Zürcher Hochschule
für Angewandte Wissenschaften

Soziale Arbeit

Institut für Delinquenz und Kriminalprävention

Cyberkriminalität gegen Organisationen im Sozialbereich

Ergebnisse einer Onlinebefragung im Kanton Zürich

August 2022

Dirk Baier, Lorenz Biberstein, Katja Girschik, Sabera Wardak

Inhaltsverzeichnis

1 Einleitung

Kriminalität verlagert sich zunehmend in den digitalen Raum. Dies zeigt sich einerseits daran, dass in der Schweiz bspw. Betrugsdelikte in der Polizeilichen Kriminalstatistik wie in Dunkelfeldbefragungen zunehmen und darüber hinaus verstärkt über das Internet praktiziert werden. So berichten Baier et al. (2022, S. 12), dass die Belastungszahl zu Betrugsdelikten in der Kriminalstatistik im Jahr 2020 mehr als dreimal höher lag als 2010. In einer Befragung zeigte sich, dass die Opferrate des Kreditkartenbetrugs von 2,9 % im Jahr 2011 auf 10,8 % im Jahr 2021 gestiegen ist (Baier et al., 2022, S. 19). Die sog. Cyberkriminalität trifft insofern immer häufiger Privatpersonen. Mindestens jede:r fünfte Schweizer:in wurde bezogen auf die letzten zwölf Monate Opfer von Cyberkriminalität, wobei am häufigsten Delikte wie Cyberbullying und Online-Belästigungen, aber ebenso Datenverluste/finanzielle Schäden durch Viren o.ä. berichtet werden (Baier, 2020).

Andererseits sind von der Kriminalität im digitalen Raum ebenso Organisationen betroffen. Sie sind als Ziel für Cyberangriffe u.a. deshalb interessant, weil sie Träger:innen von Wissen, Informationen und Know-how sind – der Grundlage für die Produktion verschiedener Güter. Der Fortbestand von Organisationen ist gefährdet, wenn dieser Grundlage ein Schaden zugefügt wird oder wenn sie in die Hände Dritter gelangt. Dies wiederum macht eine Organisation attraktiv für Erpressungsversuche. In erster Linie treffen diese Überlegungen auf Wirtschaftsunternehmen zu, speziell Kleine und Mittlere Unternehmen (KMU), weshalb es nicht überrascht, dass die Literatur zu organisationsbezogener Cyberkriminalität in der Schweiz diese Unternehmen fokussiert (u.a. Isenhardt et al, 2022; Mändli Lerch & Repic, 2017; Peter et al. 2020; Pugnetti & Casián, 2021; Zwahlen et al., 2020). Wie Meier und Burda (2020, S. 84) berichten, ist das Thema Cyberkriminalität und Cybersicherheit für Unternehmen sehr bedeutsam: Fast neun von zehn im Rahmen einer Studie befragten Schweizer Unternehmen wurden im vergangenen Jahr Ziel von Cyberangriffen; nur ein kleiner Teil der KMU verfügt zugleich über einen ausreichenden Schutz vor solchen Angriffen.

Fraglich ist, inwieweit sich die Befunde der Forschung zu KMU auch auf andere Organisationen übertragen lassen. Das Spektrum weiterer zu untersuchender Organisationen in modernen Gesellschaften ist dabei recht breit: Gedacht werden kann an NGOs, Vereine, Freiwilligenorganisationen, Parteien u.a.m. Das Forschungsprojekt, dessen Ergebnisse nachfolgend berichtet werden, richtete sich auf Organisationen des Sozialbereichs, was erstens damit zu begründen ist, dass in diesem Bereich sensible Informationen u.a. in Bezug auf die betreuten Klient:innen existieren. Zweitens ist das Institut für Delinquenz und Kriminalprävention, welches das Projekt lancierte, am Departement Soziale Arbeit der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) angesiedelt und verfolgt insofern den Auftrag, Phänomene im Themenfeld Soziale Arbeit zu untersuchen.

Da es bislang keine eigens auf Organisationen im Sozialbereich zielende Cyberkriminalitätsforschung gibt, orientiert sich der vorliegende Bericht an vorhandenen Studien zu Unternehmen als Ziele von Cyberangriffen. Die Grundlage bildete dabei insbesondere eine detaillierte Unternehmensbefragung, welche in Deutschland durchgeführt wurde (Dreißigacker et al.

2022, 2021). Der Fragebogen dieser Studie wurde weitestgehend übernommen und für die Schweiz angepasst. Im Rahmen des Forschungsprojekts und der durchgeführten Befragung sollten die folgenden Forschungsfragen beantwortet werden:

- Wie schätzen Organisationen des Sozialbereichs ihr Risiko ein, Ziel von Cyberangriffen zu werden?
- Wie häufig werden Organisationen im Sozialbereich Ziel von Cyberangriffen? Finden sich Unterschiede zwischen verschiedenen Bereichen, in denen die Organisationen tätig sind?
- Welche Schäden entstehen den Organisationen im Sozialbereich durch Cyberangriffe? Werden solche Angriffe angezeigt? Und was ist über die Tatpersonen der Angriffe bekannt?
- Inwieweit schützen sich Organisationen des Sozialbereichs vor Cyberangriffen? Wie sind sie grundsätzlich auf Cyberangriffe vorbereitet?

Im nachfolgenden Kapitel wird zunächst das methodische Vorgehen der Befragung erläutert. Im Anschluss werden die Ergebnisse entlang dieser Forschungsfragen vorgestellt. Zu betonen ist an dieser Stelle, dass es sich um eine erste, eher explorativ angelegte Studie handelte; weitere Studien zum Themenfeld Cyberkriminalität gegen Organisationen im Sozialbereich sind zweifellos wünschenswert.

2 Methode und Stichproben

Eine vollständige Übersicht mit allen Organisationen des Sozialbereichs existiert für die Schweiz bislang nicht, aus der für die Befragung Organisationen per Zufall gezogen werden könnten – dies wäre ein Vorgehen, um eine repräsentative Stichprobe zu erhalten. Ein grundsätzliches Problem ist, festzulegen, welche Organisationen überhaupt dem Sozialbereich, welche anderen Bereichen (z.B. Wirtschaftsunternehmen, Vereine) zuzuordnen sind. Dieses Problem wurde in der vorliegenden Studie nicht gelöst, d.h. eine Definition von Organisationen im Sozialbereich wurde nicht vorgenommen. Stattdessen wurde eine pragmatische Herangehensweise gewählt. Diese basierte auf der am Departement für Soziale Arbeit der ZHAW geführten Infostelle (https://adressverzeichnis.sozialearbeit.zhaw.ch/). Die Infostelle ist ein Online-Adressverzeichnis von Organisationen aus dem gesamten Sozialbereich, welche weitestgehend im Kanton Zürich ansässig sind. Dieses Verzeichnis wurde in den zurückliegenden Jahren vom Departement aufgebaut; teilweise können sich die Organisationen selbst im Verzeichnis eintragen, teilweise gelangen sie aufgrund von Veranstaltungsanmeldungen o.ä. ins Adressverzeichnis. Das Verzeichnis beansprucht keine Vollständigkeit und stellt keine systematische Erfassung von Organisationen dar. Die Stichprobe, die mit Hilfe des Infostellen-Verzeichnisses gewonnen werden kann, ist daher als Gelegenheitsstichprobe einzustufen.

Nach Löschung doppelter Adressen bzw. von Adressen ohne E-Mail-Angabe – anvisiert wurde eine Online-Befragung, die mittels eines E-Mail-Versands bekannt gemacht werden sollte – enthielt das genutzte Organisationsverzeichnis 2'178 Organisationen bzw. E-Mails. Diese Organisationen wurden am 31.5.2022 mit der Bitte angeschrieben, an einer Befragung zum Thema Cyberkriminalität teilzunehmen. Mitgeteilt wurde im E-Mail-Anschreiben, dass die Befragung stellvertretend für die gesamte Organisation von einer Person ausgefüllt werden sollte, die einen Überblick über mögliche Cyberangriffe hat und für IT-Fragen zuständig ist. Wenn die IT-Infrastruktur extern betreut wird, sollte der Fragebogen durch die entsprechende externe Stelle beantwortet werden.[1] Im E-Mail-Anschreiben wurden zudem Hinweise zur Anonymität und Vertraulichkeit der erhobenen Daten gegeben, die anvisierte Ausfüllzeit genannt[2] und der Link zum Online-Fragebogen, der mit dem Programm Unipark erstellt wurde, präsentiert. Am 13.6.2022 erfolgte einmalig ein weiteres E-Mail-Anschreiben an alle Organisationen, das einerseits für eine Teilnahme dankte und andererseits alle bis dahin nicht teilgenommen Organisationen erinnerte, noch die Befragung auszufüllen. Am 24.6.2022 wurde die Befragung geschlossen.

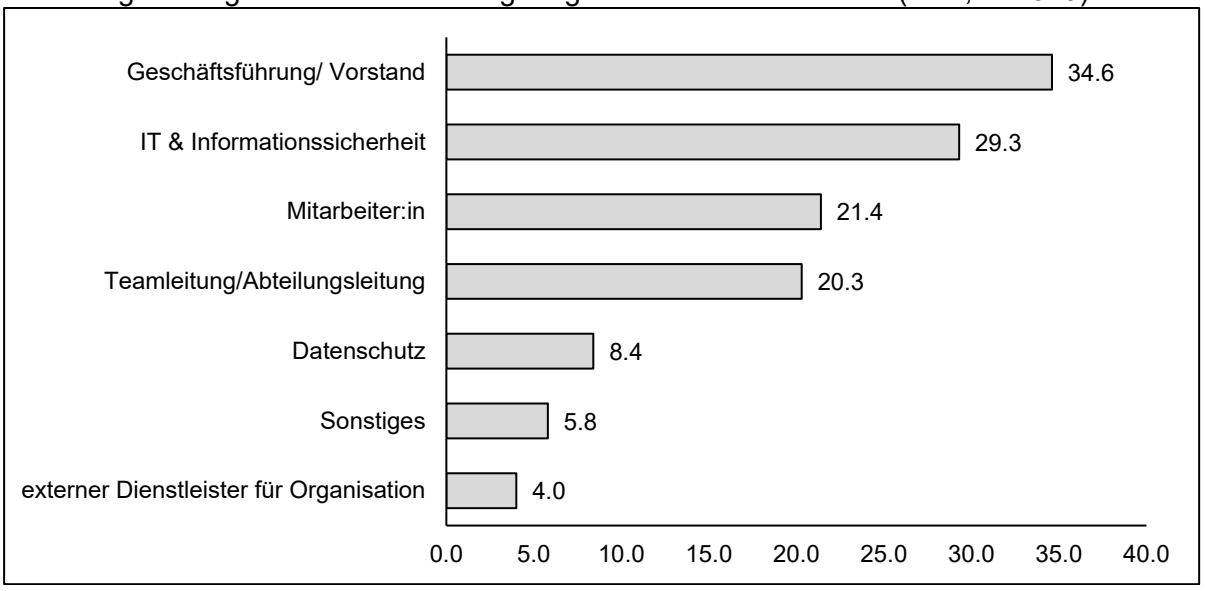
Im Zeitraum 31.5. bis 24.6.2022 haben insgesamt 381 Personen (bzw. Organisationen) an der Befragung teilgenommen. Dies entspricht einer Rücklaufquote von 17,5 %. Diese Rücklaufquote erscheint auf den ersten Blick niedrig – wünschenswert wäre zweifellos eine höhere

[1] Während der Feldphase zeigte sich, dass dies zumindest teilweise schwierig zu sein scheint, weil die externen IT-Dienstleister:innen für jede Arbeitsstunde bezahlt werden und insofern auch für eine Befragungsteilnahme bezahlt werden müssten, was die angeschriebenen Organisationen verständlicherweise nicht tun wollten. Denkbar ist daher, dass Organisationen mit externer IT-Betreuung in der Befragung unterrepräsentiert sind.
[2] Diese wurde auf 15 Minuten geschätzt; die durchschnittliche Ausfüllzeit der teilnehmenden Organisationen betrug am Ende zehn Minuten (Median).

Rücklaufquote. Gleichwohl zeigte sich auch in anderen Studien zum Thema eine ähnlich niedrige Rücklaufquote. Bei Isenhardt et al. (2022) lag sie bei 22,6 %, bei Dreißigacker et al. (2020) bei 11,6 %. Obwohl insgesamt 381 Organisationen an der Befragung teilnahmen, liegt die Anzahl an gültigen Antworten zu einzelnen Fragen meist niedriger. Dies ist primär darauf zurückzuführen, dass sich ein Teil der Fragen nur an Organisationen richtete, die Cyberangriffe erfahren haben und zu dem schwerwiegendsten Vorfall verschiedene Angaben machen sollten. Daneben ist zu beachten, dass zu einzelnen Fragen zusätzlich fehlende Werte vorliegen. Diese können verschiedene Gründe haben (Thema trifft auf Befragten bzw. Organisation nicht zu; eine Einschätzung ist für Befragte nicht möglich; Befragte möchten bewusst keine Antwort geben; Befragte haben das Ausfüllen des Fragebogens abgebrochen usw.). Um deutlich zu machen, wie viele Personen jeweils in die Auswertungen eingehen, wird bei den nachfolgenden Auswertungen die Anzahl gültiger Werte immer angegeben («n»).

