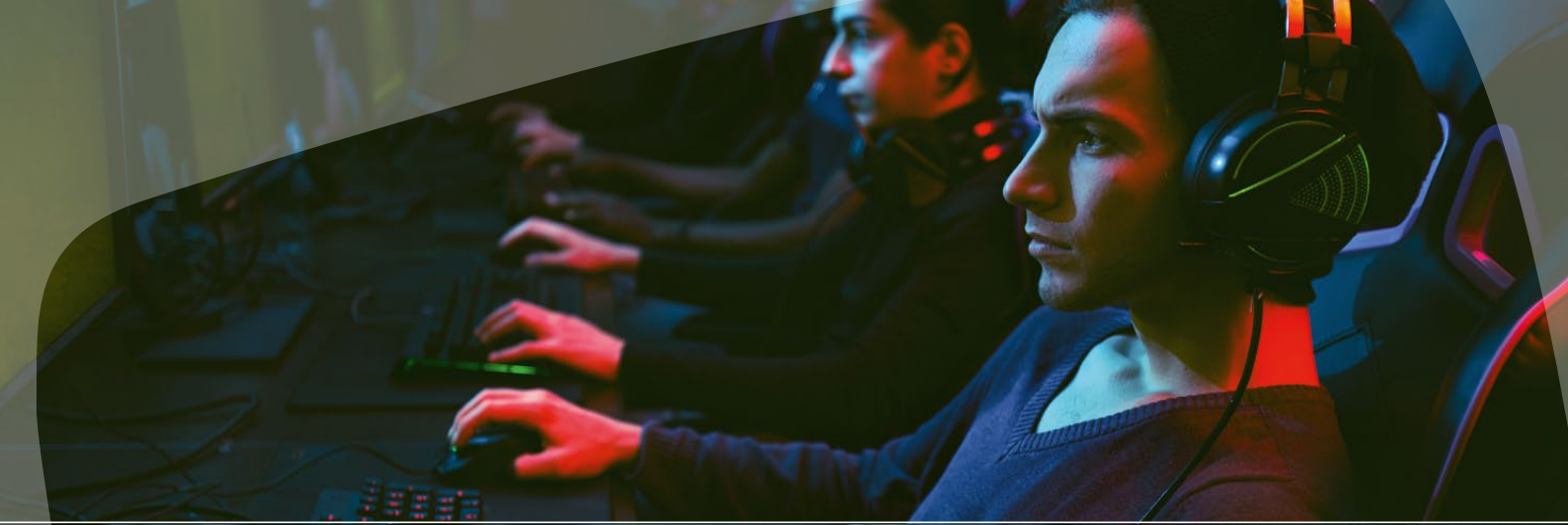


Monitor

Resilienz angesichts von Ransomware: Einblicke in die Praxis

contain

Gefördert von

Bundesministerium für Bildung und Forschung

SIFO.de

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

Bundesministerium Finanzen

1. Auflage, 2024

Herausgeberin: Prof. Dr. Ulrike Lechner

Die Broschüre ist erstellt vom deutsch-österreichischen Forschungsprojekt „Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten (CONTAIN)“.

Auf deutscher Seite wird das Projekt CONTAIN innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (FKZ 13N16581-13N16587); auf Österreichischer Seite wird CONTAIN innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS gefördert (FO999902707).

Sprecherin des Gesamtprojekts:
Prof. Dr. Ulrike Lechner

Projektleitung CONTAIN Deutschland:
Dr. Steffi Rudel (Universität der Bundeswehr München)

Projektleitung CONTAIN Österreich:
Dr. Stefan Schauer (Austrian Institute of Technology AIT)

Projektleitung und Autorenschaft CONTAIN Monitor:
Judith Strußenberg

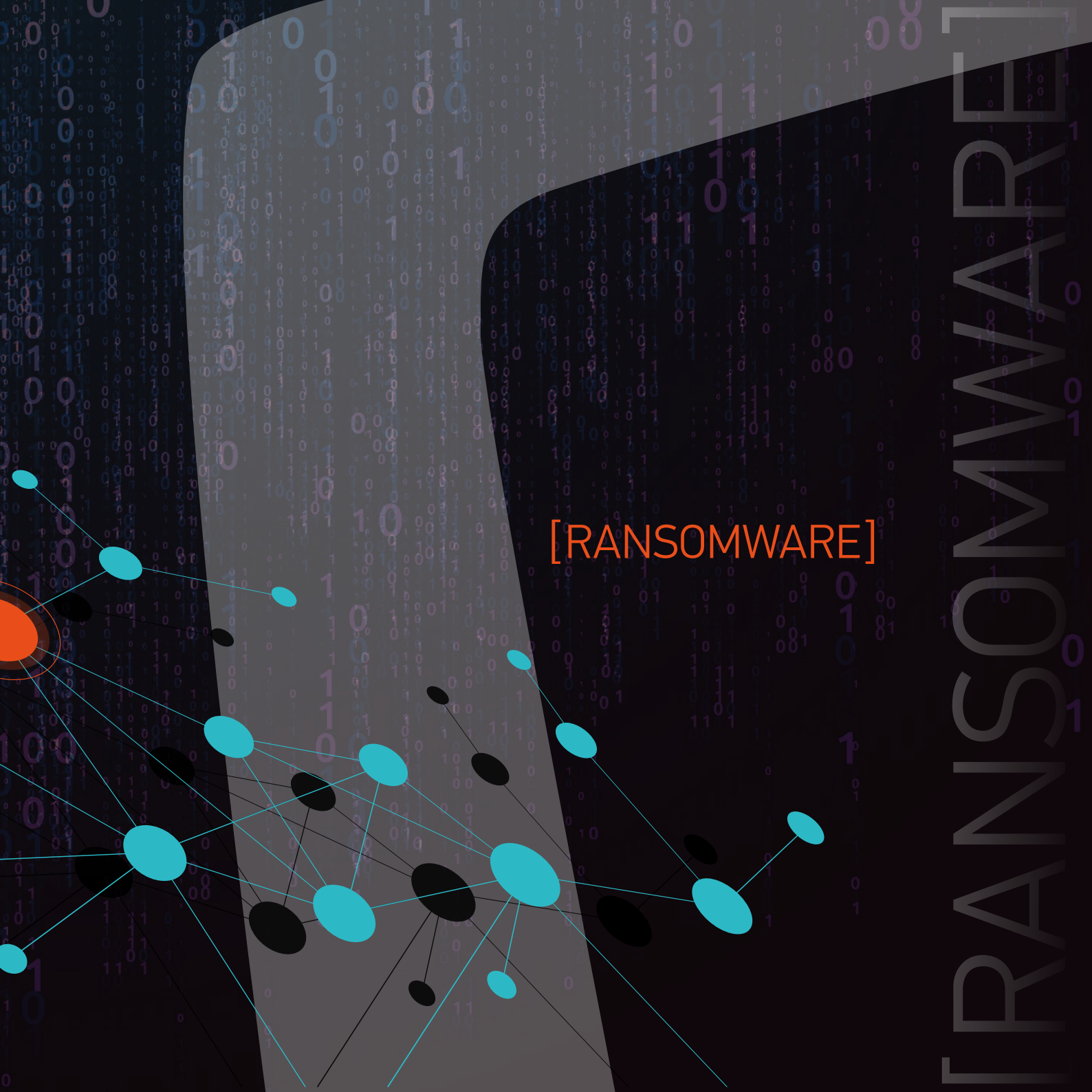
Mitwirkende:
Die Umfrage wurde von Ulrike Lechner, Judith Strußenberg, Dr. Stefan Hofbauer, Andreas Seiler und Maximilian Greiner formuliert und ausgearbeitet. Alle Projektpartner von CONTAIN in Deutschland und Österreich waren an der Erstellung der Fragen beteiligt. Die Auswertung und Aufbereitung der Ergebnisse erfolgte durch Judith Strußenberg. Für die Erhebung und Auswertung der Daten wurde das Einverständnis des Datenschutzbeauftragten der Universität der Bundeswehr München eingeholt.

