ITS KRITIS

VeSiKi

Monitor 2.0

IT-Sicherheit Kritischer Infrastrukturen

Gefördert vom

Bundesministerium für Bildung und Forschung

1. Auflage, 2018

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 16KIS0213K).

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

Projektleitung Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen:
Sebastian Dännart und Manfred Hofmeier

Die Umfrage wurde von Manfred Hofmeier, Sebastian Dännart, Ulrike Lechner, Steffi Rudel, Thomas Diefenbach und Andreas Rieb formuliert und ausgearbeitet. Die Auswertung der Ergebnisse erfolgte durch Toni Kehr, Manfred Hofmeier und Sebastian Dännart.

Lektorat: Jenifer Kind

Design: Artes Advertising GmbH, München

Druck und buchbinderische Verarbeitung:
Rechenzentrum der Universität der Bundeswehr München

ISBN 978-3-943207-30-9
URN urn:nbn:de:bvb:706-5341

VORWORT

Die Kritischen Infrastrukturen in Deutschland gehören zu den sichersten der Welt und das soll so bleiben. Betreiber Kritischer Infrastrukturen (KRITIS) und mit ihnen die IT-Sicherheitsverantwortlichen in Unternehmen und Behörden haben erhebliche Anstrengungen unternommen, um den von Gesellschaft und Gesetzgeber gestellten Anforderungen an die IT-Sicherheit, formuliert im Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und in den KRITIS-Verordnungen, zu entsprechen; vor allem aber, um ihre Organisationen vor Schadsoftware und Cyberangriffen zu schützen. Die IT-Sicherheitsverantwortlichen nehmen ihre Verantwortung für die Sicherheit ernst – das dokumentiert diese Studie, der ITS|KRITIS Monitor 2.0, ebenso wie den Fortschritt in der IT-Sicherheit im Vergleich zur ersten Studie, welche von uns vor einem Jahr veröffentlicht wurde.

Die vorliegende Studie wird zu einem Zeitpunkt veröffentlicht, zu dem bereits viele Betreiber Kritischer Infrastrukturen Anforderungen des IT-Sicherheitsgesetzes umgesetzt haben und viele Organisationen ihr Niveau der IT-Sicherheit anheben konnten – es bleibt jedoch auch weiterhin viel zu tun: Nicht zuletzt da beispielsweise alleine während der Laufzeit der Umfrage zur vorliegenden Studie neue IT-Sicherheitsbedrohungen für KRITIS zu verzeichnen waren.

Der ITS|KRITIS Monitor 2.0 thematisiert den aktuellen Stand der IT-Sicherheit Kritischer Infrastrukturen, die Umsetzung des IT-Sicherheitsgesetzes sowie die Selbsteinschätzungen der Teilnehmer bezüglich Bedrohungslage und deren Fähigkeiten Angriffe abzuwehren. Analysiert werden Anzahl und Art von Angriffen sowie die Ursachen des Erfolgs von Cyberattacken. Informationen zur IT-Sicherheit, deren Einfluss auf die IT-Sicherheit in Organisationen und auch die Reaktionen auf Informationen stellen einen inhaltlichen Schwerpunkt dieser Studie dar.

Für diese Studie wurden IT-Sicherheitsverantwortliche in Deutschland befragt. Der Fragebogen mit 41 Fragen wurde im Sommer 2017 auf Grundlage der ersten Studie sowie von Forschungsergebnissen des Förderschwerpunkts ITS|KRITIS konzipiert. Die Online-Umfrage fand von Oktober 2017 bis einschließlich Januar 2018 statt und es konnten 69 Teilnehmer für die Umfrage gewonnen werden.

Diese Studie wurde durch das Projekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi) durchgeführt. Dieses ist Teil des Förderschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS), der vom Bundesministerium für Bildung und Forschung gefördert wird.

Wir bedanken uns bei den Teilnehmern dieser Umfrage, bei den Multiplikatoren, die für die Umfrage gestreut haben, und vor allem beim Bundesministerium für Bildung und Forschung für die Förderung dieser Forschung.

Prof. Dr. Ulrike Lechner

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

INHALTSVERZEICHNIS

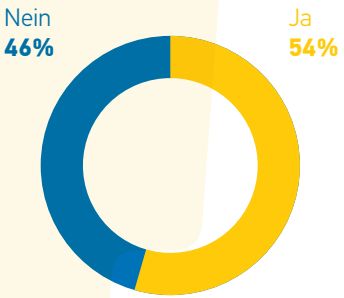
DIE TEILNEHMER

DEMOGRAFIE

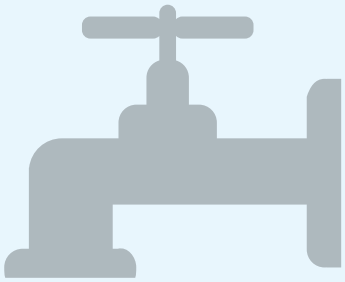
Mehr als die Hälfte der Teilnehmer dieser Umfrage sind hauptverantwortlich für die IT-Sicherheit in ihrem Unternehmen oder in ihrer Organisation. Neben CISOs und IT-Sicherheitsbeauftragten brachten auch die wesentlichen Entscheidungsebenen – mit Managementfunktionen, CIOs und IT-Leitern sowie Mitglieder der Geschäftsführung – ihre Einschätzungen mit ein.

Position der Teilnehmer im Unternehmen

Sind Sie in Ihrer Organisation hauptverantwortlich für die IT-Sicherheit?



BRANCHEN



21,3%
Wasserversorgung

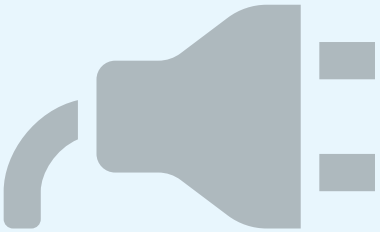
13,1%
Transport und Verkehr

42,6%
Informations- und Telekommunikationstechnik

8,2%
Staat und Verwaltung

1,6%
Medien und Kultur

1,6%
Ernährung



19,7%
Energie

14,8%
Gesundheit

8,2%
Finanz- und Versicherungswesen

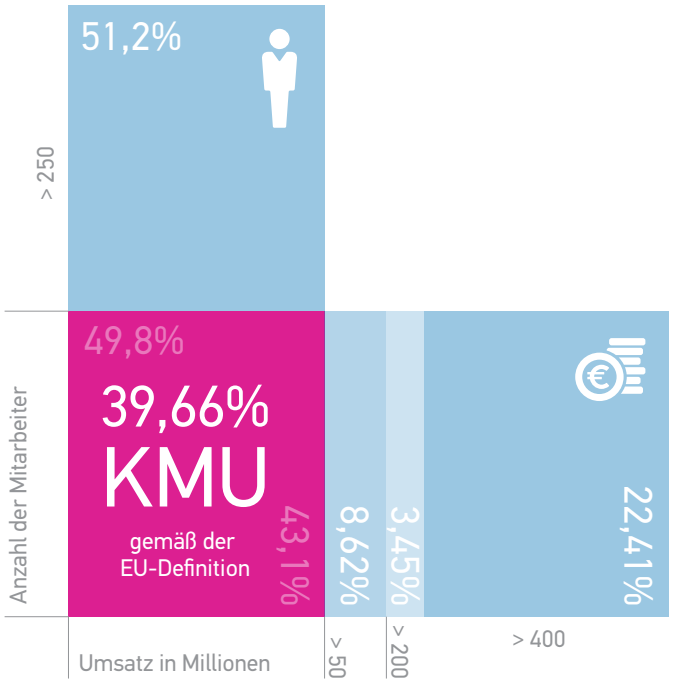
... sowie 6,6% aus anderen Branchen

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



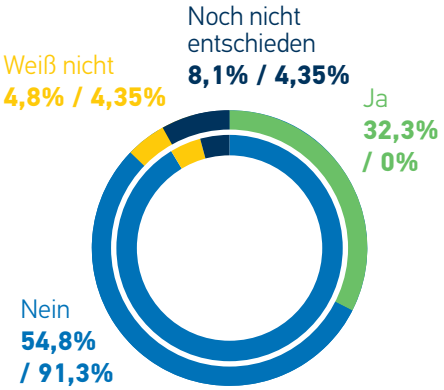
KRITISCHE INFRASTRUKTUREN

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.

