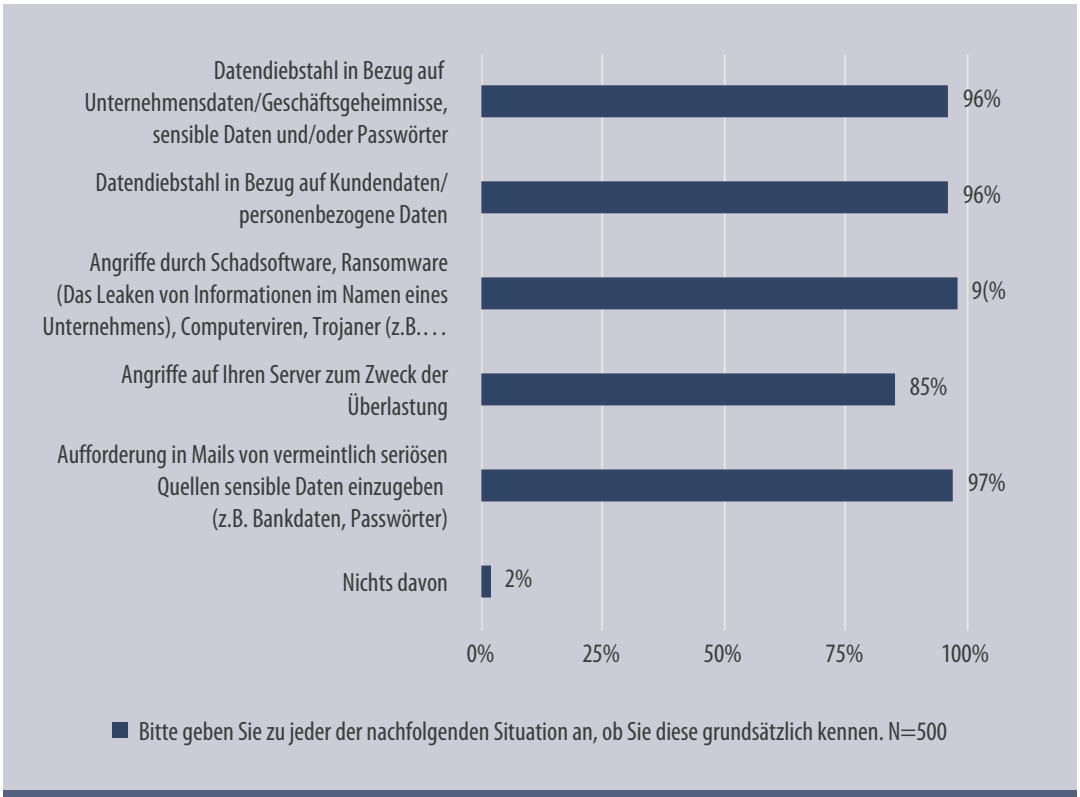

Abbildung 2: *Bekanntheit von Formen der Internetkriminalität* *Quelle: Gallup Institut 2019*

In der quantitativen Befragung wurde unterschieden zwischen versuchten und eingetretenen Fällen von Cyberkriminalität, da diese Unterscheidung für die Einschätzung der generellen Gefahrenlage durchaus von Interesse ist. Ein Versuch zeigt zum einen, dass Kriminelle nach wie vor großen Tatendrang an den Tag legen, eine niedrige oder hohe Quote an erfolgreichen Fällen zeigt andererseits, wie gut Unternehmen für die Gefahren sensibilisiert sind, wie gut sie geschützt sind und kann damit auch erste Rückschlüsse auf den allgemeinen Kenntnisstand von Unternehmen in Bezug auf ihre Cybersicherheit geben.

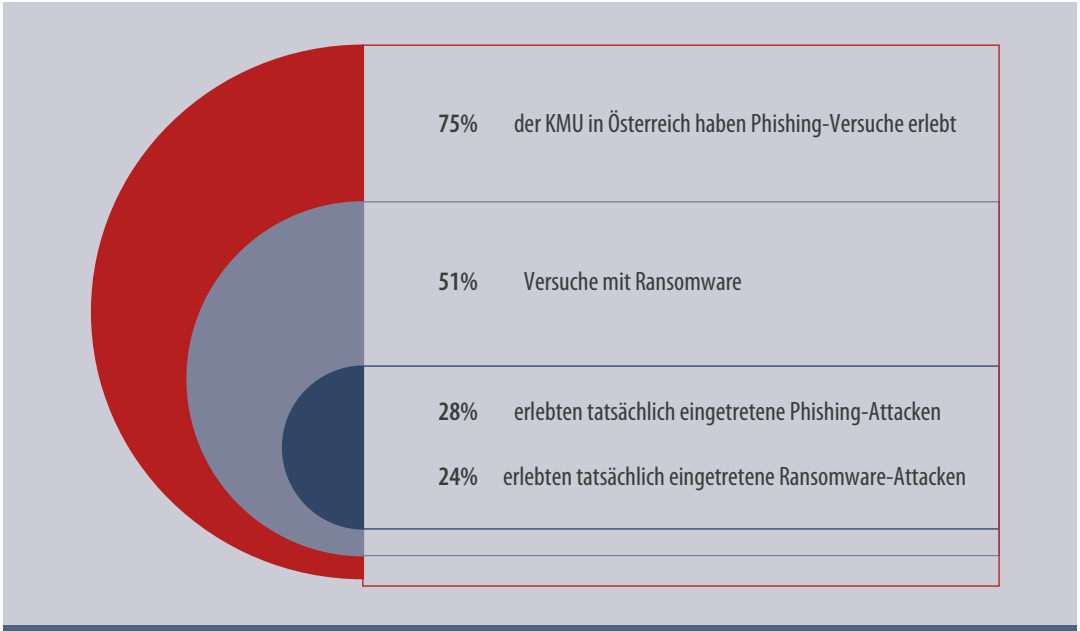

Abbildung 3: *Überblick versuchte und eingetretene Attacken* *Quelle: Gallup Institut 2019*

Versuchte Cyberattacken hat die überwältigende Mehrzahl der befragten KMU bereits erlebt. Die zwei am häufigsten versuchten Formen von Internetkriminalität bei KMU in Österreich sind Phishing und Schadsoftware (Ransomware, Viren, Trojaner) (siehe Abbildung 4). Über drei Viertel der befragten KMU haben bereits Phishing-Versuche in ihrem Unternehmen erlebt, und mehr als die Hälfte sah sich bereits mit Schadsoftware konfrontiert. Im Vergleich zum Vorjahr kam es bei allen Versuchen zu einem Rückgang. Diese konkreten Ergebnisse decken sich mit den allgemeinen Einschätzungen der befragten Experten sowie mit den allgemeinen Zahlen der Steuerungsgruppe (siehe Kapitel 2.3). Darüber hinaus berichtet Thomas Hoffmann (Radar Cyber Security) auch von häufig in seinem Arbeitsalltag auftretenden Fällen mit Versuchen, über Telefonanrufe Zugriff auf die Daten zu erhalten und anschließend erpresserisch tätig zu werden. Beispielhaft erwähnt wird der im Frühjahr 2019 häufig aufgetretene Fall der „Microsoft-Hotline".[3]

3 Bei dieser Betrugsmasche rufen Betrüger an und geben sich als Mitarbeiter von Microsoft aus. Unter dem Vorwand, dass sich Schadsoftware auf dem Computer der Opfer befinde, wird versucht, ein angebliches Tool zum Entfernen der Software durch die Nutzer selbst zu installieren. Diese Software erlaubt anschließend den vollen Zugriff auf alle Daten auf diesem Rechner. Anschließend werden die Betrüger erpresserisch tätig und fordern Barzahlungen von bis zu 250 Euro (Wegen 2019).

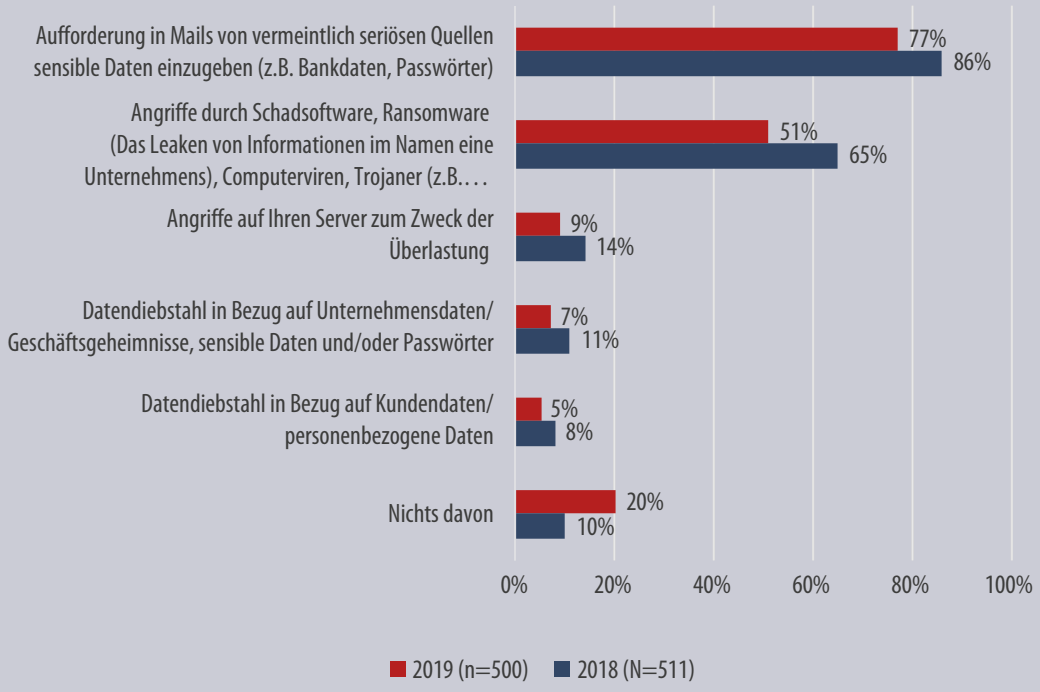

Abbildung 4: *Versuchte Formen von Cyberkriminalität: Vergleich 2018-2019* *Quelle: Gallup Institut 2019*

Im Hinblick auf die tatsächlich eingetretenen Fälle von Cyberkriminalität dominieren ebenfalls Phishing und Schadsoftware, mit jeweils ungefähr 25% „Erfolgsquote". Erfolgsquote bedeutet hier, dass die Befragten angegeben haben, dass diese Tatform bereits in ihrem Unternehmen (zu irgendeinem Zeitpunkt) eingetreten ist. Hier gab es im Vergleich zu den Ergebnissen des Vorjahres bedauerlicherweise auch keine Entspannung. Die eingetretenen Fälle von Phishing verdoppelten sich sogar, während die eingetretenen Schadsoftware-Fälle auf gleichem Niveau blieben (siehe Abbildung 5). Diese Ergebnisse korrespondieren durchaus auch mit den Trends, die durch das Bundeskriminalamt und andere Cyberabwehr-Stellen in Österreich beschrieben werden. Der Hauptgrund für die Eskalation der Phishing-Vorfälle ist sicherlich in der für TäterInnen sehr positiven Kosten-Nutzen-Rechnung zu finden. Da es wenig Aufwand bedeutet, diese Betrugsmasche massenweise zu probieren, wird zwangsläufig die Zahl der Betrogenen weiter steigen, solange die Zahl der Versuche steigt und keine absolut zuverlässige Prävention existiert. Die negative Entwicklung, speziell bei Phishing, kann außerdem Hinweis auf eine Weiterentwicklung der Täuschungsmanöver der Kriminellen sein, könnte aber auch für einen laschen Umgang der Unternehmen mit der eigenen Sicherheit sprechen. Eine Einschätzung, die auch von den befragten Experten attestiert wird (siehe dazu detaillierter Kapitel 4.3). Halbiert haben sich jedoch die Fälle der Angriffe zur Serverüberlastung (DDoS-Attacken), was auch dem von der Polizei festgestellten Trend entspricht. Auch Datendiebstahl bewegt sich auf einem sehr geringen Niveau. Zusammengefasst lässt sich sagen, dass fast zwei Fünftel der österreichischen KMU bereits irgendeine Form von Cyberkriminalität im eigenen Unternehmen erfahren haben. Dies spricht dafür, dass hier noch viel Verbesserungspotenzial im Bereich Prävention und Vorsorge ungenutzt bleibt.

