REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2017	

4. TITLE AND SUBTITLE

Monitor - IT-Sicherheit Kristischer Infrastrukturen
(Monitor –IT-Security Of Critical Infrastructures)

5. FUNDING NUMBERS

6. AUTHOR(S)

Ulrike Lechner

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

UNIBW

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES

Universität für der Bundeswehr München
Werner-Heisenberg-Weg 39
D-85577 Neubiberg Germany

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Text in German.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Public release. Copyrighted. (1 and 20)

12b. DISTRIBUTION CODE

ABSTRACT (Maximum 200 words)

Machine assisted translation.

14. SUBJECT TERMS

UNIBW, German, IT, Security, Critical Infrastructures

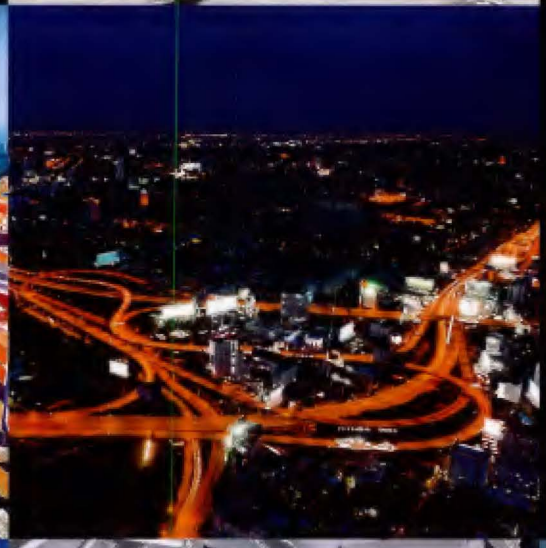
15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19, SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

ITS KRITIS

VeSiKi



Monitor

IT-Sicherheit Kritischer Infrastrukturen

Gefördert vom
Bundesministerium für Bildung und Forschung

1. Auflage, 2017

Herausgeberin: Prof. Dr. Ulrike Lechner

Broschüre ist erstellt von dem Projekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi) als Begleitforschungsprojekt im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS) des Bundesministeriums für Bildung und Forschung (FKZ 16KIS0213).

Projektleitung VeSiKi:
Prof. Dr. Ulrike Lechner und Dr. Steffi Rudel

Projektleitung Monitor IT-Sicherheit Kritischer Infrastrukturen:
Sebastian Dännart und Tamara Gurschler

Die Umfrage wurde von Christian Voß, Sebastian Dännart, Andreas Rieb, Alexander Laux und Patrick Quellmalz (VOICE e. V.) formuliert und ausgearbeitet. Die Auswertung der Ergebnisse erfolgte durch Sebastian Dännart und Tamara Gurschler.

Lektorat: Lektorat & Textagentur Dr. Heiner Lohmann

Design: Artes Advertising GmbH, München

Druck und buchbinderische Verarbeitung:
Rechenzentrum der Universität der Bundeswehr München

ISBN 978-3-943207-27-9

VORWORT

Kritische Infrastrukturen funktionieren in Deutschland zuverlässig – so zuverlässig, dass die Bevölkerung eher erstaunt reagiert, wenn auf die Möglichkeit von Ausfällen und die Notwendigkeit, sich vorzubereiten, hingewiesen wird. Die Betreiber Kritischer Infrastrukturen nehmen ihre Verantwortung ernst und das gilt auch für das neue Themenfeld der „IT-Sicherheit für Kritische Infrastrukturen". Denn die zunehmende Durchdringung aller Lebens- und Arbeitsbereiche durch Informations- und Kommunikationstechnologien bestimmt maßgeblich den technologischen Fortschritt und die Innovationsfähigkeit, birgt aber auch neue Risiken. Weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens hängen von robusten und resilienten Informations- und Kommunikationstechnologien ab. Der Schutz Kritischer Infrastrukturen vor Cyberangriffen ist für die selbstbestimmte und sichere Zivilgesellschaft lebensnotwendig.

Das IT-Sicherheitsgesetz und die KRITIS-Verordnungen schaffen seit 2015 einen Rahmen für die IT-Sicherheit Kritischer Infrastrukturen und mit UP KRITIS gibt es seit Jahren öffentlich-private Partnerschaften für die IT-Sicherheit Kritischer Infrastrukturen.

Die vorliegende Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen" will den aktuellen Stand der IT-Sicherheit für Kritische Infrastrukturen vor allem aus der Sicht der Betreiber abbilden. Themen der Umfrage sind die Bedrohungslage der IT-Sicherheit Kritischer Infrastrukturen, Selbsteinschätzung der Bedrohungslage und Cybersecurity-Fähigkeiten, Stand der IT-Sicherheitsmaßnahmen, Budgets für Sicherheit, Einfluss des IT-Sicherheitsgesetzes auf Kritische Infrastrukturen und Innovationsfähigkeit. Einen Themenschwerpunkt im Monitor stellt der Bedarf Kritischer Infrastrukturen an Konzepten, Verfahren und Technologien der IT-Sicherheit dar.

Für den Monitor IT-Sicherheit Kritischer Infrastrukturen wurden IT-Sicherheitsverantwortliche in Deutschland befragt. Der Fragebogen wurde im Frühjahr 2016 konzipiert und umfasste 51 Fragen. Die Umfrage selbst fand vom Juni 2016 bis Oktober 2016 statt. Es konnten 79 Teilnehmerinnen und Teilnehmer für die Umfrage gewonnen werden.

Diese Umfrage wurde durchgeführt von dem Projekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)" als Teil des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen (ITS|KRITIS), der vom Bundesministerium für Bildung von Forschung gefördert wird. Die Forschungsprojekte im Förderschwerpunkt konnten Fragen beitragen.

Wir bedanken uns bei den Teilnehmern an dieser Umfrage, bei den Multiplikatoren (siehe Seite 42–43), die für die Umfrage gestreut haben und vor allem beim Bundesministerium für Bildung und Forschung für die Förderung dieser Forschungsarbeit.

Prof. Dr. Ulrike Lechner

Leiterin des Forschungsprojekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen" und Professorin an der Universität der Bundeswehr München

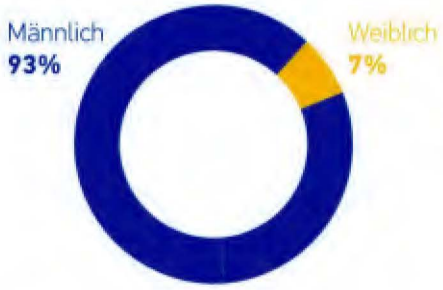
INHALTSVERZEICHNIS

DIE TEILNEHMER

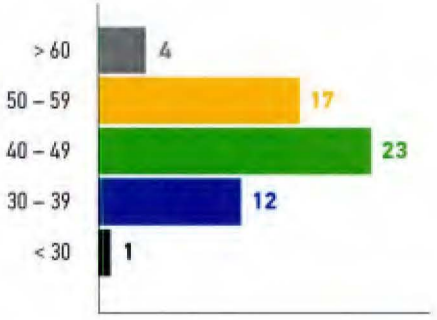
DEMOGRAFIE

Die Angabe der Position des Teilnehmers im Unternehmen zeigt ein heterogenes Teilnehmerfeld, wobei eine hohe Beteiligung der Führungsebene von CEOs, CISOs und IT-Sicherheitsbeauftragten deutlich wird. Mehr als 3/4 der Befragten sind über 40 Jahre und mehr als 1/3 sogar über 50 Jahre alt.

Geschlecht der Teilnehmer



Alter der Teilnehmer



Position der Teilnehmer im Unternehmen

BRANCHEN

12%
Gesundheit

1%
Wasserversorgung

6%
Staat und Verwaltung

37%
Informations- und Telekommunikationstechnik

3%
Medien und Kultur

7%
Transport und Verkehr

3%
Ernährung

19%
Energie

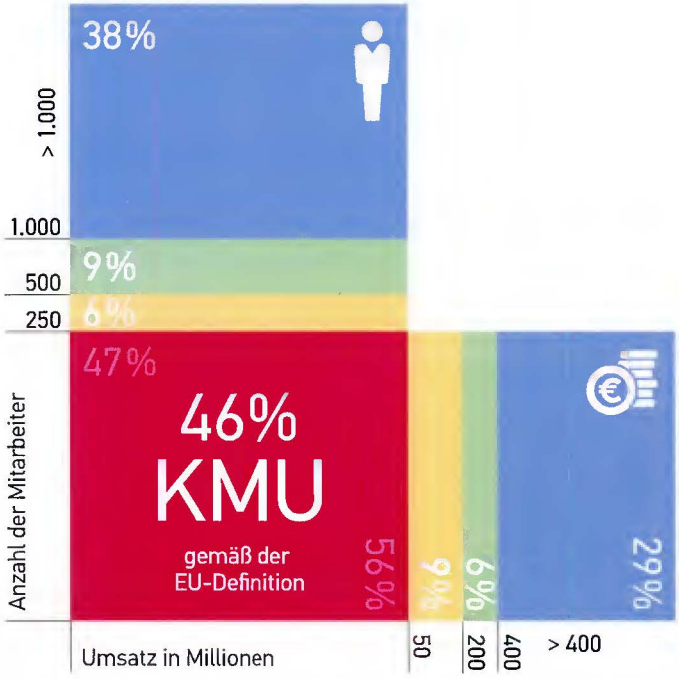
... sowie 12% aus anderen Branchen

KLEINE UND MITTLERE UNTERNEHMEN

DEFINITION: **Kleine und mittlere Unternehmen**
In der EU-Empfehlung der Kommission 2003/361 werden kleine und mittlere Unternehmen (KMU) definiert: Die Größenklasse der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft

EU-Empfehlung der Kommission 2003/361

Teilnehmer nach Anzahl der Mitarbeiter und Umsatz



KRITISCHE INFRASTRUKTUREN

Das Bundesministerium des Innern gibt in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) eine Definition für Kritische Infrastrukturen vor und veröffentlicht neun Sektoren, in die sich Organisationen und Unternehmen einordnen lassen.