Lektorat: Dr. Steffi Rudel

ISBN: 978-3-98997-000-7
URN: urn:nbn:de:bvb:706-10277

Design: Artes Advertising GmbH, München

Druck und buchbinderische Verarbeitung:
Rechenzentrum der Universität der Bundeswehr München


[RANSOMWARE]
[RANSOMWARE]

DAS PROJEKT

CONTAIN – EFFIZIENTE REAKTION AUF IT-SICHERHEITSVORFÄLLE IN TRANSNATIONALEN LIEFERKETTEN

Die Ransomware meldet sich. Was nun? Im Forschungsprojekt CONTAIN, mit Partnern aus Deutschland und Österreich, forschen Universitäten, Unternehmen, Verbände und Behörden daran, die Reaktion auf Bedrohungen aus dem digitalen Raum effektiver und effizienter zu machen: durch die zielgerichtete Vorbereitung auf einen Cyber-Vorfall.

CONTAIN erforscht Szenare, Prozesse und Entscheidungsverfahren in der Bewältigung eines Ransomware-Vorfalls. Das zentrale Ergebnis von CONTAIN ist ein Rahmenwerk von Prozessen und Verfahren zur Bewältigung eines Cyber-Vorfalls sowie Serious Games und Simulationen. In CONTAIN werden weiterhin digitale Währungen, Logistik, Liquidität im Krisenfall und Cloud-Infrastrukturen betrachtet. Die Forschung geht in Standards und Normen ein und will auch Innovationen in Produkten und Diensten identifizieren, die in der Bewältigung eines Cyber-Vorfalls unterstützen.

Auf deutscher Seite wird das Projekt CONTAIN innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (FKZ 13N16581-13N16587); auf Österreichischer Seite wird CONTAIN innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS gefördert (FO999902707).

contain

PARTNER – DEUTSCHLAND


PARTNER – ÖSTERREICH

UNSER ANGEBOT

Das Projekt CONTAIN hat im Austausch zwischen Wissenschaft und Praxis in Bereichen wie Lehre, Forschung, Veröffentlichungen, Simulationen und Präsentationen viele interessante Ergebnisse erzielt. Um diese nachhaltig nutzbar zu machen, sollen die Ergebnisse auch nach Abschluss des Projekts weiterhin zugänglich bleiben – und Ihnen dabei helfen, sich noch besser auf die Herausforderungen durch Ransomware vorzubereiten. Unsere Serious Games, die Föderierte Übung, Toolbox und Möglichkeiten, uns zu erreichen, möchten wir Ihnen im Folgenden kurz vorstellen.

TOOLBOX

Die Toolbox befindet sich im Aufbau. Das wird der Ort sein, an dem Sie die eben skizzierten Ergebnisse unseres Forschungsprojekts künftig finden werden. Ob Sie eine entsprechende Veröffentlichung suchen oder selbst eine Spielrunde zur Awarenesssteigerung in Ihrem Unternehmen planen: In der Toolbox finden Sie dann die Materialien, können nach Zielgruppen filtern und erhalten einen Hinweis, unter welcher Lizenz Sie unsere Ergebnisse verwenden können.

SERIOUS GAMES

Serious Games können eingesetzt werden zur Schulung von Inhalten, zur Awarenesssteigerung, zur Strategieentwicklung oder zur Identifikation von Bedrohungen und Schwachstellen. Sie bieten Motivation, die Einbindung relevanter Beteiligter und Spaß. Außerdem erzielen Sie dabei bessere Ergebnisse und Lerneffekte als durch herkömmliche Schulungen – speziell dann, wenn Sie gerne spielen und gezielt einen kleineren Personenkreis ansprechen wollen.

Letztendlich eignen sich Serious Games also sehr gut, um Inhalte der IT-Sicherheit zu vermitteln und beispielsweise einen Ransomware-Vorfall einmal versuchsweise durchzuspielen.

Genau das tut das Serious Game „Operation Raven“, das sich an technisch versierte Teilnehmende richtet (Seiler et al. 2024). Der Spielleiter simuliert das Vorgehen einer Ransomware-Gruppe mithilfe verschiedener Tools, Techniken und Prozeduren. Eine Gruppe spielt gemeinsam an einem Spieltisch und plant rundenweise die Reaktion auf die Ransomware, bis diese am Ende hoffentlich besiegt ist.

In „Eine Frage der Sicherheit“ meldet sich die Ransomware auf einem persönlichen Gerät, wie dem Smartphone. Jetzt ist guter Rat teuer. Oder? Rundenbasiert lernen die

Spielenden, die richtigen und wichtigen Fragen zu stellen und den Prozess zu durchdenken, der sie zur Wiederherstellung der Arbeitsfähigkeit bringt. Auch dieses Spiel wird am Tisch gespielt, technische Vorkenntnisse sind hier nicht nötig.

