

ALLIANZ CYBER-UMFRAGE „GEFAHR AUS DEM NETZ“

Mag. Xaver Wölfl
Chief Digital Officer
Allianz Gruppe in Österreich

Wien, 8. November 2017



Pressegespräch

Allianz 

ÖSTERREICH: LAND DER KLEINUNTERNEHMEN

- 307.000 Ein-Personen-Unternehmen
 - 151.000 Unternehmen mit 1-4 Mitarbeitern
 - 738.000 Beschäftigte in Kleinunternehmen
 - 99 Prozent aller österreichischen Unternehmen haben Internetzugang
 - 88 Prozent haben eine eigene Website
- } 83,7 Prozent aller österreichischen Unternehmen

**Nahezu alle österreichischen Unternehmen sind
den Risiken der Digitalisierung in vollem Umfang ausgesetzt.**



CYBERATTACKEN: ANGST UND REALE BEDROHUNG

- Wellen von Cyberangriffen (WannaCry, ...)
- Schäden in Millionenhöhe
- Lösegeldforderungen
- Verunsicherung der Bevölkerung
- Skepsis in Sachen Cybersicherheit

DATENSCHUTZGRUNDVERORDNUNG: NEUE DIMENSION DER VERANTWORTUNG

25.5.2018: Datenschutzgrundverordnung setzt neue Maßstäbe in Sachen Datenschutz

Alle Unternehmen, die personenbezogene Daten erfassen oder bearbeiten, sind betroffen:

- ✓ Datenanwendungen überprüfen
- ✓ Datenflussanalysen durchführen
- ✓ Datensicherheitsmaßnahmen optimieren
- ✓ Verzeichnis der Datenverarbeitungstätigkeiten erstellen
- ✓ Datenschutzbeauftragte nominieren (bei Bedarf)
- ✓ Mitarbeiterschulungen durchführen
- ✓ Notfallplan für Datenschutzvorfälle erstellen



ALLIANZ CYBER-UMFRAGE

- Wie gehen Einzel- und Kleinunternehmen generell mit dem Thema Datenschutz und Cybersicherheit um?
- Welchen Stellenwert hat dieses Thema, verglichen mit anderen Herausforderungen für Kleinunternehmen?
- Wie agieren EPUs und KUs im Alltag im Hinblick auf Datensicherheit?
- Welche Erfahrungen haben österreichische Kleinunternehmen mit Cyberattacken bereits gemacht?
- Wie ist der Wissensstand hinsichtlich der Datenschutzgrundverordnung?