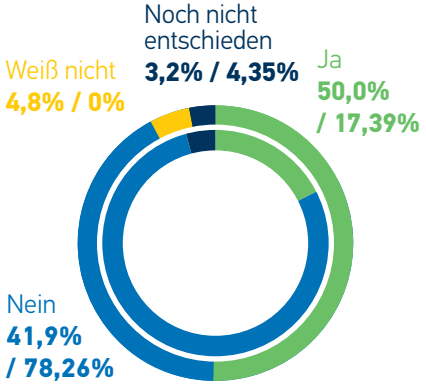
DEFINITION: **Kritische Infrastruktur**
Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Folgen eintreten würden.
Bundesministerium des Innern, KRITIS-Strategie

SIND SIE ...?

Kritische Infrastruktur gemäß IT-Sicherheitsgesetz

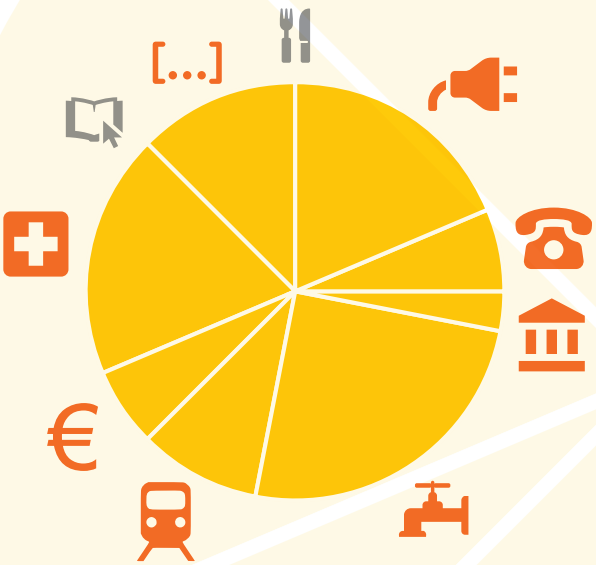


Kritische Infrastruktur gemäß eigener Wahrnehmung



Außen = alle Teilnehmer; Innen = KMU
außen / innen

SEKTORENZUGEHÖRIGKEIT DER TEILNEHMER



BEISPIELE FÜR DIE UMSETZUNG DER MELDEPFLICHT

- Benennung eines IT-Sicherheitsbeauftragten
- Selbstentwickeltes Werkzeug zur Dokumentation von Sicherheitsvorfällen mit Meldefunktion gemäß IT-Sicherheitsgesetz
- Ticket-System zum Melden/Analysieren von Vorfällen/Schwachstellen
- Abwicklung über den Helpdesk
- Übergreifender Incident/Krisenmanagement Prozess

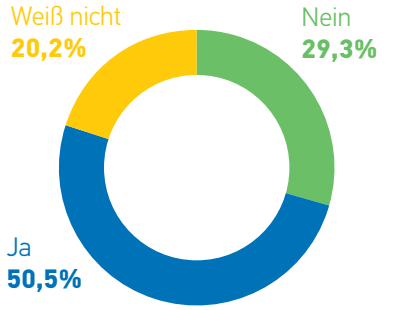
70% **der befragten Kritischen Infrastrukturen haben bereits die Meldepflicht gemäß dem IT-Sicherheitsgesetz umgesetzt.**

DIE BEDROHUNGSLAGE

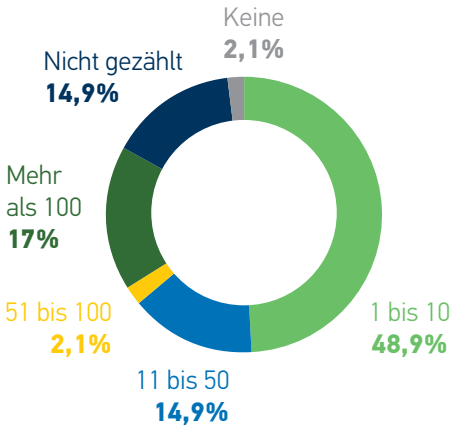
Mehr als die Hälfte der befragten Organisationen waren im letzten Jahr Ziel von Cyber-Attacken. Mit einem Anteil von 50,5% ist diese Zahl jedoch im Vergleich zum Monitor 1.0 und im Vergleich zu anderen aktuellen Studien als niedrig einzuschätzen.

17% der betroffenen Organisationen zählen dabei mehr als 100 gezielte Cyber-Attacken. Im Vergleich zur Studie Monitor 1.0 bedeutet das, dass der Anteil der Befragten mit mehr als 100 gezielten Angriffen leicht gestiegen ist. Etwa 15% können keine Angaben über die Zahl der Angriffe machen.

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



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

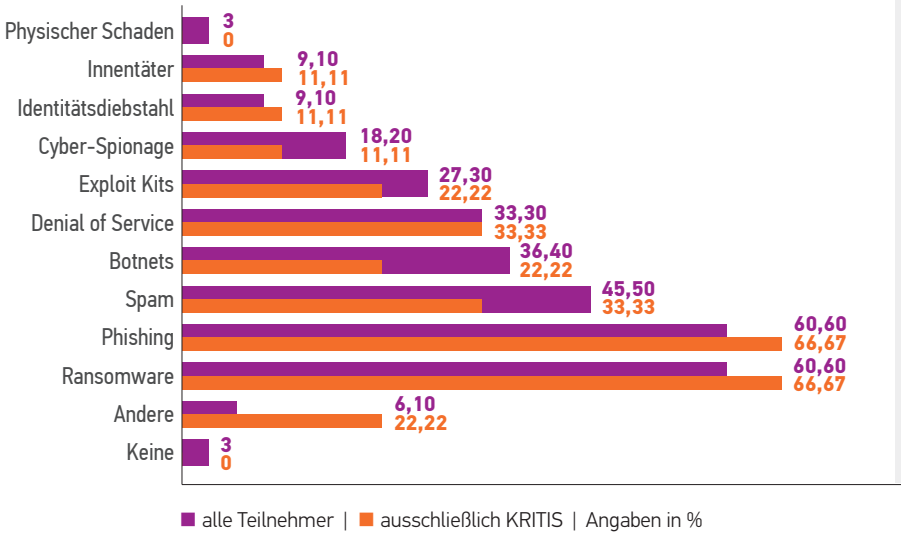


DAS SPEKTRUM DER ANGRIFFE

Das Angriffsspektrum, dem sich Kritische Infrastrukturen ausgesetzt sehen, ist vielfältig. Die beiden Angriffsvektoren Phishing und Ransomware werden dabei besonders häufig genannt und sind bei Kritischen Infrastrukturen überproportional vertreten.

Hier ist auch im Vergleich zum Monitor 1.0 ein starker Anstieg zu verzeichnen (Ransomware +39, Phishing +40 Prozentpunkte), was entweder auf die zunehmende Nutzung dieser Angriffsvektoren im betreffenden Zeitraum oder auf die gestiegene Sensibilität gegenüber diesen Vektoren zurückzuführen ist.

Welche Art von Angriffen konnte festgestellt werden?



ANGRIFFE UNTER MITWIRKUNG VON INNENTÄTERN

gab es bei 9% aller befragten Organisationen und bei 11% der befragten Kritischen Infrastrukturen.