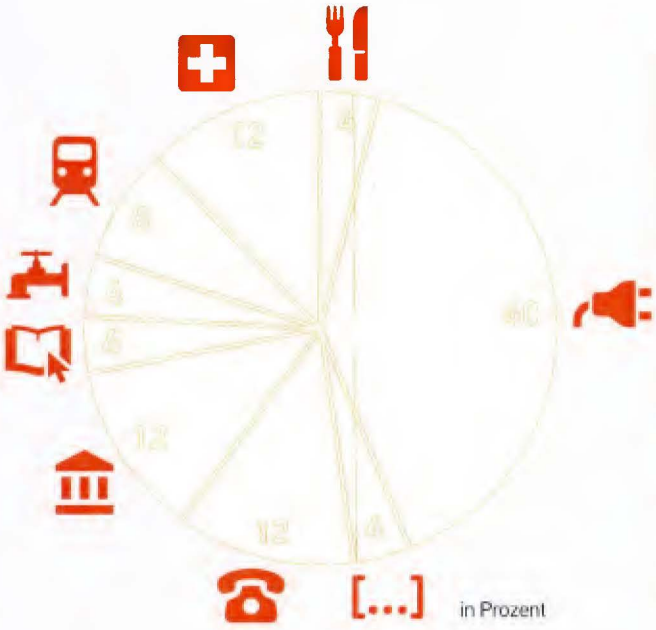
DEFINITION: **Kritische Infrastruktur**
Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Bundesministerium des Innern, KRITIS-Strategie

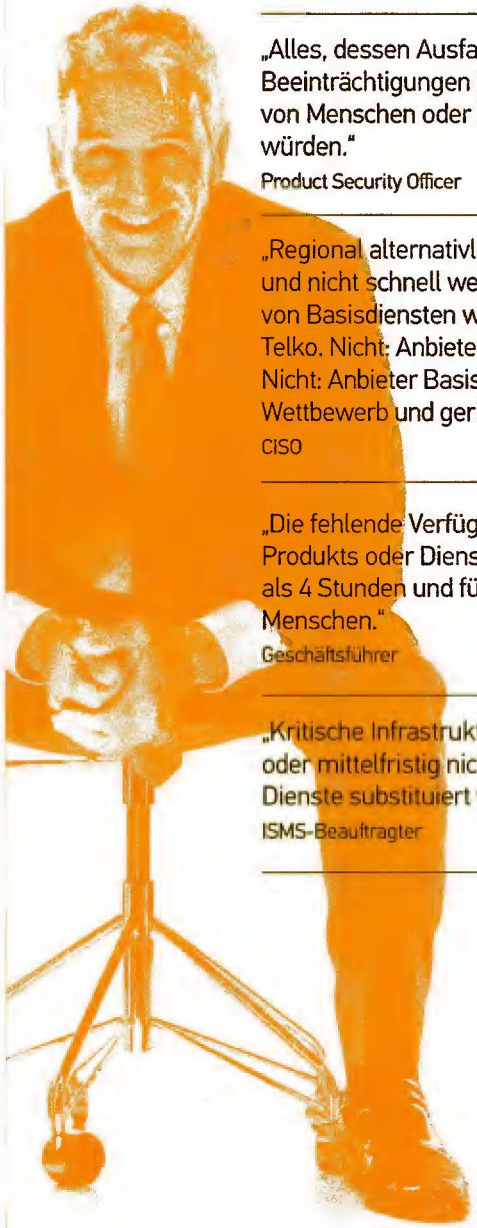
BIN ICH KRITIS?

Das Verständnis für die Bedeutung einer Kritischen Infrastruktur trägt elementar zum sicherheitstechnischen Selbstverständnis einer Organisation bei. Um die eigene Organisation als Kritische Infrastruktur einordnen zu können und zu wollen, ist ein einheitliches Bild davon, was eine Kritische Infrastruktur ausmacht, nötig. Was zeichnet eine solche in den Augen von IT-Sicherheitsverantwortlichen aus?

Die Umfrageergebnisse spiegeln nicht nur das sehr inhomogene Bild davon, was eine Kritische Infrastruktur ausmacht wider, sondern zeigen auch eine unterschiedliche Wahrnehmung, welche Organisationen in diese Kategorie fallen und entsprechend schützenswerter sind als andere. Zudem variieren die Aussagen in Bezug auf Reichweite und Auswirkung einer Beeinträchtigung stark.

Etwa 37 % der Teilnehmer bezeichneten sich selbst als Kritische Infrastrukturen (KRITIS). Eingeordnet in die vom BMI vorgeschlagenen Branchen ergibt sich folgende Verteilung:





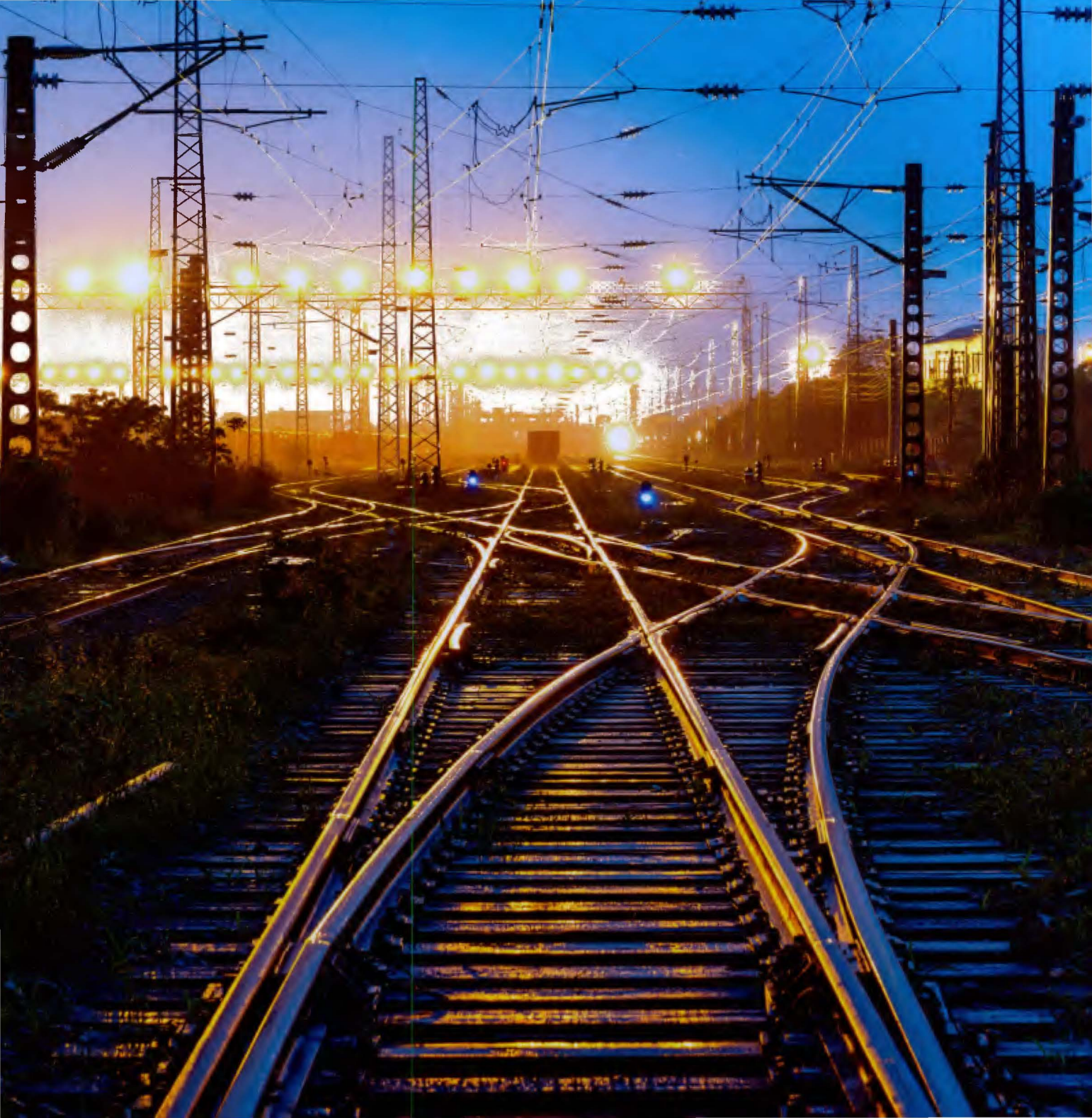
WAS MACHT KRITIS FÜR SIE AUS?