Im Serious Point-and-Klick-Spiel „Digital Detectives" schlüpfen die Spielenden online in die Rolle eines digitalen Forensikers, der einen Ransomware-Vorfall aufklären soll. Dabei gilt es nicht nur Spuren zu sichern, sondern auch mit dem Erpresser zu verhandeln. Am Ende des Spiels wurde hoffentlich nicht nur der Fall aufgeklärt, sondern auch ein besseres Verständnis für die Arbeit des digitalen Forensikers gewonnen.

In „Hack dich nicht" übernehmen die Spieler die Rolle eines Spediteurs, der mit einem Ransomware-Vorfall konfrontiert wird. Durch den geschickten Einsatz von Verteidigungs- und Ressourcenkarten gelingt es den Spielenden hoffentlich, die Angriffe abzuwehren, bzw. Unternehmen und Stakeholder zu schützen.

„COPYCAT" steht für CONTAIN Supply Chain Attack und genau diese Angriffe auf die Supply Chain gilt es im online-basierten Spiel auch zu bekämpfen (Zhao et al. 2024). Die Spielenden müssen entscheiden, mit welchen Verteidigungsmaßnahmen sie auf Angriffe reagieren und welche technischen und organisatorischen Maßnahmen hier noch weiterhelfen können. Kommen sie selbst nicht auf die Lösung, hilft das Spiel mit Hinweisen und Anleitungen.

„DuckDebugger" ist für Softwareentwickler in der Industrie gemacht und soll dabei helfen, Code sicherer zu gestalten, indem statische Codeanalyse im Spiel trainiert wird (Iosif et al. 2024). In den Übungen aus vier Programmiersprachen sind häufige Schwachstellen aus den OWASP TOP10 oder den MITRE CWE TOP25 versteckt, die es in dem Online Spiel zu entdecken und zu beheben gilt.

FÖDERIERTE ÜBUNG

Sie haben Interesse, die genannten Serious Games einmal selbst zu testen, in einer deutsch-österreichischen Cyber-Range Ihr Geschick bei der Bekämpfung der Ransomware zu testen, sich auszutauschen oder sich im Vortragsprogramm zu aktuellen Themen aus der IT-Sicherheit fortzubilden?

Dann laden wir Sie herzlich ein zur Föderierten Übung, die am 25./26.02.2025 zeitgleich in München und Wien stattfindet. Aktuelle Informationen zu Programm und Anmeldemöglichkeiten finden Sie unter der nebenstehenden LinkedIn-Seite.

Mehr erfahren

Informationen zu Veröffentlichungen, Spielrunden, Konferenzen und Veranstaltungen wie der Föderierten Übung finden Sie aktuell in unserer LinkedIn-Gruppe. Hier können Sie sich auch gerne mit uns austauschen.

Die Webseite soll künftig Informationen zum Projekt und die bereits beschriebene Toolbox enthalten.

LinkedIn:

linkedin.com/groups/9549256/

Weitere Informationen und Toolbox unter:

contain-projekt.de

contain-projekt.at

VORWORT

Sehr geehrte Leserin, sehr geehrter Leser,

das deutsch-österreichische Forschungsprojekt CONTAIN beschäftigt sich mit der effizienten Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten. Im Mittelpunkt des Forschungsprojekts steht die Frage „Die Ransomware meldet sich, was nun?“

Gemeinsam mit unseren Projektpartnern arbeiten wir an innovativen Antworten auf diese drängende Frage. Das Bundesamt für Sicherheit in der Informatikstechnik legt eindrucksvolle Zahlen zu Ransomware-Vorfällen, Art des Schadens und Schadensausmaß vor (BSI 2023). Im Kapitel „Unser Angebot“ konnten Sie bereits einen Eindruck erhalten, wie breit gefächert die Maßnahmen des Projekts sind. Sie reichen von einer ganzen Reihe an Serious Games für verschiedene Zielgruppen von Schülern bis zu IT-Sicherheits-Spezialisten über Simulationen bis hin zu einer Föderierten Übung, bei der unsere Ergebnisse live erlebt und erprobt werden können. In der Toolbox schließlich bündeln wir unsere Ergebnisse und machen sie online zugänglich.

Die Studie Monitor thematisiert die technische und organisatorische Vorbereitung auf Ransomware-Attacken, die Einschätzungen mit Blick auf die zu erwartenden Auswirkungen, einen Beispielhaften Vorfall, an den die Befragten denken sollten, aber ganz gezielt auch die Nachwirkungen und die Nachbearbeitung eines Ransomware-Vorfalls.

Für diese Studie wurden IT-Sicherheitsexperten aus Unternehmen und Behörden im deutschsprachigen Raum (DACH) sowie Entscheider befragt. Der Fragebogen wurde im Frühjahr 2024 unter Einbezug aller Projektpartner des Forschungsprojekts CONTAIN konzipiert. Die Online-Umfrage fand von Ende Mai 2024 bis Juli 2024 statt.

Die vorliegende Studie setzt die Monitor-Reihe fort, die im Rahmen des BMBF-Förderschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen“ entstanden ist und in der zuletzt der NutriSafe Monitor zu Resilienz und Blockchain-Technologie in Lebensmittelproduktion und -logistik erschienen ist.

Diese Studie wird durch das Projekt CONTAIN durchgeführt. Wir bedanken uns bei unseren Projektpartnern in Deutschland und Österreich, den Teilnehmenden an dieser Umfrage, bei den Multiplikatoren, die die Umfrage gestreut haben, und vor allem beim Bundesministerium für Bildung und Forschung (D) sowie bei SIFO und KIRAS und dem Bundesministerium für Finanzen (AT) für die Förderung.

Prof. Dr. Ulrike Lechner

Sprecherin des Forschungsprojekts CONTAIN und Professorin an der Universität der Bundeswehr München

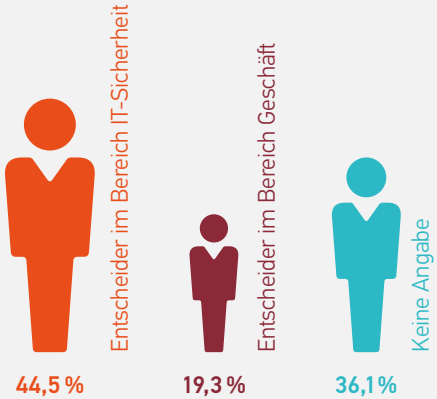
INHALTSVERZEICHNIS

DEMOGRAFIE

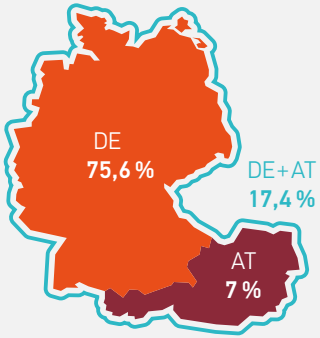
Hinweis: *Diese Studie betrachtet alle Geschlechteridentitäten gleichermaßen. Für die bessere Lesbarkeit wird im Folgenden überwiegend die männliche Schreibweise verwendet.*

Die Teilnehmenden sind Entscheider mit Verantwortung in den Bereichen IT-Sicherheit oder Geschäft. Es sind auch Erfahrungen von Beratern aus Informationssicherheit und Datenschutz sowie von Spezialisten aus der IT-Security eingeflossen.