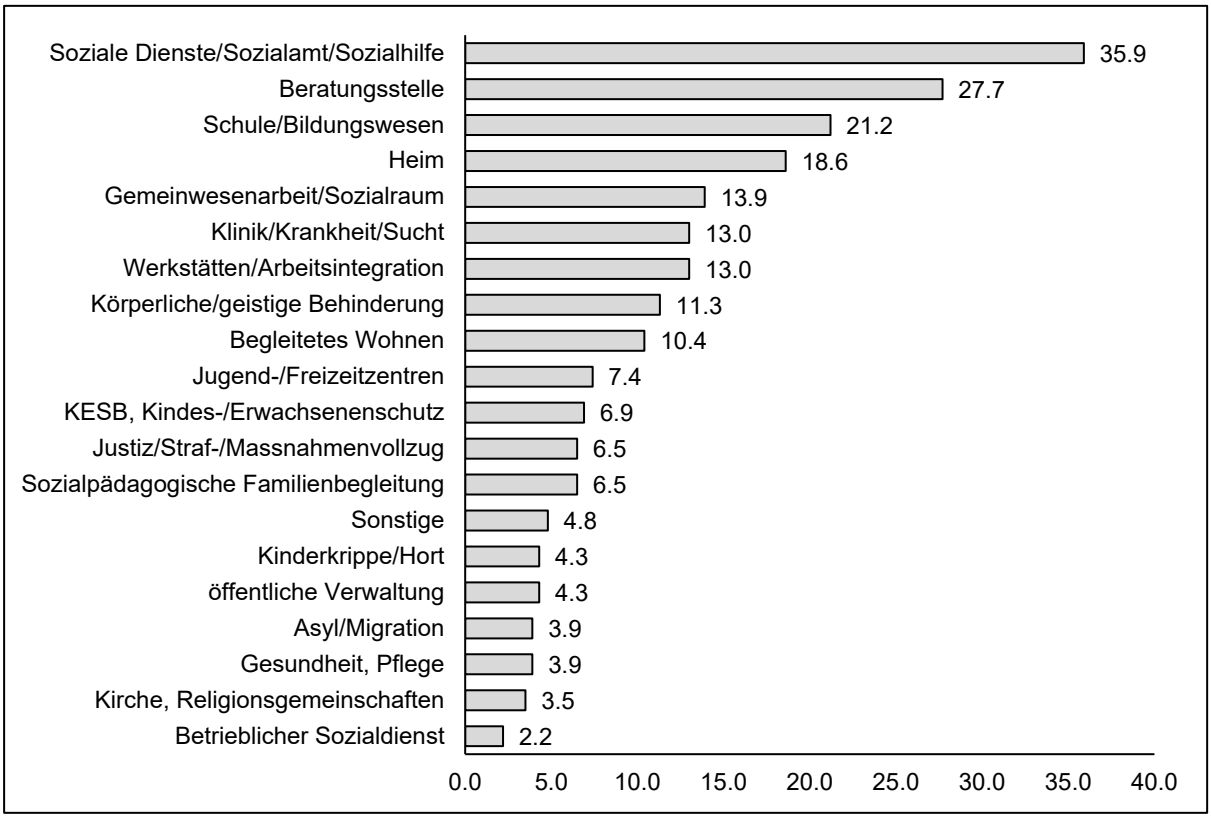
Werden die Merkmale der ausfüllenden Personen betrachtet, so ist zunächst zu konstatieren, dass diese zu 40,4 % «weiblich», zu 58,2 % «männlich» sind; weitere 1,3 % gaben bei der Frage nach dem Geschlecht «divers» an (n = 376). Abbildung 1 berichtet daneben, in welchem Tätigkeitsbereich die ausfüllende Person in der Organisation arbeitet, wobei mehrere Tätigkeitsbereiche berichtet werden konnten. Demnach sind 34,6 % der Befragten in der Geschäftsführung bzw. im Vorstand tätig, 29,3 % in der IT. Als Mitarbeiter:in der Organisation stufen sich 21,4 % der Befragten ein. Zudem gaben 5,8 % einen sonstigen Arbeitsbereich an, wobei es sich u.a. im Mitarbeitende im Bereich Administration handelte. Jede:r 25. Befragte ist als externe:r Dienstleister:in für die Organisation tätig. Nur auf die Befragten bezogen, die nicht extern für die Organisation arbeiten (n = 362), gilt zudem, dass sie zu 41,4 % bis zu fünf Jahren in der Organisation tätig sind (8,8 % arbeiten weniger als ein Jahr für die Organisation); 39,0 % sind schon länger als zehn Jahre für die Organisation tätig. Es haben insofern Personen geantwortet, die im Durchschnitt schon längere Zeit in der Organisation sind und sich entsprechend gut mit dieser auskennen dürften.

Abbildung 1: Tätigkeitsbereich der Fragebogen ausfüllenden Person (in %, n = 379)



Von grösserem Interesse als die Merkmale der ausfüllenden Person sind jedoch Merkmale der Organisation, für die Auskunft gegeben wurde. Die diesbezüglichen Fragen waren am Ende des Fragebogens zu beantworten, weshalb die Anzahl fehlender Werte recht hoch ausfällt. Angegeben werden sollte hier zunächst, zu welchem Bereich die Organisation gehört. Zur Auswahl standen 17 Bereiche (inkl. «Sonstige»); zudem konnten in ein offenes Antwortfeld weitere Bereiche notiert werden. Anhand der offenen Antworten wurden noch drei weitere Bereiche rekonstruiert («öffentliche Verwaltung», «Gesundheit, Pflege» und «Kirche, Religionsgemeinschaften»). Angegeben werden konnten jeweils mehrere Bereiche; im Durchschnitt wurden 2.19 Bereiche berichtet. Abbildung 2 zeigt, wie häufig die verschiedenen Bereiche benannt wurden. Am häufigsten gehören die Organisationen demnach zum Bereich Soziale Dienste/Sozialamt/Sozialhilfe (35,9 %). Etwa ein Viertel der Organisationen sind dem Bereich Beratungsstellen zuzuordnen (27,7 %), etwa ein Fünftel dem Bereich Schule/Bildungswesen (21,2 %). Andere Bereiche wurden z.T. deutlich seltener benannt. Jeweils unter fünf Prozent der Organisationen sind den Bereichen Kinderkrippe/Hort, öffentliche Verwaltung, Asyl/Migration, Gesundheit/Pflege, Kirche/Religionsgemeinschaften und betrieblicher Sozialdienst zuzurechnen. Für die Auswertungen wurden die Bereiche nicht weiter zusammengefasst, weil gerade in dem Fall, in dem mehrere Bereiche angegeben wurden (z.B. Soziale Dienste und Beratungsstelle) nicht entschieden werden kann, welchem Bereich eine Organisation zugeordnet werden sollte.

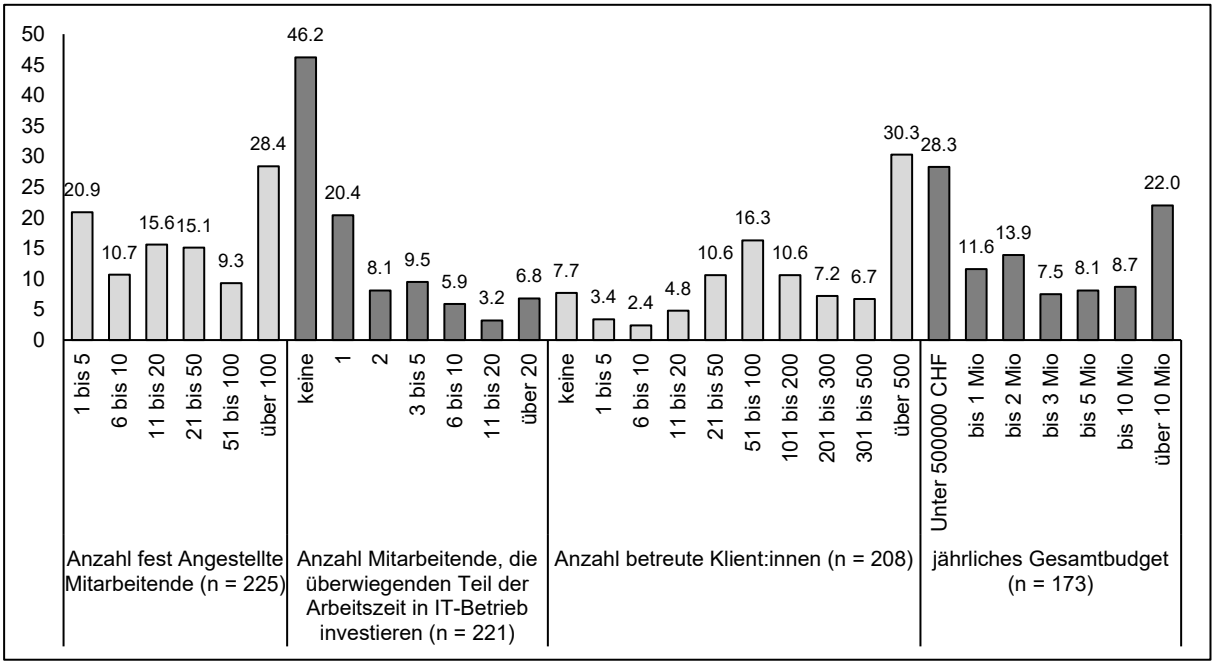
Abbildung 2: Bereich, zu dem Organisation gehört (in %, n = 231)



Ebenfalls angegeben werden sollte, mit welchen Zielgruppen die Organisation arbeitet (Mehrfachantworten waren wiederum möglich). Von allen Organisationen (n = 197) arbeiten demnach 41,1 % mit Kindern und 61,9 % mit Jugendlichen. Zudem wurde angegeben, dass 74,6 % der Organisationen mit Erwachsenen und 46,2 % mit älteren Menschen arbeiten. In vier von zehn Fällen (41,4 %) wird mit Familien gearbeitet, zu 8,6 % mit sonstigen Zielgruppen.

In Abbildung 3 sind weitere Merkmale der Organisationen dargestellt. Bei einem Fünftel der Organisationen (20,9 %) handelt es sich um sehr kleine Organisationen, insofern die Mitarbeitendenanzahl zwischen einer Person und fünf Personen liegt; in 28,4 % der Organisationen arbeiten hingegen über 100 Personen. In etwa der Hälfte der Organisationen gibt es keine auf die IT spezialisierten Mitarbeitenden (46,2 %). Die Anzahl an betreuten Klient:innen variiert ebenfalls recht stark, wobei 30,3 % der Organisationen über 500 Klient:innen haben. Auch in Bezug auf das Gesamtbudget wird die Varianz der Organisationen im Sozialbereich deutlich: Mehr als ein Viertel der Organisationen haben ein Budget von unter 500'000 CHF (28,3 %); gleichzeitig liegt das Budget bei mehr als einem Fünftel der Organisationen über zehn Millionen CHF.

Abbildung 3: Mitarbeitenden- und Klient:innenanzahl sowie Budget der Organisation (in %)

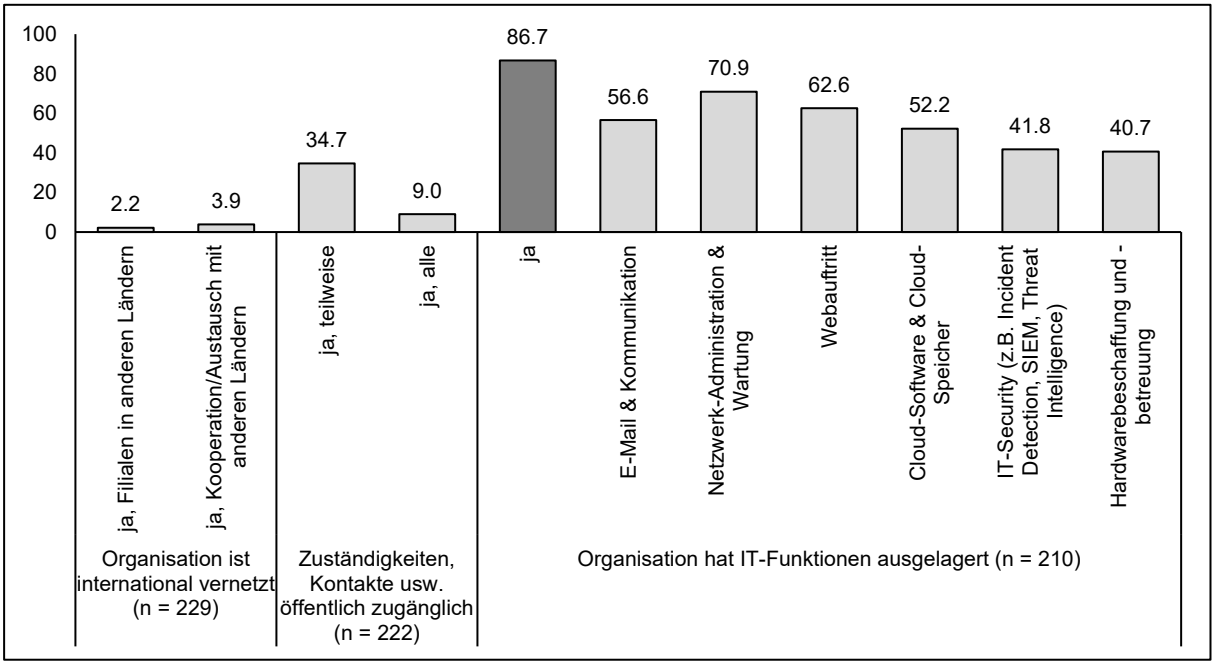


Die verschiedenen Einschätzungen zur Mitarbeitenden- und Klient:innenanzahl sowie zum Budget korrelieren zwischen .32 und .89 (Spearmans rho) signifikant miteinander ($p < .001$). Aus diesem Grund wurde wie folgt ein Index «Organisationsgrösse» berechnet: Zunächst wurden alle vier Variablen auf eine Breite zwischen 0 und 100 standardisiert. Im Anschluss wurde der Mittelwert aus den vier Variablen berechnet. Der Mittelwert wurde schliesslich genutzt, um drei Gruppen zu unterscheiden: kleinere Organisationen (Mittelwerte zwischen 0 und 33.33), mittlere Organisationen (Werte bis 66.67) und grössere Organisationen (Werte über 66.67). Insgesamt konnte auf diesem Weg für 237 Organisationen die Grösse bestimmt werden, wobei

39,2 % zu den eher kleinen, 31,2 % zu den mittleren und 29,5 % zu den eher grossen Organisationen zählen. Zu den eher grossen Organisationen zählen dabei häufiger Organisationen aus folgenden Bereichen: Klinik/Krankheit/Sucht, Justiz/Straf-/Massnahmenvollzug, KESB, Schule/Bildungswesen, Betrieblicher Sozialdienst und Kinderkrippe/Hort.