DATEN UND FAKTEN ZUR UMFRAGE

**Telefonische
Befragung**

Methode

400 Ein-Personen-
Unternehmen &
Kleinunternehmen
(max. 4 Mitarbeiter)
in ganz Österreich

Stichprobe

**Sommer
2017**

Zeitraum

**Market-
Institut**

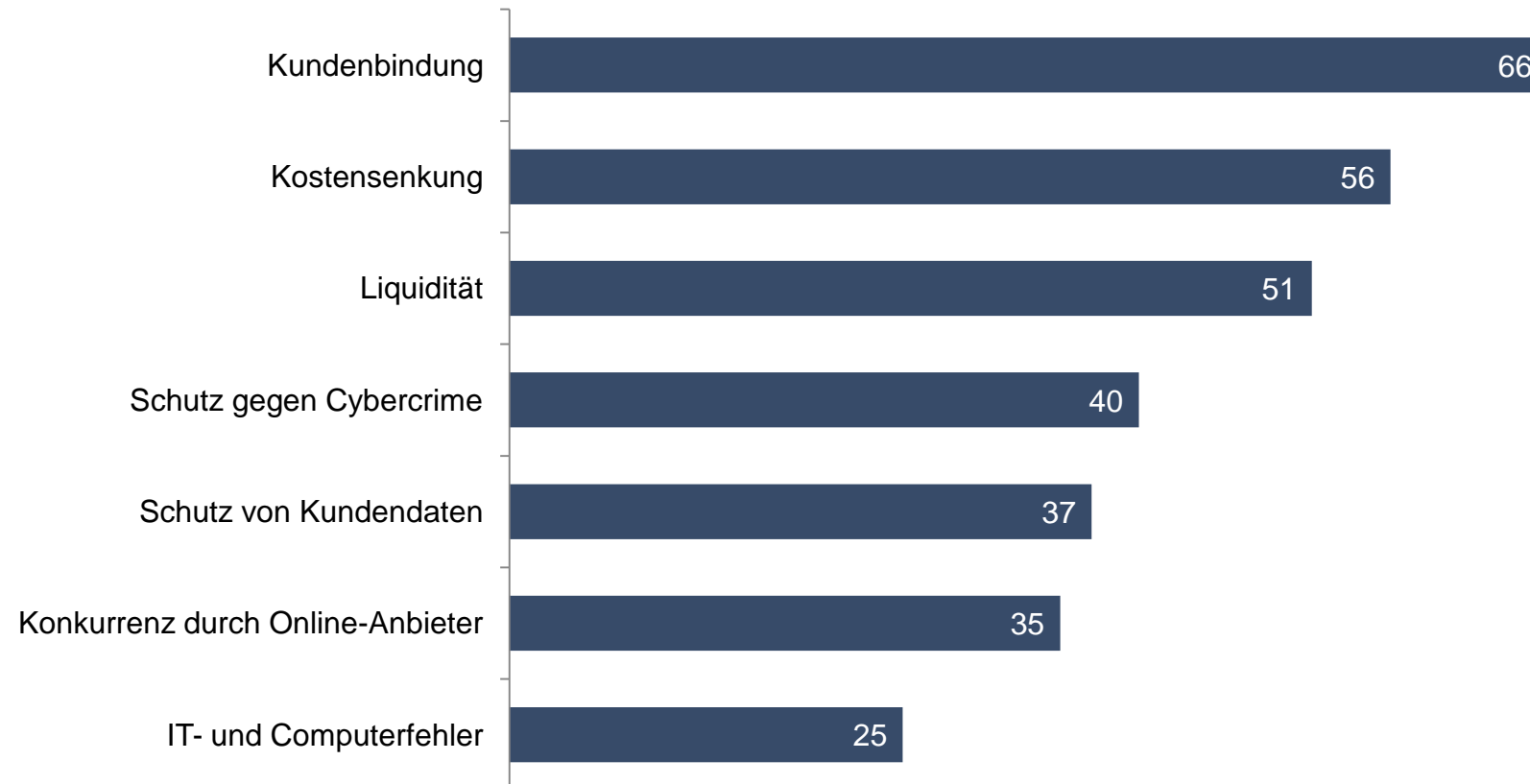
Institut



CYBERSCHUTZ IM SCHATTEN VON KUNDENBINDUNG UND KOSTENSENKUNG

FRAGE: „WIE STARK FÜHLEN SIE SICH VON DEN FOLGENDEN HERAUSFORDERUNGEN BZW. RISIKEN IN BEZUG AUF IHR UNTERNEHMEN BETROFFEN?“

SEHR STARK / STARK, IN PROZENT