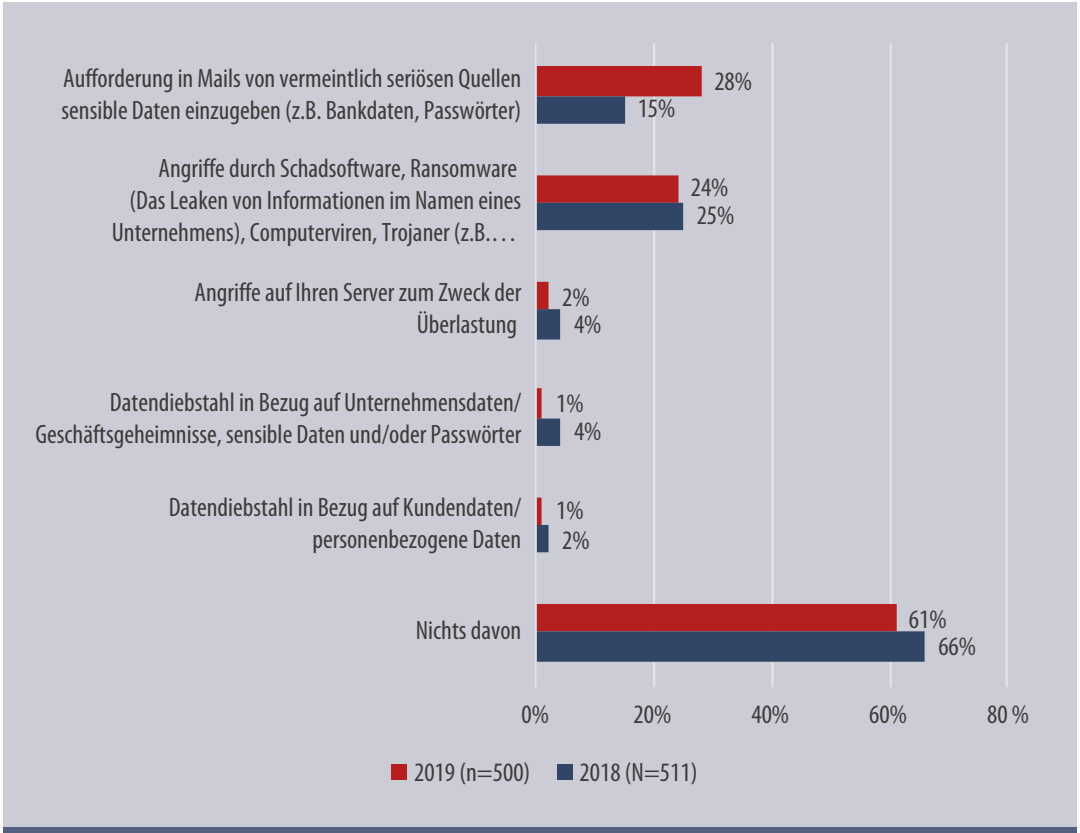

Abbildung 5: *Eingetretene Formen von Cyberkriminalität: Vergleich 2018-2019* *Quelle: Gallup Institut 2019*

Zusammenfassend kann gesagt werden, dass die Hauptgefahren für kleine und mittlere Unternehmen in Österreich im Bereich Cyberkriminalität durch Ransomware und Phishing entstehen. Dies entspricht auch den internationalen Trends, die vor allem im Bereich Phishing eine weitere Professionalisierung der TäterInnen zeigen (die enormen Fortschritte bei Deepfakes[4] sowie die vermehrte Nutzung von künstlicher Intelligenz zur Erstellung von Phishing-E-Mails sprechen hier eine deutliche Sprache).

Ransomware ist auch deswegen bei KMU so verbreitet, da die TäterInnen oft nicht auf große Geldsummen aus sind – laut Thomas Hoffmann beginnen die Forderungen meist bei etwa 100 Euro, einer Summe, die auch für kleine Unternehmen bezahlbar scheint, und daher höhere Erfolgsaussichten genießt als eine Summe, die als unverhältnismäßig hoch wahrgenommen wird. Hier ist dann auch das Risiko geringer, dass das Opfer zur Polizei geht und einen langwierigen Prozess in Gang setzt. Stattdessen, so die Spekulation der TäterInnen, bezahlt man lieber eine verhältnismäßig geringe Summe und bekommt anschließend den Zugriff auf die eigenen Daten wieder zurück.

Eher selten erleiden KMU in Österreich Datendiebstähle. Dies kann zum einen tatsächlich mit dem höheren Aufwand eines erfolgreichen Hacks zu tun haben. Dies würde bedeuten, dass TäterInnen sich lukrativere Ziele suchen, um einen relativ aufwendigen Datenhack durchzuführen. Andererseits, und dies wurde auch in den Expertengesprächen immer wieder Thema, sprechen viele Unternehmen – gerade KMU – auch ungern darüber, dass ihnen Daten gestohlen wurden. Dies geht mit massivem Imageverlust einher, und gerade für KMU, die oft ein kleiner Teil in einer langen und komplexen Produktionskette sind, ist der Malus des Gehackt-worden-Seins potenziell geschäftsgefährdend. Es

4 Deepfakes sind mit Hilfe von künstlicher Intelligenz (AI) manipulierte Video- oder Audioaufnahmen. Die AI erschafft mittels eines Arrangements aus lernfähigen und zur intelligenten Entscheidungsfindung fähigen Algorithmen eine täuschend echte Fälschung von Gesichtern oder Stimmen (Shao 2019).

könnte daher durchaus sein, dass die Unternehmen diese Vorfälle auch in der Umfrage unter den Tisch fallen ließen.

Auch die Häufigkeit des Vorkommens der verschiedenen Deliktformen ist kompatibel mit dem Wissen, das wir zu den einzelnen Formen haben (siehe Abbildung 6). Phishing-Versuche finden in massiv höherer Frequenz statt als alle anderen Formen von Cyberkriminalität, nur in den allerwenigsten Fällen wurde lediglich ein einzelner Versuch registriert. Auch die Versuche, Ransomware einzuschleusen, finden in häufiger Frequenz statt, jedoch insgesamt weniger häufig als im Jahr 2018. Im Gegensatz dazu sind die aufwendigeren Angriffsformen weit weniger häufig versucht worden. Nichtsdestotrotz erlebte fast jedes fünfte KMU öfter als viermal Versuche des Datendiebstahls.

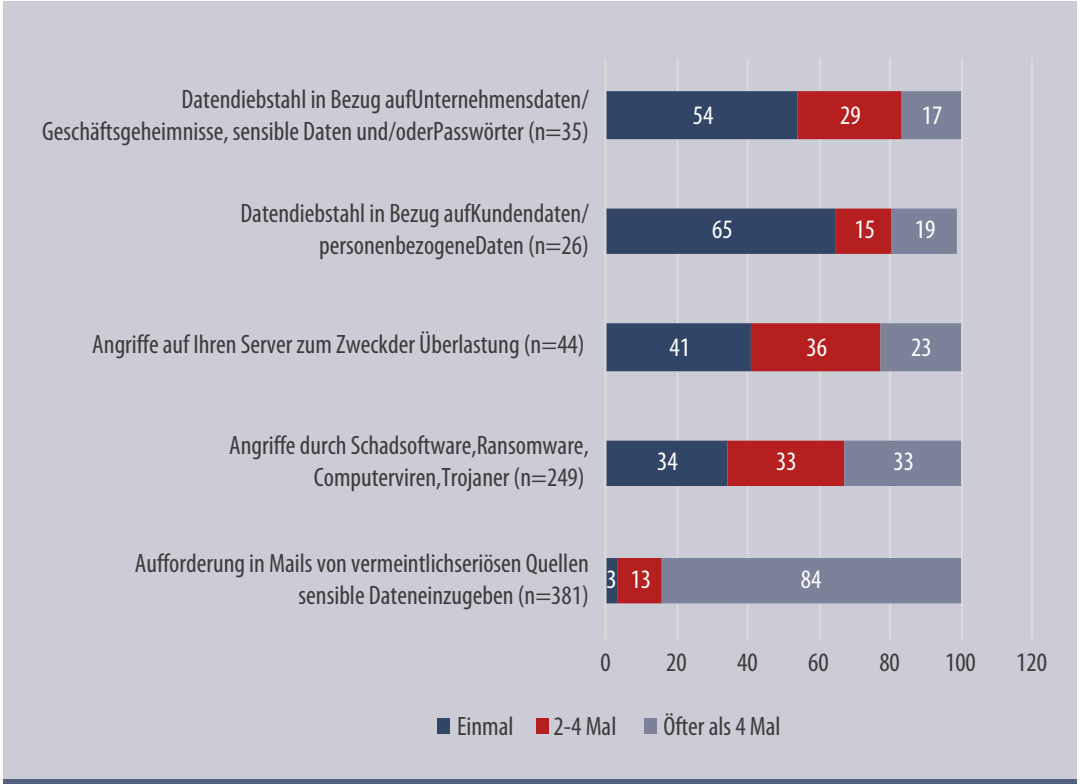

Abbildung 6: *Häufigkeit von Cyberangriffen* *Quelle: Gallup Institut 2019*

Betrachtet man außerdem den jeweiligen Zeitpunkt, zu dem die Angriffsversuche zuletzt durchgeführt wurden, ergibt sich ebenfalls ein Bild, das mit dem aus anderen Studien übereinstimmt (siehe Abbildung 7). Fast alle Unternehmen erlebten in den letzten sechs Monaten vor der Befragung Phishing-Versuche, und immerhin noch knapp über die Hälfte erlebte Versuche, Schadsoftware in ihre Systeme einzuschleusen. Die allgemein zurückgehende Angriffsform der DDoS-Attacke sowie die komplexeren Datendiebstahl-Versuche wurden in den vergangenen sechs Monaten von etwa einem Drittel der befragten KMU registriert. Interessant ist, wie wenige Unternehmen generell Cyberkriminalität vor mehr als fünf Jahren wahrgenommen haben, und wie deutlich die Einschätzung des Bundeskriminalamtes bestätigt wird, wonach die Angriffe durch DDoS-Überlastungen seit einigen Jahren massiv zurückgehen.

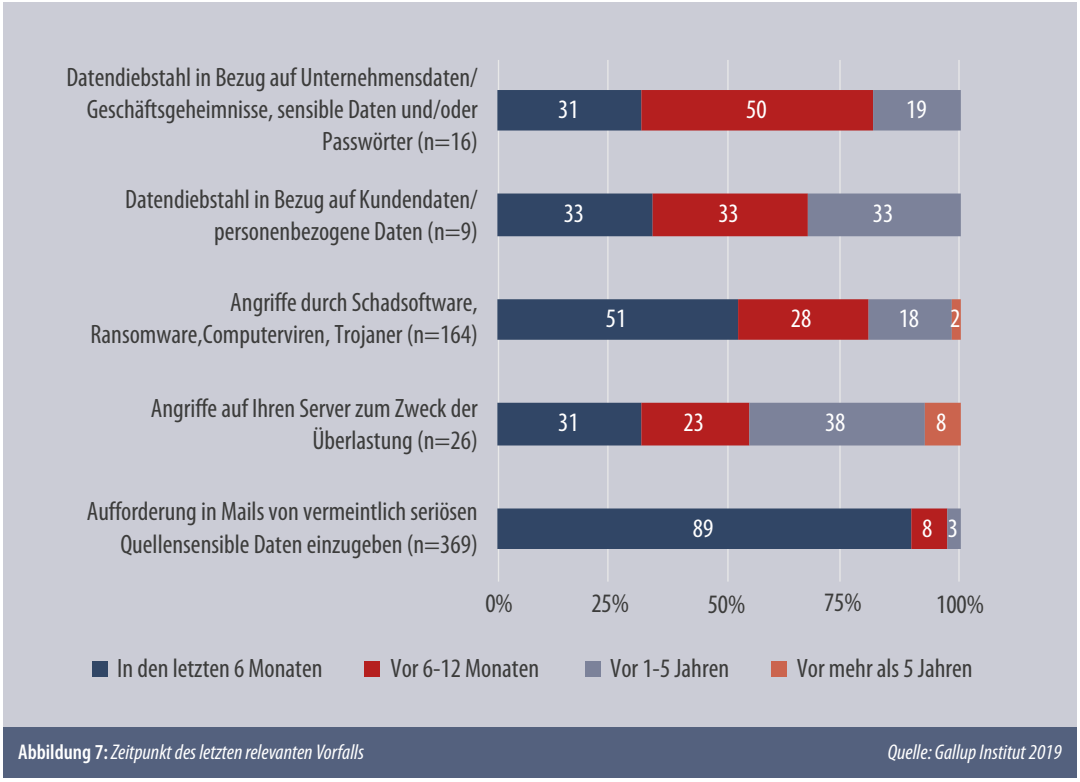

Abbildung 7: *Zeitpunkt des letzten relevanten Vorfalls* *Quelle: Gallup Institut 2019*

Betrachten wir zuletzt noch die Besorgnis der Unternehmen betreffend eine mögliche Wiederholung der Angriffe. Die zwei Deliktformen, deren mögliche Wiederholung den größten Grund zur Sorge bereitet, sind erneut Phishing- sowie Schadsoftware-Angriffe. Die Angst davor stieg im Vergleich zum Jahr 2018 um fast zehn Prozentpunkte an. Bei allen anderen Deliktformen ging die Zahl jener Unternehmen, die eine Wiederholung des Angriffsversuchs befürchten, jedoch konsequent zurück. Interessant an den Ergebnissen ist, dass die Sorge vor Wiederholung nicht mit den tatsächlich gemachten Erfahrungen zu korrelieren scheint. Denn obwohl fast 90 Prozent der betroffenen Unternehmen in den letzten sechs Monaten Vorfälle erlebt hatten und 84 Prozent bereits öfter als viermal Opfer von Versuchen wurden, haben lediglich etwas mehr als die Hälfte der betroffenen Unternehmen Sorge vor Wiederholung, wenngleich sich diese Zahl im Vergleich zum Jahr 2018 erhöht hat. Die nicht bestehende Befürchtung eines neuerlichen Angriffs könnte jedoch auch als ein Unterschätzen des Risikos interpretiert werden.