57,6%

aller Teilnehmer konnten die Cyber-Attacken nicht auf Verantwortliche zurückführen.

Fast die Hälfte der befragten Organisationen sehen im Fehlverhalten von Mitarbeitern eine Ursache für den Erfolg von Cyber-Attacken. Aber auch Fehlkonfigurationen, nicht erfolgte Patches und Sicherheitsmängel bei Partnern sind häufig genannte Ursachen für den Erfolg von Cyberattacken.

Interessant ist, dass die vieldiskutierten Zero-Day-Exploits als Ursache für den Erfolg von Cyber-Attacken bei Kritischen Infrastrukturen in dieser Umfrage keine Rolle spielen – sie werden kein einziges Mal genannt, während sie von der Gesamtheit der Befragten als Schwachstelle genannt werden.

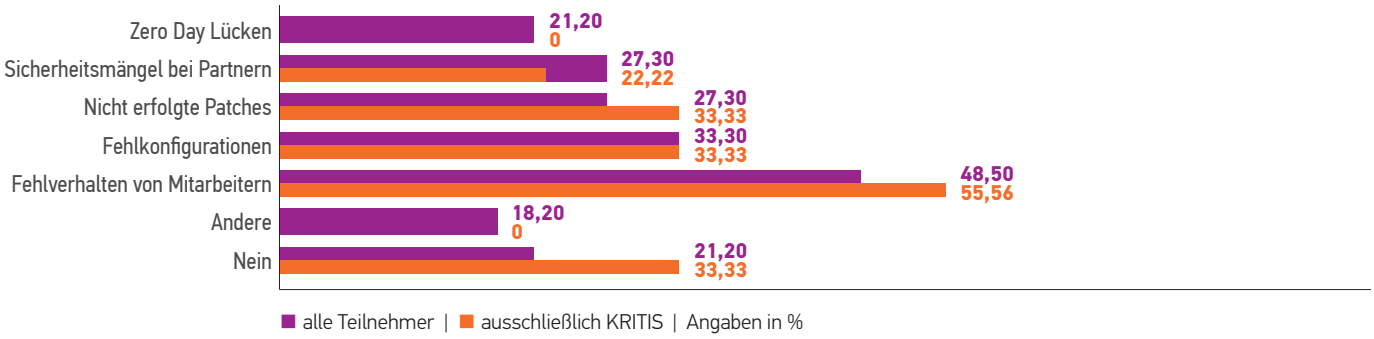
42,4%

der Befragten hatten in Folge der Attacken einen Service- oder Produktionsausfall.

Die Cyber-Sicherheits-Umfrage des BSI weist 51% für Produktions- bzw. Betriebsausfälle nach.

(BSI 2018: Cyber-Sicherheits-Umfrage 2017)

Konnten Ursachen für den Erfolg von Cyber-Attacken festgestellt werden?



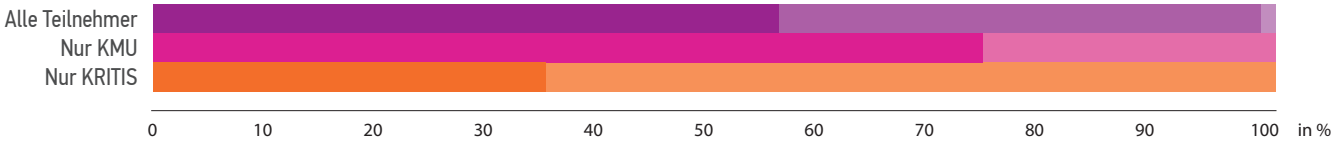
EINSCHÄTZUNG DER BEDROHUNGSLAGE

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

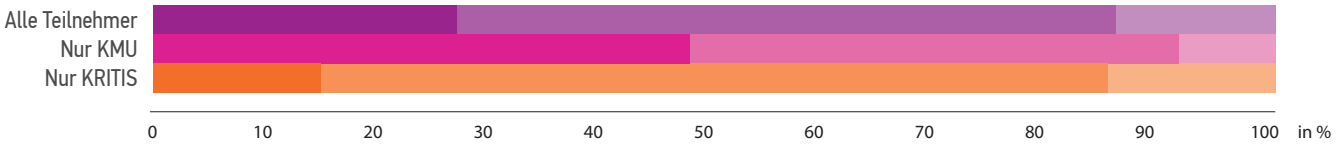
Die Bedrohungslage wird dabei für die eigene Organisation als geringer wahrgenommen als für die Branche und die Bedrohungslage für die Branche wird als geringer wahrgenommen als für den gesamten Wirtschaftsraum Deutschland.

Dieser Effekt einer für die eigene Organisation vergleichsweise niedrigen Risikoeinschätzung war bereits im Monitor 1.0 festzustellen.

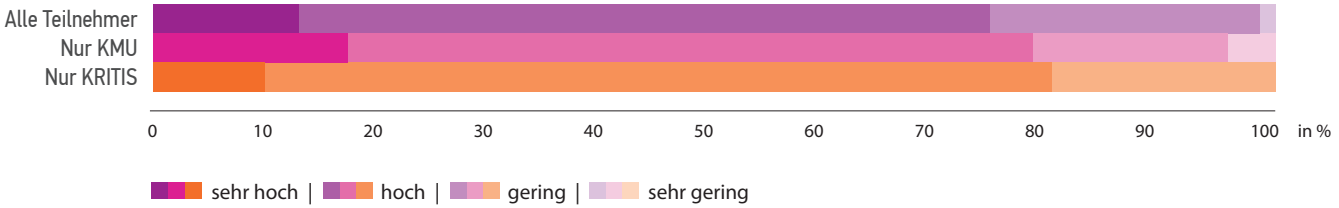
Einschätzung der Bedrohungslage für den Wirtschaftsraum Deutschland?



Einschätzung der Bedrohungslage für Ihre Branche?



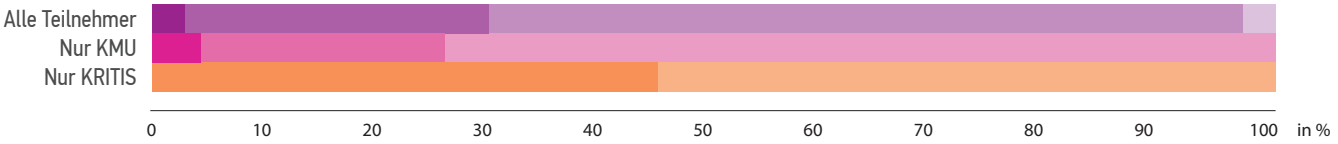
Einschätzung der Bedrohungslage für Ihre Organisation?



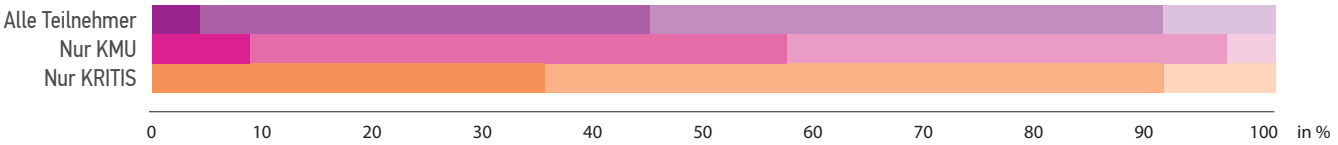
EINSCHÄTZUNG DER FÄHIGKEIT, CYBER-ANGRIFFE ABZUWEHREN

In der Fähigkeit zur Abwehr von Cyber-Attacken sehen 70% aller Teilnehmer nur „geringe“ oder „sehr geringe“ Fähigkeiten im Wirtschaftsraum Deutschland. Die eigene Fähigkeit, Cyber-Angriffe abzuwehren, wird – wie bereits in der ersten Monitor-Umfrage – durchweg als höher eingeschätzt als die der eigenen Branche und diese wiederum höher als die des Wirtschaftsraums Deutschland.