22 Prozent machen sich häufig Gedanken über das Thema Cybercrime. 53 Prozent selten oder gar nicht.



WER CYBERATTACKEN ERLEBT, ÄNDERT SEINE EINSTELLUNG.

FRAGE: „WIE STARK FÜHLEN SIE SICH VON DEN FOLGENDEN HERAUSFORDERUNGEN BZW. RISIKEN IN BEZUG AUF IHR UNTERNEHMEN BETROFFEN?“

SEHR STARK / STARK, IN PROZENT

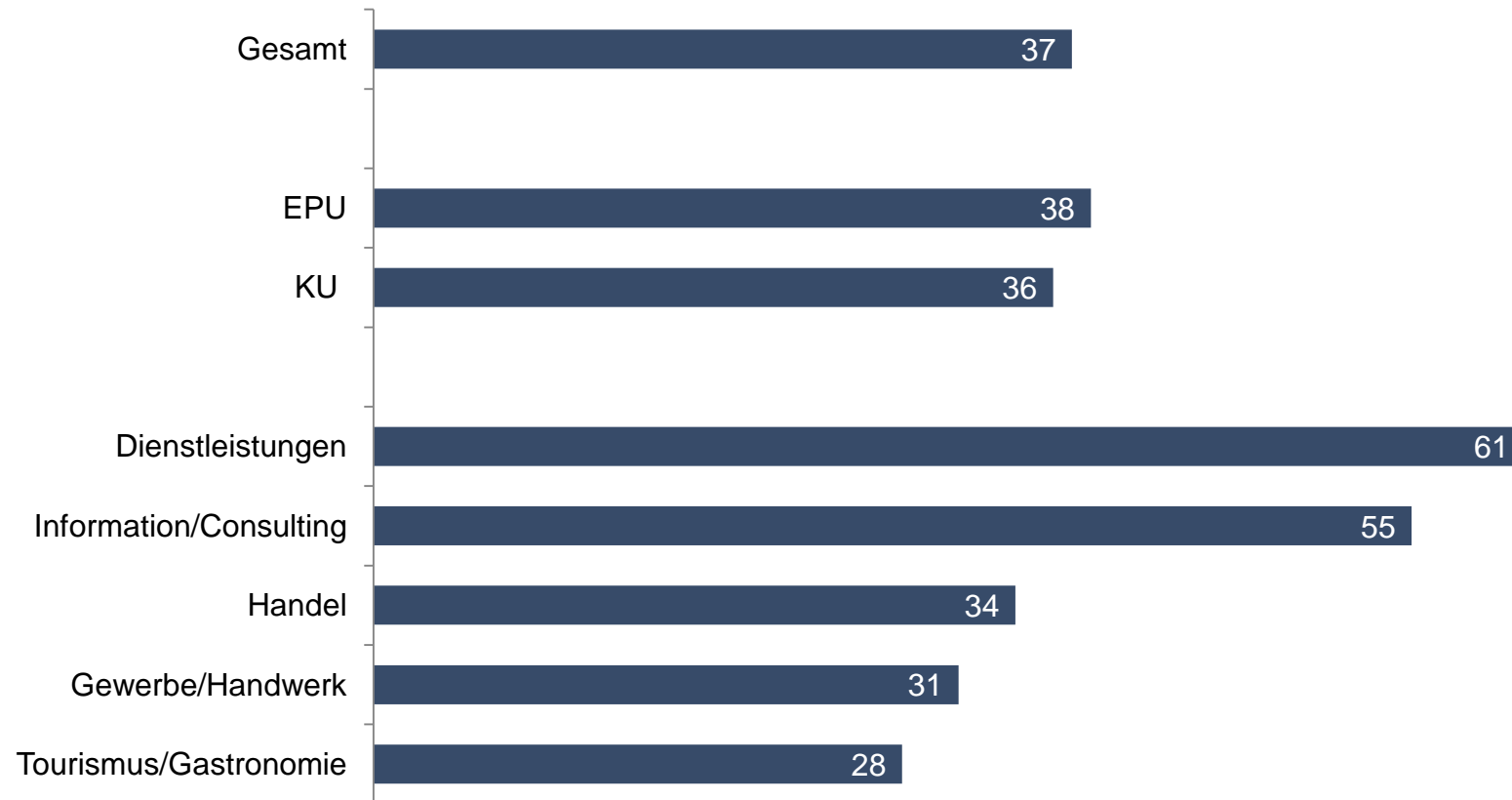
	Gesamt	EPU	KU	Mehrere Cyberattacken erlebt
Schutz gegen Cybercrime	40	34	50	75
Schutz von Kundendaten	37	34	44	54
Konkurrenz durch Online-Anbieter	35	37	33	50
IT-/Computerfehler	25	25	25	33