In Abbildung 4 finden sich Auswertungen zu weiteren Fragen, die in Bezug auf die Organisation zu beantworten waren und die in einem Zusammenhang damit stehen könnten, Ziel von Cybercrime-Angriffen zu werden. Es zeigt sich dabei zunächst, dass nur ein sehr kleiner Anteil der Organisationen in einer der beiden erfassten Formen international vernetzt ist – dies trifft auf 6,1 % der Organisationen zu. Deutlich häufiger ist es der Fall, dass «detaillierte Zuständigkeiten, Kontakte und Stellenbeschreibungen der Mitarbeiter:innen der Organisation öffentlich im Internet zugänglich» sind (Wortlaut aus Fragebogen). Bei 43,7 % der Organisationen ist dies teilweise oder komplett der Fall. Zudem haben fast neun von zehn Organisationen IT-Funktionen bzw. Hard- und Software ausgelagert (86,7 %). Von den Organisationen, die etwas ausgelagert haben, betrifft dies am häufigsten die Netzwerk-Administration und -Wartung sowie den Webauftritt (70,9 bzw. 62,6 %).

Abbildung 4: Weitere Angaben zur Organisation



3 Ergebnisse

3.1 Risikoeinschätzungen

Zu Beginn der Befragung sollte das Cyberangriff-Risiko eingeschätzt werden, dem die eigene Organisation aus Sicht der antwortenden Person ausgesetzt ist. Hierfür wurden zwei Items formuliert: Das erste Item fragte danach, wie hoch das Risiko ist, in den nächsten zwölf Monaten von einem Angriff geschädigt zu werden, der auch viele andere Organisationen triff (z.B. massenhaft versendete Schadsoftware); beim zweiten Item sollte das Risiko für einen ausschliesslich die eigene Organisation betreffenden Angriff eingeschätzt werden. Die Antwortvorgaben lauteten «1 – sehr gering», «2 – eher gering», «3 – eher hoch» und «4 – sehr hoch»; für die Auswertungen wurden die Antworten «eher hoch» und «sehr hoch» zusammengefasst. Entsprechend Tabelle 1 gehen 43,1 % der Befragten von einem (eher) hohen Risiko aus, dass die eigene Organisation durch einen ungezielten Angriff geschädigt wird; 14,4 % sehen ein (eher) hohes Risiko für einen gezielten Angriff. Diese Werte liegen höher wie in einer bundesdeutschen Studie zu Wirtschaftsunternehmen, in der 31,5 % ein (eher) hohes Risiko eines ungezielten Cyberangriffs, 7,0 % ein (eher) hohes Risiko eines gezielten Angriffs berichteten (Dreißigacker et al., 2020, S. 92).[3]

Tabelle 1: Risikoeinschätzungen nach verschiedenen Organisationsmerkmalen (in %; fett: Unterschiede signifikant bei p < .10)

	Risiko, in nächsten 12 Monaten von Cyberangriff geschädigt zu werden, der viele andere Organisationen trifft (ungezielter Angriff)	**Risiko, in nächsten 12 Monaten von Cyberangriff geschädigt zu werden, der ausschliesslich eigene Organisationen trifft (gezielter Angriff)**
gesamt (n = 362/369)	43,1	14,4
eher kleine Organisation (n = 229/233)	**33,3**	**5,6**
mittlere Organisation	**40,5**	**10,8**
eher grosse Organisation	**58,8**	**24,3**
Zuständigkeiten, Kontakte usw. öffentlich zugänglich: nein (n = 215/219)	43,4	10,4
Zuständigkeiten, Kontakte usw. öffentlich zugänglich: ja	41,9	17,0
IT-Funktion ausgelagert: nein (n = 203/206)	32,1	3,7
IT-Funktion ausgelagert: ja	46,9	14,0

Die Auswertungen der Befragung zu Organisationen im Sozialbereich macht darüber hinaus deutlich, dass in grösseren Organisationen häufiger von einem (eher) hohen Risiko sowohl eines ungezielten als auch eines gezielten Cyberangriffs ausgegangen wird. So gaben 24,3 % der Befragten aus grossen Organisationen an, dass diese einem (eher) hohen Risiko eines

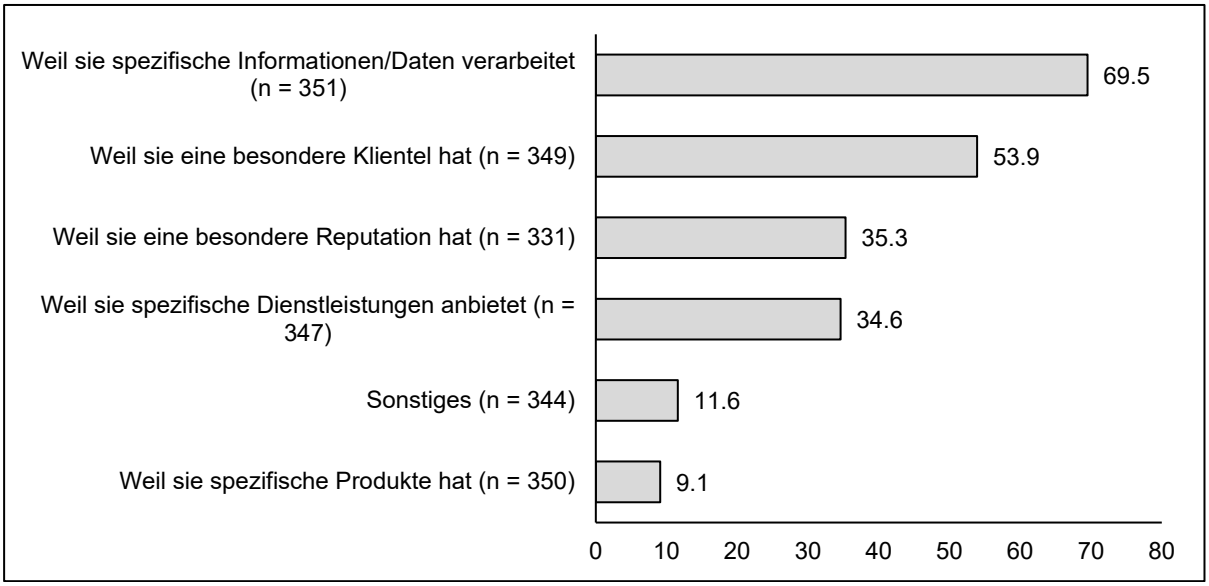
[3] Diese Unterschiede lassen sich teilweise durch den früheren Befragungszeitpunkt erklären: Die Befragung von Dreißigacker et al. (2020) erfolgte bis Januar 2019, die vorliegende Befragung fast 3,5 Jahre später. Dreißigacker et al. (2021) wiederholten ihre Befragung im September 2021, mit bereits höheren Zahlen: So gingen in der zweiten Befragung 50,3 % von einem (eher) hohen Risiko eines ungezielten Angriffs aus, 11,5 % von einem (eher) hohen Risiko eines gezielten Angriffs (S. 50).

gezielten Cyberangriffs ausgesetzt ist; bei kleinen Organisationen waren nur 5,6 % der Befragten dieser Ansicht.

In den Ergebnissen in Tabelle 1 deutet sich zudem an, dass eine öffentliche Einsehbarkeit von Zuständigkeiten usw. (in Bezug auf gezielte Angriffe) sowie die Auslagerung von IT-Funktionen mit einer erhöhten Risikowahrnehmung einher gehen; die Unterschiede sind aber nicht als signifikant einzustufen (bei $p < .10$). Werden die verschiedenen Organisationsbereiche betrachtet, so findet sich für folgende Bereiche eine erhöhte Risikoeinschätzung gezielter Angriffe: Justiz/Straf-/Massnahmenvollzug, Asyl/Migration, Schule/Bildungswesen, Betrieblicher Sozialdienst, Kinderkrippe/Hort und Sozialpädagogische Familienbegleitung (Anteil (eher) hohes Risiko jeweils über 20 Prozent; ohne Abbildung).

Die Befragten wurden zudem gebeten, anzugeben, aus welchen Gründen die Organisation Ziel eines Cyberangriffs werden könnte. Aus Abbildung 5 ist dabei zu entnehmen, dass 69,5 % der Befragten der Ansicht waren, dass spezifische Informationen bzw. Daten hierfür entscheidend sein könnten. Etwas mehr als die Hälfte der Befragten rekurrierte auf die besondere Klientel, die in der Organisation betreut wird (53,9 %). Etwas seltener wurde auf die Reputation oder besondere Dienstleistungen, die die Organisation anbietet, Bezug genommen. Zudem berichteten einige Befragte sonstige Gründe, die in einem offenen Antwortfeld spezifiziert werden konnten. Hier fanden sich u.a. Einträge wie «Zufall», «Zahlungspflichtige (z.B. Alimente) könnten wütend sein», «Weil sie eine Homepage hat und weil wir enorm viel Spam erhalten», «Weil niemand wirklich ein IT-Konzept erstellt und oft manches nicht beachtet wird. (Struktur begünstigt es)», «Weil die Mitarbeiter naiv sind», «Um Geld zu erpressen.» oder «aus Sabotagegründen». Deutlich wird, dass die Gründe auf verschiedenen Ebenen wie den Motiven der Angreifenden, den Kenntnissen bzw. Verhaltensweisen der Mitarbeitenden oder der Exposition durch Sichtbarkeit im Internet verortet werden.

Abbildung 5: Gründe, warum Organisation Ziel eines Cyberangriffs werden könnte (in %)



3.2 Prävalenzraten zu Cyberangriffen

Im Fragebogen wurde nach neun verschiedenen Cyberangriffsformen gefragt. Dabei sollte einerseits mitgeteilt werden, ob die Organisation schon jemals solche Angriffe erlebt hat; andererseits sollte die Häufigkeit von Angriffen in den zurückliegenden zwölf Monaten eingeschätzt werden. Im Folgenden werden nur die Ergebnisse zu den letzten zwölf Monaten berichtet, weil davon ausgegangen wird, dass die Befragten in verlässlicherer Weise die letzten zwölf Monate überblicken können als die gesamte bisherige Existenzdauer der Organisation. Die Cyberangriffsformen wurden dabei im Fragebogen so vorgestellt, wie in Tabelle 2 aufgeführt. Dabei wurde sich mit Ausnahme des Support-Betrugs am Fragebogen von Dreißigacker et al. (2020) orientiert. Diese definieren die verschiedenen Angriffsformen wie folgt (S. 99f):

- Bei einem Ransomware-Angriff wird ein Schadprogramm eingesetzt, das die Daten infizierter Computer oder Netzwerke verschlüsselt und somit für die Nutzer:innen unbrauchbar macht. Damit ist häufig eine Erpressung von Lösegeld (engl. ransom) verbunden.
- Als Spyware werden Programme bezeichnet, die zur Spionage (engl. spying) eingesetzt werden und möglichst unerkannt interne Daten von Unternehmen identifizieren und ausschleusen sollen.
- Unter sonstigen Schadsoftware-Angriffen werden Angriffe mit schädigender Software, wie Viren, Würmer, Trojaner usw. verstanden.
- Manuelles Hacking steht für eine nicht autorisierte Manipulation bzw. Konfiguration von Hard- und Softwareeinstellungen von Computern ohne den Einsatz von Schadprogrammen.
- Ein Denial-of-Service-(DoS-)Angriff zielt auf Web- oder E-Mail-Server von Unternehmen, die mit massenhaften Anfragen oder E-Mail-Sendungen überlastet werden sollen und somit für den regulären Betrieb nicht mehr zur Verfügung stehen.
- Unter Defacing-Angriffen werden unautorisierte Manipulationen von Inhalten der Webpräsenz oder ganzer Webseiten von Unternehmen gefasst.
- Der CEO-Fraud ist eine Form des Betruges (engl. Fraud), bei der unter Verwendung einer falschen Identität einer weisungsbefugten Person des Unternehmens, z.B. der des CEO (Chief Executive Officer), andere Beschäftigte meist mit fingierten E-Mails zu bestimmten Handlungen verleitet werden sollen. Diese Angriffsart hat das Ziel, Menschen zu täuschen bzw. zu manipulieren und wird auch als Social-Engineering bezeichnet.
- Phishing-Angriffe zielen insbesondere darauf ab, an sensible Daten, z.B. Zugangsdaten, Passwörter, Daten von Bankkonten oder Kreditkartendaten, zu gelangen. Dazu werden häufig manipulierte oder gefälschte E-Mails eingesetzt.

Zusätzlich erfragt wurde der Supportbetrug, bei dem die Notwendigkeit von Supportleistungen an der IT vorgetäuscht wird, um bestimmte Handlungen von Mitarbeiterenden zu bewirken. Ebenfalls möglich war, sonstige Cyberangriffe zu berichten. Von dieser Option wurde aber kaum Gebrauch gemacht, weshalb die Ergebnisse hierzu nicht vorgestellt werden.

Wie Tabelle 2 zeigt, hat mit Ausnahme des Phishing mindestens die Hälfte der Organisationen die verschiedenen Angriffsarten in den zurückliegenden zwölf Monaten nicht erlebt. Zusätzlich antwortete jeweils ein recht grosser Anteil der Befragten, dass man nicht weiss, ob es einen entsprechenden Angriff gegeben hat. Diese weiss-nicht-Antworten könnten aus den Auswertungen ausgeschlossen werden, was aber zur Folge hätte, dass die Prävalenzraten steigen und damit wahrscheinlich eine Überschätzung darstellen würden. An dieser Stelle wird daher davon ausgegangen, dass weiss-nicht-Antworten eher darauf hindeuten, dass ein Angriff nicht stattgefunden hat, weil man andernfalls davon erfahren hätte. Weiss-nicht- und nein-Antworten werden daher zusammengefasst.[4] Zudem belegen die Ergebnisse aus Tabelle 2, dass – wiederum mit Ausnahme des Phishing – die Mehrheit der Organisationen einen Angriff nur ein- oder zweimal erlebt hat. Häufige Angriffe sind demgegenüber eher die Ausnahme. Aus diesem Grund werden nachfolgende nur Prävalenzraten berichtet, d.h. der Anteil an Organisationen, die mindestens einmal einen Angriff in den zurückliegenden zwölf Monaten erlebt haben; die Häufigkeit der Angriffe wird nicht weiter betrachtet.

