Einführung eines KMU-CERTs in Österreich

Edith Huber[1] · Bettina Pospisil[1] · Otto Hellwig[2]
Wolfgang Rosenkranz[3]

[1]Donau-Universität Krems
{edith.huber | bettina.pospisil}@donau-uni.ac.at

[2]SBA-Research
otto.hellwig@a1.net

[3]Repuco
wolfgang.rosenkranz@repuco.at

Zusammenfassung

Im Rahmen einer Machbarkeitsstudie wurden Bedarf und Akzeptanz für die Einführung eines KMU-CERTs in Österreich repräsentativ erhoben. Der folgende Artikel beschreibt die wesentlichsten Erkenntnisse dazu. Die Studie wurde von der Österreichischen Wirtschaftskammer finanziert.

1 Ausgangssituation

Die rasch fortschreitende Digitalisierung aller Lebens- und Geschäftsbereiche bringt auch neue Bedrohungsszenarien mit sich. Insbesondere die damit verbundene Vernetzung erhöht die Komplexität, da Einzelkomponenten zu Systemen vernetzt und somit voneinander abhängig werden. Das erhöht die Anfälligkeit dieser Systeme sowohl gegen technische und menschliche Fehler als auch die Verwundbarkeit gegen gezielte Angriffe. Technische Antworten auf diese Herausforderungen werden laufend entwickelt, befinden sich aber in einem permanenten Wettlauf mit neuen Schwachstellen und Bedrohungen. In dieser Situation sind Informationsaustausch, Wissensaufbau und vor allem Zusammenarbeit das beste Mittel, um Schritt halten zu können. Fachexpertinnen und -experten sind dabei jedoch Mangelware, viele Unternehmen scheuen die Einstellung von eigenem Security Personal und überlassen daher Sicherheit der eigenen IT-Abteilung oder externen Dienstleistern. Vor diesem Hintergrund kommt dedizierten „Computer Emergency Response Teams“ (CERTs) oder „Computer Security Incident Response Teams“ (CSIRTs) eine besondere Rolle zu. Sie vereinen Fachkompetenz, Verständnis für das Gesamtsystem und Vernetzung mit anderen Expertinnen und Experten zu einer schlagkräftigen Antwort auf Bedrohungen, Angriffe und technische Notfälle. Sie werden insbesondere bei akuten Problemen tätig und schaffen zusätzlich Bewusstsein für Bedrohungen, indem sie qualifizierte Informationen über Schwachstellen und Angriffsmuster verteilen. Dieser Idealvorstellung einer Spezialeinheit für IT-Notfälle stehen ein entsprechender Aufwand beim Aufbau eines solchen CERTs und die damit verbundenen Kosten gegenüber. Aus diesem

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 142-150.

Grund hält sich die Anzahl dieser CERTs in Grenzen, obwohl sie einen wesentlichen Teil zur Erhöhung der Resilienz der österreichischen Wirtschaft beitragen könnten. In den Leistungsbeschreibungen von diversen CERTs finden sich Hinweise darauf, dass sie ihre Dienstleistungen auch für KMUs erbringen. So fand sich im RFC 2350 von CERT.at die Passage: "Pro-active and educational material will be provided for SMEs and the general public as well" die allerdings mittlerweile durch „Pro-active and educational material are provided for the general public" ersetzt wurde [9].

Die Wirtschaftskammer Österreich (WKO) und das Bundesministerium für Inneres (BMI) haben es sich deshalb im Rahmen einer seit 2010 bestehenden Kooperation mit dem Titel „GEMEINSMAM.SICHER gegen Wirtschaftskriminalität" zur Aufgabe gemacht, die Machbarkeit der Implementierung eines CERTs für Klein- und Mittelunternehmen (KMU) zu prüfen. Dies kommt zu einem Zeitpunkt, an dem einzelne Branchen den Aufbau eigener CERTs vorantreiben (z.B. das Austrian Energy CERT für die Energiebranche) bzw. prüfen (z.B. der Finanz und der Gesundheitssektor). Bei der Machbarkeitsstudie über die Einführung eines KMU-CERTs in Österreich durchgeführt. Dabei standen folgende Forschungsfragen im Vordergrund:

1. Welche nationalen und internationalen Beispiele und Erfahrungen gibt es bezüglich des Aufbaus und Betriebs von KMU- und anderen CERTs?
2. Benötigt der Markt das Angebot eines KMU-CERTs und würde der Markt ein solches Angebot durch die WKO akzeptieren? Wer ist die Zielgruppe (Constituency) eines KMU-CERTs und wie kann diese segmentiert werden?
3. Wie könnte ein solches KMU-CERT aufgebaut sein und wie ließe sich ein solches CERT in Österreich implementieren?