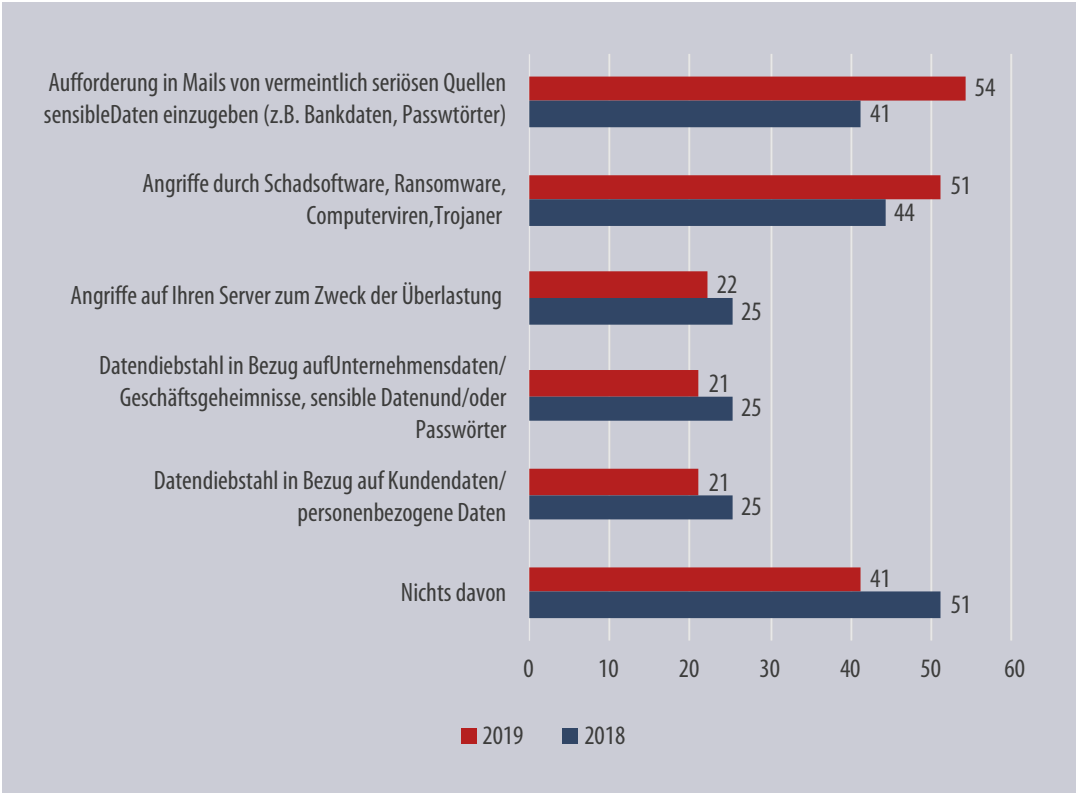

Abbildung 8: *Sorge vor Wiederholung nach Deliktformen in %: Vergleich 2018-2019* *Quelle: Gallup Institut 2019*

4.2 Schaden

In den eingetretenen Fällen dominiert nach wie vor die glückliche Situation, dass gar kein Schaden entstanden ist oder feststellbar war. Dies ist auch damit zu erklären, dass die Unternehmen Ransomware und Phishing bereits frühzeitig erkennen. Dieser Fall scheint auch immer häufiger einzutreten. War 2018 noch die Hälfte der Fälle mit einer Schadensbezifferung durch die Unternehmen ausgewiesen, ist es 2019 nur noch ein Drittel. Dies scheint auf einen gewissen Lerneffekt aus vorigen Vorfällen hinzudeuten.

In den Fällen, in denen Schaden entstanden ist, dominieren vor allem die nicht direkt monetären Schadensformen. Dies ist wenig überraschend, da der finanzielle Verlust (es sei denn, durch direkte Formen der Erpressung, einen Auftragswegfall oder ähnliches) einer Cyberattacke oftmals nur schwer konkret zu beziffern ist. Die häufigsten Schäden betreffen daher die Kategorien organisatorischer Aufwand (24%), Zeitausfall (21%) sowie Stress (18%).

Einen finanziellen Verlust erlitten lediglich 7% der befragten Unternehmen, was fast eine Halbierung im Vergleich zum Vorjahr bedeutet (12%, siehe Abbildung 9). Der finanzielle Schaden betrug zwischen 130 und 150.000 Euro, wobei viele Unternehmen hierzu keine Angaben machen wollten oder konnten. Diese große Spanne in den Beträgen zeigt zum einen, am unteren Ende, dass Cyberkriminelle im Falle von Ransomware tatsächlich eher kleinere Beträge zu fordern scheinen. Zum anderen zeigt sich aber auch, dass die Schäden, die durch Cyberattacken verursacht werden können, für KMU durchaus existenzgefährdend sein können. Glücklicherweise sind diese Fälle selten.

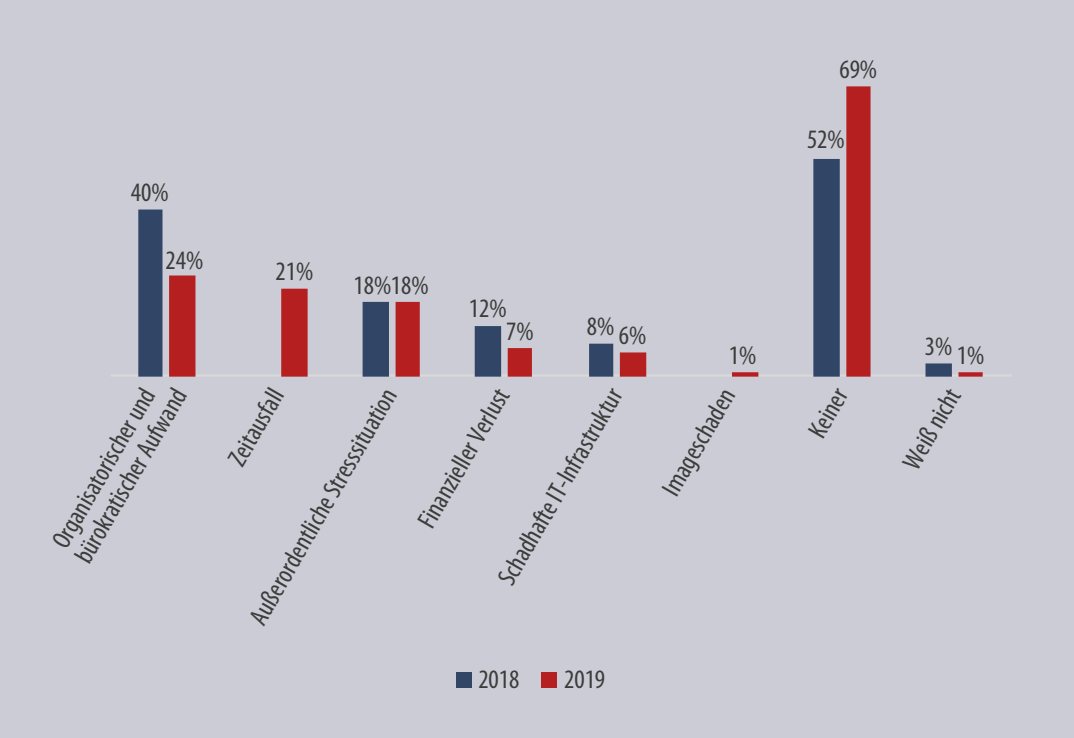

Abbildung 9: *Durch Cyberkriminalität erlittener Schaden: Vergleich 2018-2019* *Quelle: Gallup Institut 2019*

Eine aussagekräftigere Art der Darstellung von Schaden durch Cyberattacken als die Nennung von Geldbeträgen sind daher die non-monetären Konsequenzen der erfolgreichen Tat. Schadensarten wie „organisatorischer und bürokratischer Aufwand" führen nicht unmittelbar zu einem abschätzbaren Schaden am Unternehmen. Allerdings ist diese Schadensform ebenfalls nicht zu unterschätzen, da durch die Organisation von Gegenmaßnahmen durchaus Ressourcen firmenintern gebunden werden oder auch z.B. neue Endgeräte angeschafft werden müssen.

Exemplarisch sei hier der durch Zeitausfall entstandene Schaden in Bezug auf die verschiedenen Deliktformen aufgezeigt. Der geringste Schaden entstand durch Phishing, während der Zeitverlust durch den Diebstahl von Unternehmensdaten und Angriffe auf die Server am höchsten ist (siehe Abbildung 10). Die Auflistung zeigt, dass mindestens ein Arbeitstag durchschnittlich durch Cyberangriffe verloren geht. Gerade für kleine Unternehmen kann ein Tag Produktionsausfall massive Konsequenzen haben.

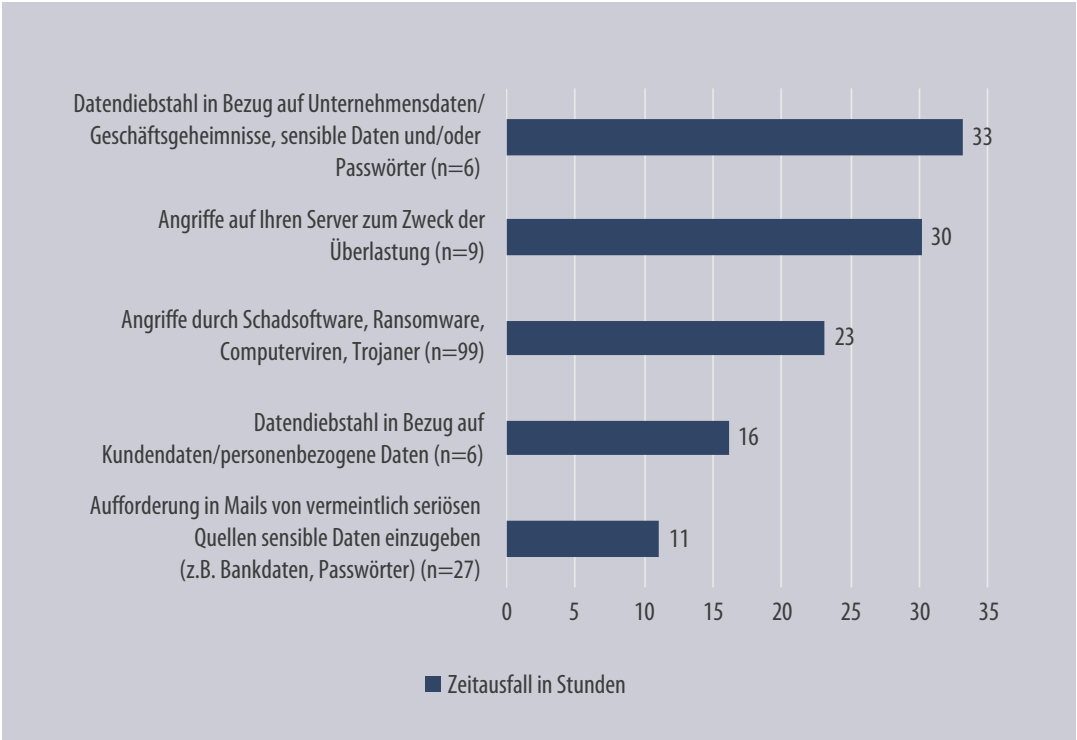

Abbildung 10: *Durch Cyberkriminalität entstandener Zeitausfall in Stunden nach Deliktform* *Quelle: Gallup Institut 2019*

Sieht man sich die Verteilung der TäterInnen an, so ergibt sich ein Bild, das sich auch in der internationalen Literatur zum Thema wiederfinden lässt. Fast drei Viertel der TäterInnen greifen „von außen" an, sind also firmenexterne Personen. Ein Viertel der Taten wurde von Menschen verübt, die im Unternehmen selbst beschäftigt waren. Diese Ergebnisse stehen im Gegensatz zu allgemeineren Aussagen der interviewten Experten. So glaubt auch Roland Sommer (Industrie 4.0), dass MitarbeiterInnen die größere Risikoquelle sind als die AngreiferInnen von außen. Er betont allerdings, dass es ihm hier nicht um bewusst und mit böser Absicht gesetzte Handlungen der MitarbeiterInnen geht – also keine TäterInnenschaft im klassischen Sinne –, sondern mehr um Handlungen, die unbewusst gesetzt werden. Beispielhaft erwähnt wird der USB-Stick, der auf dem Firmenparkplatz gefunden und achtlos eingesteckt und verwendet wird. Hier sieht Sommer die Unternehmen in der Pflicht, ihre MitarbeiterInnen zu schulen und ein Bewusstsein für die Risiken zu entwickeln. Auch Thomas Hoffmann (Radar Security) sieht ein klares Übergewicht bei den InnentäterInnen, er bezieht sich jedoch auf seine Erfahrungen mit größeren Unternehmen. Für KMU sieht Hoffmann ein vergleichsweise geringes Risiko durch InnentäterInnen, da die Tatbegehungslogik schwächer ausgeprägt ist als bei großen Unternehmen, wo tatsächlich Know-how relativ unbemerkt gestohlen werden kann. Dies ist bei kleinen Unternehmen eher nicht der Fall.