Tabelle 2: Häufigkeit des Erlebens von Cyberangriffen in den letzten zwölf Monaten (in %)

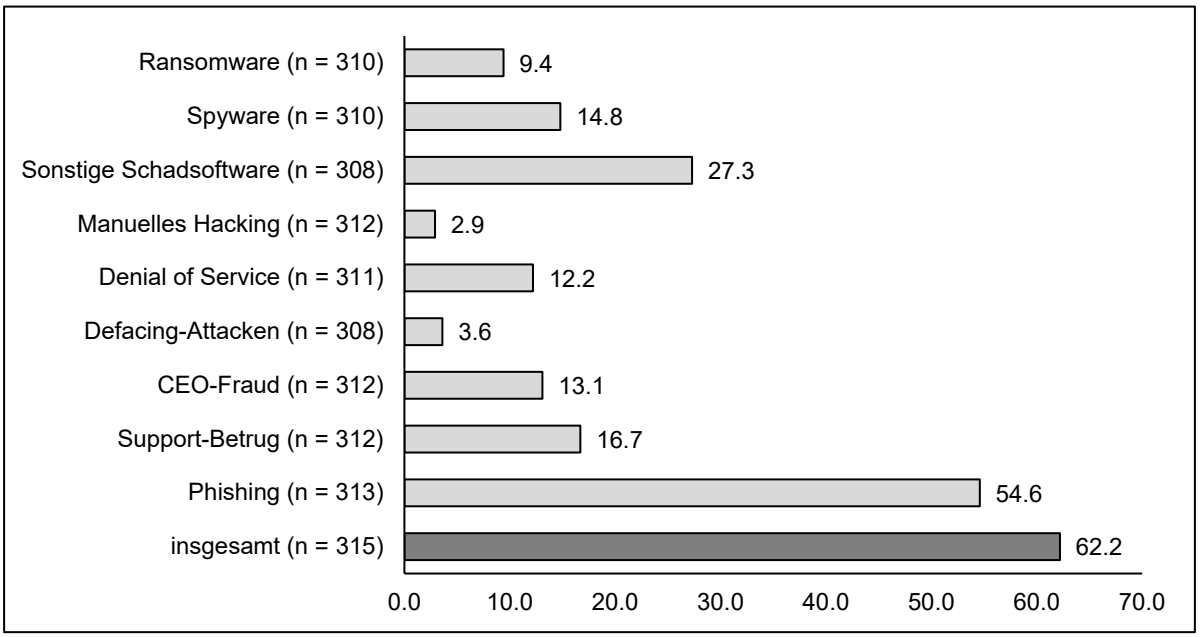
	weiss nicht	**nie**	**1mal**	**2mal**	**3-5mal**	**6-10mal**	**11mal und häufiger**
Ransomware, die das Ziel hatte, Organisationsdaten zu verschlüsseln (n = 310)	17,4	73,2	4,2	1,6	1,3	0,6	1,6
Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen (n = 310)	23,2	61,9	3,2	4,5	2,6	1,0	3,5
Sonstige Schadsoftware – z.B. Viren, Würmer oder Trojaner (n = 308)	18,8	53,9	11,4	5,5	4,5	1,0	4,9
Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware (n = 312)	20,2	76,9	1,6	0,0	0,6	0,0	0,6
Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten (n = 311)	18,6	69,1	7,4	1,0	1,6	0,6	1,6
Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte der Organisation zu verändern (n = 308)	20,8	75,6	1,9	0,6	0,3	0,0	0,6
CEO-Fraud, wobei eine Führungspersönlichkeit der Organisation vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeiterenden zu bewirken (n = 312)	15,4	71,5	5,8	2,6	3,2	1,0	0,6
Support-Betrug, wobei die Notwendigkeit von Supportleistungen an der IT vorgetäuscht wird, um bestimmte Handlungen von Mitarbeiterenden zu bewirken (n = 312)	15,4	67,9	6,7	4,5	1,9	1,0	2,6
Phishing, wobei Mitarbeitende mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Organisationsdaten zu erlangen (n = 313)	14,4	31,0	6,4	11,2	8,6	6,1	22,4

Abbildung 6 stellt die Zwölf-Monats-Prävalenzraten der verschiedenen Cyberangriffsformen dar. Von allen Organisationen haben 62,2 % im letzten Jahr mindestens eine der neun Formen von Cyberangriffen erlebt. Dies unterstreicht, dass Cyberangriffe auch für soziale Organisationen ein bedeutsames Risiko sind. Manuelles Hacking oder Defacing-Attacken kommen mit 2,9 bzw. 3,6 % eher selten vor. Phishing ist demgegenüber recht verbreitet – mehr als jede

[4] Vgl. für ein entsprechendes Vorgehen Isenhardt et al. (2022, S. 9). Nicht auszuschliessen ist freilich, dass trotz weiss-nicht-Antwort nicht doch Angriffe stattgefunden haben. Die hier präsentierten Prävalenzraten könnten daher eine Unterschätzung der tatsächlichen Raten darstellen.

zweite Organisation berichtete davon (54,6 %). Ebenfalls häufiger ist die Infizierung mit Schadsoftware (27,3 %).

Abbildung 6: Zwölf-Monats-Prävalenzraten von Cyberangriffen (in %)



Um die Prävalenzraten einordnen zu können, wird in Tabelle 3 ein Vergleich mit Prävalenzraten anderer Studien vorgenommen, die sich auf Unternehmen konzentrieren, also nicht auf soziale Organisationen. Die Vergleiche sind zudem auch in anderer Hinsicht begrenzt: Isenhardt et al. (2022) berichten nicht 12-Monats- sondern 24-Monatsraten und teilweise wurden die Angriffsformen nicht (dargestellt durch «-») oder in abweichender Form erhoben (in Klammern gesetzte Raten).[5] Trotz dieser Limitationen kann gefolgert werden, dass die Prävalenzraten recht ähnlich ausfallen. Grössere Abweichungen finden sich beim manuellen Hacking und beim CEO-Fraud im Vergleich zur Studie von Isenhardt et al. (2022), die deutlich höhere Raten berichten. Zudem weichen die Zahlen zum Phishing deutlich ab von den Ergebnissen von Dreißigacker et al. (2020). Allerdings findet sich zu dieser Angriffsform ein starker Anstieg in der Befragung ein Jahr später, so dass sich der Unterschied mit dem früheren Zeitpunkt erklären lassen könnte; aktuell scheinen Phishing-Angriffe verbreiteter zu sein, wie auch die Studie von Isenhardt et al. (2022) belegt. Grundsätzlich scheint sich das Risiko von Cyberangriffen auf Soziale Organisationen damit nicht vom Risiko zu unterscheiden, dem Wirtschaftsunternehmen ausgesetzt sind.

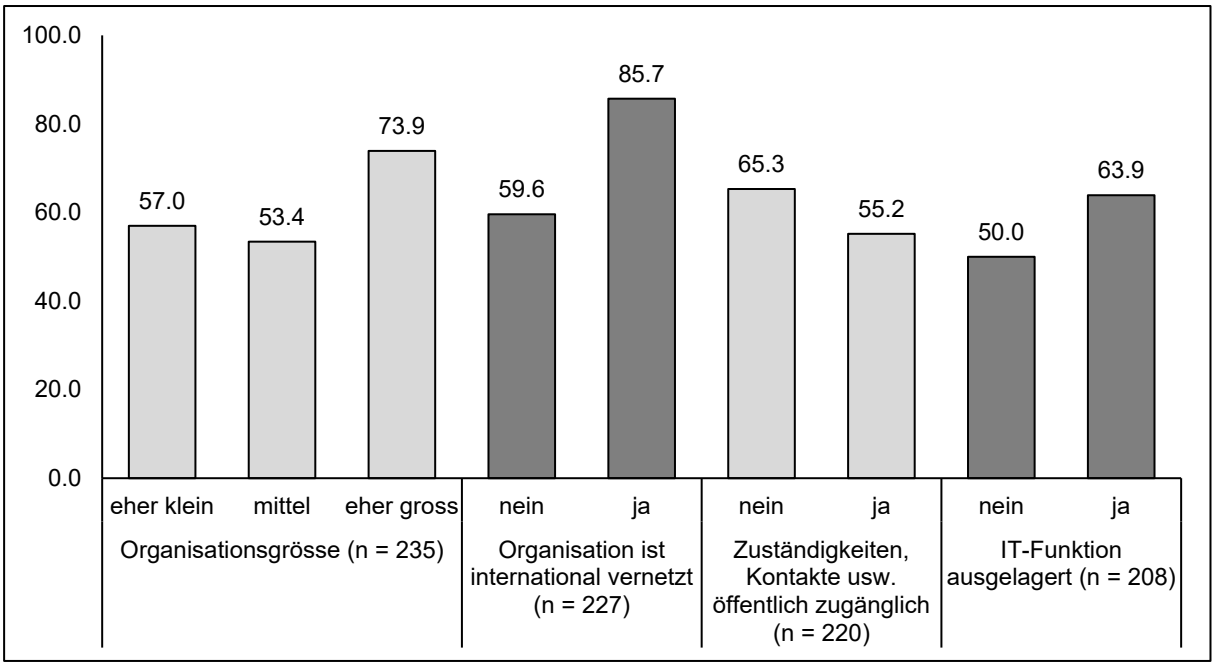
[5] So wird bei Isenhardt et al. (2022) nicht von Support-Betrug, sondern von «Sonstigem Social Engineering» gesprochen. Die Gesamtraten sind ebenfalls nur begrenzt vergleichbar, weil in der Studie von Isenhardt et al. (2022) mehr, in den Studien von Dreißigacker et al. (2020, 2021) weniger Delikte eingehen.

Tabelle 3: Vergleich der Prävalenzraten von Cyberangriffen (in %)

	Jahresprävalenz Soziale Organisationen	2-Jahres-Prävalenz Isenhardt et al. (2022, S. 13)	Jahresprävalenz Dreißigacker et al. (2020, S. 107)	Jahresprävalenz Dreißigacker et al. (2021, S. 54)
Ransomware	9,4	11,3	12,5	14,2
Spyware	14,8	8,4	11,3	16,2
Sonstige Schadsoftware	27,3	20,7	21,3	35,7
Manuelles Hacking	2,9	17,1	2,8	0,4
Denial of Service	12,2	11,5	6,4	8,3
Defacing-Attacken	3,6	-	3,1	0,9
CEO-Fraud	13,1	49,8	8,1	10,6
Support-Betrug	16,7	(16,2)	-	-
Phishing	54,6	43,1	22,0	42,1
insgesamt	**62,2**	**(70,4)**	**(41,1)**	**(59,6)**

Ein Vergleich der Cyberangriffs-Gesamtprävalenzrate für verschiedene Organisationsmerkmale ist in Abbildung 7 dargestellt. Dabei zeigt sich, dass eher grosse Organisationen signifikant häufiger von mindestens einer Form von Cyberangriffen berichten als eher kleine und mittlere Organisationen.[6] International vernetzte Organisationen (unabhängig von der konkreten Vernetzungsform) berichten ebenfalls signifikant häufiger von Cyberangriffen. Für die anderen beiden Merkmale finden sich hingegen keine signifikanten Unterschiede, wenngleich sich andeutet, dass das Auslagern von IT-Funktionen mit einer etwas erhöhten Gesamt-Prävalenzrate einhergeht.

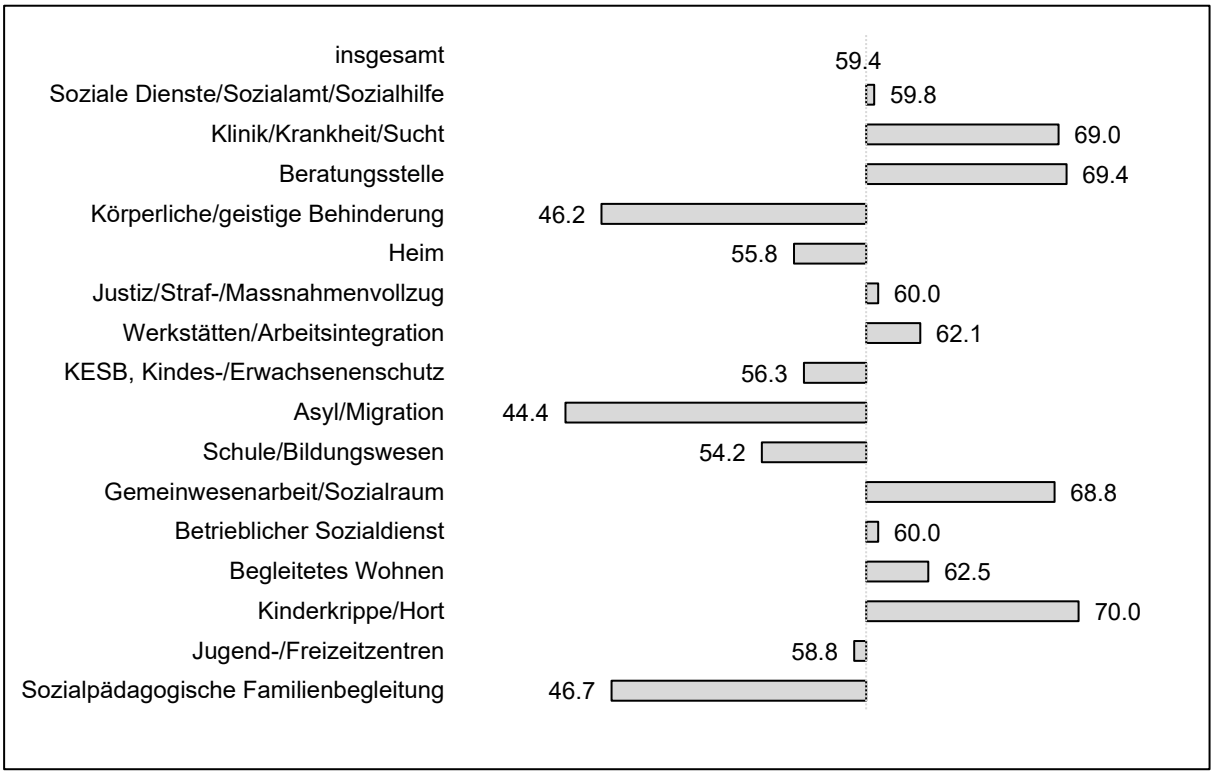
Abbildung 7: Zwölf-Monats-Prävalenzraten von Cyberangriffen insgesamt nach verschiedenen Organisationsmerkmalen (in %)



[6] Dies gilt auch für die einzelnen Angriffsformen, mit Ausnahme von manuellem Hacking, Defacing-Attacken und Support-Betrug.