2 Related Work

WKO-Studie: Bedarfs- und Akzeptanalyse für ein KMU-CERT, Machbarkeitsstudie über die Möglichkeit zur Realisierung eines CERT für KMU in Österreich im Auftrag der Wirtschaftskammer Österreich (WKO), Wien 2018, Projektpartner REPUCO Unternehmensberatung GmbH, SBA Research gGmbH, Donau-Universität Krems, nic.at GmbH (CERT.at), INTEGRAL Markt- und Meinungsforschungs-GmbH und Regina Senk, Medien- und Kommunikationsexpertin.

Studie CERT-Kommunikation (Computer Emergency Response Team (CERT) Kommunikations-Modell), finanziert vom KIRAS Programm der Österreichischen Sicherheitsforschung, www.kiras.at/gefoerderte-projekte/detail/d/cert-komm/.

Forschungsprojekt CERT-Kommunikation II (Computer Emergency Response Team (CERT) Kommunikations-Modell 2) gefördert vom KIRAS Programm der Österreichische Sicherheitsforschung, www.kiras.at/gefoerderte-projekte/detail/d/cert-komm-ii/.

3 Methodenbeschreibung

Zur Beantwortung der Forschungsfragen wurde mittels eines interdisziplinären Forschungsteams eine Metaanalyse über wissenschaftliche Fachliteratur sowie eine quantitative telefonische Befragung durchgeführt (CATI – Computer Assisted Telephone Interviews). Die zu befragenden Unternehmen wurden mittels Zufallsauswahl aus dem österr. Branchenver-

zeichnis der HEROLD Business Data GmbH ausgewählt und anhand eines Screening-Fragebogens ausgewählt. Zur Definition der Grundgesamtheit wurde die Arbeitsstättenzählung der Statistik Austria [1] herangezogen, die die bestmögliche Strukturbeschreibung der Grundgesamtheit zur Verfügung stellt und mehrere Vorteile bietet:

- Kein Ausschluss von Unternehmen, die unter einem Schwellenwert liegen
- Es werden auch Unternehmen erfasst, die saisonal tätig sind

Als KMU-Begriff wurde die österreichische KMU Definition gewählt, nämlich Unternehmen mit einer MA-Zahl bis max. 249. Das Stichprobendesign wurde disproportional definiert, um auch in den größeren Unternehmensklassen eine ausreichend große Anzahl an Interviews zu erzielen und über diese Klassen Aussagen treffen zu können. In der Gewichtung wurden zudem das Bundesland sowie die Branchengruppe berücksichtigt – sodass diese im Gesamtergebnis ebenfalls repräsentativ vertreten sind. Die Grundgesamtheit sind alle KMUs in Österreich (Stand laut Dezember 2016: 501.572) Die definierte Stichprobe betrug (n=) 400.

4 Die Entwicklung von KMU-CERTs

4.1 Deutschland

Das einzige bekannte Beispiel für ein KMU-CERT stammt aus Deutschland. Ein Gutachten von 2001 gab sehr ausführliche und konkrete Empfehlungen, wie ein KMU-CERT aufgebaut werden könnte. Bei den anzubietenden Dienstleistungen wird zwischen zentralen Basisdienstleistungen, erweiterten Basisdienstleistungen sowie Zusatzdienstleistungen unterschieden. Des Weiteren werden auch die Realisierungsvarianten Erbringung durch ein etabliertes Team und Aufbau eines neuen Teams gegenübergestellt. Schließlich wird eine Empfehlung für ein Betreibermodell samt Finanzierungsplan abgegeben [3]. Im Jahr 2002 wurde das MCERT (Mittelstand-CERT) vom BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) in gemeinsamer Finanzierung mit dem Deutschen Bundesministerium des Innern gegründet und in Betrieb genommen, es wurden allerdings die im zitierten Gutachten abgegebenen Empfehlungen nicht berücksichtigt und im Juni 2007 stellte das MCERT seinen Betrieb ein [2]. Da nur sehr wenig relevanten Informationen über das MCERT verfügbar sind, wurde bei der Recherche auch auf Artikel in der Presse zurückgegriffen. Aus einem Artikel der Computerwoche vom 2.6.2004 (Hacker werden schneller; MCERT warnt) [4] geht hervor, dass das MCERT ein E-Mail-Service mit Warnhinweisen und Handlungsempfehlungen für jährlich 50 € angeboten hat. Diese Dienstleitung wurde von den KMUs nicht angenommen.