„Alles, dessen Ausfall zu erheblichen Beeinträchtigungen für eine große Zahl von Menschen oder Firmen führen würden."
Product Security Officer

„Regional alternativlose, nicht einfach und nicht schnell wechselbare Anbieter von Basisdiensten wie Strom, Wasser, Telko. Nicht: Anbieter von Luxusdiensten. Nicht: Anbieter Basisdiensten mit hohem Wettbewerb und geringer Wechselhürde."
CISO

„Die fehlende Verfügbarkeit eines Produkts oder Dienstleistung für mehr als 4 Stunden und für mehr als 20000 Menschen."
Geschäftsführer

„Kritische Infrastrukturen können kurz- oder mittelfristig nicht durch andere Dienste substituiert werden."
ISMS-Beauftragter



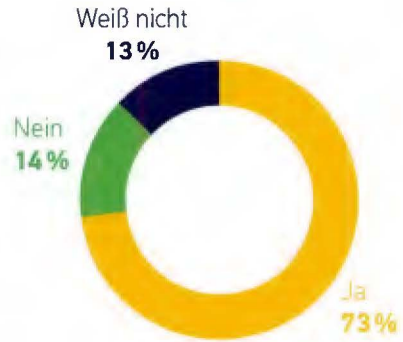
DIE BEDROHUNGSLAGE

73% der Organisationen und 85% der Kritischen Infrastrukturen, die am Monitor teilgenommenen haben, waren im letzten Jahr Ziel einer Cyber-Attacke. Mehr als die Hälfte konnte gezielte Cyber-Attacken feststellen und nur 14% der befragten Unternehmen schlossen Angriffe auf ihre IT-Infrastruktur aus.

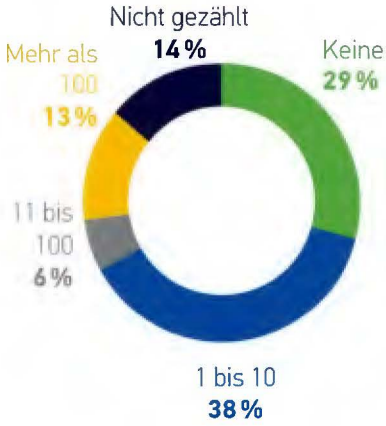
Den Stand der eigenen IT-Sicherheit beurteilt die deutliche Mehrheit der Organisationen mit „gut" oder „sehr gut". KRITIS-Unternehmen beurteilen den Stand der IT-Sicherheit insgesamt besser als der Durchschnitt aller Befragten: In KRITIS schätzen 88% den aktuellen Stand der IT-Sicherheit im eigenen Unternehmen zumindest als „gut" ein – lediglich 12% empfinden die aktuelle Situation als „schlecht". In der Gesamtheit der Unternehmen dagegen beschreiben 21% den Stand der IT-Sicherheit als „schlecht" und weitere 2% als „sehr schlecht".

Die Kritischen Infrastrukturen in Deutschland scheinen also bereits jetzt ihre Verantwortung zu kennen und ernst zu nehmen.

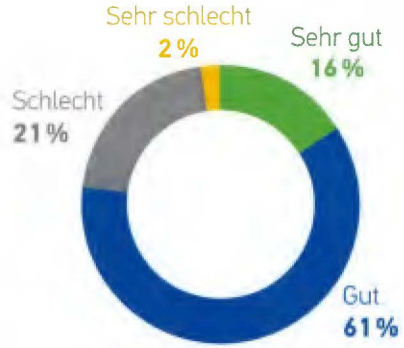
War Ihre Organisation innerhalb des letzten Jahres Ziel von Cyber-Attacken?



Wie viele gezielte Cyber-Attacken konnten Sie innerhalb des letzten Jahres feststellen?



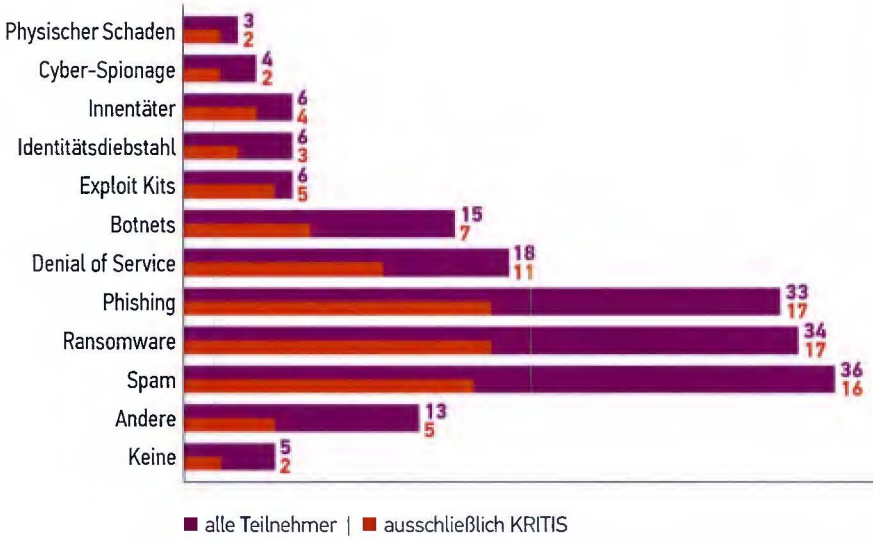
Wie bewerten Sie den aktuellen Stand der IT-Sicherheit in Ihrer Organisation?



DAS SPEKTRUM DER ANGRIFFE

Das potenzielle Angriffsspektrum mit dem sich Kritische Infrastrukturen auseinandersetzen müssen, um sichere und stabile Dienstleistungen anbieten zu können, ist groß. Besonders häufig wurden die Angriffsvektoren Phishing und Spam zusammen mit dem im Jahr 2016 vergleichsweise neuen Angriffsvektor „Ransomware" genannt. Es fällt auf, dass KRITIS-Unternehmen unterproportional häufig den Standardangriff Spam nennen, dafür aber überproportional oft spezifischere Angriffsvektoren wie Denial of Service, Innentäter oder Exploit Kits. 4 von insgesamt 6 Innentätern und 5 von 6 Angriffen durch Exploit Kits waren gegen Kritische Infrastrukturen gerichtet.

Welche Art von Angriffen konnte festgestellt werden?



ANGRIFFE MIT SERVICEAUSFALL ODER DATENVERLUST

Die Umfrage untersuchte des Weiteren, wie oft Angriffe tatsächlich einen Serviceausfall oder einen Datenverlust zur Folge hatten.

Alle Teilnehmer 40%

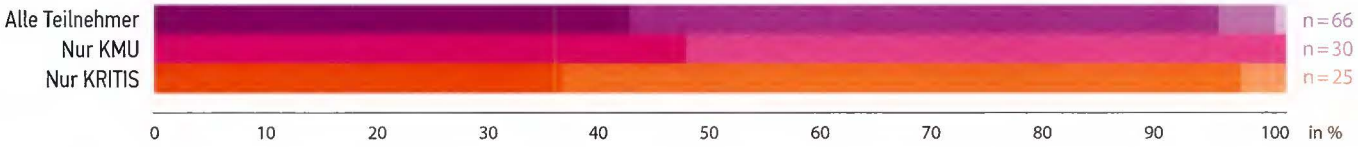
KRITIS 45%

EINSCHÄTZUNG DER BEDROHUNGSLAGE

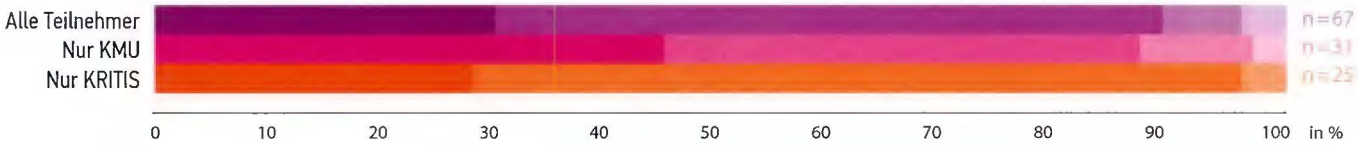
Wir baten die Teilnehmer die derzeitige Bedrohungslage im Bereich der IT-Sicherheit einzuschätzen – und zwar differenziert für den Wirtschaftsraum Deutschland, die eigene Branche und für das eigene Unternehmen. Die überwältigende Mehrheit beurteilt die Bedrohungslage als „hoch" oder „sehr hoch".