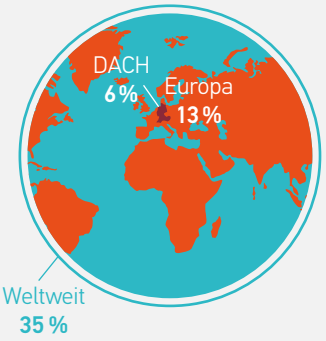
Ich bin in meinem Unternehmen...



Wo ist Ihre Organisation tätig?



Weitere Länder



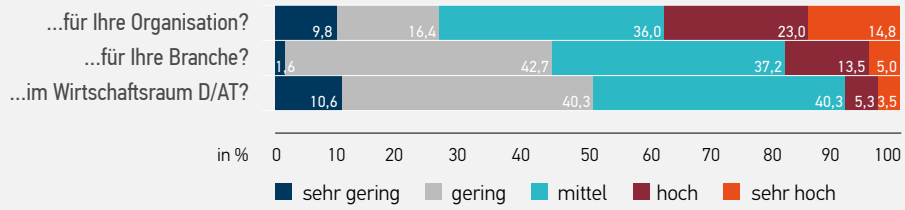
DIE AUSGANGSSITUATION

BEDROHUNGSLAGE

Die Bedrohung für die eigene Organisation im Bereich der Cyber-Sicherheit wird überwiegend mittel und hoch eingeschätzt. Die erfolgreiche Bewältigung eines fortgeschrittenen Ransomware-Vorfalls, bei dem bereits Systeme verschlüsselt wurden, wird für das eigene Unternehmen deutlich positiver beurteilt als für die eigene Branche oder gar für den Wirtschaftraum Deutschland und Österreich. Generell sind die Erwartungen an einen Ransomware-Vorfall und seine Auswirkungen niedriger als die beobachteten Auswirkungen.

Wie schätzen Sie die IT-Sicherheits-Bedrohungslage ein…

Wie schätzen Sie die Fähigkeit ein, auf einen fortgeschrittenen Ransomware-Vorfall adäquat zu reagieren und die Geschäftstätigkeit vollständig wiederaufnehmen zu können…

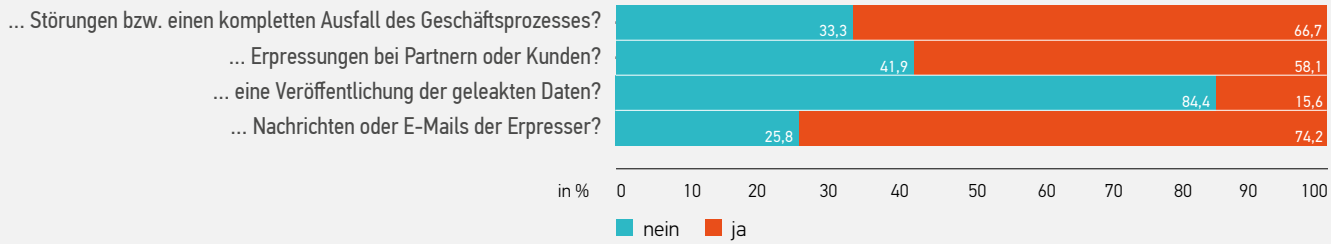


BEISPIELFALL RANSOMWARE

Wir haben die Teilnehmer der Umfrage gebeten, sich einen beispielhaften Ransomware-Vorfall vorzustellen, den sie entweder selbst miterlebt oder detailliert verfolgt haben. Dabei wurde in der Mehrzahl der Fälle der Geschäftsbetrieb beeinträchtigt oder ganz unterbrochen.

Es zeigt sich, dass Double oder Multi Extortion inzwischen immer häufiger beobachtet werden können. Damit ist die mehrfache Ausnutzung des Vorfalls durch die Erpresser gemeint, z.B. durch zusätzliches Ausleiten und Veröffentlichen der Daten, durch das Verkaufen derselben oder durch Erpressung der Kunden oder Geschäftspartner. Gleichzeitig sollten sich Unternehmen darauf vorbereiten, von Kriminellen kontaktiert zu werden.

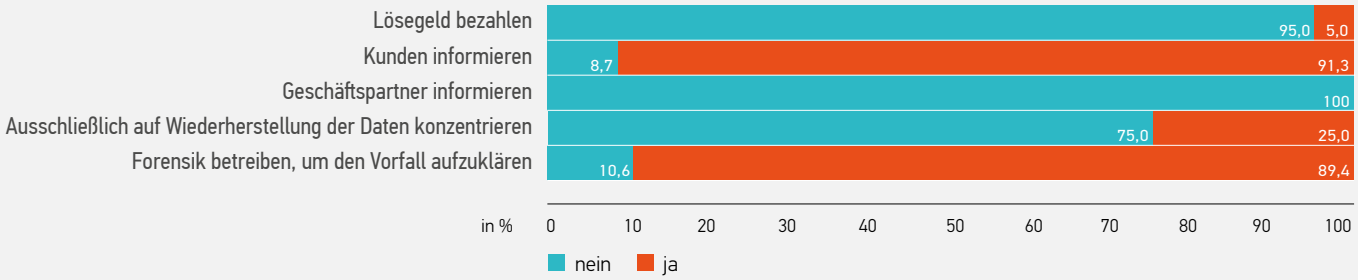
Gab es…



EMPFEHLUNGEN DER KOLLEGEN

Ist es zu einem Ransomware-Vorfall gekommen, stellen sich viele Fragen. Diese können sich damit beschäftigen, wen man denn jetzt benachrichtigen muss, aber auch, ob man auf die Forderungen der Erpresser eingehen sollte. Wir wollten wissen, was die Teilnehmenden einem betroffenen Kollegen raten würden.

Welche Empfehlungen hätten Sie für die Kollegen?