4.2 Schweiz

Im Zuge der Analyse wurde auch der Webauftritt des CERTs der Schweiz, MELANI (Melde- und Analysestelle Informationssicherung MELANI) untersucht [5]. Dabei konnte festgestellt werden, dass das Angebot von MELANI sich auch an Unternehmen richtet, sowohl was Meldungen betrifft als auch Informationen (z.B. Merkblatt IT-Sicherheit für KMUs). Im RFC 2350 des GovCERT.ch [6] (Teil von MELANI) findet sich diese Definition der Zielgruppe (constituency): “Our constituency is the network of the Swiss Federal Administration (Government) as well as the private and public sectors in Switzerland.”

5 Bedarf bei den österreichischen KMUs

Die befragten Unternehmen finden sich in vier zusammengefassten Branchengruppen:

Tab. 1: Unternehmensbeschreibung[1]

Variable	Häufigkeit	Prozent
Branche	412	
Gewerbe/Industrie/Bau	74	18
Handel	99	24
Gastronomie	45	11
Dienstleistungen	194	47
Mitarbeiter	412	
1 MA	217	53
2-4 MA	112	27
5-9 MA	45	11
10-19 MA	22	5
20-49 MA	12	3
50-99 MA	3	1
100-249 MA	2	1

IT-Sicherheit ist Chefsache. In nahezu allen Unternehmen werden technische und strategische Entscheidungen hinsichtlich der IT-Sicherheit von der Geschäftsführung getroffen. Interessant dabei ist, wieviel Geld die KMUs für IT-Sicherheit ausgeben. Die jährlichen Ausgaben betragen bei dem Großteil der Unternehmen bis zu 1.000 Euro (73 %). Ausgaben über 50.000 Euro finden sich bei keinem der befragten Unternehmen. Nichtsdestotrotz sehen die meisten Befragten einen Nachholbedarf im Bereich der IT-Sicherheit. Außerdem sieht rund ein Fünftel der Befragten das eigene Unternehmen als Nachzügler in der Umsetzung von IT-Sicherheitsmaßnahmen. Ein Viertel schätzt sich selbst als Innovator und Vorreiter in diesem Thema ein. Dennoch fühlen sich die meisten Respondenten sehr gut oder gut (55 %) über das Thema IT-Sicherheit und Maßnahmen zum Schutz vor Cyber-Attacken informiert. Lediglich 4 % geben an, dass sie sich nicht ausreichend informiert fühlen. An dieser Stelle sei darauf hingewiesen, dass es sich um eine Selbsteinschätzung der Betroffenen handelt.

Auf der Grundlage der n = 412 Befragte wurden die in den Abbildungen 1 und 2 dargestellten Umfrageergebnisse ermittelt.

Abbildung 1 zeigt Antworten auf die Frage: Wie gut fühlen Sie sich über IT-Sicherheit und Maßnahmen zum Schutz vor Cyberattacken informiert?

Abbildung 2 zeigt Antworten auf die Frage: Wie beurteilen Sie es, dass die WKÖ überlegt Services für KMUs bezüglich Cybersicherheit anzubieten?

[1] Die Werte beider Variablen stellen die Ergebnisse der gewichteten Stichprobe dar.