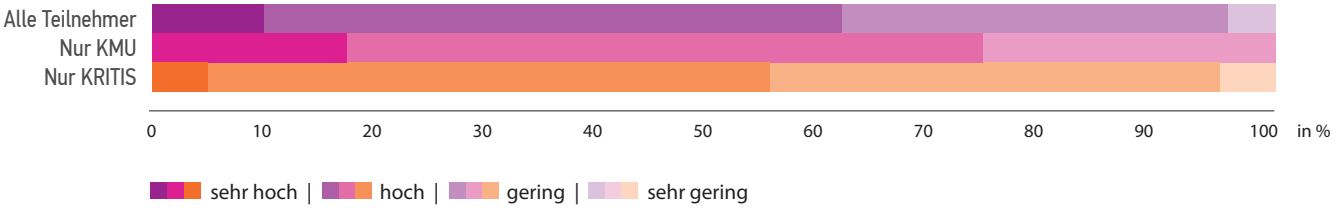
Wie hoch schätzen Sie die Fähigkeit ein, Cyber-Attacken abzuwehren für den Wirtschaftsraum Deutschland?



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?



TREIBER UND AUSLÖSER

SPEZIFISCHE EREIGNISSE

Um den Effekt von spezifischen Bedrohungen auf IT-Sicherheitsmaßnahmen zu untersuchen, wurde nach der Reaktion auf die vier Bedrohungen gefragt, die zum Start der Umfrage die meiste Aufmerksamkeit in der Öffentlichkeit erzeugt hatten: WannaCry, das Mirai-Botnetz, Industroyer und Petya beziehungsweise NotPetya.

Dabei zeigt sich, dass bei Informationen zu neuer Schadsoftware eher selten neue Maßnahmen ergriffen wurden, aber auch selten keine Maßnahmen ergriffen wurden. Meist wurden die bestehenden Maßnahmen überprüft oder die Maßnahmen waren bereits im Vorfeld getroffen, weil die Bedrohung bereits bekannt war. Bei kleinen und mittleren Unternehmen wurden im Vergleich zur Gesamtheit der Umfrageteilnehmer und zu den Kritischen Infrastrukturen häufiger keine Maßnahmen ergriffen. Besonders häufig ergriffen KMU bei Industroyer keine Maßnahmen, vermutlich weil diese Bedrohung aufgrund seines Fokusses auf Industrielle Kontrollsysteme (ICS) weniger relevant für KMU ist.

Reaktionen der Organisationen auf spezifische Bedrohungen [Gesamt]

	WannaCry	Mirai	Industroyer	(Not)Petya
Die Bedrohung war bekannt und Maßnahmen wurden bereits im Vorfeld getroffen	51%	26%	20%	38%
Es wurden keine Maßnahmen ergriffen	13%	30%	30%	20%
Es wurden neue Maßnahmen ergriffen	18%	7%	7%	12%
Bestehende Maßnahmen wurden überprüft	62%	39%	37%	50%
Weiß nicht	7%	23%	25%	15%

Reaktionen der Organisationen auf spezifische Bedrohungen [KRITIS]

	WannaCry	Mirai	Industroyer	(Not)Petya
Die Bedrohung war bekannt und Maßnahmen wurden bereits im Vorfeld getroffen	50%	25%	20%	30%
Es wurden keine Maßnahmen ergriffen	5%	30%	25%	10%
Es wurden neue Maßnahmen ergriffen	30%	10%	10%	25%
Bestehende Maßnahmen wurden überprüft	80%	35%	45%	65%
Weiß nicht	0%	25%	15%	10%

Reaktionen der Organisationen auf spezifische Bedrohungen [KMU]

	WannaCry	Mirai	Industroyer	(Not)Petya
Die Bedrohung war bekannt und Maßnahmen wurden bereits im Vorfeld getroffen	43%	26%	17%	48%
Es wurden keine Maßnahmen ergriffen	17%	30%	48%	26%
Es wurden neue Maßnahmen ergriffen	17%	9%	9%	4%
Bestehende Maßnahmen wurden überprüft	43%	43%	22%	35%
Weiß nicht	9%	13%	22%	13%

Welches Ereignis hat die Maßnahmen der IT-Sicherheit in Ihrer Organisation in der jüngeren Vergangenheit am meisten beeinflusst? (Beispiele)

- Vorfall bei EDI-Partner
- Starker Anstieg von Phishing E-Mails
- Meldung des BSI: Lessons Learned
- Gesetzgebung
- Aktionen von Insidern
- Verlorener USB-Stick mit unverschlüsselten Firmendaten
- Angriffe auf die eigenen Systeme
- Interne Analysen
- Angriffe auf Equifax und Deloitte
- Ransomware am Lukaskrankenhaus in Neuss
- Angriff auf die Leitstelle Schwäbisch Hall

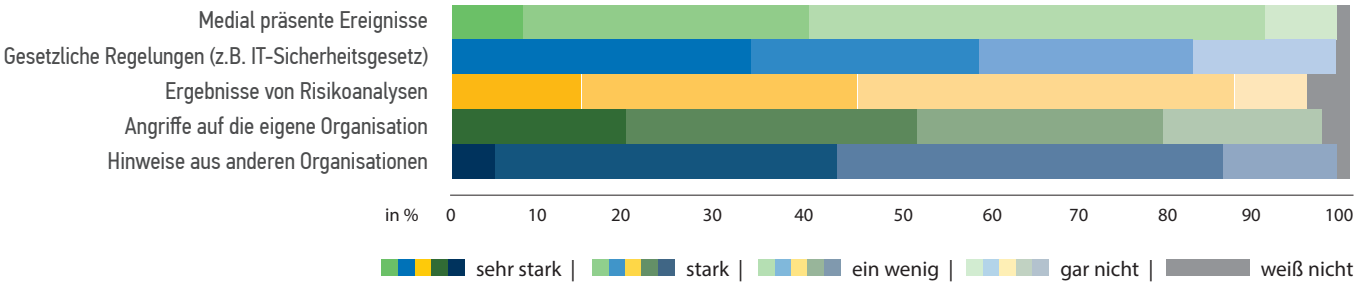
RAHMENBEDINGUNGEN

Wir haben die Umfrageteilnehmer gefragt, wie sehr die folgenden Faktoren die IT-Sicherheitsmaßnahmen in ihrer Organisation beeinflusst haben: Medial präsente Ereignisse, gesetzliche Regelungen, Ergebnisse von Risikoanalysen, Angriffe auf andere Organisationen und Hinweise aus anderen Organisationen.

Dabei wird sichtbar, dass der Einfluss variiert und die Bandbreite an Einflussfaktoren auf die IT-Sicherheit breit ist.

Gesetzliche Regelungen polarisieren stärker als die anderen Faktoren. Für ein Drittel der Befragten haben sie einen sehr starken Einfluss auf die Maßnahmen, bei etwa 16% gar keinen Einfluss. Bei medial präsenten Ereignissen gaben weniger als 8% der Befragten an, dass diese gar keinen Einfluss haben.