Die Bedrohungslage wird – bei allen Befragten – für die eigene Organisation als weitaus geringer wahrgenommen als für die Branche und für den gesamten Wirtschaftsraum Deutschland. Die KRITIS-Organisationen schätzen die Bedrohung fast durchweg höher ein. KMUs dagegen sehen die eigene Organisation durchweg weniger gefährdet als der Durchschnitt.

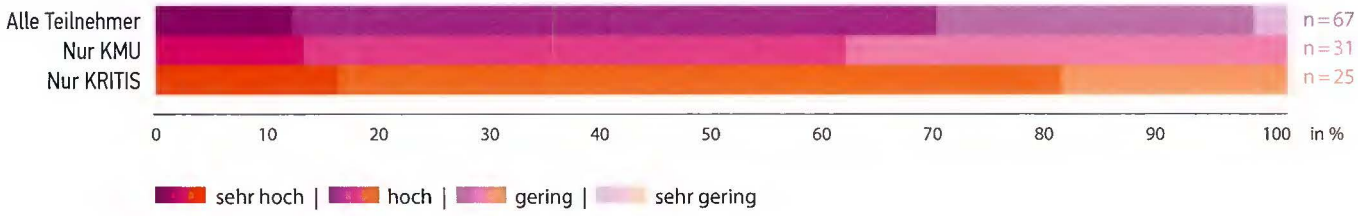
Wie hoch schätzen Sie die derzeitige Bedrohungslage im Bereich der IT-Sicherheit ein für den Wirtschaftsraum Deutschland?



Wie hoch schätzen Sie die derzeitige Bedrohungslage im Bereich der IT-Sicherheit ein für Ihre Branche?



Wie hoch schätzen Sie die derzeitige Bedrohungslage im Bereich der IT-Sicherheit ein für Ihre Organisation?

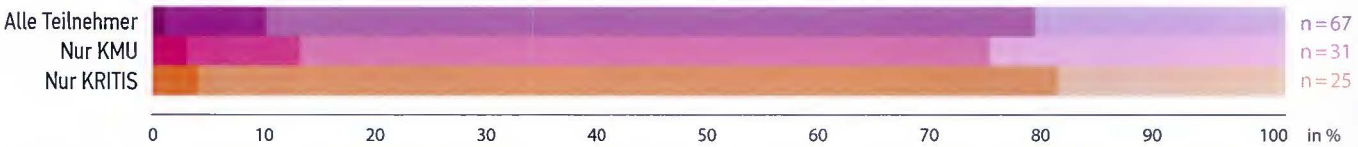


EINSCHÄTZUNG DER FÄHIGKEIT, CYBER-ANGRIFFE ABZUWEHREN

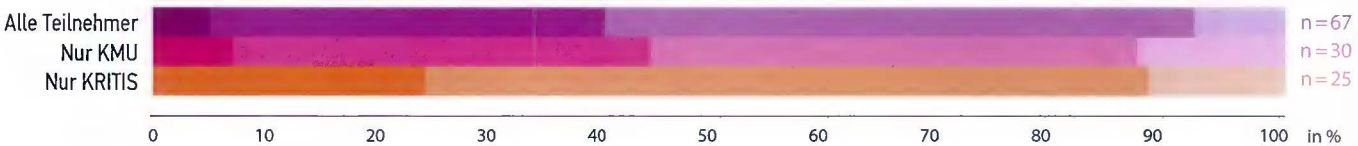
In der Fähigkeit zur Abwehr von Cyber-Attacken sehen 90 % aller Teilnehmer nur „geringe" oder „sehr geringe" Fähigkeiten im Wirtschaftsraum Deutschland. Besonders kritisch beurteilen diese Fähigkeit die Betreiber Kritischer Infrastrukturen. Die eigene Fähigkeit, Cyber-Angriffe abzuwehren, wird durchweg als höher eingeschätzt als die der eigenen Branche und diese wiederum höher als die des Wirtschaftsraums Deutschland.

Diese Wahrnehmung trifft auch auf die KRITIS-Unternehmen zu. Diese schätzen die Abwehrfähigkeiten zwar allgemein pessimistischer ein, sehen die eigene Abwehrfähigkeit von Cyber-Angriffen, im Vergleich zu KMU und allen Teilnehmern, aber am Positivsten.

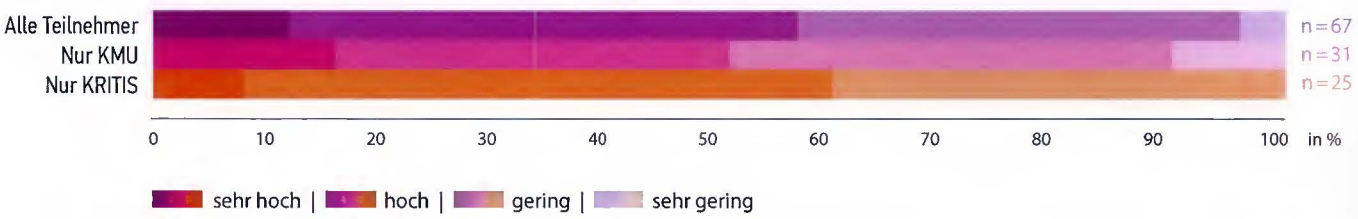
Wie hoch schätzen Sie die Fähigkeit ein, Cyber-Attacken abzuwehren, für den Wirtschaftsraum Deutschland?



Wie hoch schätzen Sie die Fähigkeit ein, Cyber-Attacken abzuwehren, für Ihre Branche?



Wie hoch schätzen Sie die Fähigkeit ein, Cyber-Attacken abzuwehren, für Ihre Organisation?



RESSOURCEN FÜR IT-SICHERHEIT

Der Anteil des Budgets für IT-Sicherheit am IT-Budget insgesamt verteilt sich bei den Befragten relativ gleichmäßig zwischen 0% und 10% – nur ein sehr geringer Anteil gibt mehr als 10% der IT-Ausgaben für die IT-Sicherheit aus.

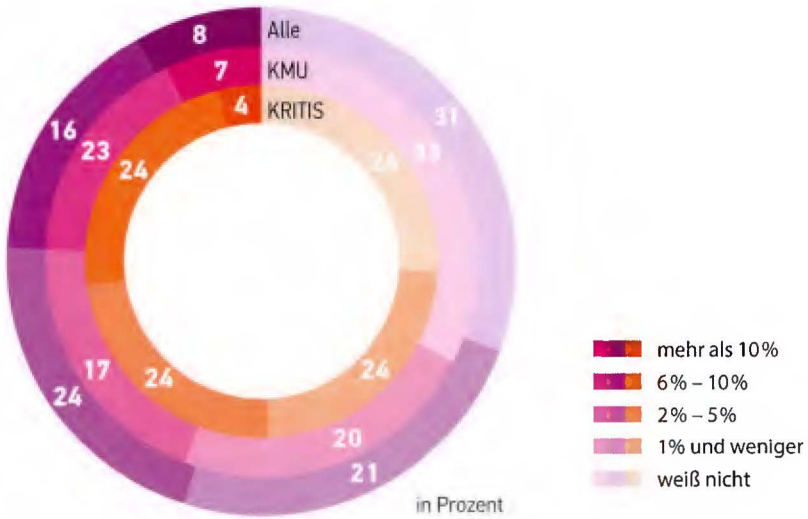
Innerhalb der Betreiber Kritischer Infrastrukturen findet mehr als die Hälfte der Befragten, dass das Budget „zu wenig" oder „viel zu wenig" ist. Bei der Betrachtung aller Befragten sinkt diese Zahl zwar ein wenig ab ist aber mit 53% immer noch sehr hoch.

Gerade in Kritischen Infrastrukturen ist das IT-Budget teilweise nur marginal – da der IT-Anteil an den Kosten für die Infrastruktur häufig gering ist. Erfreulicherweise erwarten im kommenden Jahr 64% der befragten KRITIS-Organisationen steigende Investitionen im Bereich der IT-Sicherheit. In keinem einzigen Fall werden sinkende Investitionen angenommen oder angestrebt.

Halten Sie dieses Budget für ausreichend?

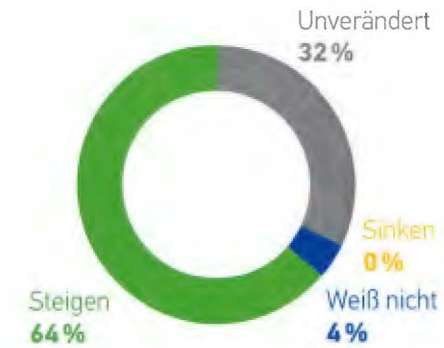
[KRITIS]

Wie hoch ist der Anteil Ihres IT-Sicherheitsbudgets, gemessen am gesamten IT-Budget Ihrer Organisation?