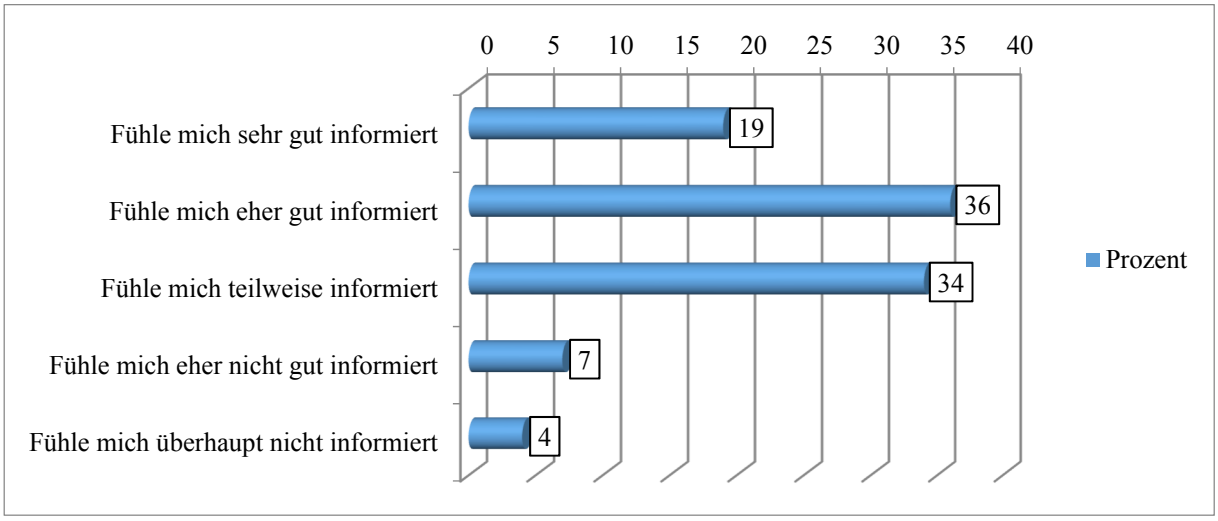

Abb. 1: Informiertheit über IT-Sicherheit und Maßnahmen zum Schutz vor Cyberattacken

Die Akzeptanz des Serviceangebotes für KMUs ist etwas zwiespältiger. So empfinden es zwar mehr Unternehmen als wahrscheinlich, dass sie den Service nutzen würden, als es Unternehmen als unwahrscheinlich empfinden, die meisten finden sich jedoch im unentschlossenen Mittelfeld wieder. Dies sollte jedoch nicht zu schwerwiegend dem Serviceangebot der WKO angerechnet werden, sondern in erster Linie unter dem Gesichtspunkt der Sicherheitsproblematik betrachtet werden. Die fehlerhafte Risikoeinschätzung (umgangssprachlich auch als Truthahn-Illusion bezeichnet) verleitet Personen dazu, zu wenig Zeit und Geld in Sicherheitsthemen zu investieren. Diese Wahrscheinlichkeitseinschätzung zeigt lediglich erneut, dass viele Unternehmen erst dann zu solchen Services greifen werden, wenn sie tatsächlich in eine Krisensituation geraten. Dies wird jedoch wiederum von einigen KMUs als sehr unwahrscheinlich erachtet, was der Hauptgrund dafür ist, dass sie sich keine Serviceangebote wünschen. Dies spiegelt wiederum nur eine fehlerhafte Risikoeinschätzung wieder, wobei wir erneut bei der ursprünglichen Sicherheitsproblematik wären. Die Akzeptanz der Wirtschaftskammer als Treiber von Services zum Thema Cyber-Sicherheit ist überaus hoch. Der größte Teil der befragten KMUs sieht es als positiv, dass die WKO sich hier einsetzen möchte.