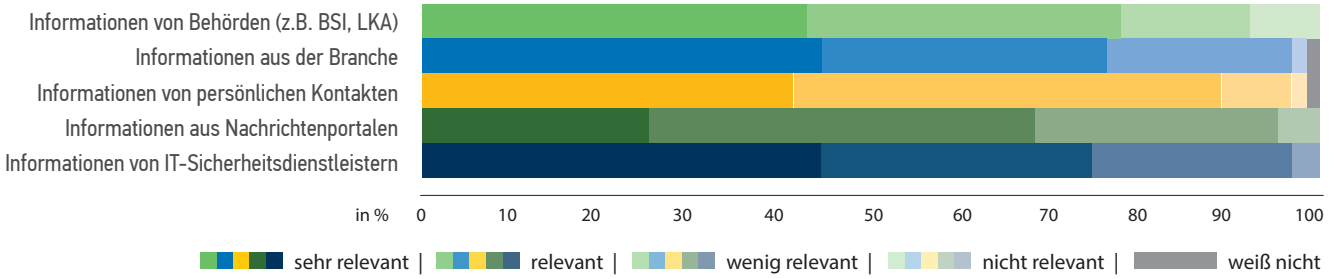
Inwiefern haben die folgenden Faktoren die Maßnahmen zur IT-Sicherheit in Ihrer Organisation beeinflusst?



Die Bandbreite an Informationsquellen, die für die IT-Sicherheit in den befragten Organisationen relevant sind, ist groß. Informationen aus der Branche, von Behörden, persönlichen Kontakten sowie IT-Sicherheitsdienstleistern werden hierbei als besonders wichtig angesehen.

Informationen aus Nachrichtenportalen spielen zwar keine so große Rolle, sind aber für mehr als 95% der Befragten zumindest „wenig relevant", bilden also eine breite Basis.

Wie relevant für die IT-Sicherheit in Ihrer Organisation sind…?



DIE REALISIERUNG VON IT-SICHERHEIT

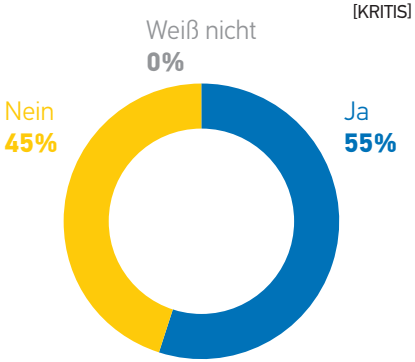
IT-SICHERHEITSBEAUFTRAGTE

Mehr als die Hälfte der befragten Organisationen beschäftigten mindestens eine Person, die ausschließlich für die IT-Sicherheit zuständig ist.

Bei rund 80% der Organisationen entfällt dabei mindestens eine vollzeitäquivalente Arbeitsstelle auf die IT- Sicherheit. Selten sind das dabei mehr als 5 Vollzeitäquivalente.

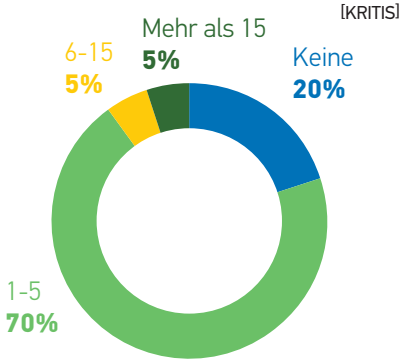
Gibt es eine einzelne Person in Ihrer Organisation, die ausschließlich für IT-Sicherheit verantwortlich ist, also nicht nur in einer Nebenfunktion?

[KRITIS]



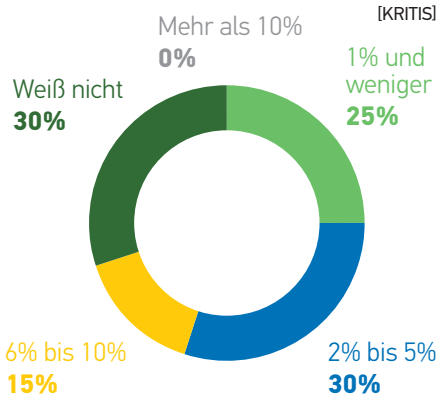
Wie viele vollzeitäquivalente Arbeitsstellen entfallen in Ihrer Organisation auf die IT-Sicherheit?

[KRITIS]

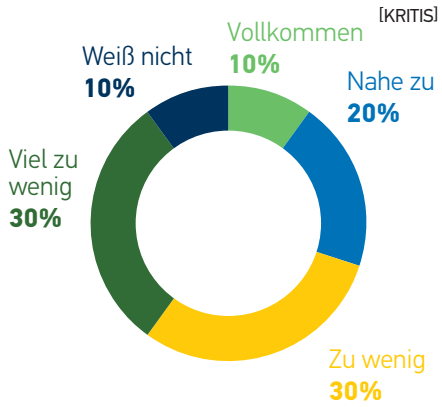


RESSOURCEN FÜR IT-SICHERHEIT

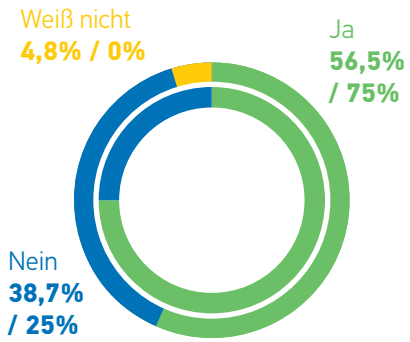
Wie hoch ist der Anteil Ihres IT-Sicherheitsbudgets, gemessen am gesamten IT-Budget Ihrer Organisation?



Halten Sie dieses Budget für ausreichend?



Findet in Ihrer Organisation eine regelmäßige Risikoanalyse statt?



Außen = alle Teilnehmer; Innen = KRITIS
außen / innen

60% **der Befragten halten das vorhandene Budget für unzureichend.**

In fast allen Fällen beträgt das Budget für IT-Sicherheit in Relation zum gesamten IT-Budget der Organisation weniger als 10%, in den meisten Fällen sogar weniger als 5%.

56% **aller befragten Organisationen und 75% der Kritischen Infrastrukturen führen eine regelmäßige Risikoanalyse durch.**

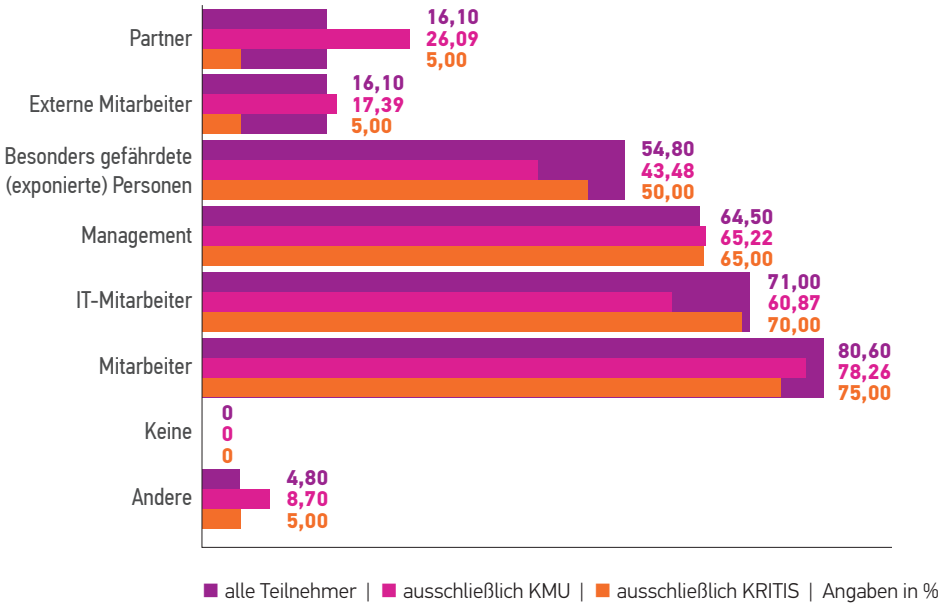
Dabei werden im Regelfall weniger als 10 Stunden pro Monat aufgebracht.