Wie werden sich die Investitionen in Ihrer Organisation im Bereich der IT-Sicherheit im nächsten Jahr entwickeln?

[KRITIS]



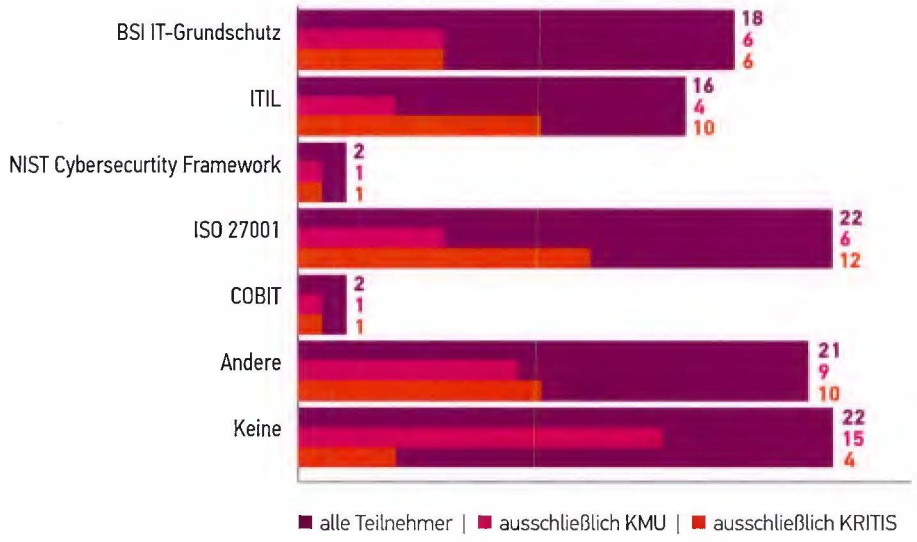
DIE REALISIERUNG VON IT-SICHERHEIT

RAHMENWERKE, STANDARDS UND ZERTIFIKATE

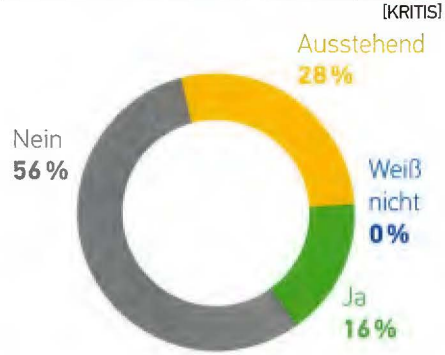
Unternehmen stützen sich beim Management der IT in der Regel auf Rahmenwerke und Standards. Häufig werden ITIL, der BSI IT-Grundschutz sowie der Standard zur Einführung eines Managementsystems für Informationssicherheit, ISO/IEC 27001, verwendet – rund 44 % der Unternehmen, die eine kritische Versorgungsdienstleistung zur Verfügung stellen, streben eine entsprechende Zertifizierung ihres Informationssicherheits-Managementsystems (ISMS) an oder haben diese bereits erhalten.

Die Betreiber Kritischer Infrastrukturen setzen überdurchschnittlich oft ISMS nach ISO/IEC 27001 und ITIL ein. Im Gegensatz dazu wenden viele KMUs häufig keine bestehenden Rahmenwerke an. Es waren Mehrfachnennungen möglich.

Wird die IT-Sicherheit in Ihrer Organisation durch ein bestehendes Rahmenwerk unterstützt?



Ist Ihre Organisation nach ISO 27001 zertifiziert?

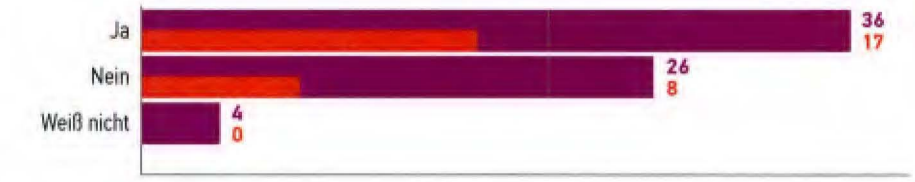


STRATEGISCHE AUSRICHTUNG

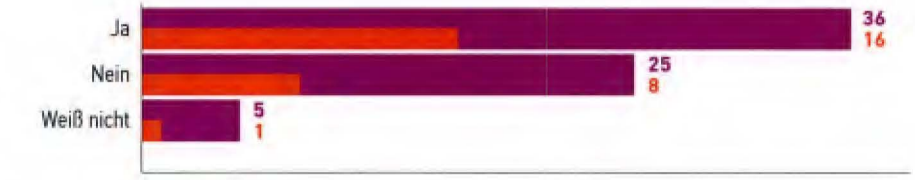
Neuen Angriffswegen, neu eingeführten Technologien und Änderungen an der IT-Infrastruktur ist es geschuldet, dass sich die Risikolage eines Unternehmens laufend verändert. Aus diesem Grund müssen Risiken in regelmäßigen Abständen neu identifiziert, analysiert und bewertet werden, damit vorbeugende Sicherheitsmaßnahmen wirksam getroffen werden können.

Die KRITIS-Unternehmen wissen über die Wichtigkeit der Risikobewertung Bescheid - der Anteil der Organisationen, die keine regelmäßige Risikobewertung durchführen, ist bei Betrachtung aller Befragten allerdings signifikant höher. Zusätzlich wird bei der IT-Sicherheit von KRITIS-Unternehmen häufiger die IT-Sicherheit von Geschäftspartnern und Zulieferern betrachtet. Die Überarbeitung des IT-Sicherheitskonzeptes erfolgt meist in einem kontinuierlichen oder jährlichen Rahmen.

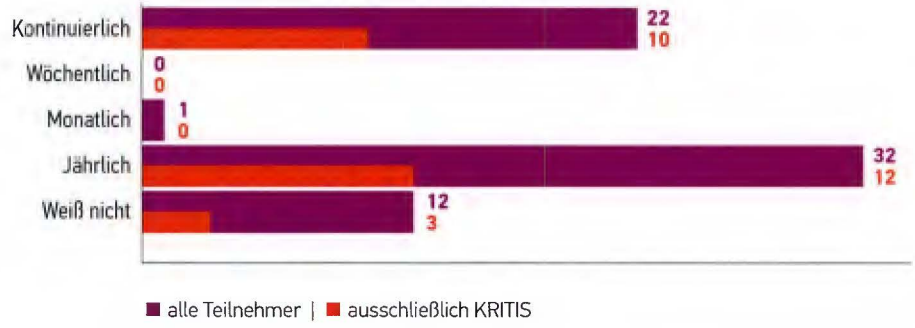
Findet in Ihrer Organisation eine regelmäßige IT-Risikobewertung statt?



Wird im Rahmen der IT-Sicherheit Ihrer Organisation die IT-Sicherheit der Geschäftspartner und der Zulieferer mit betrachtet?



In welchen Abständen wird Ihr IT-Sicherheitskonzept überarbeitet?

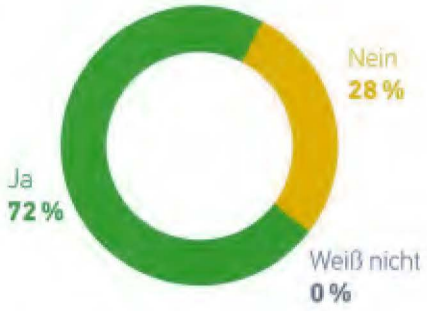


IT-SICHERHEITSBEAUFTRAGTE UND EXTERNE ZUSAMMENARBEIT

Die Aufgabe, Informationssicherheit in einem Unternehmen umzusetzen und langfristig gewährleisten zu können, erfordert Ressourcen und organisatorisches Geschick. Keine Kritische Infrastruktur gibt jedoch die Realisierung der IT-Sicherheit rein in externe Hände. Viele der befragten KRITIS-Organisationen beschäftigen mindestens einen Mitarbeiter, der sich ausschließlich um die IT-Sicherheit im Unternehmen kümmert. Für 40 % ist ein partielles Outsourcing oder eine Zusammenarbeit mit externen Dienstleistern möglich, überwiegend wird IT-Sicherheit aber intern gehandhabt.

Gibt es eine Einzelperson in Ihrer Organisation, die rein für IT-Sicherheit verantwortlich ist, nicht nur in einer Nebenfunktion?

[KRITIS]

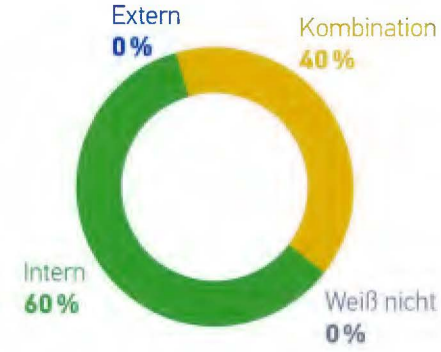


13 von 24

Unternehmen haben einen Mitarbeiter für IT-Sicherheit, arbeiten mit behördlichen Stellen zusammen und sind in einem Verband organisiert.