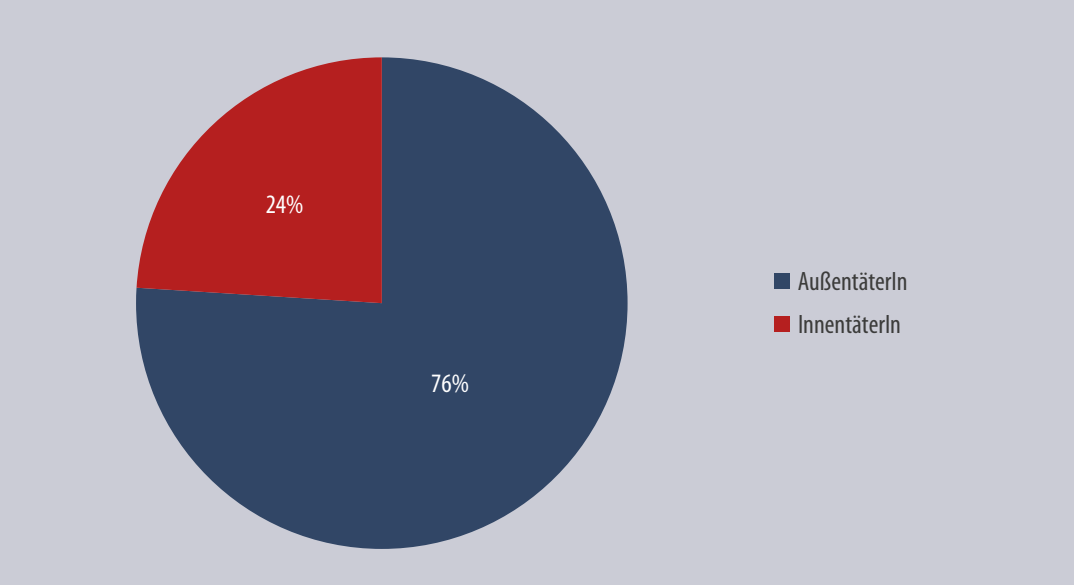

Abbildung 11: *Anteil von Innen- und AußentäterInnen an Hackversuchen* *Quelle: Gallup Institut 2019*

4.3 Risikoeinschätzung

Viele Unternehmen, ebenso wie große Teile der österreichischen Bevölkerung, bewegen sich nach wie vor mit großer Naivität durch den digitalen Raum. Thomas Hoffmann (Radar Cyber Security) meint, dass das Bewusstsein für die Wichtigkeit von Prävention bei kleinen und mittleren Unternehmen mangelhaft ist. Darüber hinaus attestieren die Experten auch ein allgemeines Fehlen von Risikobewusstsein. Roland Sommer (Industrie 4.0.) und Thomas Hoffmann betonen beiderseits, dass viele KMU sich erst ernsthaft mit dieser Problematik auseinandersetzen, nachdem sie Opfer geworden sind. Die Selbstwahrnehmung als „nicht lukrativ genug" wird dabei den Unternehmen oft zum Verhängnis. Denn Cyberkriminelle zielen keineswegs nur auf große Beträge oder großen Schaden ab – im Gegenteil. Aus organisatorischer Kosten-Nutzen-Sicht ist es für die meisten Formen der Cyberkriminalität sinnvoller, große Massen an Angriffen/Anfragen zu starten (bei Ransomware und Phishing) und sozusagen ein möglichst großes, aber wenig dichtes Netz auszuwerfen. Einige Fische bleiben trotzdem hängen. Und dann lohnt es sich bereits bei kleineren Erpressungssummen. Darüber hinaus ist es beim Diebstahl von Firmengeheimnissen oder Kundendaten eben genau dieser fehlende Schutz, der KMU für Kriminelle interessant macht. Anstatt sich ohne Aussicht auf Erfolg an den hervorragenden IT-Sicherheitssystemen großer Unternehmen abzuarbeiten, ist es für so manche Kriminelle sinnvoller, kleinere Ziele zu suchen, die schlechter geschützt, aber auch weniger lukrativ sind. Auch hier ergibt sich dann in der Summe meist wieder ein Profit für die Kriminellen.

In der quantitativen Befragung zeigt sich ebenso, dass die Bedrohung, die von Cyberkriminalität ausgeht, von den Unternehmen selbst tendenziell eher gering eingeschätzt wird, vor allem im Bereich Datendiebstahl (siehe hierzu auch Kapitel 4.4). Die Hauptbedrohungen für KMU – Phishing und Ransomware – werden allerdings von den Unternehmen durchaus als Bedrohung wahrgenommen (15% der Befragten sehen diese Angriffsarten als „sehr große" Bedrohung an, weitere 30 bzw. 31% als „große", siehe Abbildung 12). Somit sieht eine Mehrheit der Befragten die Bedrohung als nicht groß an, und zwar quer über alle Deliktformen. Diese Zahlen zeigen wiederum sehr deutlich, dass das Risikobewusstsein insgesamt nur mangelhaft ausgeprägt ist. Fast die Hälfte der österreichischen KMU sieht weder Ransomware noch Phishing als große Bedrohung an – und ein Fünftel (Ransomware) bzw. ein Viertel (Phishing) sieht es als eher oder überhaupt keine Bedrohung an.

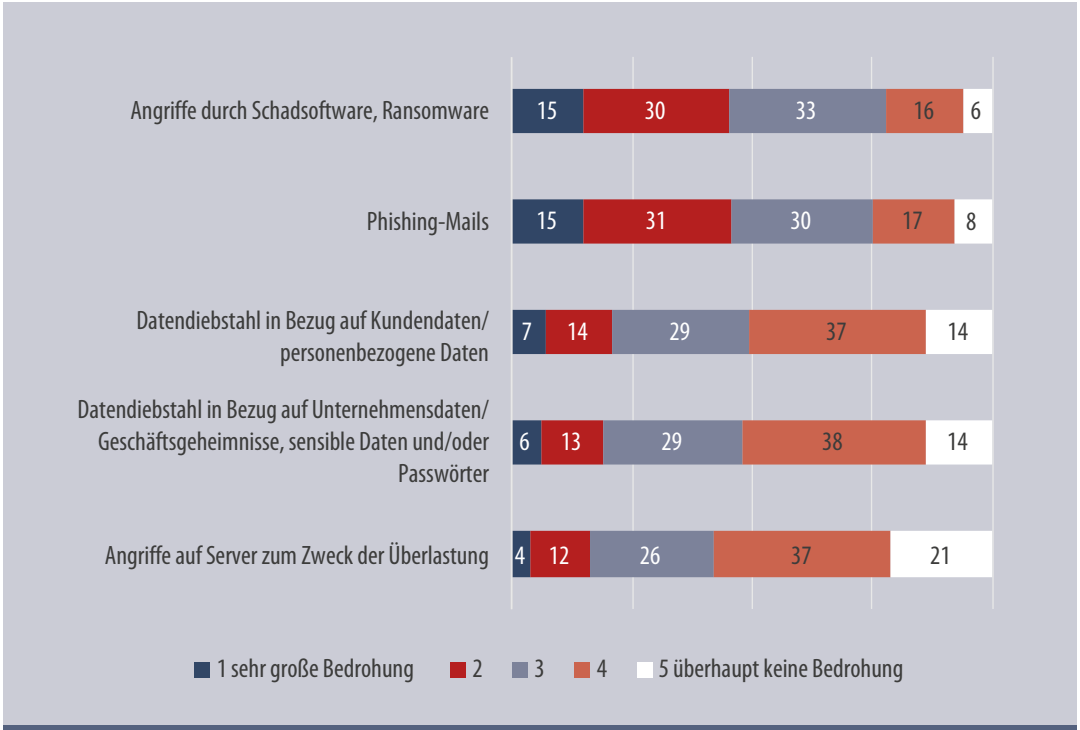

Abbildung 12: *Bedrohungseinschätzung verschiedener Formen von Cyberkriminalität* *Quelle: Gallup Institut 2019*

Betrachtet man diese Verteilung in der Feinanalyse, gestaffelt nach Unternehmensgröße, so bestätigt sich eine weitere Beobachtung der Experten: je kleiner das KMU, desto geringer ist die Selbsteinschätzung des Risikos, selbst Opfer eines Cyberangriffs zu werden (siehe Abbildung 13). So erklärt Roland Sommer von der Plattform Industrie 4.0, dass viele davon ausgehen, dass ihre geringe Unternehmensgröße einen ausreichenden Schutz darstellt („mich kennt eh niemand"). Je größer die Zahl der MitarbeiterInnen, umso höher ist das Gefahrenbewusstsein. Dieses Prinzip zieht sich durch sämtliche Experteneinschätzungen zum Risikobewusstsein der österreichischen KMU.

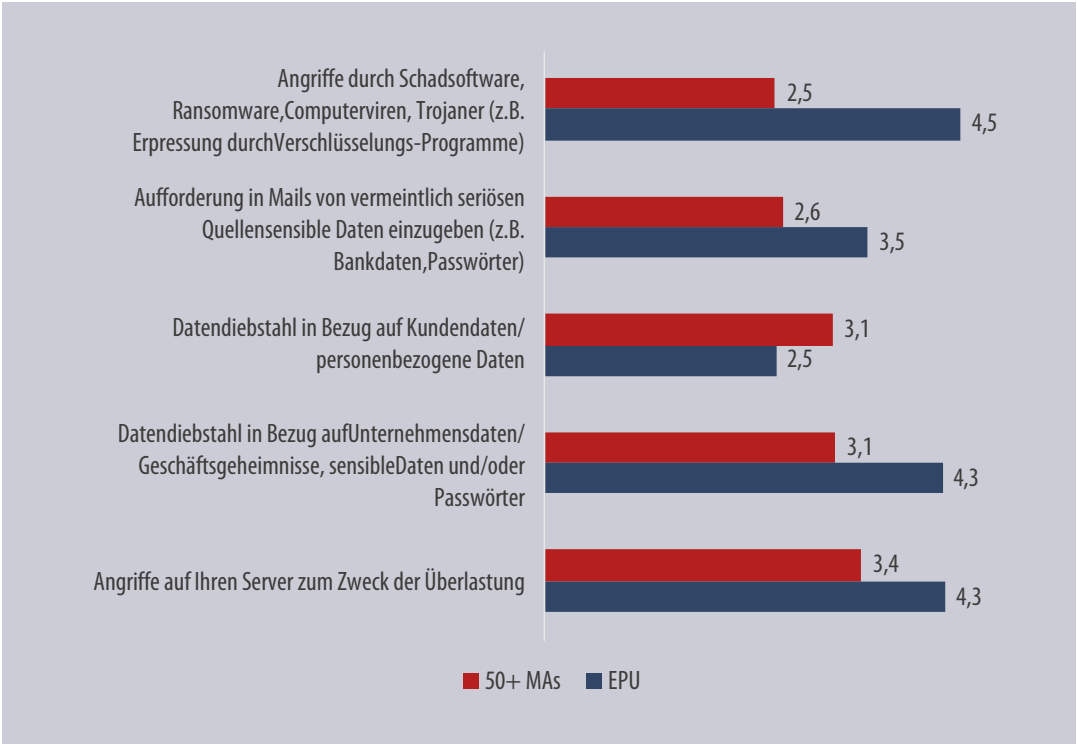

Abbildung 13: *Mittelwert der Bedrohungseinschätzung von EPU und KMU mit 50+ MA, 1=sehr große Bedrohung, 5=überhaupt keine Bedrohung*

Quelle: Gallup Institut 2019

Hier zeigt sich auch erneut, dass kleine und mittlere Unternehmen Cyberkriminalität nach wie vor durch die Linse der klassischen analogen Kriminalität betrachten. EinE EinbrecherIn suchen sich tendenziell lukrativere Ziele aus, also die größere, vermögendere Firma, da der Aufwand des Einbruches und das Risiko, erwischt zu werden, höher sind. Im Gegensatz dazu ist ein Cyberangriff billig, risikoarm und nicht aufwendig. Außerdem können tausende Ziele gleichzeitig angegriffen werden, was auch dazu führt, dass Cyberkriminelle im Bereich Phishing und Ransomware eher auf Quantität als Qualität setzen. Darüber hinaus sucht sich ein Cyberkrimineller seine Opfer meist nicht nach Bekanntheit oder Umsatzstärke aus, sondern sucht bewusst nach Schwächen in den Cyberschutzmaßnahmen. Es sind automatisch vorgehende Programme und Algorithmen, die systematisch nach Schwachstellen suchen, um diese dann auszunutzen und einzudringen, wie Roland Sommer (Industrie 4.0) weiter ausführt. Damit sind kleine Unternehmen, die sich nicht oder nur unzureichend schützen, prädestinierte Opfer.

4.4 Fokus: Informationspflicht bei Datendiebstahl – ein blinder Fleck?

Im Folgenden wird die Gemengelage zwischen Cyberkriminalität und der Anzeigemoral kleiner und mittlerer Unternehmen bei Angriffen, die persönliche Daten oder jene von KundInnen kompromittieren, näher beleuchtet. Seit 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO)[5], die unter anderem regelt, was zu tun ist, sollte ein so genannter „Data Breach" entstehen.

Als „Data Breach" kann z.B. ein Vorfall verstanden werden, durch den Unbefugten der Zugriff auf Daten möglich wird (z.B. Verlust eines Datenträgers, Hackerangriff). Dadurch kann den betroffenen Personen ein physischer, materieller oder immaterieller Schaden entstehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten, Identitätsdiebstahl oder -betrug, finanzielle Verluste,

5 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Die DSGVO definiert eine „Verletzung des Schutzes personenbezogener Daten" (Data Breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art 4 Nr. 12 DSGVO). Mit dieser Definition wird klargestellt, dass nicht nur vorsätzliche Angriffe, sondern auch zufällige Ereignisse erfasst sind.

Die DSGVO sieht für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten folgende Melde- und Benachrichtigungspflichten vor:

- Meldung an die zuständige Aufsichtsbehörde (Datenschutzbehörde)[6], wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt sowie
- Benachrichtigung der betroffenen Person(en), wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die Meldung einer solchen Datenpanne hat unverzüglich, jedenfalls aber binnen 72 Stunden ab Kenntnis angezeigt zu werden. Bei Nicht-Einhaltung dieser Frist muss diese Verzögerung begründet werden.

Laut dem Jahresbericht der österreichischen Datenschutzbehörde kam es im Jahr 2018 zu 69 Sicherheitsverletzungen (gemäß § 95a TKG, also Sicherheitsverletzungen bei öffentlichen Kommunikationsdiensten), sieben grenzüberschreitenden Sicherheitsverletzungen, 43 Sicherheitsverletzungen ausländischer Aufsichtsbehörden sowie 501 inländischen Sicherheitsverletzungen (Datenschutzbehörde Republik Österreich 2019, 44). In der gesamten EU kam es im ersten Jahr nach Einführung der DSGVO zu 89.271 Data-Breach-Meldungen an die jeweilige nationalstaatliche Behörde (Europäische Kommission 2019). Die meisten Meldungen (über 10.000) gab es dabei in Deutschland (European Digital Rights (EDRi) 2019).