VORBEREITUNG AUF EINEN RANSOMWARE-VORFALL

RESILIENZ ANGESICHTS EINES CYBER-VORFALLS

Was kann man erwarten? Systeme sind nicht mehr erreichbar oder verfügbar, Produktion und Serviceerbringung stehen still und Daten werden ausgeleitet. Mit den ausgeleiteten Daten können Kunden oder Geschäftspartner erpresst oder angegriffen werden, während der Wiederherstellung der Systeme werden andere Angriffsformen genutzt, um den Schaden zu vergrößern. Mitarbeitende, Kunden, Partner und Behörden müssen entsprechend der gesetzlichen Vorgaben über den Vorfall informiert werden.

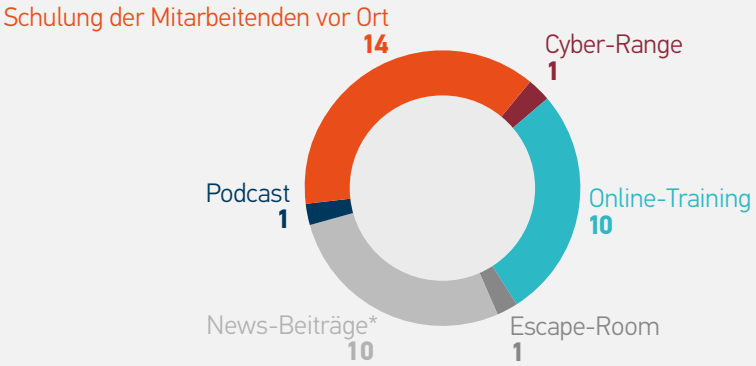
Nach der Definition des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) ist Resilienz die „Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz ist die Fähigkeit von Systemen und Lebewesen, Ereignissen zu widerstehen beziehungsweise sich daran anzupassen und dabei Funktionsfähigkeiten zu erhalten und das Überleben zu sichern."

Übertragen auf die Bedrohungslage durch Ransomware gibt es eine Reihe an Maßnahmen, die ergriffen werden können, um Vorfälle entweder zu vermeiden, oder besser mit ihnen umgehen zu können. Dazu gehören neben der Steigerung der Awareness auch technische und organisatorische Maßnahmen.

AWARENESS

IT-Sicherheit ist ein Bereich in dauerhaftem Wandel. Während auf der einen Seite die Angriffsvektoren immer ausgefeilter werden, werden auf der anderen Seite immer neue Wege der Verteidigung entwickelt. Deshalb ist es wichtig, Informationen über aktuelle Bedrohungen zu teilen und sichere Verhaltensweisen einzuüben. Das Projekt CONTAIN hat hierzu bereits eine Reihe an Serious Games entwickelt. Mehr dazu finden Sie unter „Unser Angebot". Daneben gibt es zahlreiche weitere Möglichkeiten der Awareness-Steigerung, die in der Umfrage gewählt wurden:

Welche Methoden setzen Sie zur Steigerung der Awareness ein? (Mehrfachnennung möglich)

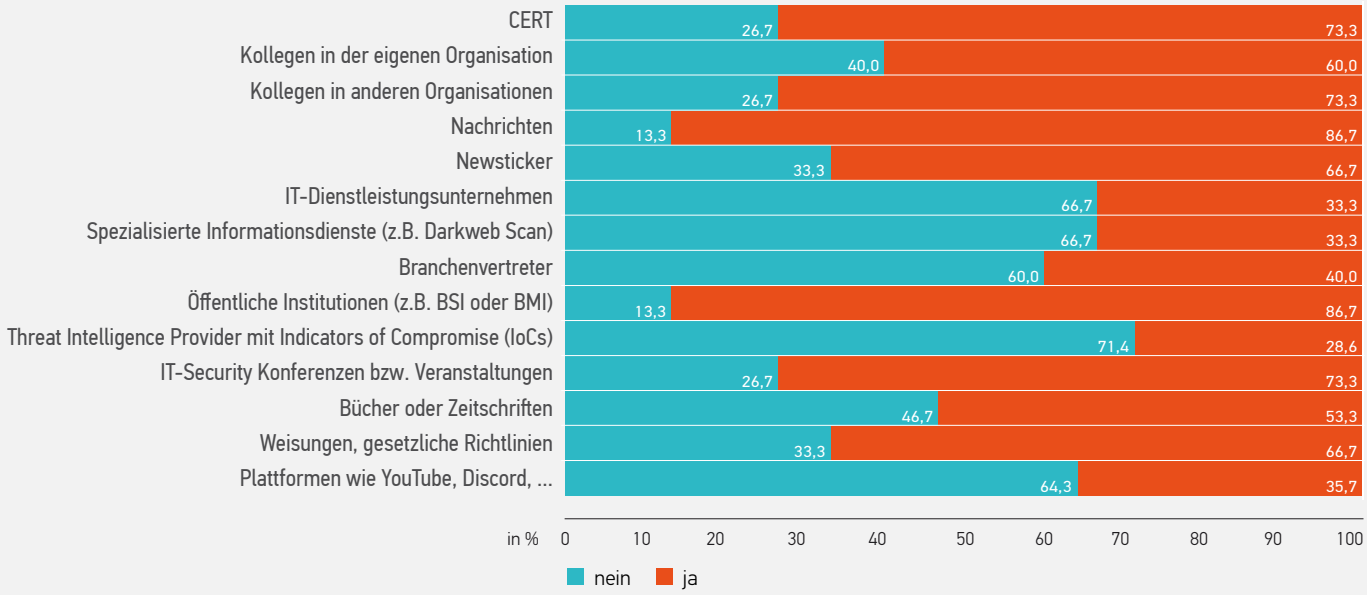


*im Internet oder per E-Mail

INFORMATIONSQUELLEN

Um das eigene Unternehmen sicher durch die Untiefen aktueller Bedrohungslagen navigieren zu können, sind aktuelle und zuverlässige Informationen unerlässlich. Deshalb haben wir gefragt, welche Kanäle aus der Vielzahl der Informationsangebote genutzt werden, um sich über IT-Sicherheit zu informieren.