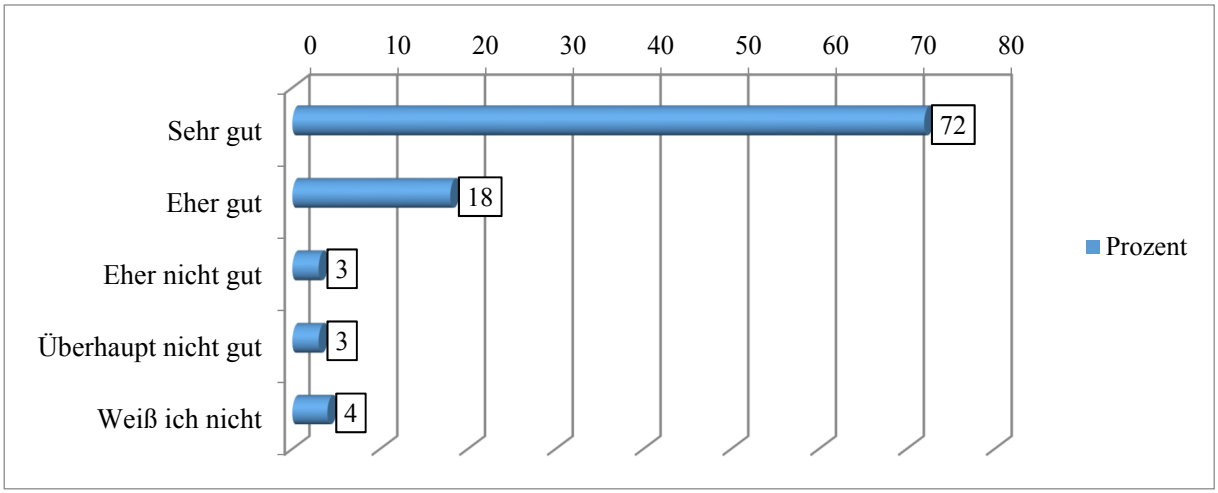

Abb. 2: Soll die WKÖ Services für KMUs bezüglich Cybersicherheit anzubieten?

6 Schlussfolgerungen

6.1 Einfach verständliche Kommunikation

In den meisten Unternehmen, bedingt durch ihre geringe Größe, ist der Geschäftsführer für IT-Sicherheitsbelange zuständig. Im Krisenfall ist es somit der Geschäftsführer der in Kontakt mit einem KMU-CERT tritt. Dieser Personengruppe ist jedoch nicht notwendigerweise ausreichend technisch ausgebildet. Dies muss in der Kommunikation mit dem KMU-CERT berücksichtigt werden. So sollten statt technischen Begrifflichkeiten, allgemeinverständliche benutzt werden und auch auf Abkürzungen und technische Codes sollte verzichtet werden. Siehe auch dazu Huber, 2015 [7] und Qurichmayr, 2015 [8] et al.

6.2 Reaktive und präventive Aufgaben übernehmen

Die Ergebnisse zeigen, dass die KMUs alle der gelisteten Aufgaben, welche ein CERT übernehmen könnte, als interessant oder zumindest teilweise interessant empfinden. Ein KMU-CERT sollte aus diesem Grund im Idealfall all diese Aufgaben erfüllen, sich in einem ersten Schritt jedoch auf die interessantesten konzentrieren. Aufgrund besonderen Interesses sollten in jedem Fall die Services „Auskunftsstelle für alle Arten von Fragen zum Thema Cyber-Sicherheit“, „Warnungen über aktuelle und neu auftretende Cyber-Attacken“, „Information falls es Hinweise auf einen Cyber-Angriff auf unser Unternehmen gibt“ und „Hilfestellung durch kompetente Ansprechpersonen im Akut-Fall“ abgedeckt sein.