Wer eine Datenpanne nicht meldet, macht sich strafbar. Die Nichtmeldung von Datenschutzverstößen selbst stellt nämlich einen – weiteren – Datenschutzverstoß dar und unterliegt dem strengen Strafenregime der DSGVO. Gleichzeitig wirkt aber auch eine rechtzeitig erstattete Meldung zwar mildernd, aber nicht strafbefreiend, wenn die Datenpanne auf einem DSGVO-Verstoß beruht – etwa, weil ein nicht ausreichendes Sicherheitssystem verwendet oder eine generell unzulässige Datenverarbeitung betrieben wurde.

Bei Verstößen gegen diese Melde- und Benachrichtigungspflicht nach DSGVO drohen Geldbußen von bis zu 10 Mio. Euro oder im Fall eines Unternehmens von bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres.[7]

6 Muster für eine Meldung:
https://www.dsb.gv.at/documents/22758/844171/Meldung+von+Verletzungen+des+Schutzes+personenbezogener+Daten+gem%C3%A4%C3%9F+Art.+33+DSGVO.pdf/cffc6756-1996-460d-a0bc-c5e29b4889ff

7 Relevante Artikel der DSGVO: Art 4 Z 12, Art 33, Art 34, Art 83 Abs 4, Relevante Erwägungsgründe: 85 - 88

Sind sich die kleinen und mittleren Unternehmen dieser Gesetzeslage bewusst? Studienergebnisse aus anderen Ländern zeigen, dass das Wissen über die neuen Pflichten, die mit der DSGVO kamen, nur mäßig ausgeprägt ist, speziell bei KMU. Laut einhelliger Meinung der Experten sollte ein optimierter Wissensstand zur DSGVO gegeben sein. Sowohl Roland Sommer als auch Thomas Hoffmann betonen, dass die Informationskampagnen von WKO und Gesetzgeber im Vorfeld des Inkrafttretens der Verordnung enorm breit gefächert und weit gestreut waren. Das heißt, es sollten alle Unternehmen in Österreich um die Meldepflicht eines Data Breaches wissen. Forschungsarbeiten zu diesem Thema kamen insgesamt zu einem zufriedenstellenden Bild. Alexander Ruzicka und Andreas Niederbacher schreiben in ihrer Studie zu „18 Monate EU-DSGVO in Österreich", dass „(…) der Großteil der Unternehmen nach wie vor mit der Umsetzung der Anforderungen beschäftigt (…)" ist (Ruzicka und Niederbacher 2019). Die Wichtigkeit des Themas allerdings sei zumeist erkannt worden, und der Datenschutz werde bei Unternehmensentscheidungen meist berücksichtigt.

Betrachtet man nun jedoch die in der quantitativen Untersuchung abgefragte Anzeigemoral von KMU generell und in Bezug auf Diebstahl von KundInnendaten oder personenbezogenen Daten im Speziellen, ergibt sich ein anderes Bild. So ist die Anzeigequote in allen eingetretenen Fällen extrem gering und wird umso geringer, je mehr eingetretene Fälle es gibt. Lediglich ein Viertel der von einem solchen Datendiebstahl betroffenen Unternehmen gibt an, auch tatsächlich Anzeige erstattet zu haben (in vier eingetretenen Fällen hat also nur ein Betrieb die Meldepflicht eingehalten, siehe Abbildung 14). Die geringe Fallzahl zeigt zwar einerseits, dass Datendiebstahl bei KMU vergleichsweise selten vorkommt. Gründe dafür sind einerseits vermutlich ein besserer Schutz dieser Daten durch die Unternehmen, andererseits der höhere Aufwand, den die TäterInnenseite für einen Datendiebstahl benötigt. Nichtsdestotrotz sollte nach den umfangreichen Informationskampagnen ein weit besserer Anzeigenschnitt vorliegen.

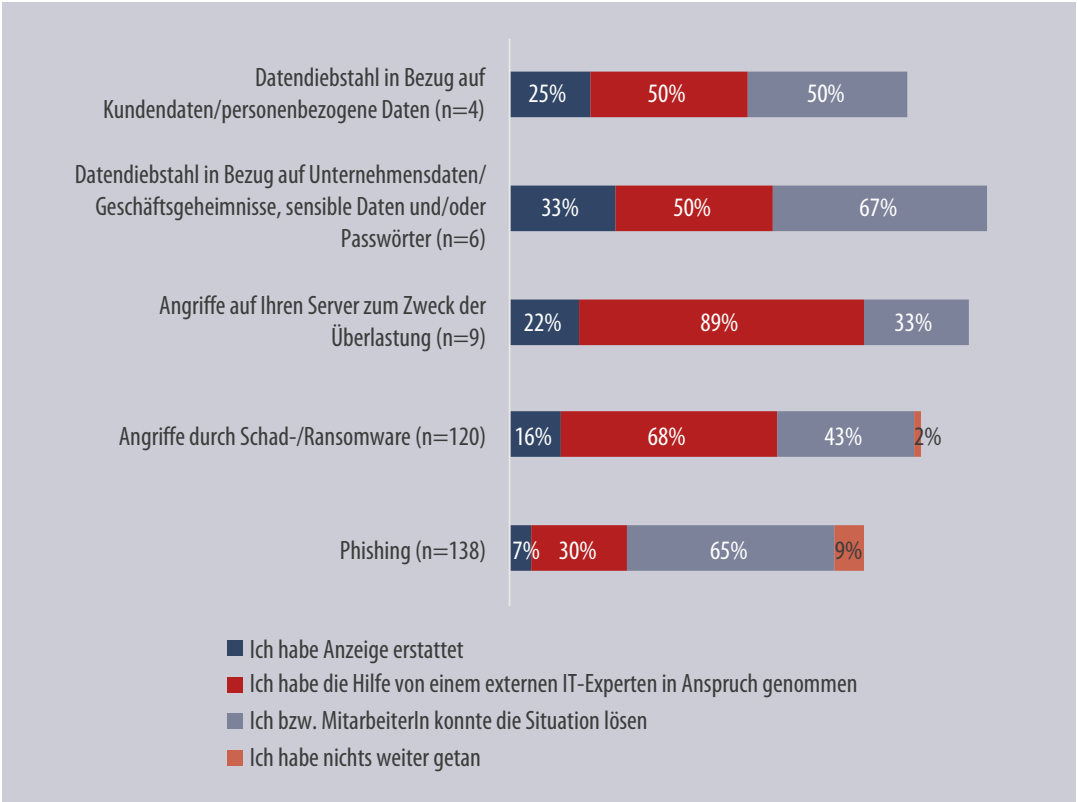

Abbildung 14: *Ergriffene Maßnahmen bei eingetretenen Fällen von Cyberkriminalität (Mehrfachnennung möglich)* *Quelle: Gallup Institut 2019*

Gefragt nach den Gründen für die Nicht-Anzeige, gab die Mehrzahl der Geschädigten an, dass es entweder keinen Grund dafür gegeben hätte (34%) oder eine Anzeige sinnlos sei (21%). Weitere 12% gaben an, dass der Schaden zu gering gewesen sei bzw. kein Schaden entstanden sei (ebenfalls 12%). Womit kann man diese geringe Anzeigenquote und die angegebenen Gründe erklären? Speziell für die meldepflichtigen Diebstähle personenbezogener Daten, aber auch für alle anderen Formen? Ein möglicher Indikator ist hier erneut das geringe Gefahrenbewusstsein der Unternehmen. Wenn die Bedrohung durch Datendiebstahl generell gering eingeschätzt wird, ist es durchaus plausibel, dass der dadurch entstandene (nicht-monetäre) Schaden geringgeschätzt wird und von einer Anzeige abgesehen wird. Diese Einschätzung teilt auch Michael Mörz (Cybercrime Competence Center BKA), der betont, dass im digitalen Raum nur selten mit demselben Risikobewusstsein verkehrt wird wie in der analogen Welt. Das bedeutet auch, dass die Einschätzung der Ernsthaftigkeit von Cyberkriminalität oft noch bagatellisiert wird. Sich im digitalen Raum nicht adäquat zu schützen bedeutet auch, dass die Gefahren, denen man sich damit aussetzt, als nicht relevant oder nicht bedrohlich angesehen werden. Hinzu kommt, dass bei Cyberdelikten generell wenige Anreize für eine Anzeige bei der Polizei (als zusätzliche Maßnahme) bestehen, da die Polizei nach Anzeigenlegung lediglich reaktiv strafverfolgend tätig wird, wie Michael Mörz anmerkt. Das heißt, der Schaden ist bereits eingetreten, eine Anzeige ändert nichts mehr daran. Dieser Umstand könnte die hohe Zahl der mit „sinnlos“ bezeichneten Begründungen in der Befragung erklären.

Ein weiterer Aspekt, den Unternehmen anführen, wenn sie von der Meldung eines eingetretenen Data Breaches absehen, ist der damit aus Unternehmenssicht einhergehende Reputationsverlust. Speziell die Benachrichtigungspflicht an die KundInnen wird von Unternehmensseite oft als großer Imageschaden wahrgenommen, sagt Harald Wenisch von der IT Security Experts Group der WKO. Daher tendieren Unternehmen dazu, eher restriktiv mit den Meldungen umzugehen, um negative Auswirkungen in Sachen Image zu vermeiden.

Geeignete Schutzmaßnahmen minimieren sowohl das Risiko einer Cyberattacke als auch das Risiko eines tatsächlichen Schadens. Im folgenden Kapitel werden die von den Unternehmen in der repräsentativen Befragung angegebenen Schutzmaßnahmen mit den Empfehlungen der Experten verglichen.

4.5 Schutzmaßnahmen: Experten-Empfehlungen versus Unternehmensrealität

Österreichs kleine und mittlere Unternehmen ergreifen die klassischen Schutzmaßnahmen in großem Maße (siehe Abbildung 15). So geben 99% der Befragten an, Anti-Viren-Programme oder Firewalls zu nutzen. Dies ist auch laut Thomas Hoffmann (Radar Cyber Security) der wichtigste erste Schritt in einem mehrstufigen IT-Sicherheitskonzept, der nach Ansicht des Cybersecurity-Experten einen guten, aber nicht vollends ausreichenden Schutz ermöglicht. Neben dem Antivirusprogramm beinhaltet diese erste Sicherheitsstufe eine Scansoftware, die aktiv nachscannt, und im Optimalfall zusätzlich ein externes Monitoring. In der Befragung gaben immerhin 78% der Unternehmen an, sich von externen Unternehmen beraten zu lassen, lediglich 35% lassen auch eine Risikobewertung durch Experten durchführen. Aufgeschlüsselt nach MitarbeiterInnenzahl tritt eine quer durch alle abgefragten Maßnahmen hohe Schutzquote erst bei Unternehmen mit mehr als 50 MitarbeiterInnen auf.

Als Hindernis für eine durchgängig hohe Präventionspolitik der Unternehmen sehen die Experten vor allem eine falsche Kosten-Nutzen-Rechnung vonseiten der KMU: Da die Investition in Cybersicherheit zunächst keinen direkten Return on Investment bietet, sind viele Firmen zögerlich, was größere Ausgaben in diesem Bereich betrifft. Dies führt dann zu der Situation, dass viele erst tätig werden, nachdem sie bereits Opfer geworden sind.

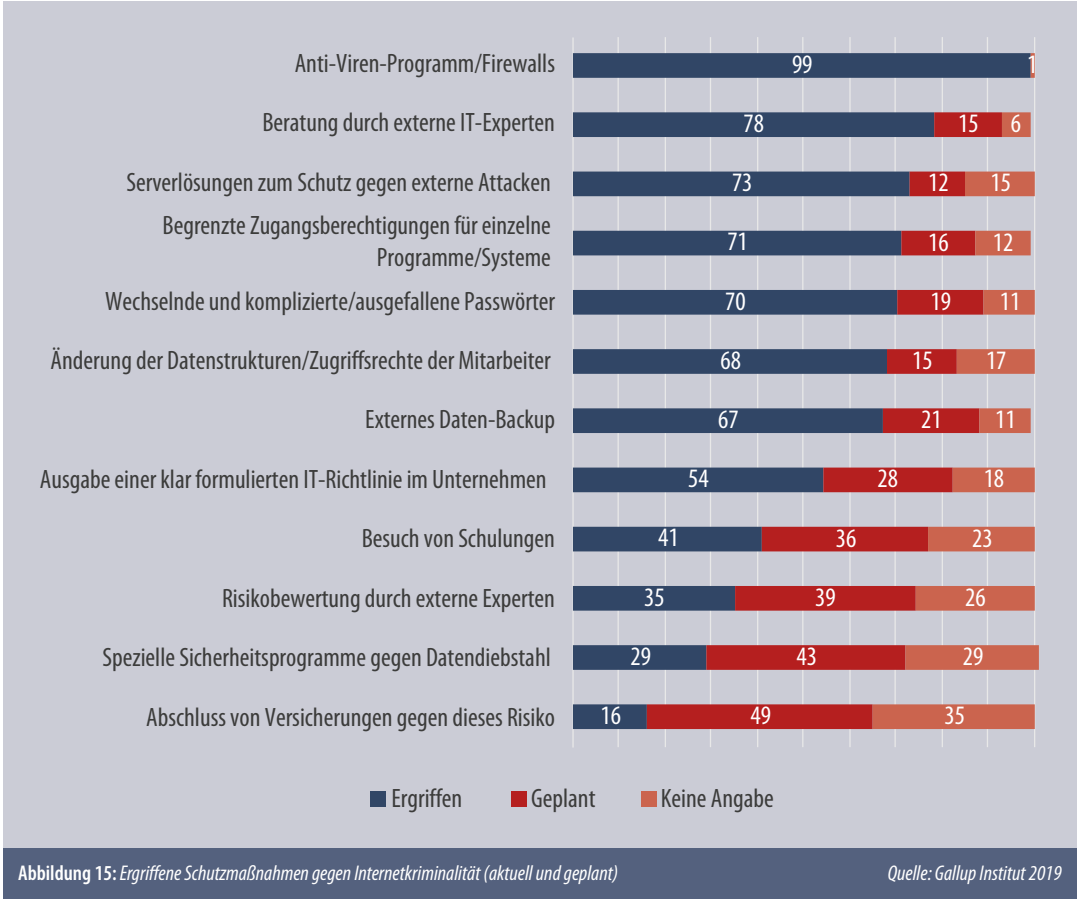

Abbildung 15: *Ergriffene Schutzmaßnahmen gegen Internetkriminalität (aktuell und geplant)* *Quelle: Gallup Institut 2019*