MODERNE IT-AUSSTATTUNG IST MANGELWARE.

FRAGE: „WIE FORTSCHRITTLICH NEHMEN SIE IHR UNTERNEHMEN IM BEREICH DIGITALISIERUNG/IT/COMPUTER WAHR?“

SEHR FORTSCHRITTLICH / FORTSCHRITTLICH, IN PROZENT

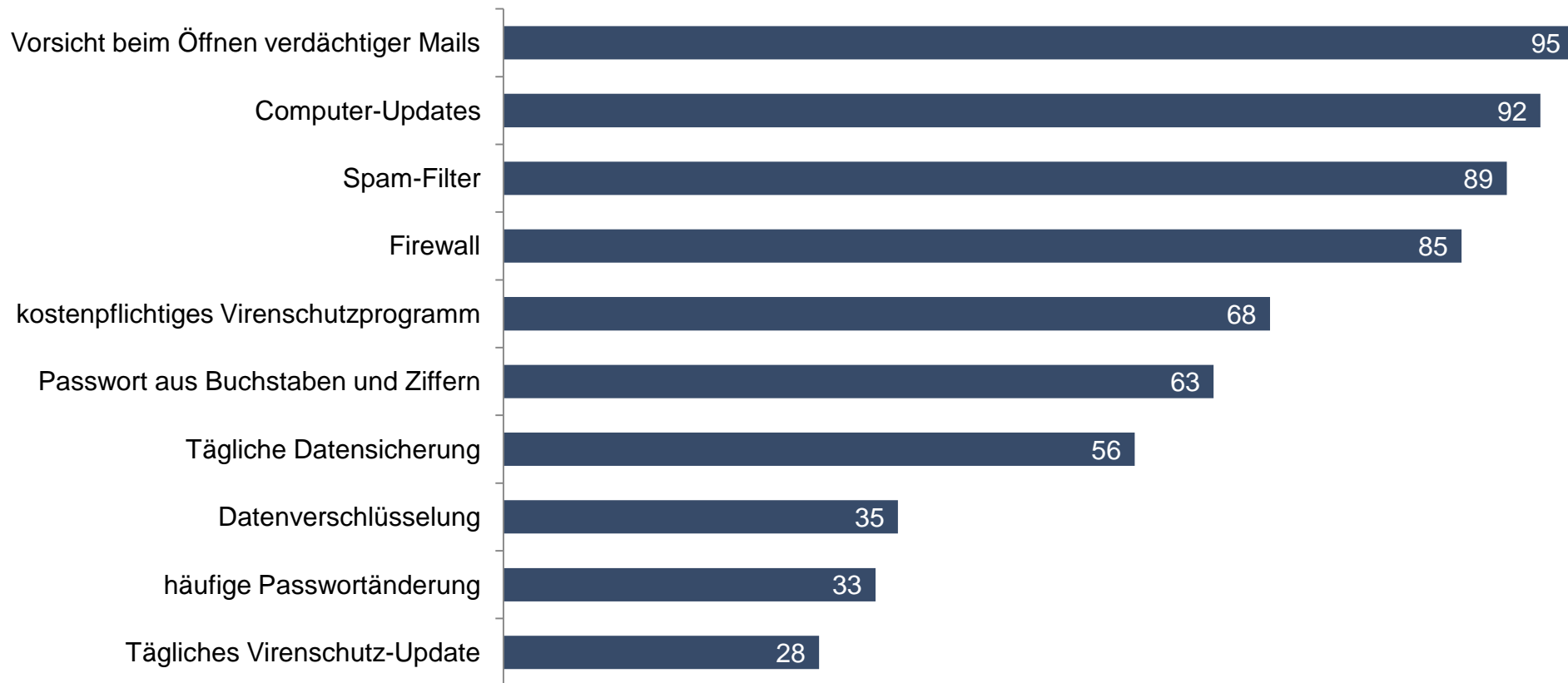




MANGELHAFTER CYBERSCHUTZ IM ALLTAG

FRAGE: „WELCHE DER FOLGENDEN MAßNAHMEN ZUR ABSICHERUNG GEGEN CYBERCRIME (HACKERANGRIFFE, DATENDIEBSTAHL ETC.) NUTZEN SIE IN IHREM UNTERNEHMEN?“

IN PROZENT

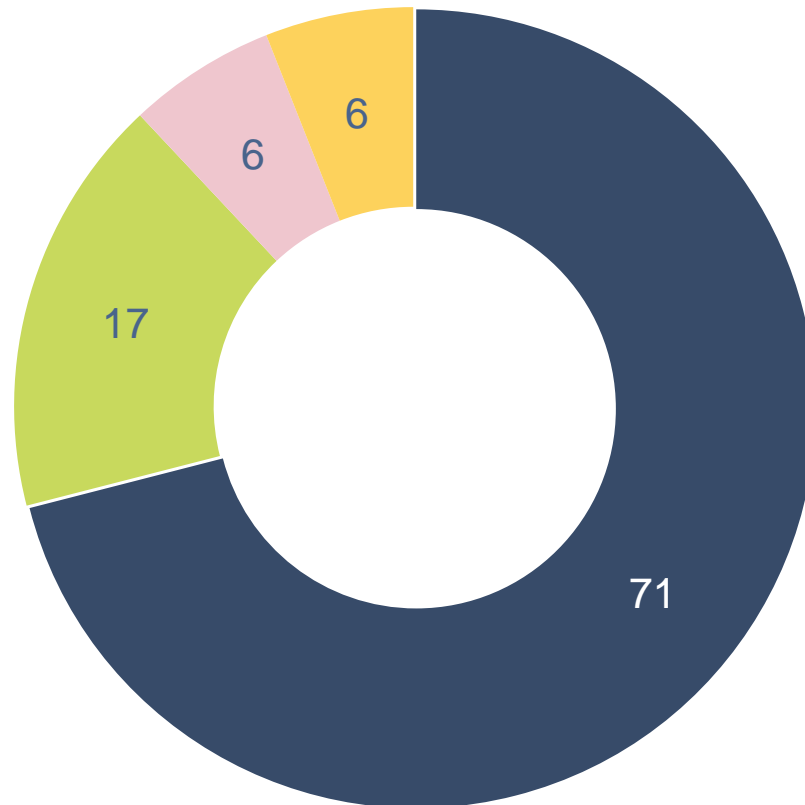




KLEINUNTERNEHMEN ERLEDIGEN DIGITALMANAGEMENT NEBENBEI.

FRAGE: „WER IST IN IHREM UNTERNEHMEN FÜR DAS IT- UND DIGITALMANAGEMENT ZUSTÄNDIG?“

IN PROZENT



56 Prozent der Zuständigen für IT- und Digitalmanagement wenden dafür weniger als ein Zehntel ihrer Arbeitszeit auf.

- Inhaber / Geschäftsführer
- externer Berater
- Mitarbeiter
- Keine fixe Zuständigkeit



JEDES SECHSTE KLEINUNTERNEHMEN HAT SCHON EINE CYBERATTACKE ERLEBT.