60 Min. **oder mehr würden die meisten Organisationen in einen vierteljährlichen Schnellcheck investieren, welcher Ihnen als Ergebnis eine Kennzahl ausgibt, die das IT-Risikoniveau Ihrer Organisation repräsentiert.**

WEITERBILDUNG DER MITARBEITER / AWARENESS

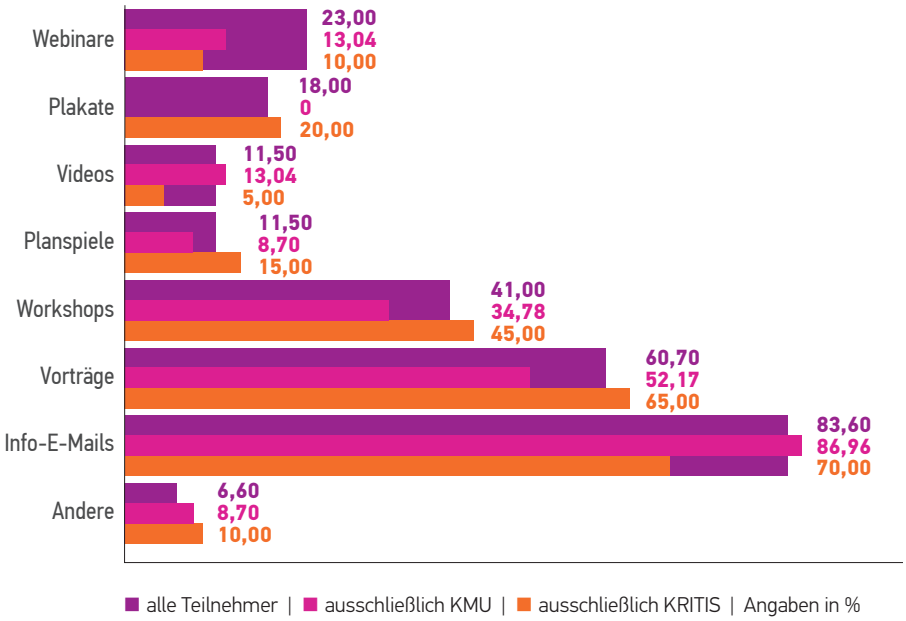
Der Anteil der Organisationen, die ihre Mitarbeiter für das Thema IT-Sicherheit sensibilisieren, ist groß. Dabei spielt es kaum eine Rolle, ob die Organisation als Kritische Infrastruktur und/oder KMU eingestuft ist. Auffällig ist, dass nur wenige Organisationen Partner und externe Mitarbeiter mit einbeziehen.

Welche Personengruppen werden in Ihrer Organisation durch gezielte IT-Sicherheits-Awareness-Maßnahmen adressiert?



Um die IT-Sicherheits-Awareness in einer Organisation zu erhöhen, werden verschiedene Maßnahmen eingesetzt. Dabei kommen am häufigsten Informations-Emails und Vorträge, gefolgt von Workshops zum Einsatz. Bei den Antworten auf diese Frage gibt es nur geringe Unterschiede zwischen allen Befragten und KRITIS bzw. KMU.

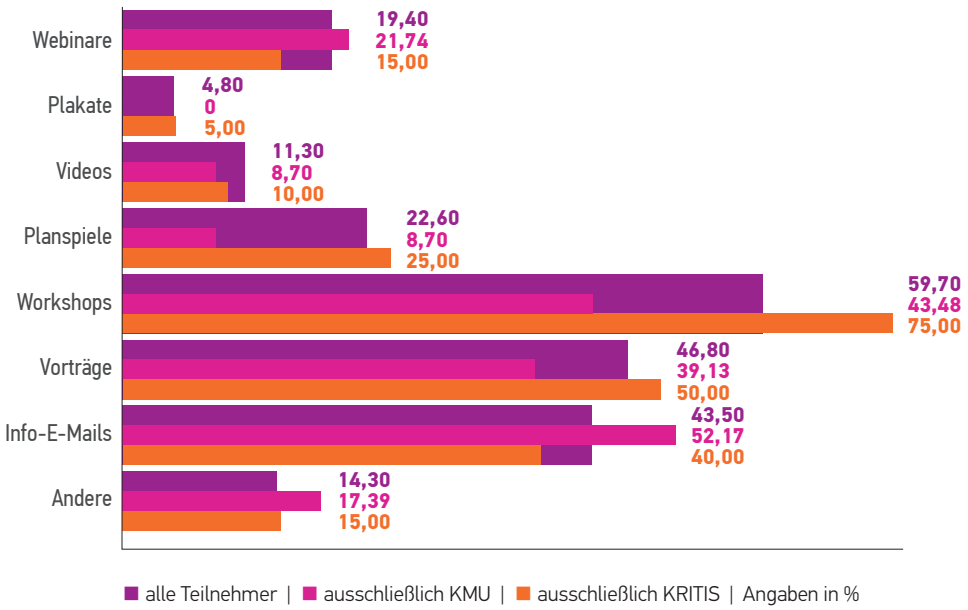
Welche Arten von IT-Sicherheits-Awareness-Maßnahmen werden in Ihrer Organisation eingesetzt?



In der Einschätzung der Wirksamkeit der Maßnahmen werden besonders Workshops, gefolgt von Vorträgen und Informations-Emails als einflussreich bewertet. Dabei zeigt sich, dass eine Korrelation zwischen der Einschätzung und dem Einsatz der Maßnahmen besteht.

Das kann darauf zurückgeführt werden, dass die Maßnahmen eingesetzt werden, weil sie als wirksam eingeschätzt werden, oder dass die Maßnahmen wegen ihres Einsatzes als wirksam eingeschätzt werden – im Sinne eines Confirmation Bias. Für letzteres spricht die überraschend positive Einschätzung der Wirksamkeit von Informations-Emails.

Welche Arten von Awareness-Maßnahmen haben Ihrer Meinung nach den größten Einfluss auf die IT-Sicherheits-Awareness in Ihrer Organisation?

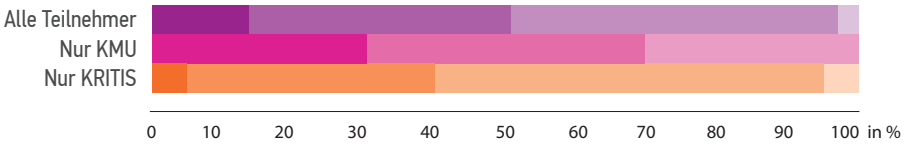


POLITIK UND WISSENSCHAFT

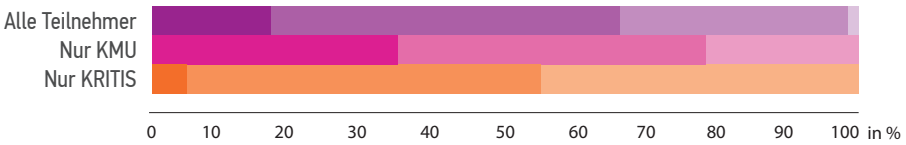
DEUTSCHE GESETZGEBUNG

Wie viel tut die deutsche Gesetzgebung Ihrer Meinung nach für ...?

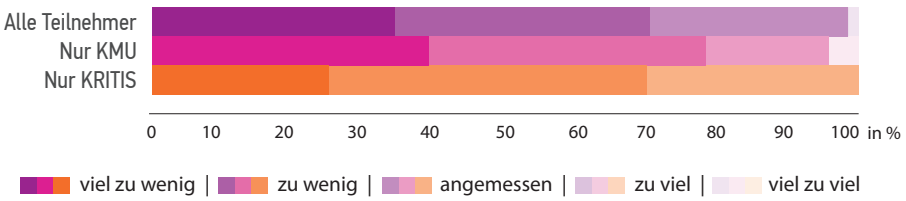
... den Schutz Kritischer Infrastrukturen?



... die IT-Sicherheit von Organisationen?



... die digitale Souveränität Deutschlands?



Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und die Datenschutzgrundverordnung sind zwei aktuelle Beispiele für die Regulierung der IT-Sicherheit. Trotz dieser medial präsenten Aktivitäten nehmen mehr als die Hälfte der Befragten die Eingriffe der deutschen Gesetzgebung als zu wenig oder viel zu wenig war - sowohl für den Schutz der kritischen Infrastrukturen, als auch für die IT-Sicherheit von Organisationen im Allgemeinen. Für etwa 70% der Befragten wird seitens der Gesetzgebung zu wenig für die digitale Souveränität Deutschlands getan.

Die befragten KRITIS sehen den weiteren Bedarf deutlich weniger stark ausgeprägt, als es die befragten KMU tun. Es bleibt unklar, ob diese Wahrnehmung durch die besondere Beachtung von Kritischen Infrastrukturen in der bereits bestehenden Regulierung durch den Gesetzgeber herrührt.

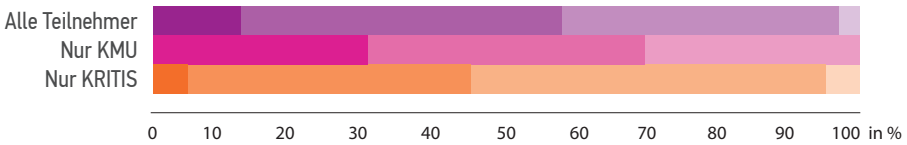
FORSCHUNG

Über die Hälfte aller Befragten sieht einen erhöhten Forschungsbedarf im Bereich des Schutzes Kritischer Infrastrukturen. Nach Einschätzung der Befragten besteht ebenfalls weiterer Forschungsbedarf für die Digitale Souveränität Deutschlands.

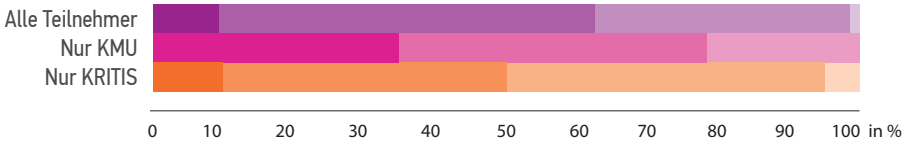
Die Wahrnehmung der Forschung ist ähnlich ausgeprägt wie die der Aktivitäten der deutschen Gesetzgebung. Auch hier nehmen die befragten KRITIS eine weniger fordernde Haltung ein, als die befragten KMU.

Wie viel wird Ihrer Meinung nach geforscht für ...?

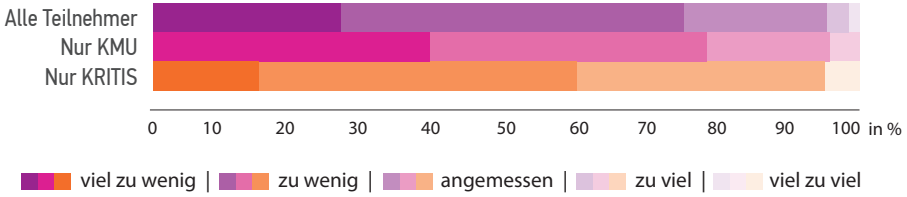
... den Schutz Kritischer Infrastrukturen?



... die IT-Sicherheit von Organisationen?



... die digitale Souveränität Deutschlands?



FALLSTUDIEN

Das Ziel ist klar und die Zeit ist knapp. Doch wie baue ich meine IT-Sicherheit auf und was ist in meinem speziellen Fall zu beachten? Wie aufwändig ist eine IT-Sicherheitsmaßnahme und gibt es vielleicht Fallstricke oder Tricks und Kniffe, die die Umsetzung einer Maßnahme einfach machen?

Schnell kommt da die Frage auf:
wie machen es andere?

90% **und mehr der Befragten finden Beispiele der Umsetzung von IT-Sicherheit in anderen Organisationen hilfreich, um sich zu orientieren und Impulse und Denkanstöße für die eigene Umsetzung zu gewinnen.**

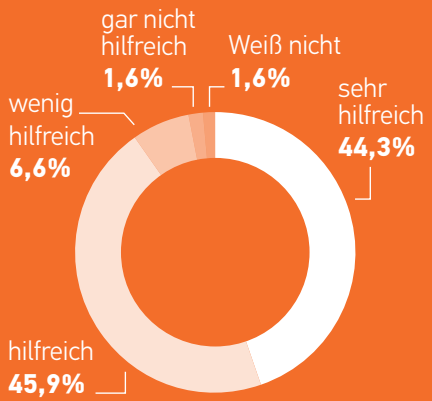
„Tue Gutes und rede darüber“ - getreu diesem Motto haben Unternehmen und Behörden die Möglichkeit, ihre „Good Practices“ zu präsentieren. Im Rahmen des Forschungsprojekts VeSiKi entstand so die Fallstudienreihe CASE|KRITIS, die im Sommer 2018 digital und in Buchform erscheinen wird.

CASE|KRITIS

Gerade kleine und mittelständische Unternehmen haben so die Möglichkeit, sich über erprobte Praktiken aus den Bereichen Mensch, Organisation und Technik für Ihre Branche zu informieren.

Unter den Teilnehmern dieser Studie Monitor 2.0 besteht für nahezu jede Branche großes Interesse an Fallstudien, besonders für die Informations- und Kommunikationstechnik, die Wasserversorgung und den Energiesektor.

Sind Beispiele der Umsetzung von IT-Sicherheit in anderen Organisationen (z.B. Good/Best Practices) für die Umsetzung Ihrer Organisation hilfreich?



FAZIT

Für die IT-Sicherheit in Kritischen Infrastrukturen bestehen Risiken. Eine große Anzahl der befragten Betreiber Kritischer Infrastrukturen musste im letzten Jahr Angriffe verzeichnen. Dabei fallen zwei Angriffsvektoren besonders auf: Phishing und Ransomware. Im Vergleich zur ersten Monitor-Umfrage ist bei diesen beiden Vektoren ein starker Anstieg zu verzeichnen. Diese Vektoren erhalten also nicht nur medial mehr Aufmerksamkeit, sondern spielen auch für die IT-Sicherheit eine große Rolle.

Bemerkenswert ist, dass die am häufigsten genannte Ursache für den Erfolg von Cyberangriffen das Fehlverhalten von Mitarbeitern ist. Dies macht vor allem den Bedarf an geeigneten IT-Sicherheitsschulungen deutlich. Der Anteil der Organisationen, die ihre Mitarbeiter für das Thema IT-Sicherheit sensibilisieren, ist groß. Nur selten werden dabei aber Partner und externe Mitarbeiter mit einbezogen.

Betreiber schätzen ihre Bedrohungssituation sowie ihre eigenen Fähigkeiten, Cyberangriffe erfolgreich abzuwehren, optimistischer ein als für die eigene Branche oder für den Wirtschaftsraum Deutschland. Dieser Effekt war schon in der ersten Monitor-Umfrage sichtbar und ist nun erneut festzustellen.

Bedrohungen mit großer Medienaufmerksamkeit – wie WannaCry, das Mirai-Botnetz, Industroyer und (Not)Petya - lösen in den Organisationen Reaktionen aus, die IT-Sicherheit zu überdenken. Auch wenn die Betreiber auf neue Bedrohungen reagieren, ergreifen nur wenige Organisationen neue Maßnahmen angesichts einer dieser vier Bedrohungen. Die meisten Organisationen haben die bestehenden Maßnahmen überprüft oder die Maßnahmen wurden bereits im Vorfeld getroffen, weil die Bedrohung bereits bekannt war.

Dieses Ergebnis illustriert, dass die Betreiber Kritischer Infrastrukturen ihre Verantwortung ernst nehmen und reagieren, aber auch, dass die IT-Sicherheit laufend an aktuelle Bedrohungen angepasst werden muss.