Ein von allen Experten betonter wichtiger Aspekt der Prävention ist eine regelmäßig und gründlich durchgeführte Update-Politik. Hier sehen die Experten das größte Risiko für Unternehmen. Nicht nur Updates der Antivirus-Software, sondern auch des Betriebssystems sowie der Software auf Nicht-Endgeräten leisten einen großen Beitrag zum Schutz der IT-Infrastruktur. Hier sieht Roland Sommer von der Plattform Industrie 4.0 jedoch zusätzlich speziell im Bereich der OT (Operational Technology) großen Nachholbedarf. Hierbei sind vor allem die Computer in den Produktionsmaschinen gemeint. Diese Systeme werden oftmals nicht upgedatet, um den Produktionsprozess nicht zu unterbrechen, was dazu führt, dass sie nur äußerst mangelhaft vor Angriffen geschützt sind. Dadurch sind diese Systeme enorm anfällig für Hackangriffe von außen, die nicht nur zu Produktionsausfall, sondern auch zum Diebstahl von Betriebsgeheimnissen (z.B. Produktionsketten) führen können.

Windows Updates werden regelmäßig von knapp zwei Dritteln der Unternehmen durchgeführt. In einigen wenigen Unternehmen können MitarbeiterInnen diese Updates abschalten. Die geringste Update-Dichte findet sich bei Ein-Personen-Unternehmen. Hier gibt mehr als ein Drittel an, keine regelmäßigen Windows-Updates durchzuführen (siehe Abbildung 16).

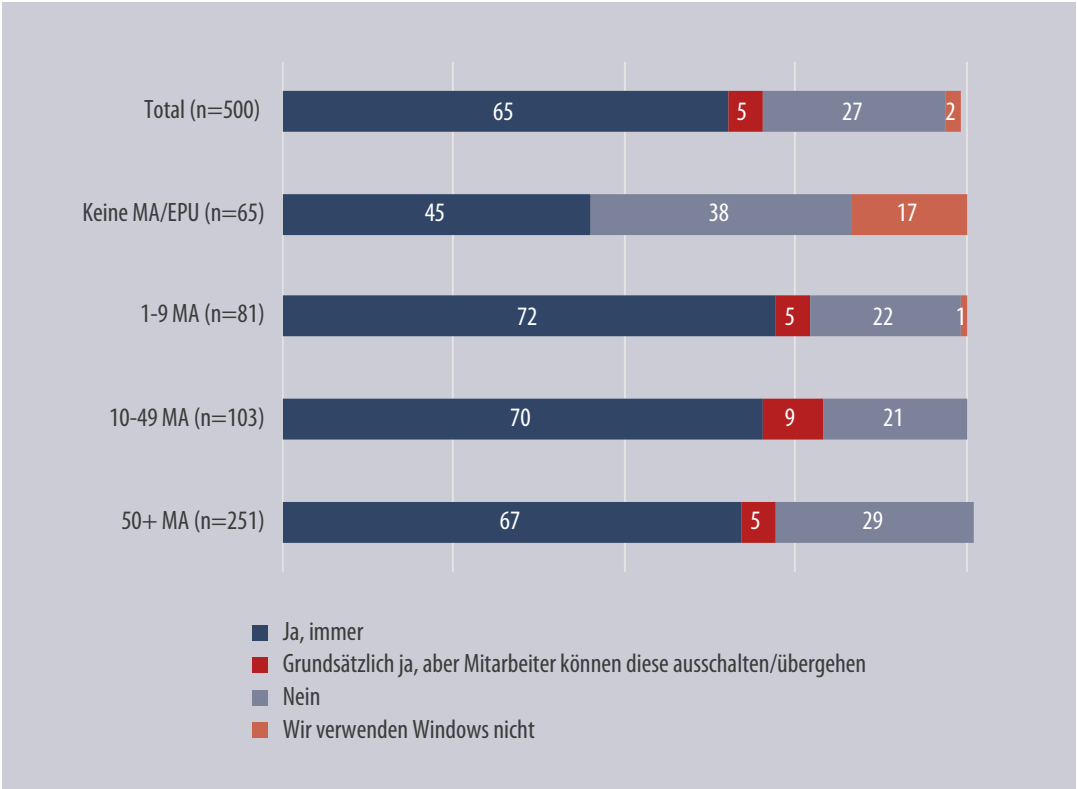

Abbildung 16: *Durchführung von automatischen Windows-Updates* *Quelle: Gallup Institut 2019*

Lediglich knapp über die Hälfte der Unternehmen hat eine klare IT-Richtlinie für MitarbeiterInnen verabschiedet. Dies bedeutet, dass in vielen Unternehmen keine Einigung über den Gebrauch von Endgeräten, die Nutzung des Internets oder in puncto Update-Policy besteht. Dies erhöht das Risiko von Schwachstellen, da somit die Verantwortung dem/der einzelnen MitarbeiterIn obliegt. Die wichtigste Maßnahme, die alle Experten einhellig identifizieren, ist eine verantwortungsvolle, regelmäßige und gründliche Update-Politik. Auch Thomas Hoffmann und Roland Sommer weisen darauf hin, dass klare Regeln für MitarbeiterInnen hier präventiv wirksam sein können.

Einen eindringlichen Appell setzt Roland Sommer für eine konkrete Präventionsmaßnahme: Es sei von großer Wichtigkeit, die MitarbeiterInnen regelmäßig zu schulen. Dies erhöht nicht nur das Problembewusstsein der Belegschaft, sondern kann auch zu einer größeren internen Lösungskompetenz im Ernstfall führen. Diese Maßnahme wird von zwei Fünfteln der befragten Unternehmen umgesetzt, etwas mehr als ein Drittel plant, diese im kommenden Jahr zu ergreifen.

Immerhin zwei Drittel der Unternehmen geben an, ein externes Daten-Back-up durchzuführen, eine Maßnahme, die Michael Mörz (Bundeskriminalamt) als besonders wichtig betont. Denn sollte man einmal Opfer werden und z.B. mit verschlüsselten Daten konfrontiert sein, kann man durch ein zuverlässiges Back-up-System den Verlust gering halten, indem man das Back-up neu aufspielt. Einschränkend weist Mörz darauf hin, dass mittlerweile Ransomware existiert, die zunächst „schlafend" verbleibt, also sich nicht aktiviert. Damit sickert sie auch in das Back-up ein. Erst nach Ablauf einer gewissen Zeit aktiviert sie sich; damit ist dann auch das Back-up kompromittiert. Das heißt, es reicht nicht, lediglich eine regelmäßige Back-up-Schleife zu haben, es muss auch regelmäßig kontrolliert werden, ob das Back-up funktionsfähig ist. Nichtsdestotrotz ist eine sorgfältige Back-up-Politik ein weiteres wichtiges Werkzeug zur Prävention von Schaden im Fall eines Cyberangriffes.

Ein weiterer wichtiger Faktor, der zum Schutz der Unternehmen vor Cyberattacken beitragen kann, ist eine genaue Bestandsaufnahme darüber, was eigentlich an Einfallspunkten und potenziellen Schwachstellen im Unternehmen vorhanden ist und wie diese geschützt sind. Dies ist für größere Unternehmen mit komplexeren IT-Systemen von größerer Relevanz als für einen Betrieb ohne MitarbeiterInnen. Hier geht es vor allem darum, festzustellen, was abseits der klassischen IT (Information Technology, also Endgeräte in Büros, Netzwerke usw.) noch für Angriffe anfällig ist. In Produktionsbetrieben sind das die OT-Geräte (Operational Technology), wie Roland Sommer (Industrie 4.0) betont (s.o.). Dieser Lücke sind sich sehr viele KMU nicht bewusst. Hier besteht auch ein erhöhtes Risiko in einer mangelhaften Passwort-Politik. Während in der IT mittlerweile meist klare Sicherheitsvorgaben für Passwörter existieren und diese auch regelmäßig geändert werden, ist dies bei OT-Systemen selten der Fall, gibt Sommer zu bedenken. Diese weisen oft noch das Passwort der Werkseinstellungen auf, die leicht zu knacken sind („Admin123“ als häufiges Beispiel). Diese Passwörter werden in vielen Fällen nicht geändert, da eine Produktionsverzögerung durch fehlende Kommunikation (die Änderung des Passwortes wird der nächsten Schicht nicht mitgeteilt) befürchtet wird. Da kaum Bewusstsein für das immense Risiko existiert, dem sich die Unternehmen damit aussetzen, wird das Passwort schlicht beibehalten.

Darüber hinaus kann es auch sinnvoll sein, festzustellen, welche Unternehmensbereiche bzw. welche Daten besonders schützenswert sind. Diese können dann spezifisch abgesichert werden, zusätzlich zu allgemeinen Schutzmaßnahmen. Lediglich 30 Prozent der Unternehmen gaben in der Befragung an, solche speziellen Sicherheitsprogramme gegen Datendiebstahl zu verwenden.

Die befragten Unternehmen zeigen auch großen Willen, zusätzliche Maßnahmen im nächsten Jahr umzusetzen (siehe Abbildung 17). Bei den geplanten Maßnahmen gibt es einen großen Anstieg im Vergleich zur Befragung im Vorjahr, und zwar quer durch alle einzelnen Items. So hat knapp die Hälfte der befragten Unternehmen angegeben, im nächsten Jahr eine Versicherung gegen Cyberkriminalität abschließen zu wollen. Laut Thomas Hoffmann (Radar Cyber Security) ist dies eine gute zusätzliche Maßnahme, um trotz aller Schutzvorkehrungen eingetretene Schäden abgegolten zu bekommen, die aber durchaus auch eine Kostenfrage bedeutet, gerade für KMU. Einzelpersonen-Unternehmen haben die meisten Maßnahmen in Planung, was auch damit zu erklären ist, dass ihr Status quo bei Schutzmaßnahmen relativ gering ist, sobald es über Antiviren-Programme hinaus geht. Unternehmen mit mehr als 50 MitarbeiterInnen erweisen sich hier bereits als sehr gut aufgestellt und zeigen entsprechend geringeren Nachholbedarf.

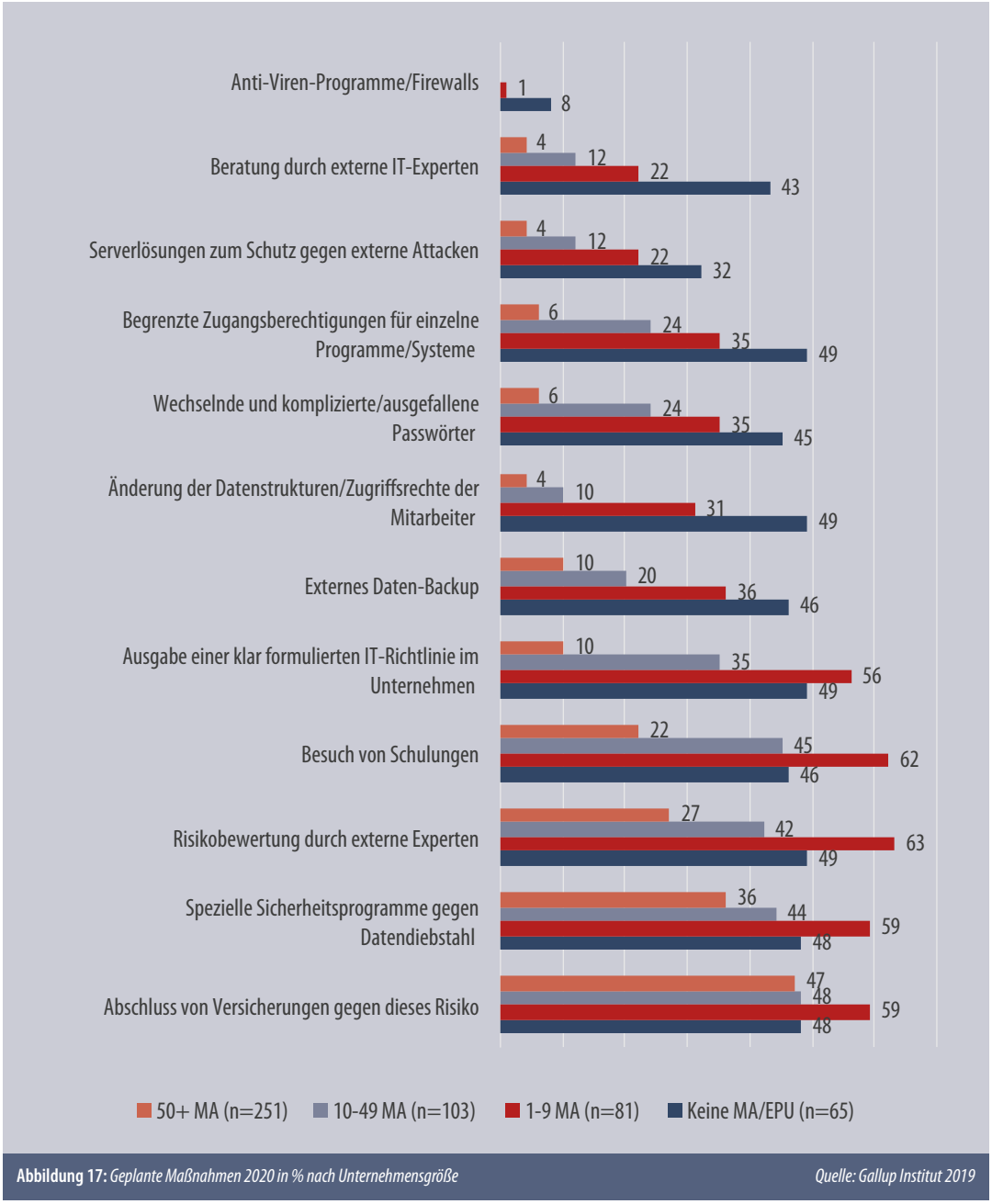

Abbildung 17: *Geplante Maßnahmen 2020 in % nach Unternehmensgröße* *Quelle: Gallup Institut 2019*