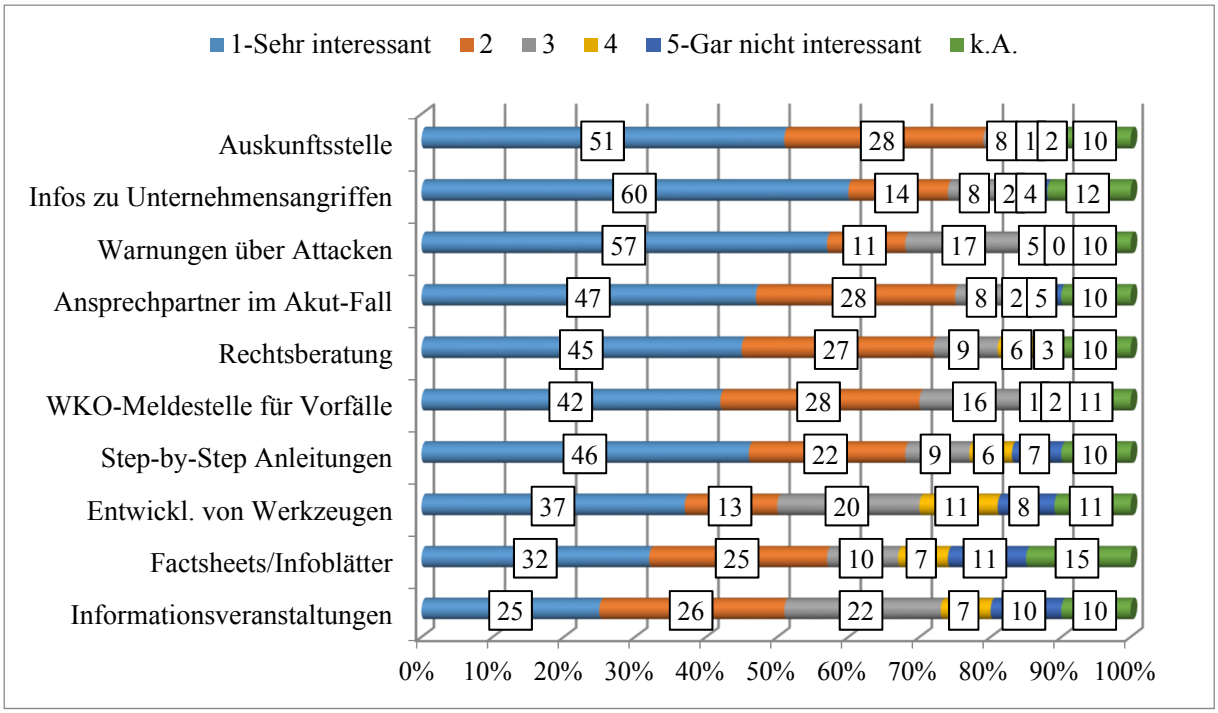

Abb. 3: Wie interessant wären diese Services für Ihre KMU? (n=412)

6.3 Bestehende Services anpassen

Die bereits bestehenden Services der WKO, werden unterschiedlich bewertet. Die Cyber-Security-Hotline ist nur 21 % der Personen bekannt und wurde auch im Falle von Cyber-Angriffen nicht zu Rate gezogen. Dies ist besonders interessant, wird nochmals der Wunsch der KMUs betrachtet in erster Linie eine „Auskunftsstelle für alle Arten von Fragen zum Thema Cyber-Sicherheit“ zu erhalten. Bei einer Implementierung eines KMU-CERTs sollte dieses Service unbedingt komplementär erhalten bleiben. In jedem Fall könnte eine mögliche Einführung eines KMU-CERTs jedoch auch für Marketingzwecke der Hotline genutzt werden um deren Bekanntheit zu erhöhen. Weitere Serviceangebote wie Websites und Online-Ratgeber sind bereits 38 % der Befragten bekannt und werden auch von 30 % genutzt. Diese Services könnten besonders dann als ergänzend weitergeführt werden, wenn das KMU-CERT diese für die KMUs als weniger interessante Aufgabe in dessen Profil ausspart.

6.4 Kritische Betrachtung der Selbsteinschätzung

Eine Thematik, welche mit vielen anderen Faktoren in Beziehung steht ist die Selbsteinschätzung der KMUs. Aus den Daten ist ersichtlich, dass jene KMUs welche sich über das Thema Cyber-Sicherheit und Cyber-Attacken gut informiert fühlen, weniger Interesse an Serviceangeboten der WKO haben. Frei nach der Ansicht: „Ich weiß genug, ich brauche keine Hilfe.“ Gleichzeitig zeigen die Ergebnisse, dass vor allem nicht technisch ausgebildete Personen befragt wurden. Dies und die oft geringen personellen Ressourcen in den vor allem vertretenen Kleinunternehmen, lässt die Vermutung zu, dass es möglicherweise zu einer falschen Selbsteinschätzung kommt, die sich aus einem fehlenden Maß an Wissen ergibt. Tritt diese Vermutung zu, so könnten diese KMUs im Krisenfall mehr vom KMU-CERT profitieren als sie vielleicht zurzeit vermuten.