Beziehen Sie Informationen zu Ransomware und zur allgemeinen IT-Sicherheitslage von... (Mehrfachnennung möglich)

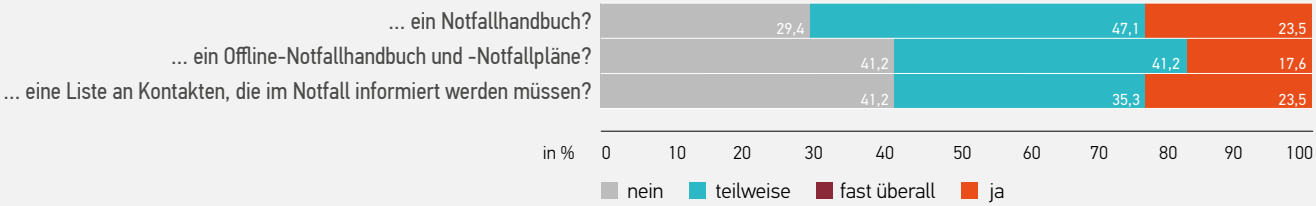


ORGANISATORISCHE SICHERHEITSMASSNAHMEN

Viele der Weichen, die über die erfolgreiche Bewältigung eines Ransomware-Vorfalls entscheiden, lassen sich schon vorher stellen: Während sorgfältiger Planung und der Probung des Notfalls. Doch gerade letztere kommt bei den Teilnehmenden unseres Monitors aktuell zu kurz, bis auf eine sehr wichtige Ausnahme: Die überwiegende Mehrheit der Befragten testet regelmäßig ihre Backups.

Haben Sie…

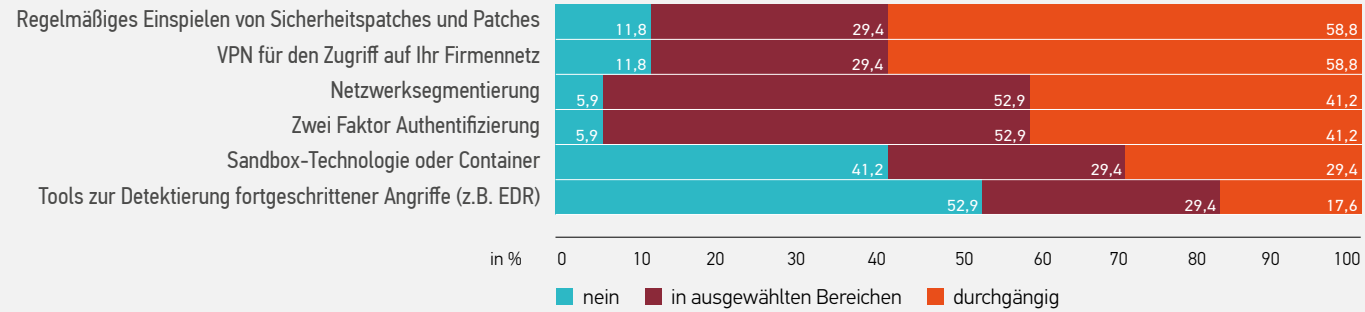
Verfügen Sie über…



TECHNISCHE SICHERHEITSMASSNAHMEN

Zu wissen, welche Geräte im Firmennetzwerk sind, das Patchmanagement geregelt zu haben und zu wissen, wo im Netzwerk Schwachstellen zu finden sind, sind Bausteine auf dem Weg zu einer resilienten IT-Infrastruktur. Wir haben uns angesehen, welche Sicherheitsmaßnahmen am häufigsten umgesetzt wurden.

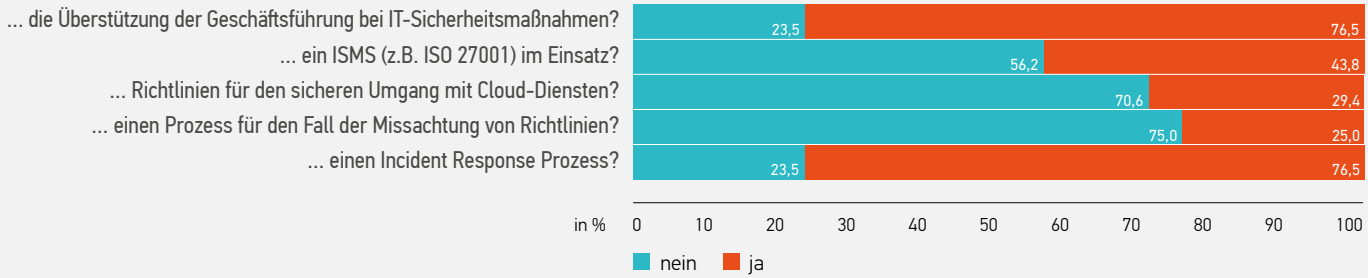
Welche IT-Sicherheitstechnologien setzen Sie in Ihrer Organisation ein?



COMPLIANCE

Ob selbst gegeben oder gesetzlich vorgeschrieben: Es gibt zahlreiche Regelungen, die die Informationssicherheit erhöhen und Organisationen widerstandsfähiger gegen Angriffe machen sollen. Während die meisten Unternehmen klare Regelungen zur Arbeit im Homeoffice haben, gibt es kaum Regelungen zum Umgang mit beliebten cloudbasierten Tools. Über ein Informationssicherheits-Managementsystem (ISMS), das hilft, die Regeln und Maßnahmen zu überblicken und einer regelmäßigen Überprüfung zu unterziehen, verfügt etwas weniger als die Hälfte der Organisationen.

Haben Sie…



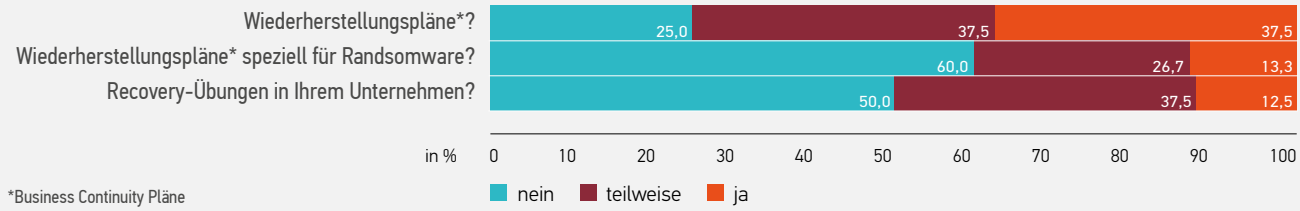

RANSOMWARE
ATTACK!

VISUALISIERUNG DES VORFALLS

WIEDERHERSTELLUNG – RECOVERY

Der Wiederherstellung und der Nachbearbeitung eines Vorfalls kommt im Zuge der Aufarbeitung eines Ransomware-Vorfalls eine wichtige Rolle zu. Richtig aufbereitet und dokumentiert, können die Erfahrungen helfen, bestehende technische und organisatorische Maßnahmen zu verbessern. Doch unsere Ergebnisse zeigen: Entsprechende Prozesse sind nur teilweise definiert.