Das hohe Ausmaß geplanter Aktivitäten, vor allem vonseiten jener Unternehmen, die derzeit noch einige Schwächen im Bereich Cybersicherheit aufweisen, erzeugt ein positives Bild des bereits vorhandenen Bewusstseins, dass Prävention ein wichtiger Schritt zur Abwehr von Cyberangriffen ist. Die weitere Entwicklung bleibt dabei abzuwarten. Ein proaktives Vorgehen in Bezug auf die Cybersicherheit des eigenen Unternehmens ist ein wichtiger Schritt hin zu einer größeren Resilienz gegenüber Angriffsversuchen. Im Folgenden werden nun die Empfehlungen des KFV (Kuratorium für Verkehrssicherheit) an kleine und mittlere Unternehmen zum Schutz vor Cybercrime präsentiert.

5

5 CONCLUSIO 51

5.1 Sicherheit als Chance sehen! 51

5.2 Präventionstipps 52

5.3 Politische Empfehlungen 54

5 CONCLUSIO

5.1 Sicherheit als Chance sehen!

Die Ergebnisse der quantitativen Befragung und die Erkenntnisse aus den qualitativen Interviews zeigen, dass Österreichs KMU durchaus noch Nachholbedarf haben, was die Prävention von Cyberkriminalität angeht. Das prinzipielle Risikobewusstsein ist durchaus vorhanden, sinkt jedoch rapide, je kleiner das Unternehmen ist. Die häufige Annahme, dass man „too small to matter" sei, ist eine weitverbreitete Fehleinschätzung. Diese Kluft zwischen Kleinstunternehmen und größeren Unternehmen lässt sich anhand von drei Indikatoren aus den Ergebnissen herleiten: Erstens besitzen EPU im Vergleich das geringste Wissen über die Formen von Cyberkriminalität. Zweitens führen sie in geringstem Ausmaß regelmäßige Updates ihres Windows-Betriebssystems durch. Drittens wurde festgestellt: Je kleiner das KMU, desto geringer ist die Einschätzung des Risikos, selbst Opfer eines Cyberangriffs zu werden („mich kennt eh niemand"). Darüber hinaus, dies wurde in den Interviews mehrmals erwähnt, verwenden EPU oft auch private IT-Infrastruktur, mit lediglich privaten Schutzmaßnahmen.

Die Hauptbedrohungen für KMU – Phishing und Ransomware – werden von den Unternehmen durchaus als Bedrohung wahrgenommen (15% sehen diese Angriffsarten als „sehr große" Bedrohung an, weitere 30 bzw. 31% als „große"). Dies bedeutet allerdings im Umkehrschluss, dass eine Mehrheit der Befragten die Bedrohung als nicht groß ansieht. Dies gilt für alle Deliktformen. Je größer die Zahl der MitarbeiterInnen, umso höher ist das Gefahrenbewusstsein. Diese relative Unbedarftheit widerspricht den tatsächlichen Vorfallzahlen von Cybercrime, wie sie von den Unternehmen selbst wahrgenommen werden. Drei Viertel aller Unternehmen sahen sich bereits Phishing-Versuchen ausgesetzt, und jeweils bei etwa einem Viertel der Unternehmen sind Phishing- und Ransomware-Attacken tatsächlich auch eingetreten. Gerade Phishing ist hier besorgniserregend, es kam zu einer Verdopplung der eingetretenen Fälle.

Die häufigsten Schäden sind immaterieller Art, sie betreffen organisatorischen Aufwand, Zeitausfall sowie entstandenen Stress. Einen finanziellen Verlust erlitten lediglich 7% der befragten Unternehmen, was fast eine Halbierung im Vergleich zum Vorjahr bedeutet (12%). Der finanzielle Schaden betrug zwischen 130 und 150.000 Euro, wobei viele Unternehmen hierzu keine Angaben machen wollten oder konnten.

Nachholbedarf gibt es auch im Bereich der Meldepflicht von Data Breaches im Sinne der DSGVO. Hier wurde bei lediglich einem Viertel der vorgekommenen Diebstähle auch tatsächlich Meldung erstattet. Gründe hierfür sind zum einen die Angst vor Reputationsverlust, zum anderen aber auch die Wahrnehmung, dass eine Anzeige keinen Sinn für das Unternehmen selbst hätte.

In puncto Präventionsmaßnahmen wurde festgestellt, dass die Standard-Schutzmaßnahmen von fast allen Unternehmen ergriffen werden, jedoch bleibt es noch zu oft lediglich bei einem Antivirus-Programm und einer Firewall. Weiterführende Maßnahmen, die speziell dem Schutz der eigenen Betriebsgeheimnisse, der Sicherheit der Kundendaten und der Funktionsfähigkeit der Produktionsabläufe dienen, werden noch zu selten angewendet. Es herrscht jedoch hohe Bereitschaft, zusätzliche Maßnahmen zu setzen.

Die aktuelle KFV-Studie hat zwei wesentliche Fakten aufgezeigt: Erstens besteht nach wie vor eine Lücke zwischen dem vorhandenen Gefahrenbewusstsein und der realen Bedrohungslage durch Cyberkriminalität bei kleinen und mittleren Unternehmen in Österreich. Dieses mangelnde Gefahrenbewusstsein rührt zum einen von einem falschen Blick auf die Gefahren im digitalen Raum her, zum anderen aber auch von fehlenden Anreizen, sich umfassend zu schützen. Dieses mangelnde Bewusstsein kann jedoch nicht nur dazu führen, selbst Opfer zu werden, sondern kann auch weitreichende Konsequenzen im Nachklang der Tat haben: Die Studie zeigte, dass die Verpflichtung, Data Breaches an die Datenschutzbehörde zu melden, von Unternehmen nach wie vor nicht unisono umgesetzt wird. Dies hängt zusammen mit einem generellen Umsetzungsstau der DSGVO, aber auch mit einer problematischen Kosten-Nutzen-Rechnung der Unternehmen. Der Reputationsverlust, den man durch die Meldung an die DSB und die betroffenen KundInnen erleidet, wird als höher eingeschätzt als der Schaden, der durch das Nicht-Melden entsteht. In Anbetracht der potenziellen Probleme für alle von dem Breach betroffenen KundInnen sowie der hohen Strafen für die Nicht-Meldung kann diese Rechnung jedoch nicht aufgehen.

Zweitens zeigt die Studie auf, dass Cybersicherheit nach wie vor von einigen Unternehmen eher als Belastung und Kostenfaktor gesehen wird. Die primäre Botschaft aller befragten Experten war unisono, dass Prävention gerade für kleine und mittlere Unternehmen enorme Vorteile bringt. Wenngleich es keinen direkten „return on investment" gibt, stärkt ein angemessener Schutz vor Cyberkriminellen das Unternehmen jedenfalls enorm. Daher lautet wohl die zentrale Botschaft an Unternehmen, dass man nicht erst aktiv werden darf, nachdem man Opfer geworden ist. Harald Wenisch (IT Security Experts Group) und Roland Sommer (Industrie 4.0) sind sich beide einig in ihrem Aufruf, dass Unternehmen Sicherheit als Chance begreifen sollen. Durch einen adäquaten Level an IT- und Cybersicherheit können sich Unternehmen im Wettbewerb hervorheben und damit ihren Ruf als zuverlässige und sichere Partner verbessern. Gerade kleine und mittlere Unternehmen sind oft Teil einer Produktionskette, und hier sind Verlässlichkeit und Sicherheit wichtige Faktoren.

Das KFV liefert mit dieser Studie erstmalig einen Überblick über die Betroffenheit kleiner und mittlerer österreichischer Unternehmen in Sachen Cyberkriminalität. Eingedenk der Tatsache, dass KMU das Rückgrat der österreichischen Wirtschaft darstellen, kann diese Studie einen wertvollen Beitrag dazu leisten, zielgerichtet und bedarfsorientiert dort zu helfen, wo für KMU noch die größten Fallstricke im digitalen Raum lauern. Gleichzeitig dient die Studie aber auch den KMU selbst als Möglichkeit, die eigenen Prozesse zu reflektieren und gegebenenfalls Prävention auf eine höhere Prioritätsstufe zu heben. Denn Cyberkriminalität, dies wurde im Rahmen der Studie klar nachgewiesen, kann jedes Unternehmen treffen. Die richtige Form des Schutzes und das Bewusstsein darüber, dass Gefahren im digitalen Raum lauern, können Unternehmen nicht nur schützen, sondern auch Vorteile im Wettbewerb sichern.

Es folgt eine Zusammenfassung der wichtigsten Präventionstipps für größtmögliche Cybersicherheit kleiner und mittlerer Unternehmen. Abschließend werden politische Empfehlungen formuliert, die Österreichs Unternehmen und speziell KMU im digitalen Raum noch sicherer machen können.

5.2 Präventionstipps

Hier folgen einige konkrete Präventionstipps, die die Sicherheit der Unternehmen verbessern können:

- Für Passwortsicherheit sorgen: Gerade kleine Unternehmen können bereits durch eine ausgereifte Passwort-Politik ein Mehr an Sicherheit schaffen. Das bedeutet, dass es eine regelmäßig durchgeführte Änderung aller relevanten Passwörter gibt, dass betriebsfremde Personen keine Passwörter erhalten und dass die Passwörter nach bestimmten Kriterien gewählt werden.[8]

8 Im Blog der Abteilung Eigentumsschutz des KFV können Sie hierzu die wichtigsten Punkte nachlesen: https://www.kfv.at/passwort-sicherheit-so-sorgen-sie-fuer-schutz-im-netz/.

- Regelmäßige Updates durchführen: Hier sehen die Experten das am schnellsten und einfachsten umsetzbare Verbesserungspotenzial. Regelmäßige Updates des Betriebssystems, von Schutzsoftware, aber auch von kleinen Elementen, die Software beinhalten, wie etwa Routern, Produktionsmaschinen usw., können Sicherheitslücken schließen und somit unerlaubtes Eindringen in die IT-Infrastruktur zumindest massiv erschweren.
- Sich um einen guten Basisschutz kümmern: Dieser Basisschutz besteht, wie bereits in Kapitel 4.5 erwähnt, aus einem Antivirus-Programm, einer Scansoftware sowie im Idealfall einem externen Sicherheitsmonitoring. Hier können Unternehmen von spezialisierten Unternehmen für ihre jeweiligen Anforderungen maßgeschneiderte Lösungen zukaufen, was laut Harald Wenisch (IT Security Group der WKO) die ideale Variante darstellt, da nur so ein optimaler Schutz sichergestellt werden kann. Ansonsten gibt es sehr gute fertige Produktlösungen und Pakete für einen ganzheitlichen IT-Security-Ansatz, so der Tipp von Thomas Hoffmann (Radar Cyber Security).
- Regelmäßige Back-ups erstellen: Ein weiterer wesentlicher Punkt ist, dass für die zentralen Datensätze, Datenbanken und Systeme regelmäßige Back-ups erstellt werden sollten, wie Michael Mörz vom BKA und Harald Wenisch von der IT Security Group der WKO betonen. Diese Vorkehrungsmaßnahme sorgt dafür, dass selbst bei einem erfolgreichen Angriff der Schaden für das Unternehmen möglichst gering gehalten wird, da der Status quo ante zügig wiederhergestellt werden kann.
- Datenträger und -systeme verschlüsseln: Eine Verschlüsselung der Datenträger und Datensysteme kann ebenfalls dazu beitragen, die Datensicherheit zu optimieren.
- IT-Sicherheitsbeauftragte schulen und ausbilden lassen: Hier bietet sich zum Beispiel der Lehrgang „Data & IT Security“ an[9], an dessen Ende auch eine Zertifizierung für den/die MitarbeiterIn mit der entsprechenden Ausbildung stehen kann. Darüber hinaus sind auch regelmäßige Schulungen der Belegschaft/der zuständigen Personen ein wichtiger Aspekt umfassender Prävention.

Sollte ein Unternehmen doch einmal Opfer eines Cyberangriffs geworden sein, so empfehlen die Experten, auf jeden Fall Anzeige zu erstatten. Hier geht es unter anderem darum, der Exekutive aufzuzeigen, dass dieses Problem aktuell existiert, aber auch darum, den Schaden möglichst gering zu halten. Jedenfalls verpflichtend ist die Meldung an die DSB im Fall von Datenverstößen.