Wird die IT-Sicherheit in Ihrer Organisation durch einen externen Dienstleister bereitgestellt oder intern behandelt?

[KRITIS]



3 von 24

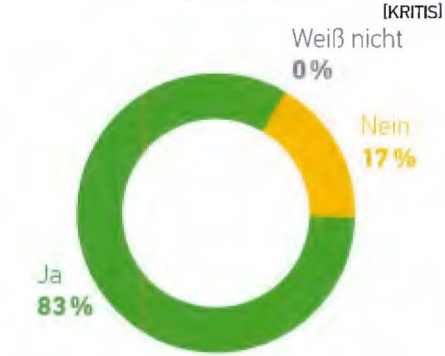
Unternehmen haben einen Mitarbeiter für IT-Sicherheit, arbeiten nicht mit behördlichen Stellen zusammen, sind aber in einem Verband organisiert.

Bereits 83% der Betreiber einer Kritischen Infrastruktur sind in Verbänden, die sich mit der IT-Sicherheit auseinandersetzen, organisiert. Das Interesse an Austausch und Kooperation scheint in diesem Bereich besonders groß zu sein, denn auch der Anteil der KRITIS, die mit behördlichen Stellen zusammenarbeiten, liegt bei 72%.

Bemerkenswerterweise sind bei der Betrachtung aller Befragten deutlich weniger in einem Verband organisiert oder arbeiten mit behördlichen Stellen zusammen:

58 % aller Teilnehmer sind in mindestens einem Verband organisiert

Ist Ihre Organisation in einem Verband organisiert, der sich mit der IT-Sicherheit befasst?

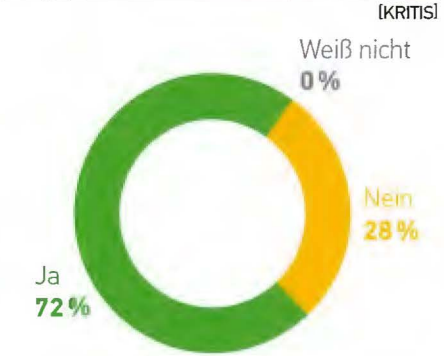


3 von 24

Unternehmen haben keinen Mitarbeiter für IT-Sicherheit, arbeiten aber mit behördlichen Stellen zusammen und sind in einem Verband organisiert.

51 % aller Teilnehmer arbeiten mit behördlichen Stellen zusammen

Arbeitet Ihre Organisation im Bereich IT-Sicherheit in irgendeiner Form mit behördlichen Stellen zusammen?



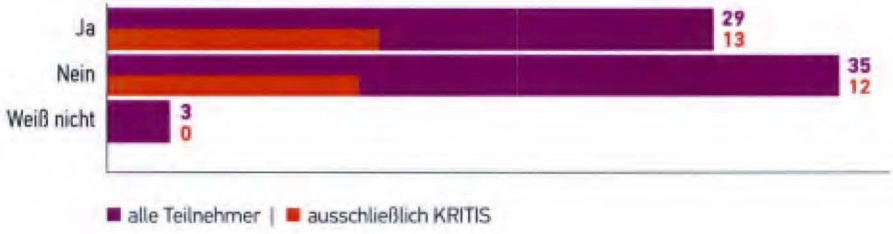
3 von 24

Unternehmen haben keinen Mitarbeiter für IT-Sicherheit, arbeiten nicht mit behördlichen Stellen zusammen und sind in keinem Verband organisiert.

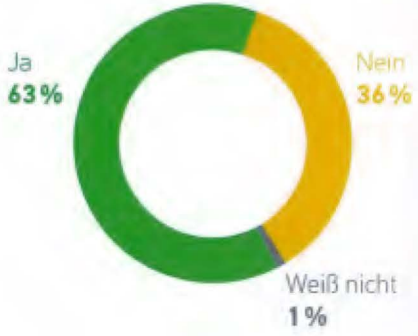
WEITERBILDUNG DER MITARBEITER

Der „Faktor Mensch" ist in der IT-Sicherheit ein zentraler Punkt. 52 % der Kritischen Infrastrukturen setzen weiterführende Schulungen zur IT-Sicherheit für ihre IT-Mitarbeiter bereits um – hier sind KRITIS überdurchschnittlich vertreten, denn bei der Betrachtung aller teilnehmenden Organisationen sinkt dieser Anteil auf 43 % ab. Auch in Hinblick auf Awareness – also das Sicherheitsbewusstsein – bilden viele der befragten Unternehmen ihre Mitarbeiter weiter. Dieser Anteil liegt über 60 %.

Werden in Ihrer Organisation regelmäßig weiterführende IT-Sicherheitsschulungen für Ihre IT-Mitarbeiter durchgeführt?



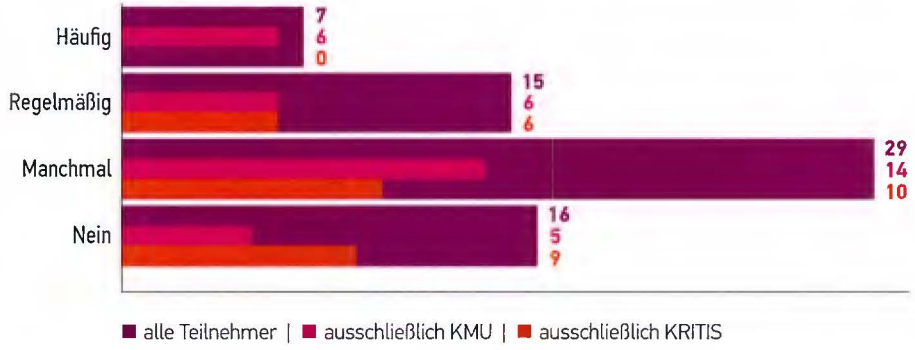
Werden in Ihrer Organisation regelmäßige Awareness-Schulungen für Ihre Mitarbeiter durchgeführt?



EINSATZ NEUER TECHNOLOGIE

Speziell in Hinblick darauf, ob IT-Sicherheit als Hürde für den Einsatz neuer Technologie wahrgenommen wird, wurde das Thema „Verhältnis von Innovation und IT-Sicherheit" untersucht. Unter allen Befragten identifizieren 11 % „häufig", 22 % „regelmäßig" und 43 % „manchmal" IT-Sicherheit als Barriere für die Einführung und Nutzung neuer Technologie. Fragen der IT-Sicherheit hemmen die Innovationsfähigkeit – insbesondere bei KMU und weniger bei KRITIS als bei Nicht-KRITIS-Organisationen.

Sehen Sie IT-Sicherheit als Hinderungsgrund für die Umsetzung neuer Technologien?



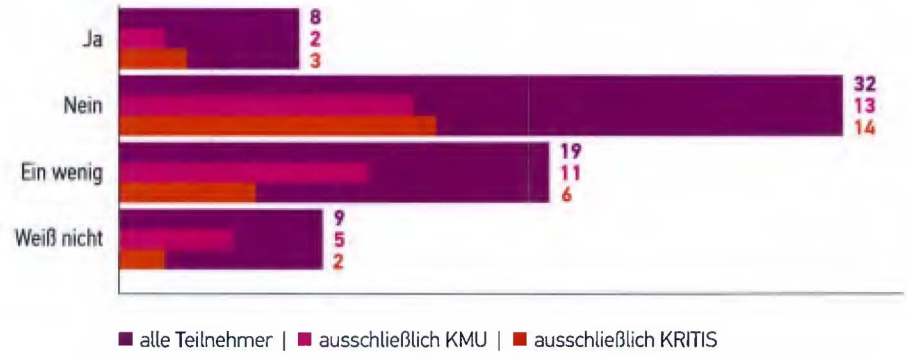
DAS IT-SICHERHEITSGESETZ

Mehr als die Hälfte der KRITIS-Organisationen, die am Monitor teilgenommen haben, sind von diesem Gesetz betroffen und schätzen die Auswirkungen des Gesetzes als signifikant ein.

Es liegt auf der Hand, dass die Umsetzung der gesetzlichen Vorgaben vor allem die kleinen und mittleren Unternehmen (KMU) vor große Herausforderungen stellt. Interessanterweise schätzen 47 % aller Befragten die gesetzlichen Forderungen für KMU nicht als überdimensioniert ein. Selbst KMU schätzen die Anforderungen ganz überwiegend nur als „ein wenig" überdimensioniert oder nicht überdimensioniert ein.

Diese Zahlen können sowohl als Indiz für eine Gesetzgebung mit Augenmaß wie auch als Indiz für das Verantwortungsbewusstsein der KRITIS-Betreiber interpretiert werden.

Halten Sie die gesetzlichen Forderungen bezüglich der IT-Sicherheit für KMU für überdimensioniert?



Hat das IT-Sicherheitsgesetz signifikante Auswirkungen auf die IT-Sicherheit in Ihrem Unternehmen?