Die Gesamt-Prävalenzrate wurde auch für die verschiedenen Organisationsbereiche betrachtet. Abbildung 8 berichtet die Ergebnisse.[7] Als Referenzpunkt dient hier die Gesamtrate von 59,4 %. Dese weicht von der oben dargestellten Rate geringfügig ab (62,2 %), weil in die Auswertungen weniger Fälle eingehen, nämlich jene, die Angaben zum Bereich, in dem die Organisation tätig ist, gemacht haben. In Abbildung 8 sind dann die Differenzen der Bereiche zur Gesamtrate aufgeführt. Für vier Bereiche findet sich eine deutlich erhöhte Gesamtrate: Klinik/Krankheit/Sucht, Beratungsstellen, Gemeinwesenarbeit/Sozialraum und Kinderkrippe/Hort. Für drei weitere Bereiche fällt die Gesamtrate hingegen erkennbar niedriger aus: Körperliche/geistige Behinderung, Asyl/Migration und Sozialpädagogische Familienbegleitung.

Abbildung 8: Zwölf-Monats-Prävalenzraten von Cyberangriffen insgesamt nach Organisationsbereich (in %)



Die Befragten wurden zudem gebeten, eine Frage zu beantworten bzw. eine Einschätzung abzugeben. Der Wortlaut war:

- Wurde der Organisation in den letzten 12 Monaten einer der beschriebenen Cyberangriffe angedroht? (Antwortvorgaben: weiss nicht, nein, ja)
- Für wie wahrscheinlich halten Sie es, dass ein Cyberangriff auf die Organisation in den letzten 12 Monaten erfolgt ist, aber nicht bemerkt wurde? (Antwortvorgaben: Sehr unwahrscheinlich, Eher unwahrscheinlich, Eher wahrscheinlich, Sehr wahrscheinlich).

[7] Dargestellt sind alle Bereiche, die in der Befragung aufgeführt wurden, ohne Sonstige-Organisationen bzw. aus den Sonstigen-Antworten nachträglich rekodierte Organisationsbereiche.

Insgesamt gaben 11,3 % der Befragten an, dass ein Angriff angedroht wurde (n = 319); 20,5 % der Befragten stuften es als eher oder sehr wahrscheinlich ein, dass ein Cyberangriff erfolgte, aber unerkannt blieb. Eher kleine, mittlere und eher grosse Organisationen unterscheiden sich hinsichtlich dieser Einschätzungen nicht signifikant voneinander. Auch zwischen den verschiedenen Organisationsbereichen finden sich kaum Unterschiede in Bezug auf die Einschätzungen.

3.3 Schwerwiegendster Cyberangriff

Alle Befragten, die in Bezug auf ihre Organisation angegeben haben, dass diese bereits einmal einen Cyberangriff erlebt hat, wurden gebeten, detaillierte Informationen zum schwerwiegendsten Angriff zu berichten. Wenn der schwerwiegendste Angriff aus mehreren Angriffen bestand, sollte jener Angriff ausgewählt werden, der den höchsten Schaden (materiell oder immateriell bspw. in Form von Reputationsschaden) verursachte. Insgesamt machten 137 Befragte Angaben zu einem schwerwiegendsten Vorfall. In 58 Fällen (42,3 %) handelte es sich um Phishing-Attacken, in 29 Fällen (21,2 %) um Randsomware-Angriffe und in 27 Fällen (19,7 %) um Angriffe mit sonstiger Schadsoftware. Alle anderen Angriffsformen wurden so selten berichtet, dass sie nachfolgend nicht einzeln ausgewiesen werden.[8] Diese Verteilung stimmt in etwa mit der Verteilung in der Studie von Dreißigacker et al. (2020, S. 127) überein, bei denen 26,0 % der schwerwiegendsten Delikte aus Phishing-Attacken, 22,3 % aus Ransomware-Angriffe und 23,5 % aus Angriffen mit sonstiger Schadsoftware bestanden. Nachfolgend werden zentrale Befunde zu diesem schwerwiegendsten Angriff berichtet; dabei werden jeweils die «weiss nicht» Angaben bei der Berechnung von Prozentwerten mitberücksichtigt, so dass die vorgestellten Prozentwerte tendenziell eine Unterschätzung darstellen.

Zeitpunkt: 49,3 % der berichteten Fälle ereigneten sich in den letzten 12 Monaten, 36,6 % davor (14,2 % weiss nicht; n = 134). Nur sehr selten (in 3,0 % der Fälle) wurde der Angriff im Vorhinein angedroht (n = 135).

Aufdeckung: Der Cyberangriff wurde im Wesentlichen durch nicht in der IT angestellte Mitarbeitende (66,4 %) oder durch in der IT angestellte Mitarbeitende (27,0 %) aufgedeckt (n = 137).[9] Durch Klient:innen wurde kein Angriff aufgedeckt. In Bezug auf die Frage, wie der Angriff entdeckt wurde, zeigt sich folgende Verteilung (n = 131):

- durch Eintritt negativer Auswirkungen (Ausfall, Störungen, Erpressungen usw.): 26,7 %; bei Ransomwareattacken war dies häufiger der Fall (50,0 %)
- zufällig: 23,7 %; bei Phishing-Attacken war dies häufiger der Fall (37,0 %)
- durch reguläre/automatisierte Sicherheitsmassnahmen: 22,9 %
- durch Kontrollen/Monitoring: 13,7 %

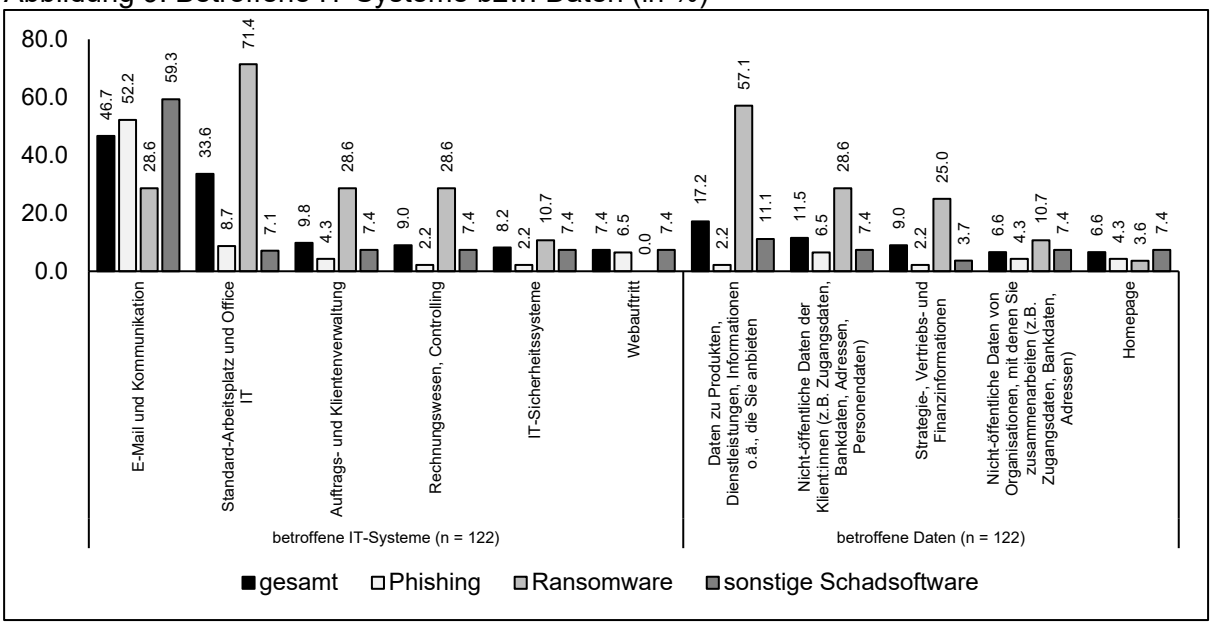
[8] Drei Fälle von Spyware, sechs Fälle manuellen Hackings, fünf Fälle von Denial of Service Attacken, einen Fall von Defacing-Attacken, zwei Fälle von CEO-Fraud und sechs Fälle von Support-Betrug.
[9] Ramsomware-Angriffe wurden dabei häufiger von IT-Mitarbeitenden entdeckt (48,3 %) als Phishing-Attacken (19,0 %) und Angriffe mit sonstiger Schadsoftware (18,5 %).

Täter:innen: Über die Täter:innen können die Befragten meist keine Auskunft geben. Danach gefragt, ob es Vermutungen bzw. Informationen zu den Täter:innen gibt, antworteten 71,4 % mit «nein», 15,9 % mit «weiss nicht» (n = 126). Weitere 7,2 % der Befragten vermuteten «sonstige Personen» wie bspw. Hacker oder Cyberkriminelle. Andere Täter:innen wurde kaum benannt (aktuelle Mitarbeiter:innen: 0,8 %; ehemalige Mitarbeiter:innen: 3,2 %; Person aus Organisation, mit der zusammenarbeitet wird: 0,8 %; aktuelle Klient:innen: 1,6 %; ehemalige Klient:innen: 0,8 %). In jedem zehnten Fall (9,5 %; n = 126) forderten die Täter:innen Lösegeld (meist bei Ransomwareangriffen), und zwar zwischen zwischen 1'000 und 12'000 CHF bzw. 0.16 und 1'400 Bitcoin; dies entspricht insgesamt zwölf Fällen, wobei in einem Fall berichtet wurde, dass das Lösegeld tatsächlich gezahlt wurde (und die Täter:innen den Versprechungen nachgekommen sind).

Infektionswege: Nur für die drei Arten der Ransomware-, Spyware und sonstigen Schadsoftware-Angriffe wurde der vermutete Infektionsweg erfragt (n = 58). Am häufigsten ist demnach die Infektion über E-Mail (72,4 %), gefolgt von der Infektion über Internetseiten (z.B. aktive Inhalte, Downloads; 24,1 %). Andere Wege wurden hingegen deutlich seltener genannt (Speichermedien wie USB, SD-Cards, CD: 5,2 %; mobile Endgeräte wie Net-/Notebooks, Tablets, Smartphones: 3,4 %; aktive Schnittstelle wie WLAN, Bluetooth, NFC: 1,7 %).

Betroffene IT-Systeme/Daten: Abbildung 9 zeigt, dass am häufigsten E-Mail und Standard-Arbeitsplätze von den Angriffen betroffen waren. Dabei gilt, dass bei Ransomware-Angriffen seltener E-Mails, dafür häufiger Standard-Arbeitsplätze betroffen waren. Der Webauftritt oder IT-Sicherheitssysteme waren demgegenüber seltener Ziele der Angriffe. Mit Blick auf die Daten zeigt sich, dass insbesondere Produktdaten und Daten der Klient:innen im Mittelpunkt der Angriffe standen; allerdings sind diese und andere Daten vor allem bei Ramsomewareangriffen betroffen.

Abbildung 9: Betroffene IT-Systeme bzw. Daten (in %)

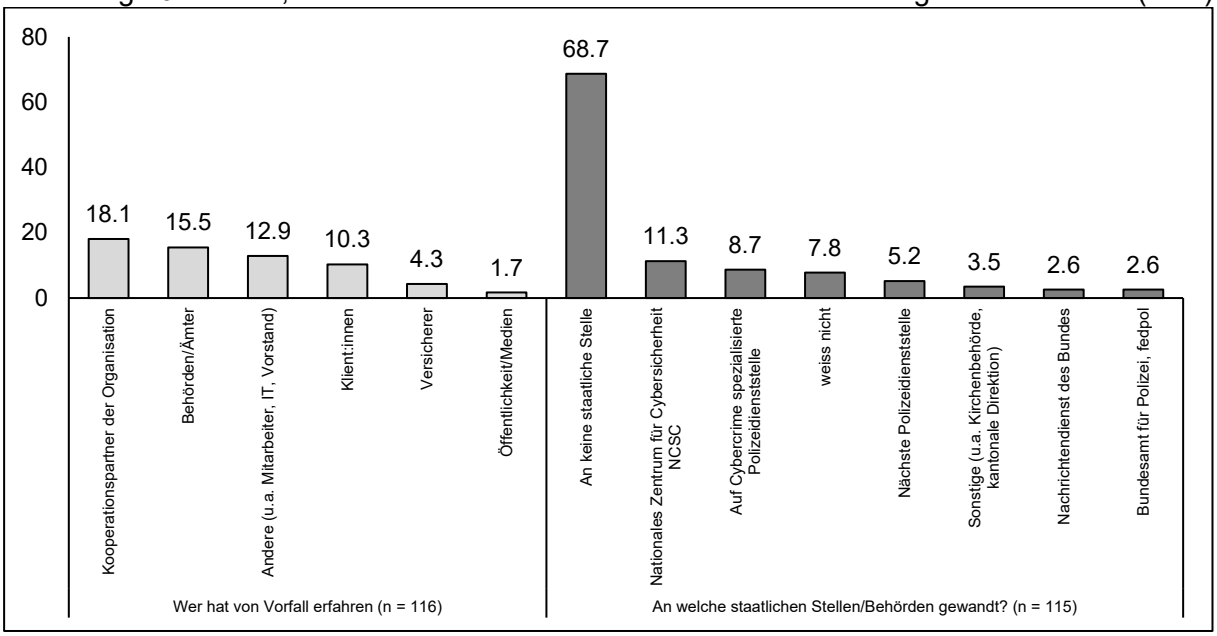


Weitere Schadenseinschätzungen: Von den Befragten wurden drei weitere Einschätzungen bzgl. der Schäden erfragt:

1. finanzielle Kosten: 52,1 % der Befragten berichteten, dass finanzielle Kosten entstanden sind (n = 121), dabei häufiger bei Ransomwareangriffen (75,0 %) und Angriffen mit sonstiger Schadsoftware (66,7 %; Phishing: 30,4 %). Wenn Kosten entstanden sind, dann betrugen diese im Mittel 2'000 CHF (Median; zwischen 50 und 150'000 CHF). Die Kosten wurden dabei nur selten von einer Versicherung gedeckt (zu 6,7 %), d.h. die Organisationen mussten i.d.R. die Kosten selbst tragen. Als Bereiche, in denen Kosten entstanden sind, wurden benannt: Sofortmassnahmen zur Abwehr und Aufklärung (in 76,2 % der Fälle mit Kosten benannt), Wiederherstellung/Wiederbeschaffung (60,3 %), Betriebsunterbrechung (42,9 %) und externe Beratung (z.B. Rechtsberatung, Notfallmanagement; 34,9 %).
2. Auswirkung auf Arbeit der Mitarbeitenden: Fast die Hälfte der Befragten (46,5 %, n = 118) gab ab, dass mindestens ein:e Mitarbeiter:in aufgrund des Vorfalls ihre Arbeit unterbrechen musste (darunter 16,1 % ein:e Mitarbeiter:in; 30,4 % mehr als ein:e Mitarbeiter:in). An der Beseitigung des Vorfalls musste in 71,3 % aller Fälle mindestens eine Person arbeiten (darunter 34,8 % ein:e Mitarbeiter:in; 36,5 % mehr als ein:e Mitarbeiter:in).
3. Allgemeine Schadenseinschätzung: Für drei Bereiche (materieller Schaden Organisation, nicht-materieller Schaden Organisation wie z.B. Reputationsverlust, Schaden bei Dritten wie anderen Organisationen oder Klient:innen) sollte von «kein Schaden» bis «hoher Schaden» eine allgemeine Schadenseinschätzung vorgenommen werden. Wird nur der Anteil an Befragten betrachtet, die mit «mittlerer Schaden» und «hoher Schaden» geantwortet haben, zeigt sich Folgendes (n_{Min} = 111): 8,5 % der Befragten stufen den materiellen Schaden als mittel bis hoch ein, 4,5 % den nicht-materiellen Schaden; 0,9 % geben an, dass bei Dritten ein mittlerer oder hoher Schaden entstanden ist. Die Anteile fallen jeweils bei Ransomwareangriffen am höchsten aus.

Informierte Stellen: Mitgeteilt werden sollte einerseits, welche Stellen bzw. Personengruppen von dem Vorfall erfahren haben. Andererseits sollte mitgeteilt werden, an welche staatlichen Stellen bzw. Behörden man sich wegen des Vorfalls gewendet hat (Mehrfachantworten waren möglich). Abbildung 10 stellt die Ergebnisse zu beiden Fragen dar. Erkennbar ist, dass es eher selten der Fall ist, dass organisationsexterne Stellen bzw. Personengruppen von dem Cyberangriff erfahren. Am häufigsten betrifft dies Kooperationspartner oder andere Behörden/Ämter. In jedem zehnten Fall haben Klient:innen von dem Vorfall erfahren. In mehr als zwei von drei Fällen wurde sich an keine staatliche Stelle gewendet (68,7 %). Wenn sich an eine staatliche Stelle/Behörde gewendet wurde, dann am häufigsten an das Nationale Zentrum für Cybersicherheit (11,3 %).

Abbildung 10: Stellen, die von Vorfall erfahren haben bzw. an die sich gewendet wurde (in %)



Anzeigeverhalten: Zuletzt sollte in Bezug auf den schwerwiegendsten Vorfall mitgeteilt werden, ob dieser bei der Polizei angezeigt wurde. Dies ist den Ergebnissen entsprechend nur selten der Fall: 7,6 % der Befragten gaben an, dass Anzeige erstattet wurde. Diese geringe Anzeigerate ist nicht überraschend: So berichten Dreißigacker et al. (2020, S. 149) bspw. eine Rate von 11,9 %. Im Vergleich der Angriffsformen ist die Anzeigerate bei Ransomwareangriffen am höchsten (19,2 %), bei Angriffen mit sonstiger Schadsoftware am niedrigsten (0,0 %; Phishing: 6,8 %). Je nach Anzeigeverhalten wurden die Befragten um weitere Einschätzungen gebeten:

- Wenn Anzeige erstattet wurde: In drei von vier Fällen wurde berichtet, dass die internen Abläufe durch Ermittlungen nicht gestört wurden; in 71,4 % der Fälle äusserte man Zufriedenheit mit der Arbeit der Polizei. Alle Befragten würden anderen Organisationen empfehlen, einen Cyberangriff anzuzeigen. Gleichwohl zeigt sich, dass in keinem der angezeigten Fälle ein:e Täter:in ermittelt werden konnte.
- Wenn keine Anzeige erstattet wurde: Als Gründe für den Verzicht auf eine Anzeige wurden die fehlende Aussicht auf Ermittlungserfolg (41,2 %) und sonstige Gründe (45,4 %; meist: kein oder zu geringer Schaden) benannt. Deutlich seltener wurde angegeben, dass man nicht wusste, an wen man sich wenden muss (11,3 %) bzw. dass ein Imageschaden zu befürchten war (2,1 %). Folgende Gründe wurden von keinem Befragten benannt: weil Arbeitsbehinderungen zu befürchten waren, weil Behörden Einsicht in vertrauliche Daten fordern könnten und Angst vor Folgekosten.

3.4 Schutzmassnahmen

In einem letzten Fragebogenkomplex wurde erhoben, welche Massnahmen die Organisationen ergreifen, um sich gegen Cyberangriffe zu schützen. In Tabelle 4 sind die 23 erfragten Schutzmassnahmen aufgeführt; zudem finden sich Vergleiche mit anderen Studien, wobei

diese teilweise nicht nach den Massnahmen gefragt haben (kenntlich gemacht durch «-») oder die Massnahmen in etwas veränderter Form erhoben haben (in Klammern gesetzte Anteile). Die Vergleiche, auf die nicht im Detail eingegangen werden soll, machen deutlich, dass auch in Organisationen des Sozialbereichs auf verschiedene Massnahmen häufiger, auf andere Massnahmen seltener zurückgegriffen wird. Ein bedeutsamer Befund ist daneben, dass die Anteile an Organisationen im Sozialbereich, die Massnahmen umsetzen, fast durchgängig niedriger ausfällt als bei Wirtschaftsunternehmen, auf die sich die Vergleichsdaten beziehen. Organisationen des Sozialbereichs schützen sich mithin insgesamt noch etwas seltener als Unternehmen für Cyberangriffen.

Tabelle 4: Häufigkeit verschiedener Schutzmassnahmen (in %)

	nein	weiss nicht	ja	Isenhardt et al. 2022, S. 48ff)	Dreißigacker et al. (2020, S. 73ff)	Dreißigacker et al. (2022, S. 28ff)
regelmässige Backups/Datensicherungen (n = 250)	2,4	3,2	94,4	99,2	98,8	99,6
Schutz der IT-Systeme mit einer Firewall (n = 247)	4,9	6,5	88,7	98,4	98,0	99,9
aktuelle Antivirensoftware (n = 248)	5,2	6,5	88,3	98,8	98,8	98,3
individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe (n = 249)	14,9	2,8	82,3	93,9	84,7	88,2
Mindestanforderungen für Passwörter (n = 249)	18,1	0,4	81,5	(91,9)	86,3	88,7
Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates (n = 249)	12,4	9,2	78,3	(96,3)	(95,7)	90,9
schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit (n = 251)	32,3	5,6	62,2	79,7	66,2	67,8
Verschlüsselung von sensiblen Daten (n = 246)	35,8	10,6	53,7	(53,9)	-	65,2
Zwei-Faktor Authentifizierung (n = 242)	41,7	5,0	53,3	-	-	32,0
Verschlüsselung von Kommunikation (n = 247)	35,2	11,7	53,0	(35,1)	-	60,4
Test der Datenwiederherstellung (Restoring) (n = 243)	28,8	19,3	51,9	-	-	77,4
Speichern von Daten in der Cloud (n = 241)	37,8	11,6	50,6	-	-	-
Risiko- und Schwachstellenanalyse (n = 243)	42,4	13,6	44,0	(69,5)	(51,6)	39,3
Netzwerksegmentierung (n = 244)	26,6	29,5	43,9	-	-	62,6
Verstärkte physische Sicherheit (n = 242)	41,3	20,2	38,4	(86,8)	-	56,2
schriftlich fixierte Richtlinien zum Notfallmanagement bei Cyberangriff (n = 244)	56,1	13,1	30,7	74,6	54,9	48,4
Zertifizierung der IT-Sicherheit (n = 242)	57,4	12,8	29,8	-	24,8	5,7
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme (n = 245)	69,8	11,8	18,4	67,1	25,0	30,7
Informationssicherheitsmanagementsystem (ISMS) (n = 243)	46,9	35,4	17,7	64,2	-	15,2
Austausch von Bedrohungsdaten (z.B. Threat Intelligence) (n = 242)	48,3	34,7	16,9	-	-	21,2
Security Information and Event Management (SIEM) (n = 245)	44,5	40,0	15,5	-	-	21,6
Security Operation Center (SOC) (n = 243)	47,7	38,7	13,6	-	-	11,6
Künstliche Intelligenz basierte Massnahmen (n = 243)	56,0	33,3	10,7	-	-	14,6

Wird sich im Folgenden nur auf die Organisationen des Sozialbereichs konzentriert, so zeigt sich, dass etwa neun von zehn Organisationen auf diese drei Massnahmen zurückgreifen: regelmässige Backups/Datensicherungen[10], Schutz der IT-Systeme mit einer Firewall und

[10] Dabei erfolgen in 65,4 % der Fälle die Backups täglich, in 16,7 % wöchentlich; in 81,6 % der Fälle werden die Backups physisch getrennt aufbewahrt.

Nutzung aktueller Antivirensoftware. In acht von zehn Organisationen kommen diese Massnahmen zum Einsatz: individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe, Mindestanforderungen für Passwörter und aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates. Nur ein kleiner Teil der Organisationen greift demgegenüber auf Massnahmen der künstlichen Intelligenz, des Security Information and Event Management[11] sowie ein Security Operation Center[12] zurück.

Tabelle 5 berichtet zudem, wie häufig in den verschiedenen Organisationsbereichen auf die Schutzmassnahmen zurückgegriffen wird. Zur besseren Lesbarkeit wurden die drei niedrigsten Anteilwerte je Massnahme unterstrichen, die drei höchsten fett dargestellt. Dadurch wird sichtbar, dass in folgenden Bereichen insgesamt häufiger auf Schutzmassnahmen zurückgegriffen wird: Justiz/Straf-/Massnahmenvollzug, KESB, Betrieblicher Sozialdienst und Kinderkrippe/Hort. Demgegenüber stehen Bereiche, in denen unterdurchschnittlich häufig Schutzmassnahmen umgesetzt werden; hierzu gehören Beratungsstellen, die Gemeinwesenarbeit und der Bereich Jugend-/Freizeitzentren. Für die Bereiche Beratungsstellen und Gemeinwesenarbeit hatten sich entsprechend Abbildung 8 erhöhte Prävalenzraten für Cyberangriffe ergeben; dies ist ein Hinweis darauf, dass seltenere Schutzmassnahmen und häufigere Betroffenheit von Cyberkriminalität miteinander einhergehen können.

Ebenfalls geprüft wurde, ob die Häufigkeit von Schutzmassnahen mit der Grösse der Organisation in Verbindung steht. Mit Ausnahme einiger weniger Massnahmen (Zertifizierung der IT-Sicherheit, regelmässige Backups/Datensicherungen, aktuelle Antivirensoftware, Schutz der IT-Systeme mit einer Firewall, Speichern von Daten in der Cloud) ist es jeweils der Fall, dass eher grosse Organisationen signifikant häufiger Massnahmen umsetzen als eher kleine Organisationen. Je grösser eine Organisation ist, umso eher stehen anscheinend Ressourcen für den Schutz vor Cyberkriminalität zur Verfügung.