FRAGE: „HAT ES AUF IHR UNTERNEHMEN SCHON EINEN ODER MEHRERE CYBERANGRIFFE GEgeben?“

JA, IN PROZENT

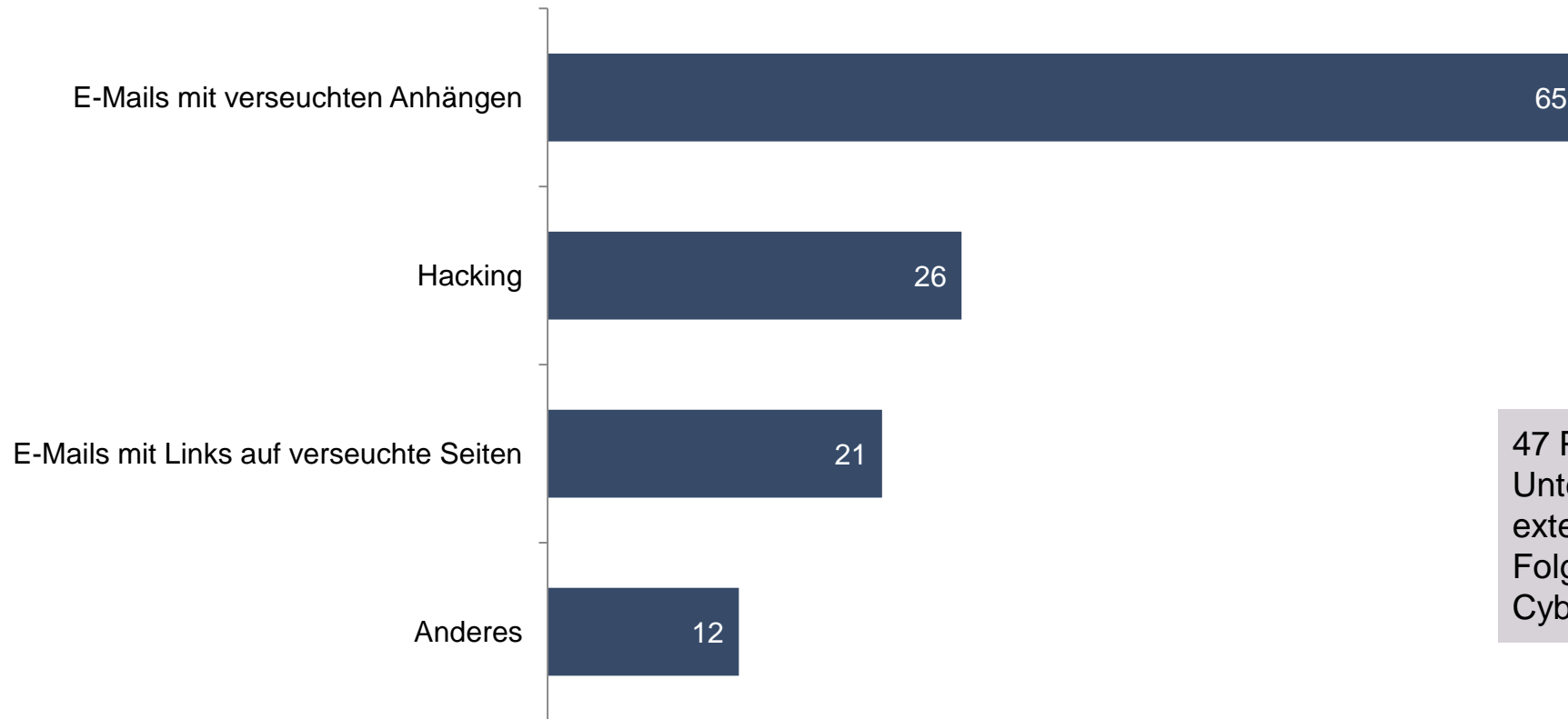




HAUPTGEFAHR: „VERSEUCHTE“ E-MAILS

FOLGEFRAGE: „AUF WELCHE WEISE WURDE DER ANGRIFF AUF IHR UNTERNEHMEN VERÜBT?“

IN PROZENT



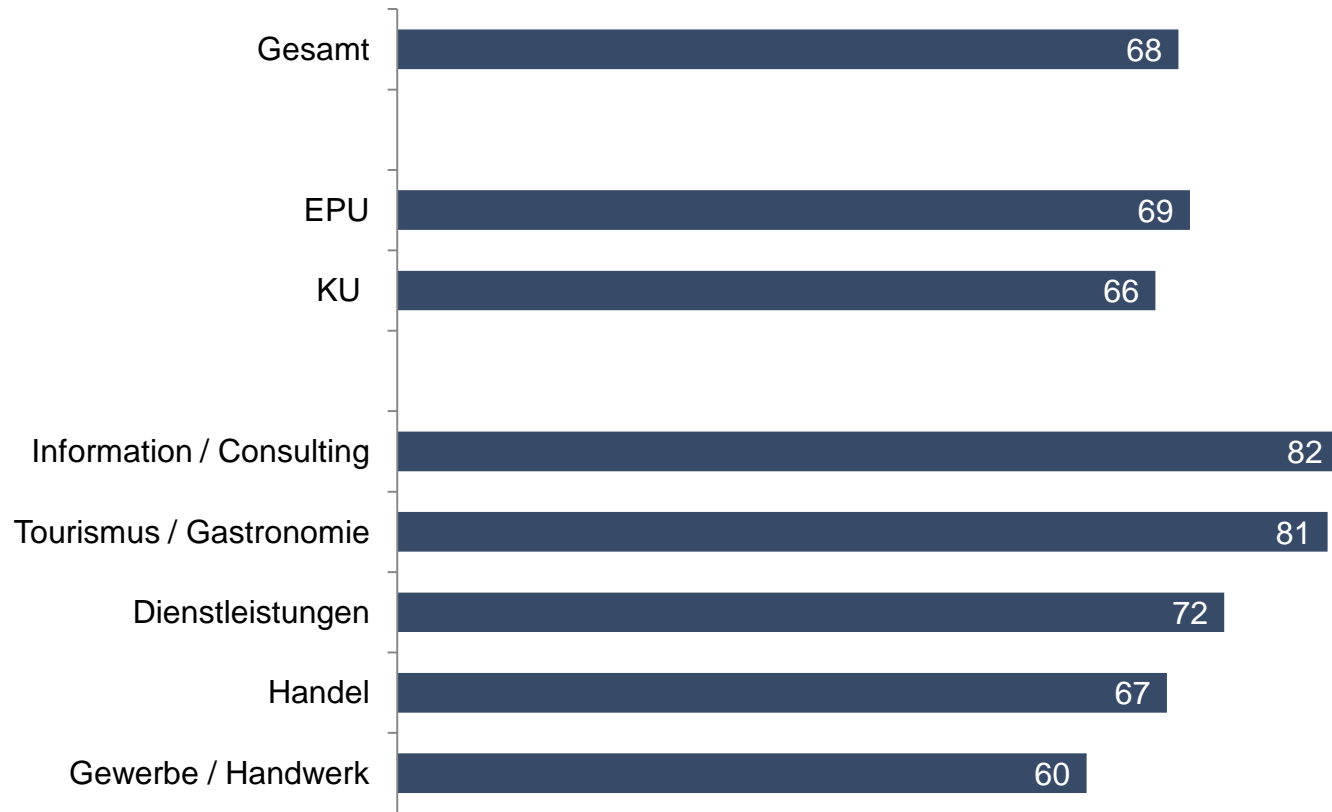
47 Prozent der betroffenen Unternehmen bedienten sich externer Unterstützung, um Folgeschäden des Cyberangriffes abzuwehren.



ALLES PALETTI IN SACHEN DATENSCHUTZ?

FRAGE: „DENKEN SIE, DASS IN IHREM UNTERNEHMEN PERSONENBEZOGENE DATEN SO SICHER GEHANDHABT WERDEN, DASS SIE VOR ZUGRIFF DURCH DRITTE SICHER SIND?“