IT-SICHERHEITSGESETZ

Das IT-Sicherheitsgesetz (IT-SiG) wurde im Juli 2015 erlassen und beinhaltet Vorgaben zur Verbesserung der IT-Sicherheit. Das Gesetz gilt für Unternehmen, die kritische Versorgungsdienstleistungen zur Verfügung stellen – ausgenommen sind die Sektoren Staat und Verwaltung sowie Medien und Kultur. Im Sinne des IT-SiG sollen gem. § 8a BSIG technisch-organisatorische Mindeststandards festgeschrieben werden und gem. § 8b BSIG sicherheitskritische Vorfälle an das BSI gemeldet werden.

DER BEDARF AN FORSCHUNG

FORSCHUNGSRESULTATE VON ITS|KRITIS

Kritische Infrastrukturen bilden das Rückgrat moderner Industrienationen, sie gewährleisten die grundlegende Versorgung in vielen Bereichen, wie Energie, Informationstechnik und Kommunikation, Transport und Verkehr, Medien und Kultur oder Staat und Verwaltung.

Diese Infrastrukturen werden zunehmend von IT-Systemen gesteuert, die mit dem Internet verbunden sind. Damit ist ein Angriff von außen möglich und der Schutz vor Cyber-Angriffen zu einer neuen Herausforderung geworden.

Das Bundesministerium für Bildung und Forschung fördert 13 Verbundprojekte in dem Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen" – ITS|KRITIS. Den Verbundprojekten wurde im Rahmen des Monitor IT-Sicherheit Kritischer Infrastrukturen die Möglichkeit geboten, den IT-Sicherheitsverantwortlichen in Deutschland Fragen zu stellen. Diese haben das Ziel, die fachliche und somit auch die wirtschaftliche Relevanz der Forschungsergebnisse zu ermitteln.

Ausgewählte Ergebnisse sind in diesem Teil des Berichts dargestellt und die Fragen sind mit dem jeweiligen Verbundprojekt verknüpft.

ITS|KRITIS

Gefördert vom

Bundesministerium
für Bildung
und Forschung

AQUA-IT-Lab

Entwicklung von Lösungsansätzen zum Schutz vor Cyber-Angriffen für kleine und mittlere Betreiber von Kritischen Infrastrukturen am Beispiel der Wasserversorgung.

83 % **fänden es interessant, ihre IT-Sicherheit in einem Testlabor mittels Simulation überprüfen zu können.**

12 % tun dies bereits.

Erhöhung der IT-Sicherheit von Verkehrsleitzentralen und Schutz vor Cyber-Angriffen.

89 % **würden sich gerne mehr über branchenspezifische Strategien der IT-Sicherheit austauschen.**

45 % der Unternehmen sind bereits mit ihrer Branche vernetzt.

50 % der Unternehmen führen Penetrationstests durch.

32 % **wären daran interessiert, allerdings ist die konkrete Umsetzung noch nicht geplant bzw. fehlen nötige Mittel oder Werkzeuge.**

Erforschung einer neuartigen Technologie zur Erkennung und Eindämmung von Cyber-Angriffen in Industrienetzwerken.

85 % **der Unternehmen fänden es interessant, Auffälligkeiten in ihrem Industrienetzwerk automatisiert erkennen zu können.**

12 % setzen hierfür erst ein System ein.

ITS APT

Erweiterung klassischer Testmethoden für die Bewertung der IT-Sicherheit durch Einbeziehen des Sicherheitsbewusstseins.

17 % der teilnehmenden Unternehmen können das IT-Sicherheitsbewusstsein ihrer Mitarbeiter messen.

59 % **können dies zurzeit noch nicht realisieren.**

FORSCHUNGSPROJEKTE ITS|KRITIS

MOSAIK

Methoden für eine effiziente Risikoanalyse Kritischer Infrastrukturen und die Bewertung ihres Sicherheitsniveaus.

72 % der befragten Unternehmen meinen, dass kleine und mittlere Unternehmen besondere Methoden und Werkzeuge benötigen, um die gesetzlichen Forderungen des IT-Sicherheitsgesetzes eigenständig umsetzen zu können.

PREVENT

Konzeption, Entwicklung und Implementation einer in Rechenzentren integrierbaren Software für präventives Risiko- und Krisenmanagement.

23 % der teilnehmenden Unternehmen verwenden ein Framework für das präventive Risiko- und Krisenmanagement.

23 % dagegen fehlen hierfür die nötigen Werkzeuge oder Mittel.

PortSec

Erforschung eines systematischen und umfassenden IT-Risikomanagements in der Hafentelematik.

RISKVIZ

Entwicklung einer Suchmaschine zum Auffinden industrieller Kontrollsysteme (ICS) und zur Bewertung der Risiken.

71 % der Unternehmen fänden es interessant, die externe Erreichbarkeit ihrer Industrieanlagen analysieren zu können.

27 % schaffen dies momentan erst.

83 % fänden es darüber hinaus durchaus von Bedeutung, die Risiken dieser Erreichbarkeit bewerten zu können.

SecMaaS

Erarbeitung von Lösungswegen für die Gewährleistung von IT-Sicherheit in der öffentlichen Verwaltung.

62 % fänden es reizvoll, das IT-Sicherheitsmanagement mithilfe eines Services umsetzen und planen zu können.

25 % fehlen die nötigen Mittel oder Werkzeuge dazu.

SICIA

Entwicklung eines neuartigen Verfahrens zur Ermittlung des Ist-Zustandes der IT-Sicherheit bis auf die Geräteebene.

84 % fänden es interessant, anhand technischer Parameter ihre IT-Sicherheit präzise messen zu können.

10 % können dies jetzt schon.

SIDATE

Konzepte und Werkzeuge für eine schnelle Einschätzung und Verbesserung des vorhandenen Sicherheitsniveaus besonders für kleine und mittlere Energienetzbetreiber.

11 % der teilnehmenden Unternehmen können ihr IT-Sicherheitsniveau anhand von Kennzahlen schnell einschätzen.

75 % würden das auch gerne können.

SORF

Entwicklung einer ganzheitlichen Lösung zur Verbesserung der Schutzsysteme für Kritische Infrastrukturen.

94 % **der Unternehmen wären daran interessiert, ein Hilfsmittel zu haben, das Sicherheitsvorfälle aufdecken und Gegenmaßnahmen vorschlagen könnte.**

9 % nutzen ein solches System bislang erst.

VeSiKi

Wissenschaftliche Begleitforschung des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen.

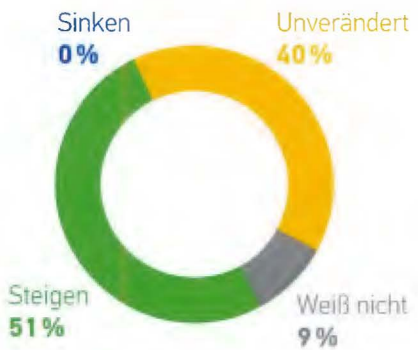
DIE ZUKUNFT DER IT-SICHERHEIT

Der Monitor untersucht, wie die Unternehmen die Entwicklungen der IT-Sicherheit in der Zukunft sehen. Wird IT-Sicherheit wichtiger werden oder wird IT-Sicherheit in Zukunft risikofreudiger und somit reaktiver?

Die befragten Unternehmen beabsichtigen im Schnitt ihre Ausgaben für IT-Sicherheit zu steigern (51 %), oder mindestens beizubehalten (40 %). Keiner der Umfrageteilnehmer plant die Ausgaben für IT-Sicherheit zu senken. Diese Entwicklung stimmt mit dem Bedarf an Forschungsergebnissen überein – Unternehmen würden investieren, wenn entsprechende Technologien verfügbar wären.

Die Planung der Ausgaben für IT-Sicherheit kann nicht unabhängig von der Entwicklung der Bedrohungslage gesehen werden. Denn alle Befragten gehen davon aus, dass die Bedrohungslage im nächsten Jahr zumindest „unverändert" bleiben, „steigen" oder „stark steigen" wird.

Wie werden sich die Investitionen in Ihrer Organisation im Bereich der IT-Sicherheit im nächsten Jahr entwickeln?



13 %
denken, die Bedrohungslage werde im nächsten Jahr unverändert bleiben

60 %
denken, die Bedrohungslage werde im nächsten Jahr steigen

27 %
denken, die Bedrohungslage werde im nächsten Jahr stark steigen

FAZIT

Die IT-Sicherheit Kritischer Infrastrukturen scheint bedroht zu sein. Eine große Anzahl der Betreiber Kritischer Infrastrukturen musste im letzten Jahr Angriffe verzeichnen. Neben den bekannten Arten von Schadsoftware, wie Denial of Service oder Spam, fällt hier eine Bedrohung, die 2016 vergleichsweise neu und in den Schlagzeilen war, auf: Ransomware. Bemerkenswert ist, dass bei den Kritischen Infrastrukturen Bedrohungen durch Innentäter zu verzeichnen waren, während hochprofessionelle Angriffe – APTs – kaum entdeckt wurden. Die Betreiber schätzen ihre Bedrohungssituation genau wie ihre eigenen Fähigkeiten, Angriffe erfolgreich abzuwehren, optimistisch ein – optimistischer als für die eigene Branche oder Deutschland. Dies motiviert den Bedarf an IT-Sicherheitsmanagement-Ansätzen und an Methoden und Technologien, Angriffe zu detektieren, um die Sicherheitssituation valide einschätzen zu können.