Des Weiteren beeinflusst die subjektive Wahrnehmung des eigenen Wissensstands zu Cyber-Sicherheit die Bereitschaft der Befragten Services bei der WKO zu nutzen. Die Ergebnisse zeigten, dass ein Zusammenhang besteht, zwischen der Selbsteinschätzung, wie gut sich ein Befragter über Themen der Cyber-Sicherheit und Cyber-Angriffe informiert fühlt und wie er die Services der WKO bewertet. Fühlt sich der Befragte sehr schlecht über die Themen Cybersicherheit und Cyberangriffe informiert, so wünscht er sich signifikant (0,000) stärker Serviceangebote der WKO (Spearman -0,300). Außerdem beurteilt er es signifikant (0,003) besser, dass die WKO Services zur Verfügung stellen möchte (Spearman -0,144). Darüber hinaus steigt mit der geringen Einschätzung des Wissens die Wahrscheinlichkeit, dass diese Person die Services der WKO nutzt signifikant (0,000) (Spearman -0,204).

Auch zwischen der Größe des Unternehmens und der Beurteilung von Services der WKO zum Thema Cyber-Sicherheit konnte ein signifikanter Zusammenhang festgestellt werden. Größere Unternehmen, mit einer höheren Mitarbeiteranzahl, wünschen sich signifikant (0,001) stärker Serviceangebote der WKO (Spearman -0,171). Außerdem würden sie mit einer signifikant (0,000) höheren Wahrscheinlichkeit die Services der WKO nutzen (Spearman -0,232).

6.5 Zahlungsbereitschaft

Das Potenzial für Services der Wirtschaftskammer zu zahlen erscheint sehr hoch, was darauf hinweist, dass es einen ziemlich hohen Bedarf von Seiten der KMUs gibt. Das theoretische Kernpotenzial beläuft sich für das Angebot bei Kosten von 150 Euro auf 19 %. Liegen die Kosten bei 100 Euro steigt das Kernpotenzial auf 26 %. Bei 75 Euro liegt es bei 31 %.

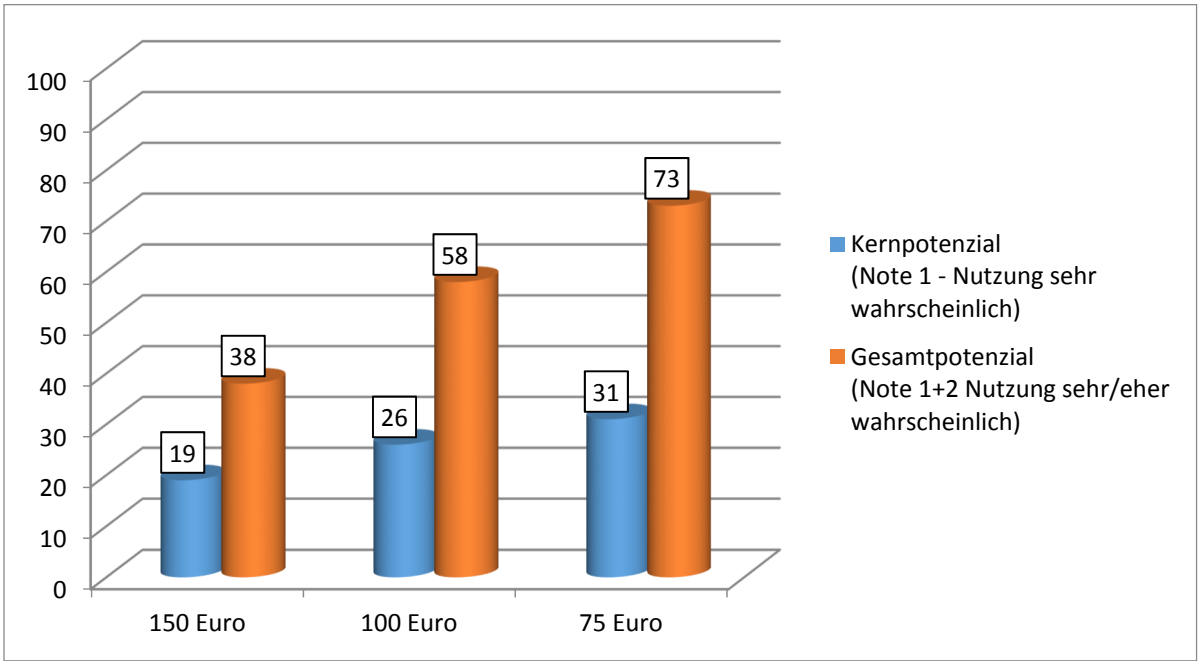

Abb. 4: Wie viel wären Sie bereit für diese Services zu zahlen? (n=412)