[11] Vgl. z.B. https://www.computerweekly.com/de/definition/Security-Information-and-Event-Management-SIEM.
[12] Vgl. z.B. https://www.splunk.com/de_de/data-insider/what-is-a-security-operations-center.html

Tabelle 5: Häufigkeit verschiedener Schutzmassnahmen nach Organisationsbereich (in %)

	Soziale Dienste/Sozialamt/Sozialhilfe	Klinik/Krankheit/Sucht	Beratungsstelle	Körperliche/geistige Behinderung	Heim	Justiz/Straf-/Massnahmenvollzug	Werkstätten/Arbeitsintegration	KESB, Kindes-/Erwachsenenschutz	Asyl/Migration	Schule/Bildungswesen	Gemeinwesenarbeit/Sozialraum	Betrieblicher Sozialdienst	Begleitetes Wohnen	Kinderkrippe/Hort	Jugend-/Freizeitzentren	Sozialpädagogische Familienbegleitung
regelmässige Backups/Datensicherungen	97.6	93.1	96.8	96.2	97.7	**100.0**	**100.0**	**100.0**	88.9	95.9	96.9	**100.0**	**100.0**	**100.0**	**100.0**	93.3
Schutz der IT-Systeme mit einer Firewall	87.8	82.1	88.7	96.0	97.6	**100.0**	93.1	**100.0**	**100.0**	91.8	81.3	80.0	95.7	**100.0**	70.6	**100.0**
aktuelle Antivirensoftware	87.7	89.3	90.2	**100.0**	97.6	92.9	93.1	**100.0**	**100.0**	93.8	86.7	**100.0**	95.8	**100.0**	81.3	92.9
individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe	86.6	93.1	88.9	88.5	93.0	93.3	93.3	93.3	**100.0**	89.8	71.9	**100.0**	**95.8**	80.0	76.5	86.7
Mindestanforderungen für Passwörter	91.5	82.8	79.4	84.6	86.1	86.7	86.7	**100.0**	**100.0**	95.9	78.1	**100.0**	83.3	80.0	88.2	73.3
Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates	78.1	75.9	72.6	88.5	90.7	93.3	86.7	**100.0**	**100.0**	83.7	81.3	**100.0**	83.3	90.0	76.5	80.0
schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit	66.3	82.8	57.1	69.2	79.1	**93.3**	**96.7**	81.3	77.8	71.4	56.3	**100.0**	87.5	90.0	64.7	73.3
Verschlüsselung von sensiblen Daten	56.8	66.7	53.2	57.7	64.3	73.3	75.9	73.3	**88.9**	63.3	53.1	**100.0**	**78.3**	60.0	64.7	53.3
Zwei-Faktor Authentifizierung	63.0	53.6	54.1	64.0	58.5	66.7	50.0	78.6	**88.9**	61.7	68.8	**80.0**	34.8	**80.0**	76.5	66.7
Verschlüsselung von Kommunikation	59.8	75.9	52.4	50.0	61.9	**86.7**	75.9	**86.7**	**88.9**	65.3	43.8	80.0	69.6	70.0	52.9	73.3
Test der Datenwiederherstellung (Restoring)	61.3	60.7	51.6	73.1	61.9	**80.0**	75.0	**80.0**	77.8	**81.6**	40.0	60.0	60.9	**80.0**	56.3	73.3
Speichern von Daten in der Cloud	52.6	37.0	51.7	**60.0**	53.7	**66.7**	59.3	53.9	44.4	**63.8**	46.9	40.0	47.8	**60.0**	52.9	57.1
Risiko- und Schwachstellenanalyse	48.8	46.4	50.8	42.3	54.8	**60.0**	55.6	**78.6**	55.6	54.2	45.2	**60.0**	47.8	**70.0**	37.5	53.3
Netzwerksegmentierung	46.3	53.6	47.5	52.0	68.3	**85.7**	74.1	**85.7**	75.0	72.9	41.4	60.0	52.2	**100.0**	50.0	78.6
Verstärkte physische Sicherheit	38.0	48.2	45.0	48.0	56.1	**71.4**	**65.4**	**76.9**	37.5	56.3	30.0	40.0	43.5	50.0	20.0	35.7
schriftlich fixierte Richtlinien zum Notfallmanagement bei Cyberangriff	41.8	42.9	29.5	30.8	35.7	53.3	50.0	53.3	**66.7**	42.9	45.2	**60.0**	39.1	**60.0**	43.8	40.0
Zertifizierung der IT-Sicherheit	41.8	37.0	38.3	33.3	29.0	60.0	42.3	**61.5**	55.6	39.6	32.3	**80.0**	30.4	**70.0**	37.5	50.0
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	30.4	34.6	28.8	16.0	14.6	**35.7**	23.1	23.1	**50.0**	31.3	26.7	**80.0**	17.4	33.3	26.7	28.6
Informationssicherheitsmanagementsystem (ISMS)	25.3	33.3	23.0	33.3	25.0	50.0	25.9	**53.9**	50.0	29.8	29.0	**80.0**	17.4	**55.6**	25.0	50.0
Austausch von Bedrohungsdaten (z.B. Threat Intelligence)	25.3	25.9	25.4	28.0	19.5	35.7	26.9	**38.5**	25.0	27.7	26.7	**40.0**	17.4	**44.4**	26.7	28.6
Security Information and Event Management (SIEM)	22.5	28.6	26.2	26.9	21.4	33.3	25.9	42.9	**55.6**	34.7	25.8	**60.0**	8.7	**80.0**	37.5	53.3
Security Operation Center (SOC)	20.0	25.0	21.7	32.0	17.1	**40.0**	26.9	**42.9**	33.3	25.0	22.6	**40.0**	13.0	**60.0**	25.0	**40.0**
Künstliche Intelligenz basierte Massnahmen	10.3	3.9	6.8	12.0	**17.1**	14.3	3.9	15.4	12.5	12.8	**16.7**	**20.0**	8.7	11.1	6.7	14.3

Zum Thema Sicherheit wurden noch drei weitere Aspekte erhoben: 1. das Verfügen über eine Versicherung; 2. Das Informationsverhalten zu Sicherheitsthemen; 3. Das organisationale Sicherheitsbewusstsein.

Versicherung: Auf die Frage, ob für die Organisation eine Versicherung gegen Informationssicherheitsverletzungen existiert, antworten 16,9 % mit «ja», 30,5 % mit «weiss nicht» (52,6 % «nein»; n = 249).[13] In eher grossen Organisationen (21,4 %) wurde dies häufiger bejaht als in

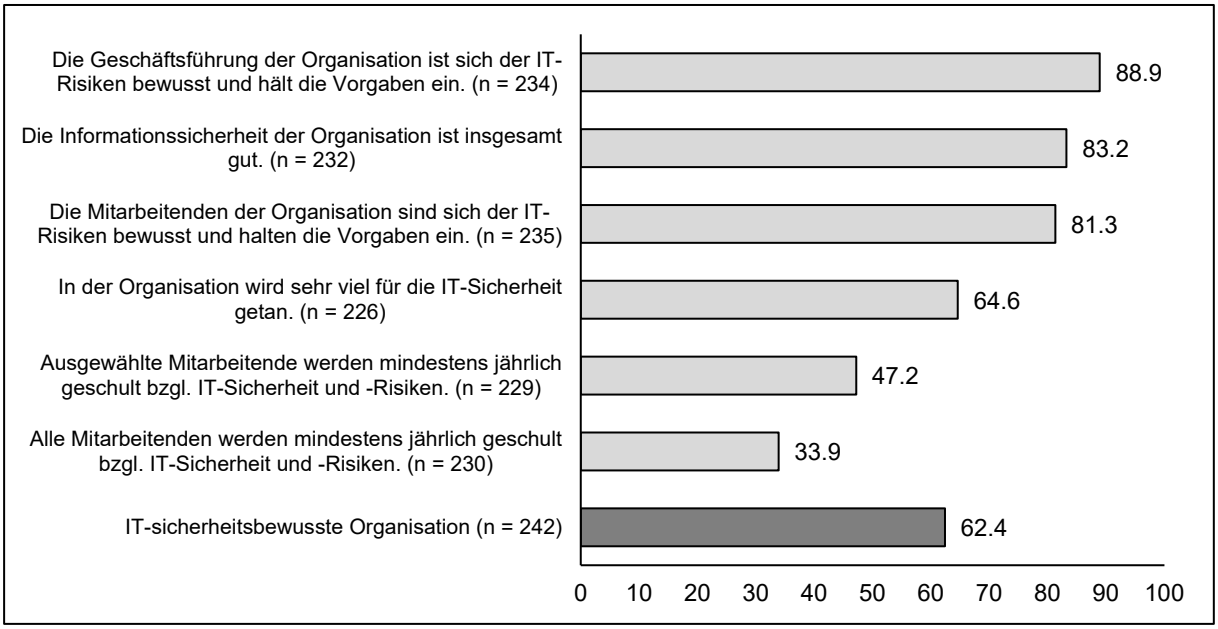
[13] In der Befragung von Dreißigacker et al. (2020, S. 84) gaben 17,9 % der Unternehmen an, eine solche Versicherung zu besitzen. In der Befragung ein Jahr später stieg dieser Anteil aber auf 24,4 % (Dreißigacker et al., 2021, S. 31). Es kann daher gefolgert werden, dass die Abdeckung mit entsprechenden Versicherungen im Bereich Soziale Organisationen eher unterdurchschnittlich ausfällt.

eher kleinen Organisationen (9,7 %). Organisationen, die eine Versicherung haben, würden sie zu 64,3 % weiterempfehlen (Rest: «weiss nicht»). Nur drei Organisationen mussten bereits Leistungen der Versicherung in Anspruch nehmen, die sie auch erhalten haben und bei denen der entstandene Schaden gedeckt wurde. Auf die Frage, warum eine Organisation bislang keine solche Versicherung hat (n = 131), wurde wie folgt geantwortet: 39,7 % haben sich noch nicht damit beschäftigt, 26,7 % gaben einen sonstigen Grund an (z.B. wird sich aktuell damit beschäftigt, oder die Versicherung wird nicht als sinnvoll oder nötig eingestuft), für 24,4 % stimmt das Preis-Leistungs-Verhältnis nicht.

Informationsverhalten: Die Befragten wurden gebeten, mitzuteilen, an wen sie sich wenden, um Informationen zur IT- und Informationssicherheit einzuholen. Am häufigsten wurde dabei angegeben, dass sich an Beratungsdienstleister gewendet wird (57,4 %, n = 139). Die Internetrecherche (36,8 %), IT-Sicherheitssoftwarehersteller (32,6 %), staatliche Institutionen (z.B. Nachrichtendienst des Bundes, Polizei, Bundesamt für Informatik und Telekommunikation, 28,5 %) und Fachliteratur/Fachzeitschriften (26,9 %) werden ebenfalls noch häufiger konsultiert. In 20,2 % der Fälle wurden sonstige Informationswege benannt, wobei u.a. auf IT-Dienstleister oder private Netzwerke verwiesen wurde. Berufsverbände (z.B. AvenirSocial) wurden sehr selten als Anlaufstelle benannt (5,8 %).

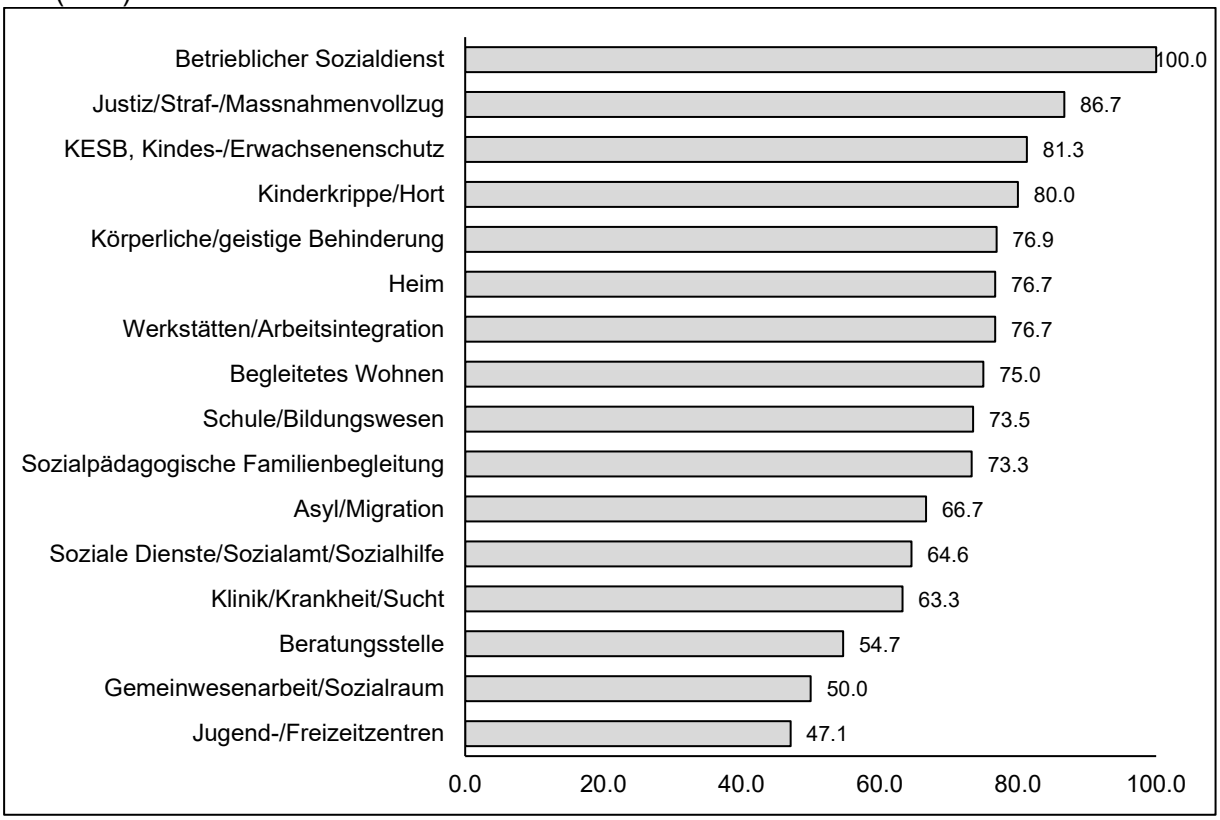
Sicherheitsbewusstsein: Um das organisationale Sicherheitsbewusstein zu messen, wurden den Befragten sechs Items zur Beantwortung vorgelegt, die in Abbildung 11 aufgeführt sind. Dargestellt ist dabei jeweils der Anteil an Befragten, die mit «trifft eher zu» oder «trifft voll und ganz zu» geantwortet haben. Am häufigsten wird den Aussagen zugestimmt, dass sich die Geschäftsführung der Organisation der IT-Risiken bewusst ist, dass gleiches auch für die Mitarbeitenden gilt und dass die Informationssicherheit in der Organisation alles in allem gut ist. Dass es in der Organisation regelmässige Schulungen zur IT-Sicherheit gibt, wird hingegen nur von der Minderheit der Befragten bejaht.