Abschließend lässt sich feststellen, dass ein Bedarf nach mehr Aktivität in Gesetzgebung und Forschung im Themenfeld der IT-Sicherheit von Kritischen Infrastrukturen und anderen Organisationen sowie für die digitale Souveränität Deutschlands besteht. Das untermauert die Wichtigkeit der Forschung zu IT-Sicherheit Kritischer Infrastrukturen.

DIE MULTIPLIKATOREN

FRAGENÜBERSICHT

Frage	Stichprobenumfang n	Kommentar
War Ihre Organisation innerhalb des letzten Jahres Ziel von Cyber-Attacken?	n = Alle 99	
Wie viele gezielte Cyberattacken konnten Sie innerhalb des letzten Jahres feststellen?	n = Alle 47	
Konnten Ursachen für den Erfolg von Cyber-Attacken festgestellt werden?	n = KRITIS 16; Alle 65	Mehrfachselektion
Welche Art von Angriffen konnten festgestellt werden?	n = KRITIS 27; Alle 103	Mehrfachselektion
Konnten die Cyber-Attacken auf Verantwortliche zurückgeführt werden?	n = Alle 45	Mehrfachselektion
Welche Konsequenzen hatten die Cyber-Attacken zur Folge?	n = Alle 41	Mehrfachselektion
Wie hoch schätzen Sie die derzeitige Bedrohungslage im Bereich der IT-Sicherheit ein für ...	Deutschland: n = KRITIS 20; Alle 70; KMU 23 Branche: n = KRITIS 20, Alle 70, KMU 23 Organisation: n = KRITIS 20, Alle 70, KMU 23	
Wie hoch schätzen Sie die Fähigkeit ein Cyber-Attacken abzuwehren für ...	Deutschland: n = KRITIS 20; Alle 70; KMU 23 Branche: n = KRITIS 20, Alle 70, KMU 23 Organisation: n = KRITIS 20, Alle 70, KMU 23	
Wie viel tut die deutsche Gesetzgebung Ihrer Meinung nach für...	KRITIS: n = KRITIS 20; Alle 65; KMU 23 Deutschland: n = KRITIS 20, Alle 64, KMU 23 Organisation: n = KRITIS 20, Alle 65, KMU 23	
Wie viel wird Ihrer Meinung nach geforscht für...	KRITIS: n = KRITIS 20; Alle 64; KMU 23 Deutschland: n = KRITIS 20, Alle 64, KMU 23 Organisation: n = KRITIS 20, Alle 64, KMU 23	
Inwiefern haben die folgenden Faktoren die Maßnahmen zur IT-Sicherheit in Ihrer Organisation beeinflusst?	Medial präsente Ereignisse: n = Alle 63 Gesetzliche Regelungen: n = Alle 63 Ergebnisse von Risikoanalysen: n = Alle 62 Angriffe auf Ihre Organisation: n = Alle 62 Hinweise aus anderen Organisationen: n = Alle 63	

Frage	Stichprobenumfang n	Kommentar
Wie relevant für die IT-Sicherheit in Ihrer Organisation sind…	Informationen von Behörden: n = Alle 63 Informationen aus Ihrer Branchen/Branchenverbund: n = Alle 63 Informationen von persönlichen Kontakten: n = Alle 63 Informationen aus Nachrichtenportalen: n = Alle 63 Informationen von IT-Sicherheitsdienstleistern: n = Alle 63 Informationen aus Datenbanken: n = Alle 63	
Wie hat Ihre Organisation auf das Auftreten von WannaCry reagiert?	n = KRITIS 33; Alle 92; KMU 30	Mehrfachselektion
Wie hat Ihre Organisation auf das Auftreten von Mirai reagiert?	n = KRITIS 25; Alle 76; KMU 28	Mehrfachselektion
Wie hat Ihre Organisation auf das Auftreten von Industroyer reagiert?	n = KRITIS 23; Alle 71; KMU 27	Mehrfachselektion
Wie hat Ihre Organisation auf das Auftreten von (Not)Petya reagiert?	n = KRITIS 28; Alle 81; KMU 29	Mehrfachselektion
Welches Ereignis hat die Maßnahmen der IT-Sicherheit in Ihrer Organisation in der jüngeren Vergangenheit am meisten beeinflusst?	n = 33	offene Frage
Sind Beispiele der Umsetzung von IT-Sicherheit in anderen Organisationen (z.B. Good/Best Practices) für die Umsetzung in Ihrer Organisation hilfreich?	n = 61	
Von welchen Sektoren/Branchen würden Sie solche Umsetzungsbeispiele besonders interessieren?	n = 181	Mehrfachselektion
Welche Personengruppen werden in Ihrer Organisation durch gezielte IT-Sicherheits-Awarenessmaßnahmen adressiert?	n = KRITIS 55; Alle 191; KMU 69	Mehrfachselektion
Welche Arten von IT-Sicherheits-Awarenessmaßnahmen werden in Ihrer Organisation eingesetzt?	n = KRITIS 48; Alle 156; KMU 50	Mehrfachselektion
Welche Arten von Awareness-Maßnahmen haben Ihrer Meinung nach den größten Einfluss auf die IT-Sicherheits-Awareness in Ihrer Organisation?	n = KRITIS 47; Alle 138; KMU 24	Mehrfachselektion
Findet in Ihrer Organisation eine regelmäßige IT-Risikoanalyse statt?	n = KRITIS 20, Alle 62	
Falls ja, wie viele Stunden investieren Sie dafür pro Monat?	n = KRITIS 20, Alle 34	
Wie viele Minuten würden Sie in einen vierteljährlichen Schnellcheck investieren, welcher Ihnen als Ergebnis eine Kennzahl ausgibt, die das IT-Risikoniveau Ihrer Organisation repräsentiert?	n = KRITIS 20, Alle 61	
Gibt es eine einzelne Person in Ihrer Organisation, die rein für IT-Sicherheit verantwortlich ist, nicht nur in einer Nebenfunktion?	n = KRITIS 20	

Frage	Stichprobenumfang n	Kommentar
Wie viele vollzeitäquivalente Arbeitsstellen* entfallen in Ihrer Organisation auf die IT-Sicherheit?*	n = KRITIS 20	
Wie hoch ist der Anteil Ihres IT-Sicherheitsbudgets, gemessen am gesamten IT-Budget Ihrer Organisation?	n = KRITIS 20	
Halten Sie dieses Budget für ausreichend?	n = KRITIS 20	
In welcher Branche / welchem Sektor ist Ihre Organisation tätig?	n = Alle 84	Mehrfachselektion
Ist Ihre Organisation gemäß IT-Sicherheitsgesetz als "Kritische Infrastruktur" eingestuft?	n = Alle 62; KMU 23	
Würden Sie persönlich Ihre Organisation als "Kritische Infrastruktur" einschätzen?	n = Alle 62; KMU 23	
Haben Sie die Meldepflicht gemäß IT-Sicherheitsgesetz bereits organisatorisch implementiert?	n = KRITIS 20; Alle 62	
Wenn ja, wie?	n = Alle 7	offene Frage
Wie viele Angestellte beschäftigt Ihre Organisation?	n = Alle 60	
Wie hoch ist der jährliche Umsatz Ihrer Organisation?	n = Alle 60	
Welche Position nehmen Sie in Ihrer Organisation ein?	n = Alle 50	offene Frage
Sind Sie in Ihrer Organisation hauptverantwortlich für die IT-Sicherheit?	n = Alle 61	

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.

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903), Bundesministerium des Innern, 2017.

Cyber-Sicherheits-Umfrage 2017, Allianz für Cyber-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik, 2018.

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

https://www.itskritis.de

oder bei Twitter

https://twitter.com/itskritis

Die digitale Version dieser Broschüre und die Ergebnisse der ersten Monitor-Umfrage finden Sie unter

https://www.itskritis.de

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