JA, IN PROZENT

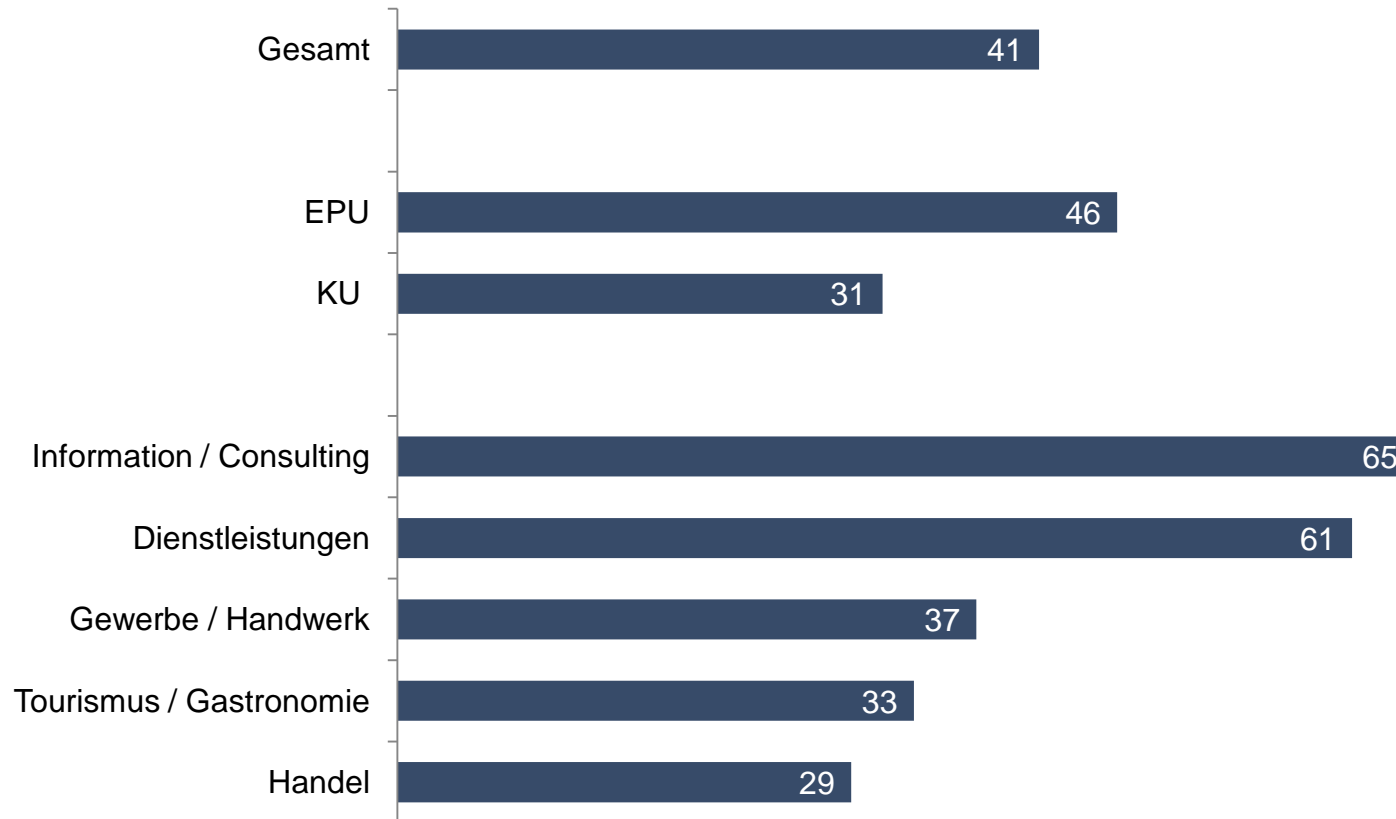


„Unternehmen wiegen sich in trügerischer Sicherheit: Es gibt keine 100-prozentige Sicherheit vor Cyberattacken.“

DATENSCHUTZGRUNDVERORDNUNG: FÜR VIELE EIN FREMDWORT

FRAGE: „HABEN SIE SCHON VON DER DATENSCHUTZGRUNDVERORDNUNG GEHÖRT, DIE IM MAI 2018 IN ÖSTERREICH IN KRAFT TRETEN WIRD?“

JA, IN PROZENT



Nur 51 Prozent der Einzel- und Kleinunternehmen fühlen sich von den durch die DSGVO geforderten verschärften Datenschutzbestimmungen betroffen.



8 VON 10 KLEINUNTERNEHMEN SIND GEGEN CYBERATTACKEN NICHT VERSICHERT.

FRAGE: „IST IHR UNTERNEHMEN GEGEN RISIKEN, DIE DURCH CYBERCRIME ODER EIN FEHLVERHALTEN IN IT-ANWENDUNG ODER DATENSCHUTZ ENTSTEHEN, VERSICHERT?“

IN PROZENT

	JA, in einer speziellen Versicherung	JA, mit anderen Risiken mitversichert	NEIN
Gesamt	5	9	79
EPU	4	9	82
KU	7	9	73
Information / Consulting	7	11	77
Dienstleistungen	6	28	56
Handel	5	9	78
Gewerbe / Handwerk	5	8	79
Tourismus / Gastronomie	5	2	91

43 Prozent finden eine Versicherung gegen Cyberrisiken grundsätzlich sinnvoll.

ZUSAMMENFASSUNG DER UMFRAGEERGEBNISSE

- Cybersicherheit wird nicht als vorrangiges Problem eingestuft und liegt weit hinter Themen wie Kundenbindung und Kostenfragen.
- Cybersicherheit wird auch im Alltag nicht konsequent beachtet. Jeder dritte Kleinbetrieb spart sich die Ausgaben für Virenschutz.
- Firmen, die mehrfach Cyberattacken ausgesetzt waren, ändern ihre Einstellung.
- Die Datenschutzgrundverordnung ist in den meisten Kleinunternehmen unbekannt.