Gibt es…



*Business Continuity Pläne

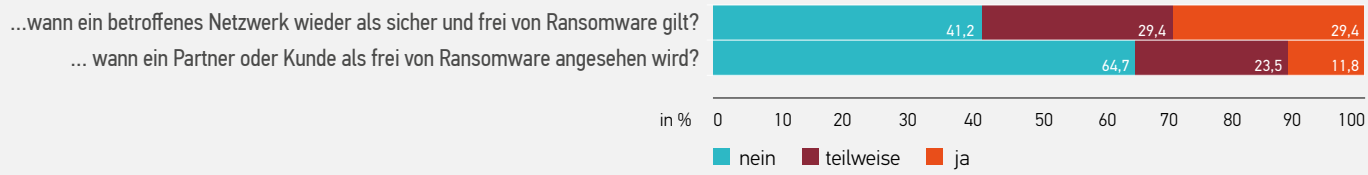
NACHBEREITUNG DES VORFALLS

DEFINITION OF DONE

Der Ransomware-Vorfall ist vorüber, die Systeme wieder hergestellt. Jetzt kann es wieder an die Arbeit gehen. Doch wann gilt ein System oder ein Gerät als frei von Ransomware? Größtenteils Einigkeit herrscht bei der Feststellung, dass die Ursachen des Vorfalls identifiziert und abgestellt sein müssen, damit die IT wieder als sicher gilt. Gleichzeitig gibt es unter den Befragten überwiegend keine oder nur teilweise definierte Prozesse, die festlegen, ob und wann dieser Zustand wieder erreicht ist. Am häufigsten wurden Prozesse definiert für betroffene Netze, aber nur sehr selten für die Frage, wann Kunden oder Partner als wieder frei von Ransomware gelten.

Stimmen Sie folgender Aussage zu:

Gibt es einen Prozess, ...



FAZIT

Die befragten Unternehmen schätzen die Bedrohungslage für die eigene Organisation mittel bis hoch ein. Die eigenen Fähigkeiten im Umgang mit einem fortgeschrittenen Ransomware-Vorfall, bei dem bereits Systeme verschlüsselt wurden, werden höher eingeschätzt als die der eigenen Branche.

Wir haben die Teilnehmenden der Umfrage gebeten, einem Kollegen, der von einem Ransomware-Vorfall betroffen ist, Empfehlungen für den Umgang damit zu geben. Die Empfehlungen der Befragten zeigen, dass Wissen über den richtigen Umgang mit IT-Sicherheitsvorfällen ganz überwiegend vorhanden ist.

Beim beispielhaften Ransomware-Vorfall, den die Befragten sich für die Beantwortung vergegenwärtigen sollten, kam es überwiegend zu Beeinträchtigungen oder einem kompletten Ausfall des Geschäftsprozesses. Neben der Erpressung von Kunden und Partnern der betroffenen Organisation kam es auch zur Veröffentlichung von gestohlenen Daten. Dieser mehrfachen Gefahr müssen sich die Verantwortlichen bewusst sein.

Die Befragten nutzen eine Vielzahl an Informationsquellen, um sich über aktuelle Bedrohungen zu informieren. Dabei steht neben den Öffentlichen Institutionen wie dem BSI bzw. den Landesbehörden (in Deutschland) oder BMI, DSN oder WKO (in Österreich) der fachliche Austausch mit Kollegen besonders hoch im Kurs, sei es auf Veranstaltungen und Kongressen oder direkt.

Awarenessmaßnahmen sind ein wichtiger Baustein, die Resilienz einer Organisation gegen Bedrohungen von außen zu steigern. Hier überwiegen klassische Maßnahmen wie Schulungen vor Ort oder Online-Trainings und News-Beiträge im Intranet oder per E-Mail. Innovative Formate wie Serious Games oder eine Cyber-Range waren unter den Befragten noch kaum anzutreffen. Wir hoffen, hier mit der Föderierten Übung und der Toolbox mit ihren Serious Games (siehe Kapitel „Unser Angebot“) einen Anreiz zu schaffen, das Portfolio um spielerisch inspirierte Formate zu erweitern.

Insgesamt ist zu beobachten, dass noch viele Entscheidungen getroffen und Prozesse definiert werden müssen, die dabei helfen, Ransomware-Vorfälle oder ganz allgemein IT-Sicherheitsvorfälle besser zu handhaben. Das zeigt sich ganz besonders in der Nachbearbeitung von Vorfällen und der Frage nach der „Definition of Done“. Die Frage, wann eine Lieferkette, ein System oder ein Gerät als frei von Ransomware gilt, sollte für die eigene IT genauso gestellt und beantwortet werden, wie für evtl. vorhandene OT-Systeme oder Partner in der Lieferkette.

DIE MULTIPLIKATOREN

Wir bedanken uns bei allen Projektpartnern, Organisationen und Einzelpersonen, die die Umfrage ausgefüllt oder verteilt haben. Besonders danken wollen wir:

bitmi
Bundesverband
IT-Mittelstand e.V.

ibi systems

secuvera:
Cybersicherheit. Nachhaltig.

SEMPACON

SWI
INFORMATIONSSICHERHEIT
FÜR DEN MITTELSTAND GmbH

FRAGENÜBERSICHT

Frage	Stichprobenumfang n
Sind Sie Entscheider mit Verantwortung im Bereich IT-Sicherheit? Sind Sie Entscheider mit Verantwortung im Bereich Geschäft?	n = 166
Wo ist Ihre Organisation tätig? ▸ Deutschland ▸ Österreich ▸ In beiden Ländern	n = 172
Wie schätzen Sie die IT-Sicherheits-Bedrohungslage für Ihre Organisation ein?	n = 62
Wie schätzen Sie die Fähigkeit, auf einen fortgeschrittenen Ransomware-Vorfall adäquat zu reagieren und die Geschäftstätigkeit vollständig wiederaufnehmen zu können für Ihre Organisation?	n = 61
Wie schätzen Sie die Fähigkeit, auf einen fortgeschrittenen Ransomware-Vorfall adäquat zu reagieren und die Geschäftstätigkeit vollständig wiederaufnehmen zu können für Ihre Branche?	n = 59
Wie schätzen Sie die Fähigkeit, auf einen fortgeschrittenen Ransomware-Vorfall adäquat zu reagieren und die Geschäftstätigkeit vollständig wiederaufnehmen zu können im Wirtschaftsraum D/AT?	n = 57
Gab es Störungen bzw. einen kompletten Ausfall des Geschäftsprozesses?	n = 33
Gab es Erpressungen bei Partnern oder Kunden?	n = 31
Gab es eine Veröffentlichung der geleakten Daten?	n = 32
Gab es Nachrichten oder E-Mails der Erpresser?	n = 31
Empfehlungen für die Kollegen: Lösegeld bezahlen?	n = 40
Empfehlungen für die Kollegen: Kunden informieren?	n = 46
Empfehlungen für die Kollegen: Geschäftspartner informieren?	n = 47
Empfehlungen für die Kollegen: Ausschließlich auf Wiederherstellung der Daten konzentrieren?	n = 44
Empfehlungen für die Kollegen: Forensik betreiben, um den Vorfall aufzuklären?	n = 47
Welche Methoden setzen Sie zur Steigerung der Awareness ein? ▸ Schulung der Mitarbeitenden vor Ort ▸ Online-Training ▸ News-Beiträge im Intranet/ per E-Mail ▸ Cyber-Range ▸ Escape-Room ▸ Podcast	n = 21