7 Nächste Schritte

Im Rahmen der Studie wurden auch die für einen effektiven Betrieb eines KMU-CERT notwendigen Ressourcen geprüft und eine Empfehlung ausgesprochen. Die Auftraggeber WKO und BMI können damit in einem nächsten Schritt in eine Budgetplanung gehen um in weiterer Folge über die Realisierung eines KMU CERT zu entscheiden. Zum Zeitpunkt der Erstellung dieses Textes war die Umsetzung der EU NIS-Richtlinie in Österreich noch nicht abgeschlossen und es ist noch nicht klar, wie hoch der behördliche Anteil an der Übernahme von CERT-Aufgaben tatsächlich sein wird und wie weit die WKO bzw. die Wirtschaft mit einem KMU CERT Aufgaben übernehmen muss bzw. sollte. Bei einer Entscheidung für ein Engagement von Seite der WKO kann mit einer Projektumsetzung in den nächsten 2-3 Jahren gerechnet werden.

Literatur

[1] Statistik Österreich, www.statistik.at, 18.06.2018.

[2] https://web.archive.org/web/20070701202727/http://www.mcert.de:80/, 18.06.2018.

[3] M. Pattloch, K.-P. Kossakowski: (2001) CERT-Dienstleistungen für kleine und mittlere Unternehmen (KMU). www.kossakowski.de/kmucert-gutachten.pdf

[4] https://www.computerwoche.de/a/mcert-warnt,561747, 18.06.2018.

[5] https://www.melani.admin.ch, 18.06.2018.

[6] https://www.govcert.admin.ch, 18.06.2018.

[7] E. Huber (Hrg.): Sicherheit in Cyber-Netzwerken – Computer Emergency Response Teams und ihre Kommunikation, Springer (2015).

[8] G. Quirchmayr, O. Hellwig, E. Huber, M. Huber, T. Mischitz: Towards a CERT-Communication Model as Basis to Software Assurance. IEEE Proceedings 10th International Conference on Availability, Reliability and Security (ARES) (2015) 481-485.

[9] CERT.at, www.cert.at, 18.06.2018.

[10] E. Huber, B. Pospisil, W. Hötzendorfer, G. Quirchmayr, L. Löschl, C. Tschohl: Die Cyber-Kriminellen in Wien: Eine Analyse von 2006-2016, Tredition (2018).

[11] B. Pospisil, M. Gusenbauer, E. Huber et al.: Datenschutz und Datensicherheit – DuD, Vol. 41 (2017) 628–632.

[12] C. Tschohl, W. Hötzendorfer, G. Quirchmayr, E. Huber, O. Hellwig: Die NIS-Richtlinie und der rechtliche Rahmen von CERTs. In: Trends und Communities der Rechtsinformatik – Tagungsband des 20. IRIS (2017) 50-62.

[13] G. Quirchmayr, O. Hellwig, E. Huber, M. Huber: Studie CERT Kommunikation. In: BMVIT (Hrg) Wissenschaf(f)t Sicherheit, KIRAS Studienband 3, Wien (2016).

[14] G. Quirchmayr, O. Hellwig, E. Huber, F. Vock: Major Challenges in Structuring and Institutionalizing CERT-Communication, ARES-Conference Paper, IEEE (2016).

[15] E. Huber, O. Hellwig, G. Qurichmayr: Wissensaustausch und Vertrauen unter Computer Emergency Response Teams – eine europäische Herausforderung, Datenschutz und Datensicherheit – DuD, Vol. 40 (2016) 162-166.

[16] E. Huber, G. Quirchmayr, O. Hellwig: Wissensmanagement bei CERTs – eine europäische Herausforderung. In: Tagungsband zum 14. Deutschen IT-Sicherheitskongress (2015) 493-504.