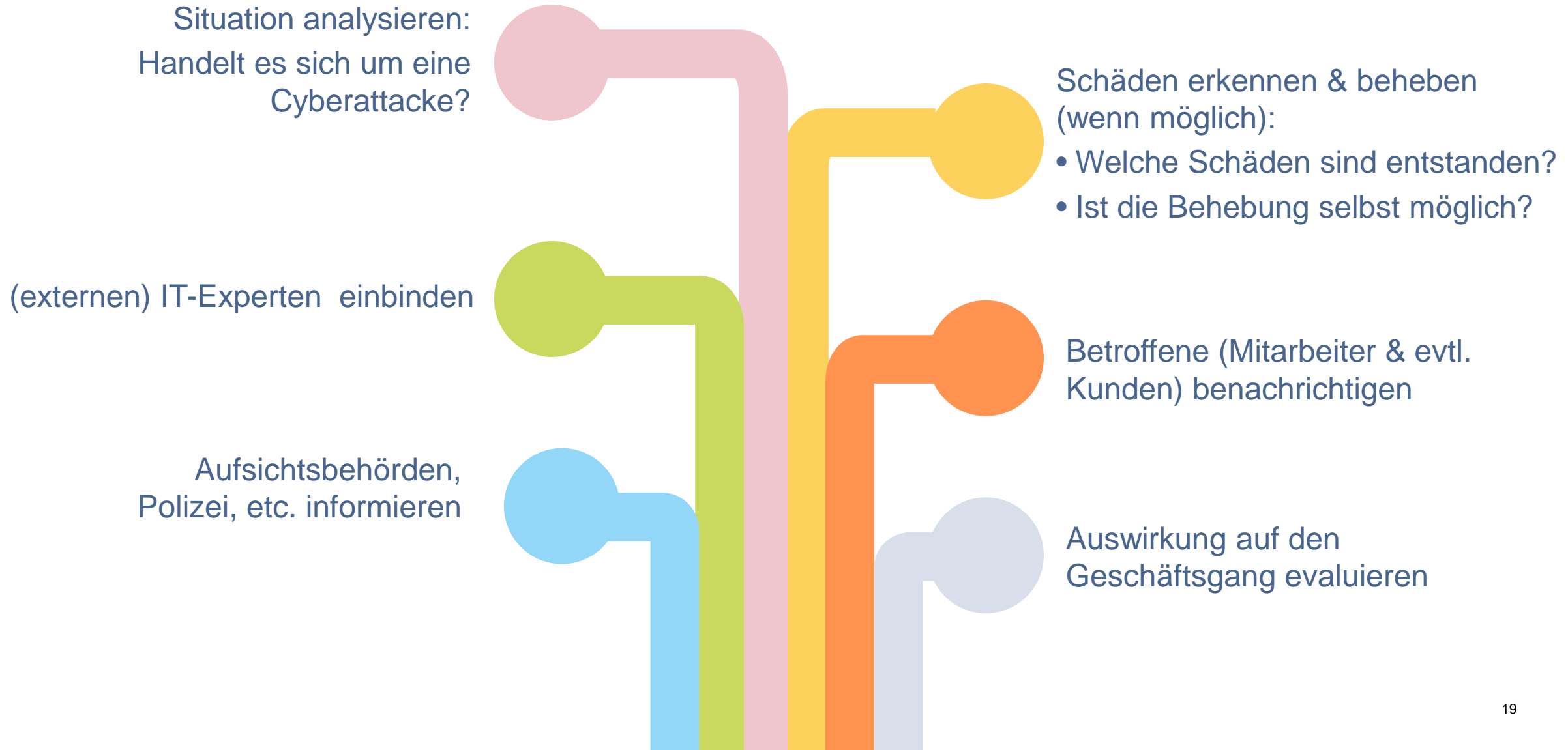
PRÄVENTION: TO-DOS FÜR ÖSTERREICHS KLEIN- UNTERNEHMEN

Datenschutz und Cybersicherheit sind auch für Kleinunternehmen Fragen höchster Priorität.

- ✓ Schärfung des **Bewusstseins** für Cybergefahren & **Eigeninitiative**: Was kann ich selbst zum Schutz beitragen (zB vorsichtiger Umgang mit E-Mails, Vorsicht bei Zahlungen im Internet)?
- ✓ Kennen und Einhaltung **rechtlicher Verpflichtungen** (DGSVO o.ä.)
- ✓ **Awareness** -Training (auch für Mitarbeiter)
- ✓ **Installation und Wartung** von Sicherheitsfeatures des Betriebssystems, Virenschutzprogrammen, Firewalls, ...
- ✓ Regelmäßige **Updates** von Betriebssystem, verwendeten Programmen, Virenschutzprogrammen, ...
- ✓ Erstellung und regelmäßige **Änderung** von komplexen Passwörtern
- ✓ Regelmäßige **Daten- und Programmsicherung**
- ✓ Einbindung von **externen Experten** & Abklären von Verfügbarkeit im Krisenfall
- ✓ **Prozess / Aufgaben / Zuständigkeiten** klären: IT-Verantwortung, Koordination im Krisenfall, Ansprechpartner/Beteiligte, Rechtliches, ...
- ✓ **Versicherung** gegen Cyberattacken



CYBERANGRIFF: WAS TUN?



DIE ALLIANZ LÖSUNG IM BEREICH CYBER

Vertrauens- schaden- versicherung

- Vermögensschäden, die arglistig durch Eingriffe Dritter oder auch arglistig durch eigene Mitarbeiter herbeigeführt werden

Cyber-Schutz

- im Zusammenhang mit Datenschutz- oder Vertraulichkeitsverletzungen sowie Cyberattacken (Haftpflichtansprüche, Betriebsunterbrechung und Wiederherstellungsaufwand, Abwehrkosten bei behördlichen Datenschutzverfahren, Kosten forensischer Dienstleistungen, Krisenkommunikationskosten)

Notfall-IT-Assistance

- (kommunikations-)technischer Support im IT-Notfall – nicht nur bei Cyber-Attacke

Computerversicherung

- Hardware & Software



KONTAKT

MMag. Manfred Rapolter, MA

Allianz Gruppe in Österreich
Hietzinger Kai 101-105
1130 Wien

Tel.: +43 5 9009 80 955

Fax: +43 5 9009 40261

manfred.rapolter@allianz.at

www.allianz.at