Die befragten Betreiber Kritischer Infrastrukturen halten ihre IT-Sicherheitsbudgets überwiegend für zu gering und sehen wenig Implikationen des IT-Sicherheitsgesetzes für ihre eigene Organisation. Die Anforderungen des IT-Sicherheitsgesetzes an kleine oder mittlere Unternehmen als Betreiber Kritischer Infrastrukturen werden überwiegend als machbar angesehen. Verantwortung, Professionalität der Betreiber Kritischer Infrastrukturen und vor allem auch eine Gesetzgebung in Abstimmung mit der Realität Kritischer Infrastrukturen zeigen hier Erfolge – das IT-Sicherheitsgesetz wird den Stand der IT-Sicherheit verbessern und die Anforderungen an die Betreiber scheinen im Rahmen zu liegen.

Der Bedarf an neuen Konzepten, Verfahren und Technologien ist vorhanden. Es wurde mit Fragen der Verbundprojekte des Förderschwerpunkts ITS|KRITIS nach dem Stand bei Kritischen Infrastrukturen und dem Bedarf an neuen IT-Sicherheitsprodukten und Dienstleistungen gefragt. Überraschend ist, wie hoch der Bedarf an solchen Technologien ist und wie viele der Befragten solche Technologien kurz- und mittelfristig einsetzen würden. Die Projekte im Förderschwerpunkt erforschen also Konzepte, Verfahren und Technologien, die bei den Betreibern benötigt werden und auch eingesetzt würden.

DIE MULTIPLIKATOREN

BDI

BICC NET
Bavarian Information and Communication Technology Cluster

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Bundesamt für Sicherheit in der Informationstechnik

BVMW
Bundesverband mittelständische Wirtschaft

DIHK
Deutscher Industrie- und Handelskammertag

GÖTZENBERGER
EDV-Service und -Beratung

IHK Berlin

IHK
Industrie- und Handelskammer für München und Oberbayern


IHK
Oldenburgische
Industrie- und Handelskammer


ITSECURITY
Bavarian IT Security & Safety Cluster


Security
Insider


Sicherheitsnetzwerk
München


VDI


VOICE
Bundesverband der
IT-Anwender e.V.


ZVEI:
Die Elektroindustrie

FRAGENÜBERSICHT

Frage	Stichprobenumfang n	Kommentar
War Ihre Organisation innerhalb des letzten Jahres Ziel von Cyber-Attacken?	n = 55	
Wie viele gezielte Cyberattacken konnten Sie innerhalb des letzten Jahres feststellen?	n = 69	
Welche Art von Angriffen konnte festgestellt werden?	n = KRITIS 84; Alle 161	Mehrfachselektion
Welche Konsequenzen hatten die Cyber-Attacken zur Folge?	n = 40	Mehrfachselektion
Wird die IT-Sicherheit in Ihrer Organisation durch ein bestehendes Rahmenwerk unterstützt?	n = KRITIS 44; Alle 103; KMU 42	Mehrfachselektion
Wird die IT-Sicherheit in Ihrer Organisation durch einen externen Dienstleister bereitgestellt oder intern behandelt?	n = KRITIS 25	
Ist Ihre Organisation nach ISO 27001 zertifiziert?	n = KRITIS 25	
Gibt es eine einzelne Person in Ihrer Organisation, die rein für IT-Sicherheit verantwortlich ist, nicht nur in einer Nebenfunktion?	n = KRITIS 25	
Arbeitet Ihre Organisation im Bereich IT-Sicherheit in irgendeiner Form mit behördlichen Stellen zusammen? (LKA, BKA, BSI, o.ä.)	n = KRITIS 25	
Ist Ihre Organisation in einem Verband organisiert, der sich mit der IT-Sicherheit befasst? (Allianz für Cyber-Sicherheit, VOICE, Sicherheitsnetzwerk München, o.ä.)	n = KRITIS 24	
Werden in Ihrer Organisation regelmäßige Awareness-Schulungen für Ihre Mitarbeiter durchgeführt?	n = 67	
Werden in Ihrer Organisation regelmäßig weiterführende IT-Sicherheitsschulungen für Ihre IT-Mitarbeiter durchgeführt?	n = KRITIS 25; Alle 67	
Findet in Ihrer Organisation eine regelmäßige IT-Risikobewertung statt?	n = KRITIS 25; Alle 66	
Wird im Rahmen der IT-Sicherheit Ihrer Organisation die IT-Sicherheit der Geschäftspartner und Zulieferer mit betrachtet?	n = KRITIS 25; Alle 66	
In welchen Abständen wird Ihr IT-Sicherheitskonzept überarbeitet?	n = KRITIS 25; Alle 67	
Wie hoch ist der Anteil Ihres IT-Sicherheitsbudgets, gemessen am gesamten IT-Budget Ihrer Organisation?	n = KRITIS 25; Alle 67; KMU 30	
Halten Sie dieses Budget für ausreichend?	n = KRITIS 25	
Wie werden sich die Investitionen in Ihrer Organisation im Bereich der IT-Sicherheit im nächsten Jahr entwickeln?	n = KRITIS 25; Alle 67	
Wie bewerten Sie den aktuellen Stand der IT-Sicherheit in Ihrer Organisation?	n = 67	
Hat das IT-Sicherheitsgesetz signifikante Auswirkungen auf die IT-Sicherheit in Ihrem Unternehmen?	n = 25	
Halten Sie die gesetzlichen Forderungen bezüglich der IT-Sicherheit für KMU für überdimensioniert?	n = KRITS 25; Alle 68; KMU 31	

Frage	Stichprobenumfang n	Kommentar
Meinen Sie, dass KMUs zur eigenständigen Umsetzung dieser gesetzlichen Forderungen besondere Methoden und Werkzeuge benötigen?	n = 68	Bedarf nach Forschung – Projekt MoSaIK
Wie hoch schätzen Sie die derzeitige Bedrohungslage im Bereich der IT-Sicherheit ein für ...	Organisation: n = KRITIS 25; Alle 67; KMU 31 Branche: n = KRITIS 25; Alle 67; KMU 31 Deutschland: n = KRITIS 25; Alle 66; KMU 30	
Wie hoch schätzen Sie die Fähigkeit ein Cyber-Attacken abzuwehren für ...	Organisation: n = KRITIS 25; Alle 67; KMU 31 Branche: n = KRITIS 25; Alle 67; KMU 30 Deutschland: n = KRITIS 25; Alle 67; KMU 31	
Sehen Sie IT-Sicherheit als Hinderungsgrund für die Umsetzung neuer Technologien?	n = KRITIS 25; Alle 67; KMU 31	
Wie schätzen Sie, wird sich die Bedrohungslage innerhalb des nächsten Jahres verändern?	n = 67	
Wäre es für Sie interessant ..	AQUA-IT Lab n = 66 CyberSafe n = 66 INDI n = 65 IST.APT n = 66 PREVENT n = 66 RiskViz 71% und 27% n = 66; 83% n = 65 SecMaaS n = 66 Sicia n = 63 Sidate n = 63 Surf n = 66	
In welcher Branche ist Ihre Organisation tätig?	n = 68	
Wie viele Angestellte beschäftigt Ihre Organisation?	n = 68	

Frage	Stichprobenumfang n	Kommentar
Wie hoch ist der jährliche Umsatz Ihrer Organisation?	n = 65	
Was macht für Sie eine Kritische Infrastruktur aus?	n = 32	offene Frage
Würden Sie Ihre Organisation anhand der genannten Definition als „Kritische Infrastruktur" bezeichnen?	n = 67	
Welche Position nehmen Sie in Ihrer Organisation ein?	n = 47	
Alter	n = 57	
Geschlecht	n = 60	

QUELLEN

Empfehlung der Kommission vom 6. Mai 2003 betreffend der Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124 vom 20. Mai 2003.

Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Bundesministerium des Innern (BMI), Juni 2009.

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015.

Weitere Informationen zum Förderschwerpunkt ITS|KRITIS und zu den Verbundprojekten finden Sie auf der Plattform

https://www.itskritis.de

oder unter Twitter

https://twitter.com/itskritis

Diese Broschüre wurde erstellt von
VeSiKi für ITS|KRITIS

Universität der Bundeswehr München
Prof. Dr. Ulrike Lechner und Dr. Steffi Rudel
Werner-Heisenberg-Weg 39
85577 Neubiberg
Tel: +49 89 6004-2504 / -2207
E-Mail: info@vesiki.de