Abbildung 11: Zustimmung zu Items des Sicherheitsbewusstsein (in %)



Die sechs Items korrelieren hoch miteinander; die Reliabilität der Skala kann mit Cronbachs Alpha = .83 als ausreichend eingestuft werden. Aus den Antworten wurde daher der Mittelwert gebildet; Mittelwerte über 2,5 werden als Zustimmung gewertet (die Antworten reichten von «1 – trifft gar nicht zu» bis «4 – trifft voll und ganz zu»). Wie Abbildung 11 zu entnehmen ist, wird in etwa zwei von drei Organisationen das Sicherheitsbewusstsein als (eher) hoch eingestuft (62,4 %). Erneut ist die Grösse einer Organisation ein Merkmal, welches mit dieser Einschätzung signifikant zusammenhängt: In eher kleinen Organisation bestätigen 45,7 % ein entsprechendes Bewusstsein, in eher grossen Organisationen 72,9 % (mittlere Organisation: 71,6 %). Zudem findet sich in folgenden drei Organisationsbereichen ein stärker ausgeprägtes Bewusstsein: Justiz/Straf-/Massnahmenvollzug, KESB/Kindes-/Erwachsenenschutz und betrieblicher Sozialdienst (vgl. Abbildung 12). Die drei Bereiche mit den geringsten Anteilen an Befragten, die ein hohes Bewusstsein attestieren, sind demgegenüber Beratungsstellen, Gemeinwesenarbeit/Sozialraum und Jugend-/Freizeitzentren.

Abbildung 12: Anteil Befragte, die Organisation (eher) hohes Sicherheitsbewusstsein attestieren (in %)



4 Fazit

Die vorliegende Studie untersucht erstmalig für die Schweiz das Thema Cyberkriminalität für Organisationen des Sozialbereichs. Die bisherige Forschung konzentriert sich auf Wirtschaftsunternehmen und hier meist auf Kleine und Mittlere Unternehmen, was sich u.a. damit erklären lässt, dass der Schaden, den Cyberkriminalität bei diesen Unternehmen anrichten kann, im Zweifelsfall existenziell ist. Um Informationen zu Organisationen des Sozialbereichs zu erhalten, wurde eine Online-Befragung durchgeführt, die sich weitestgehend auf Organisationen aus dem Kanton Zürich beschränkte. Auf Basis des Adressverzeichnisses der am Departement für Soziale Arbeit der ZHAW geführten Infostelle konnten entsprechende Organisationen zur Befragung eingeladen werden. Diese Basis ist weder vollständig noch systematisch erstellt worden, weshalb die Stichprobe als Gelegenheitsstichprobe zu klassifizieren ist, die keinen Anspruch auf Repräsentativität erhebt. Dies schränkt die vorgestellten Ergebnisse zweifellos ein. Eine weitere Einschränkung ist, dass nur etwa jede sechste eingeladene Organisation an der Befragung teilgenommen hat (Rücklaufquote 17,5 %). Zwar liegt auch in vergleichbaren Befragungen die Rücklaufquote selten deutlich höher; es kann aber nicht ausgeschlossen werden, dass sich gerade solche Organisationen beteiligt haben, die ein höheres Interesse an der Thematik haben, bspw. weil sie Cyberangriffe erlebt haben. Zu wünschen ist deshalb, dass in weiteren, bestenfalls repräsentativ angelegten Befragungen die hier vorgestellten Ergebnisse einer Prüfung unterzogen werden.

Die befragten Organisationen gehören häufiger den Bereichen Soziale Dienste, Beratungsstellen und Schulen an. Eher seltener handelte es sich um Organisationen aus den Bereichen Kinderkrippe/Hort, Asyl/Migration und betrieblicher Sozialdienst. Die Varianz der Organisationen hinsichtlich verschiedener Merkmale ist gross: So nahmen Organisationen mit weniger als sechs Mitarbeitenden ebenso teil wie Organisationen mit über 100 Mitarbeitenden; Antworten liegen von Organisationen vor, die wenige Klient:innen betreuen, aber ebenso von Organisationen, die über 500 Klient:innen betreuen. Es kann daher davon ausgegangen werden, dass mit der Stichprobe eine gewisse Bandbereite an Organisationen des Sozialbereichs abgebildet wurde.

Ein zentrales Ergebnis der Befragung ist, dass das Risiko, Cyberkriminalität zu erfahren, für Organisationen des Sozialbereichs ähnlich hoch ausfällt wie für Wirtschaftsunternehmen. Zwar sind die Vergleiche zu anderen Studien in verschiedener Hinsicht begrenzt: Teilweise sind diese bereits etwas älter, erfassten Cyberangriffe in etwas veränderter Form oder bezogen ihre Prävalenzraten auf andere Zeiträume. Dennoch lässt sich im Grossen und Ganzen ein vergleichbares Ausmass an Viktimisierung feststellen. So gaben 62,2 % der befragten Organisationen des Sozialbereichs an, mindestens eine der insgesamt neun erhobenen Formen von Cyberangriffen in den letzten zwölf Monaten erlebt zu haben. Bei Dreißigacker et al. (2021, S. 54) wird für deutsche Unternehmen eine Rate von 59,6 % berichtet, bei Isenhardt et al. (2022, S. 12) eine Rate von 70,4 % für Schweizer Unternehmen. Phishing-Attacken sind die am häufigsten vorkommende Form von Cyberangriffen, gefolgt von Angriffen mit sonstiger Schadsoftware und Support-Betrug.

Grössere Organisationen sind entsprechend der vorliegenden Ergebnisse häufiger Ziel von Cyberattacken, was möglicherweise damit in Zusammenhang steht, dass sie attraktivere Ziele für Cyberkriminelle sind. Möglicherweise werden die Angriffe aber auch hier häufiger erkannt, insofern hier häufiger Massnahmen zur Abwehr bzw. Entdeckung von Angriffen implementiert sind. Je stärker eine Organisation international vernetzt ist, umso eher hat sie Cyberangriffe erlebt. Obwohl dieser Befund als signifikant ausgewiesen wird, sollte er an dieser Stelle nicht vertieft interpretiert werden, weil ihm wenige Fälle zugrunde liegen. Organisationen des Sozialbereichs sind sehr selten international vernetzt: Nur 6,1 % aller Organisationen bestätigten dies in der Befragung. Bedeutsamer als der Befund zur Vernetzung ist der Befund zur differenziellen Betroffenheit von Organisationen je nach Tätigkeitsbereich. Für vier Bereiche findet sich eine deutlich erhöhte Gesamtrate (Klinik/Krankheit/Sucht, Beratungsstellen, Gemeinwesenarbeit/Sozialraum und Kinderkrippe/Hort); für drei weitere Bereiche fällt die Gesamtrate hingegen unterdurchschnittlich aus (Körperliche/geistige Behinderung, Asyl/Migration und Sozialpädagogische Familienbegleitung). Wie sich diese Unterschiede genau erklären lassen, konnte im Rahmen der hier vorgelegten Analysen nicht im Detail geklärt werden. Auffällig ist aber bspw., dass Beratungsstellen und die Gemeinwesenarbeit seltener von der Implementation von Schutzmassnahmen berichten und hier auch ein geringeres Sicherheitsbewusstsein beobachtet wurde. Möglicherweise geht eine noch geringer ausgebildete Sensibilität für die Cyberkriminalitätsthematik in diesen Bereichen mit einer erhöhten Vulnerabilität einher.

Dass es einer Aufmerksamkeit für Cyberattacken bedarf, unterstreichen die Befunde zu den durch sie angerichteten Schäden. Zwar sollte in der Befragung das schwerwiegendste erlebte Delikt im Detail beschrieben werden, also ein Delikt, das per se einen höheren Schaden verursachte – nicht jeder Cyberangriff führt zu entsprechenden Schäden. Dennoch geben die Befunde einen Hinweis, welche Schäden in bestimmten Fällen zu erwarten sind. In mehr als der Hälfte der schwerwiegendsten Delikte entstand ein finanzieller Schaden, der im Mittel 2'000 CHF betrug. Zusätzlich mussten nicht wenige Mitarbeitende ihre Arbeit unterbrechen; andere Mitarbeitende mussten Zeit aufwenden, um den Angriff zu bearbeiten; auch hierdurch entstehen einer Organisation Kosten. Dennoch scheinen diese eher selten wirklich existenziell zu sein: 8,5 % der Befragten stuften den erlittenen materiellen Schaden als mittel bis hoch ein, 4,5 % den nicht-materiellen Schaden (also z.B. den Reputationsverlust). Damit zusammen hängt dann auch, dass die Delikte selten angezeigt werden: 7,6 % der schwerwiegendsten Delikte wurden bei der Polizei angezeigt. Als Gründe für eine Nicht-Anzeige wurde u.a. genannt, dass kein oder nur ein geringer Schaden vorlag; ebenfalls häufiger wurde auf die fehlende Aussicht auf Ermittlungserfolg verwiesen. Der fehlende Ermittlungserfolg bestätigt sich dabei auch in der Befragung, insofern in keinem Fall von erstatteter Anzeige ein:e Täter:in ermittelt werden konnte.

Ein Schwerpunkt der Befragung galt der Frage, welche Schutzmassnahmen die Organisationen umsetzen. Die Befunde lassen sehr allgemein ausgedrückt die Folgerung zu, dass die Organisationen hier noch aktiver werden können, insofern sie im Vergleich mit Wirtschaftsunternehmen etwas schlechter abschneiden. Zwar werden verschiedene Massnahmen von mindestens acht von zehn Organisationen umgesetzt (regelmässige Backups/Datensicherungen, Schutz der IT-Systeme mit einer Firewall, aktuelle Antivirensoftware, individuelle Vergabe von

Zugangs- und Nutzerrechten je nach Aufgabe, Mindestanforderungen für Passwörter, aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates); bei Vergleichsbefragungen zu Unternehmen finden sich diese Massnahmen aber bei mindestens neun von zehn Unternehmen. Auch Versicherungen gegen Informationssicherheitsverletzungen finden sich in Organisationen des Sozialbereichs seltener als in Unternehmen. Möglicherweise schätzen die Organisationen des Sozialbereichs ihre Situation daher als zu optimistisch ein: Für etwa zwei von drei Organisationen ergibt sich auf Basis verschiedener Einschätzungen zu Mitarbeitenden und Vorgesetzten ein eher hoch ausgeprägtes Bewusstsein. Die Befunde zu den Schutzmassnahmen wie auch einzelne Einschätzungen bspw. zur Fortbildungskultur in den Organisationen unterstreichen aber, dass es noch Handlungsbedarf gibt. Um diesen Handlungsbedarf zu erkennen und zu beheben, braucht es sicherlich auch Impulse und Informationen von aussen. Dies könnte auch eine Aufgabe von Berufsverbänden der Sozialen Arbeit sein. Diese werden bislang noch sehr selten zu Rate gezogen, wenn man Informationen zu Fragen der IT-Sicherheit benötigt. Dienstleister:innen, eigene Recherchen oder Unterstützung aus dem privaten Netzwerk sind hierfür deutlich wichtiger. Wenn das Thema Cyberkriminalität in sozialen Organisationen aber noch weitere Aufmerksamkeit benötigt (insbesondere die Frage des Schutzes vor Angriffen), dann wäre es sicherlich wichtig, wenn es auch auf übergeordneter Ebene, also auf Ebene der Verbände, verstärkt Aufmerksamkeit erhält und wenn auf dieser Ebene weitere Angebote für die einzelnen, teilweise kleinen und auf Unterstützung angewiesenen Organisationen zur Verfügung gestellt werden.

Literatur

Baier, D. (2020). Cybercrime-Opfererfahrungen in der Schweiz. *Kriminalistik, 74*(6), 407-413.

Baier, D., Biberstein, L. & Markwalder, N. (2022). *Kriminalitätsopfererfahrungen der Schweizer Bevölkerung: Entwicklungen im Dunkelfeld 2011 bis 2021*. Zürich: Zürcher Hochschule für Angewandte Wissenschaften.

Dreißigacker, A, von Skarczinski, B. & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*. Hannover: KFN-Forschungsbericht Nr. 152.

Dreißigacker, A, von Skarczinski, B. & Wollinger, G. R. (2021). *Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020*. Hannover: KFN-Forschungsbericht Nr. 162.

Isenhardt, A., Frey, L. & Hostettler, U. (2022). *Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe. Auswertungsbericht zuhanden des Verbands Swissmem*. Bern: Universität Bern – Institut für Strafrecht und Kriminologie. http://dx.doi.org/10.48350/172496.

Mändli Lerch, K. & Repic, A. (2017). *Cyberrisiken in Schweizer KMUs. Befragung von GeschäftsführerInnen Schweizer KMUs*. Zürich: gfs-zürich.

Meier, D.A. & Burda, D. (2020). Cybersicherheit als Führungsaufgabe in Schweizer KMU. Herausforderungen und Chancen im Zuge der Digitalisierung. In J. Schellinger, K. Tokarski & I. Kissling-Näf (Hrsg.), *Digitale Transformation und Unternehmensführung* (83-104). Wiesbaden: Springer.

Peter, M. K., Hölzli, A., Kaelin, A. W. Mändli Lerch, K., Vifian, P. & Wettstein, N. (2020). *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU: Ein Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4-49 Mitarbeitenden im Umfeld von Corona (COVID-19)*. Bern: Die Mobiliar, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-Zürich.

Pugnetti, C. & Casián, C. (2021). *Cyberrisiken und Schweizer KMU. Eine Untersuchung der Einstellungen von Mitarbeitenden und verhaltensbedingter Anfälligkeiten*. Zürich: Zürcher Hochschule für Angewandte Wissenschaften.

Zwahlen, F., Marti, I., Richter, M., Konopatsch, C. & Hostettler, U. (2020). *Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB)*. Bern: Universität Bern.

Zürcher Hochschule
für Angewandte Wissenschaften

Departement Soziale Arbeit

Institut für Delinquenz und Kriminalprävention

Pfingstweidstrasse 96
Postfach 707
CH-8005 Zürich

Telefon +41 58 934 89 04
Idk.sozialearbeit@zhaw.ch
www.zhaw.ch/sozialearbeit