Frage	Stichprobenumfang n
Beziehen Sie Informationen zu Ransomware und zur allgemeinen IT-Sicherheitslage von...	n = 15
▸ CERT ▸ Kollegen in der eigenen Organisation ▸ Kollegen in anderen Organisationen ▸ Nachrichten ▸ Newsticker ▸ IT-Dienstleistungsunternehmen ▸ Spezialisierte Informationsdienste (z.B. Darkweb Scan) ▸ Branchenvertreter ▸ Öffentliche Institutionen (z.B. BSI oder BMI) ▸ IT-Security Konferenzen bzw. Veranstaltungen ▸ Bücher oder Zeitschriften ▸ Weisungen, gesetzliche Richtlinien	
▸ Plattformen wie YouTube, Discord, etc. ▸ Threat Intelligence Provider mit Indicators of Compromise (IoCs)	n = 14
Haben Sie ein regelmäßiges Testing für die Wiederherstellung von Backups?	n = 17
Verfügen Sie über ein Notfallhandbuch?	n = 17
... und ein Offline-Notfallhandbuch und -Notfallpläne?	n = 17
... eine Liste an Kontakten (z.B. Behörden, Partner, etc.) welche Sie im Notfall informieren müssen?	n = 17
Unterstützt die Geschäftsführung Sie in IT-Sicherheitsmaßnahmen?	n = 17
Haben Sie ein ISMS (z.B. ISO 27001) im Einsatz?	n = 16
Haben Sie Richtlinien für den sicheren Umgang mit Cloud-Diensten?	n = 17
Haben Sie einen Prozess für den Fall, dass Richtlinien nicht eingehalten werden?	n = 16
Haben Sie einen Incident Response Prozess?	n = 17
Welche IT-Sicherheitstechnologien setzen Sie in Ihrer Organisation ein?	n = 17
▸ Regelmäßiges Einspielen von Sicherheitspatches und Patches ▸ VPN für den Zugriff auf Ihr Firmennetz ▸ Netzwerksegmentierung ▸ Zwei Faktor Authentifizierung ▸ Sandbox-Technologie oder Container ▸ Tools zur Detektierung fortgeschrittener Angriffe (z.B. EDR)	

Frage	Stichprobenumfang n
Existieren Wiederherstellungspläne (Business Continuity Pläne)?	n = 16
Gibt es Wiederherstellungspläne (Business Continuity Pläne) speziell für den Fall Ransomware?	n = 15
Gibt es Recovery-Übungen in Ihrem Unternehmen?	n = 16
Stimmen Sie folgender Aussage zu: Die Ursachen müssen identifiziert und abgestellt sein. Nur dann gilt die IT als sicher.	n = 16
Gibt es einen Prozess, wann ein betroffenes Netzwerk wieder als sicher und frei von Ransomware gilt?	n = 17
Gibt es einen Prozess, wann ein Partner oder Kunde als frei von Ransomware angesehen wird?	n = 17

QUELLEN

BBK (o. J.): Glossar des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.
https://www.bbk.bund.de/DE/Infothek/Glossar/_functions/glossar.html?nn=19742&lv2=19836

BSI 2023. Die Lage der IT-Sicherheit in Deutschland 2023. Bundesamt für Sicherheit in der Informationstechnik 2023.
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

Greiner, M., Strussenberg, J., Seiler A., Hofbauer, S., Schuster M., Stano, D., Fahrnberger, G., Schauer, S., Lechner, U. (2024). Scared? Prepared? Toward a Ransomware Incident Response Scenario. In: Phillipson, F., Eichler, G., Erfurth, C., Fahrnberger, G. (eds) Innovations for Community Services. I4CS 2024. Communications in Computer and Information Science, vol 2109. Springer, Cham.
https://doi.org/10.1007/978-3-031-60433-1_17

Iosif, A-C., Lechner, U., Pinto-Albuquerque, M., Espinha Gasiba, T. (2024). Serious Game for Industrial Cybersecurity: Experiential Learning through Code Review. In: Conference on Software Engineering Education and Training (CSEE&T 2024), IEEE.

Seiler, A., Lechner, U., Strussenberg, J., Hofbauer, S. (2024). Operation Raven. In: Phillipson, F., Eichler, G., Erfurth, C., Fahrnberger, G. (eds) Innovations for Community Services. I4CS 2024. Communications in Computer and Information Science, vol 2109. Springer, Cham.
https://doi.org/10.1007/978-3-031-60433-1_19

Zhao, T., Gasiba, T., Lechner, U., Pinto-Albuquerque, M., Ongu, D. (2024). COPYCAT: Applying Serious Games in Industry for Defending Supply Chain Attack. In: Phillipson, F., Eichler, G., Erfurth, C., Fahrnberger, G. (eds) Innovations for Community Services. I4CS 2024. Communications in Computer and Information Science, vol 2109. Springer, Cham.
https://doi.org/10.1007/978-3-031-60433-1_18

contain

Weitere Informationen zum Projekt CONTAIN finden Sie unter:

contain-projekt.de

contain-projekt.at

oder

linkedin.com/groups/9549256/

Die digitale Version dieser Broschüre finden Sie unter:

unibw.de/wirtschaftsinformatik/publikationen

Diese Broschüre wurde erstellt von
CONTAIN Deutschland

Institut für Schutz und Zuverlässigkeit
Fakultät für Informatik
Universität der Bundeswehr München

Prof. Dr. Ulrike Lechner
Werner-Heisenberg-Weg 39
85577 Neubiberg

Tel: +49 89 6004-2504
E-Mail: Ulrike.Lechner@unibw.de

Ansprechpartnerin CONTAIN Monitor:
Judith Strußenberg
E-Mail: judith.strussenberg@unibw.de