- Anzeige kann unkompliziert bei der nächsten Polizeidienststelle erstattet werden.
- Darüber hinaus gibt es die 24-Stunden-Meldestelle des C4 im BMI: Tel.: +43-1-24836-986500,
- E-Mail: against-cybercrime(at)bmi.gv.at
- Meldung an die DSB, sofern personenbezogene Daten betroffen sind

Im Fall eines Angriffs mit Ransomware empfiehlt Thomas Hoffmann die Seite https://www.nomoreransom.org/, die von Europol gemeinsam mit Cybersecurity-Dienstleistern betrieben wird. Hier gibt es regelmäßige Updates mit Entschlüsselungsprogrammen für die gängigsten Ransomware-Varianten. Zur Analyse, welche Art von Ransomware in das System eingespielt wurde, bietet die Website https://id-ransomware.malwarehunterteam.com/index.php eine Identifizierungsmöglichkeit an.
Für von Cybercrime betroffene Mitgliedsunternehmen bietet die WKO darüber hinaus die Cyber-Security-Hotline an.[10]

- Die Cyber-Security-Hotline ist rund um die Uhr aus dem österreichischen Festnetz und Mobilfunk unter der Telefonnummer 0800 888 133 erreichbar.

9 Siehe https://www.incite.at/de/zertifizierungen/certified-data-it-security-expert/.

10 Für mehr Informationen siehe https://id-ransomware.malwarehunterteam.com/index.php.

5.3 Politische Empfehlungen

Wie kann die Cybersicherheit österreichischer kleiner und mittlerer Unternehmen durch den Gesetzgeber verbessert werden? Aus Sicht des KFV (Kuratorium für Verkehrssicherheit) gibt es drei zentrale Punkte, denen die Legislative Aufmerksamkeit schenken sollte:

1. Die Mindestqualifikation für die Rolle des/der IT-Sicherheitsbeauftragten ist gesetzlich zu definieren. Derzeit gibt es keinerlei gesetzliche Vorgaben, welche Ausbildung o.ä. für die Ausübung der Funktion des/der IT-Sicherheitsbeauftragten vorzuweisen ist. Dies bedeutet, dass auch keine einheitlichen Mindeststandards zur objektiven Beurteilung von IT-Sicherheit in Unternehmen bestehen. Damit einhergehend wäre es sinnvoll, Personen in dieser Funktion durch ein Zertifikat standardisiert ausbilden zu lassen, wie es die WKO bereits anbietet (s.o.). Um hier die Belastung für Ein-Personen-Betriebe sowie Kleinstunternehmen zu verhindern, könnte, analog zum Netz- und Informationssicherheitsgesetz (NIS)[11], der Standard einer Unternehmensgröße von +50 MitarbeiterInnen und von mehr als 10 Millionen Euro Jahresumsatz eingeführt werden. Ab dieser Unternehmensgröße sollte die Zertifizierung des/der IT-Sicherheitsbeauftragten verpflichtend sein.
2. Regelungen betreffend den Mindeststandard in Sachen Cybersicherheit sollten für alle Unternehmen getroffen werden. So könnten etwa ein Mindest-Virenschutz sowie eine Scansoftware für sensible Unternehmensinfrastruktur gesetzlich gefordert werden. Besondere Anreize, wie z.B. staatliche Förderungen, könnten dazu führen, dass diese Regelung als positive Maßnahme, nicht als lästige Pflicht gesehen wird. Damit wäre sichergestellt, dass ein Basisschutz (ähnlich dem, den Thomas Hoffmann von Radar Cyber Security definiert, siehe Kapitel 4.5) in jedem Unternehmen zum Einsatz kommt. Hier ist sicherzustellen, dass der administrative und finanzielle Aufwand speziell für Kleinstunternehmen gering gehalten wird. Diese Sicherheitsvorkehrungen müssen dann auch regelmäßig nachgewiesen werden.
3. Schaffung nationaler Zertifizierungen auf Basis des Cyber Security Acts[12] und entsprechender Anreize, um den Erwerb dieser Zertifizierungen auch für KMU umfassend attraktiv zu gestalten.

11 Das Netz- und Informationssicherheitsgesetz (NISG) ist die österreichische innerstaatliche Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen. Diese regelt ein EU-weites hohes Sicherheitsniveau von Netz- und Informationssystemen und betrifft Betreiber strategisch wichtiger Dienste (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung, digitale Infrastruktur, Anbieter digitaler Dienste, öffentliche Verwaltung). Für mehr Informationen siehe z.B. https://www.wko.at/site/it-safe/cybersicherheit-das-neue-nisg.html.

12 Cyber Security Act: schafft den EU-Rahmen für die Cybersicherheitszertifizierung, der die Cybersicherheit von Online-Diensten und von Endgeräten für Verbraucher fördert – Ziel ist, dass IKT-Produkte und Dienste, die gemäß diesem System zertifiziert wurden, bestimmte Cybersicherheitsanforderungen erfüllen. Siehe z.B. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

6

6 TABELLENVERZEICHNIS 59

6 TABELLENVERZEICHNIS

Tabelle 1: Trends bei Vorfallarten und Motivationen von Cyberkriminalität bei Unternehmen 15
Tabelle 2: Struktur der befragten KMU 23
Tabelle 3: Liste Experteninterviews 24

7

7 ABBILDUNGSVERZEICHNIS 63

7 ABBILDUNGSVERZEICHNIS

Abbildung 1: Anteil der KMU an allen Unternehmen in Österreich. 13
Abbildung 2: Bekanntheit von Formen der Internetkriminalität 29
Abbildung 3: Überblick versuchte und eingetretene Attacken 30
Abbildung 4: Versuchte Formen von Cyberkriminalität: Vergleich 2018-2019. 31
Abbildung 5: Eingetretene Formen von Cyberkriminalität: Vergleich 2018-2019. 32
Abbildung 6: Häufigkeit von Cyberangriffen. 33
Abbildung 7: Zeitpunkt des letzten relevanten Vorfalls. 34
Abbildung 8: Sorge vor Wiederholung nach Deliktformen in %: Vergleich 2018-2019. 35
Abbildung 9: Durch Cyberkriminalität erlittener Schaden: Vergleich 2018-2019. 36
Abbildung 10: Durch Cyberkriminalität entstandener Zeitausfall in Stunden nach Deliktform. 37
Abbildung 11: Anteil von Innen- und AußentäterInnen an Hackversuchen. 38
Abbildung 12: Bedrohungseinschätzung verschiedener Formen von Cyberkriminalität. 39
Abbildung 13: Mittelwert der Bedrohungseinschätzung von EPU und KMU mit 50+ MA, 1=sehr große Bedrohu 40
Abbildung 14: Ergriffene Maßnahmen bei eingetretenen Fällen von Cyberkriminalität (Mehrfachnennung m 42
Abbildung 15: Ergriffene Schutzmaßnahmen gegen Internetkriminalität (aktuell und geplant) 44
Abbildung 16: Durchführung von automatischen Windows-Updates. 45
Abbildung 17: Geplante Maßnahmen 2020 in % nach Unternehmensgröße. 47

8

8 LITERATURVERZEICHNIS 67

8 LITERATURVERZEICHNIS

APA OTS. CYBERATTACKEN: Worauf man beim Abschluss einer Cyber-Versicherung achten muss. 2019. https://www.ots.at/presseaussendung/OTS_20191014_OTS0004/cyberattacken-worauf-man-beim-abschluss-einer-cyber-versicherung-achten-muss-bild (Zugriff am 28. Oktober 2019).

—. Ein Jahr DSGVO: Unternehmen sind nicht sicherer geworden. 2019. https://www.ots.at/presseaussendung/OTS_20190528_OTS0072/ein-jahr-dsgvo-unternehmen-sind-nicht-sicherer-geworden-anhang (Zugriff am 26. Januar 2020).

—. KMU Digitalisierungsstudie: DSGVO nahezu bewältigt – Handlungsbedarf bei digitalen Prozessen. 2018. https://www.ots.at/presseaussendung/OTS_20180917_OTS0134/kmu-digitalisierungsstudie-dsgvo-nahezu-bewaeltigt-handlungsbedarf-bei-digitalen-prozessen-video (Zugriff am 23. Januar 2020).

Bundeskriminalamt. „Die Polizeiliche Kriminalstatistik 2018: Österreich ist so sicher wie noch nie.“ 2019. https://www.bundeskriminalamt.at/501/files/PKS_18_Broschuere.pdf (Zugriff am 22. Juli 2019).

Bundesministerium für Digitalisierung und Wirtschaftsstandort. Mittelstandsbericht 2018. 2019. https://www.bmdw.gv.at/Themen/Wirtschaftsstandort-Oesterreich/KMU/Mittelstandsbericht.html (Zugriff am 08. Oktober 2019).

Cyber Sicherheit Steuerungsgruppe. Bericht Cyber Sicherheit 2018. Wien: Cyber Sicherheit Steuerungsgruppe, 2018.

Cyber Sicherheit Steuerungsgruppe. Cyber Sicherheit 2019. Wien: Cyber Sicherheit Steuerungsgruppe, 2019.

Datenschutzbehörde Republik Österreich. „Datenschutzbericht 2018.“ Wien, 2019.

Europäische Kommission. „GDPR in Numbers.“ Brüssel, 2019.

European Digital Rights (EDRi). GDPR Today: GDPR in Numbers. 2019. https://www.gdprtoday.org/gdpr-in-numbers-1yeargdpr/ (Zugriff am 23. Januar 2020).

Fearn, Nicholas. Why SMEs are at a higher risk to cyber crime. 2019. https://www.idgconnect.com/opinion/1502916/smes-risk-cyber-crime (Zugriff am 28. Oktober 2019).

Prosser, David. Cyber Criminals Target Poorly Protected Small Businesses. 2019. https://www.forbes.com/sites/davidprosser/2019/04/17/cyber-criminals-target-poorly-protected-small-businesses/#143d4de87177 (Zugriff am 28. Oktober 2019).

Ruzicka, Alexander, und Andreas Niederbacher. Deloitte Umfrage: Bestandsaufnahme nach 18 Monaten EU-DSGVO. Wien: Deloitte, 2019.

Sauermann, Michael. Studie: Mittelstand unterschätzt Gefahren von Cyberkriminalität. 2019. https://www.zdnet.de/88368347/studie-mittelstand-unterschaetzt-gefahren-von-cyberkriminalitaet/ (Zugriff am 28. Oktober 2019).

Schmitz, Peter. Viele Unternehmen noch immer nicht DSGVO-konform! 2019. https://www.security-insider.de/viele-unternehmen-noch-immer-nicht-dsgvo-konform-a-850933/ (Zugriff am 21. Januar 2020).

Shao, Grace. What ‚deepfakes‘ are and how they may be dangerous. 2019. https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html (Zugriff am 04. November 2019).

Walker, Ivy. „Cybercriminals Have Your Business In Their Crosshairs And Your Employees Are In Cahoots With Them.“ 2019.

Wegen, Nicoali van. Vorsicht Telefonbetrug: Microsoft-Anrufe sind eine Fälschung. 2019. https://www.online-warnungen.de/warnungsticker/telefonbetrug-microsoft-anrufe-faelschung/ (Zugriff am 31. Oktober 2019).

Wirtschaftskammer Österreich. Klein- und Mittelbetriebe in Österreich. 2019. https://www.wko.at/service/zahlen-daten-fakten/KMU-definition.html (Zugriff am 08. Oktober 2019).

Wirtschaftskammer Österreich. Wirtschaftskraft KMU 2018. Wien: Wirtschaftskammer Österreich, 2017.

IMPRESSUM

Medieninhaber und Herausgeber
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
Tel: +43 (0)5 77 0 77-1919
Fax: +43 (0)5 77 0 77-8000
kfv@kfv.at
www.kfv.at

Vereinszweck und Richtung
Der Verein ist eine Einrichtung für alle Vorhaben der Unfallverhütung und eine Koordinierungsstelle für Maßnahmen, die der Sicherheit im Verkehr sowie in sonstigen Bereichen des täglichen Lebens dienen. Er gliedert sich in die Bereiche Verkehr und Mobilität, Heim, Freizeit, Sport, Eigentum und Feuer sowie weitere Bereiche der Sicherheitsarbeit.

Geschäftsführung
Dr. Othmar Thann, Dr. Louis Norman-Audenhove

ZVR-Zahl
801 397 500

Grundlegende Richtung
Die Publikationsreihe „KFV – Sicher Leben" dient der Veröffentlichung von Studien aus den Bereichen Sicherheit und Prävention, die vom KFV oder in dessen Auftrag durchgeführt wurden.

Autor
Dr. Georg Plattner

Mitarbeit
Mag.ª Monika Pilgerstorfer
Mag.ª Dagmar Lehner
Dr.in Claudia Riccabona-Zecha

Fachliche Verantwortung
Dr. Armin Kaltenegger

Redaktion
Mag.ª Andrea Feymann
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien

Verlagsort
Wien, 2020

Lektorat
Mag.ª Eveline Wögerbauer

Grafik
Catharina Ballan.com

Fotos
pixabay.com

ISBN – pdf-Version
978-3-7070-0167-9

Zitiervorschlag
KFV – Sicher Leben. Band #23. Cybersicherheit als Chance – Cyberkriminalität und ihre Prävention bei kleinen und mittleren Unternehmen in Österreich. Wien, 2020

Aufgrund von Rundungen kann es bei Summenbildungen zur Unter- oder Überschreitung des 100%-Wertes kommen.

Alle personenbezogenen Bezeichnungen gelten geschlechtsunabhängig.

Offenlegung gemäß § 25 Mediengesetz und Informationspflicht nach § 5 ECG abrufbar unter www.kfv.at/footer-links/impressum/

ISBN (PDF) 978-3-7070-0167-9