MARKTFORSCHUNG

Ransomware in der C-Suite: Eine Studie von (ISC)²

Deutsche Führungskräfte unterschätzen Ransomware-Bedrohungen

(ISC)²® | Inspiring a Safe and Secure Cyber World

EINLEITUNG

Ransomware ist eine der größten und disruptivsten Herausforderungen für die Cybersicherheit von Unternehmen im Jahr 2021 und in den Jahren davor. Seit dem aufsehenerregenden globalen Wannacry-Ransomware-Ausbruch im Mai 2017 ist das ganze Ausmaß der finanziellen und betrieblichen Auswirkungen von Ransomware für Cybersicherheitsexperten und ihre Unternehmen in den Vordergrund gerückt, und ein kontinuierlicher Strom von Ransomware-Angriffen folgte im Kielwasser von Wannacry. Da neben Privatpersonen auch Unternehmen, Behörden und kritische Infrastrukturen angegriffen werden, sind die Auswirkungen von Ransomware auf allen Ebenen der Gesellschaft zu spüren.

Mit einer Bevölkerung von 84 Millionen Einwohnern und einem Bruttoinlandsprodukt (BIP) von fast 4 Billionen Dollar ist Deutschland - und seine Wirtschaft - eine bedeutende globale Präsenz und damit eine ideale Zielscheibe für Ransomware-Angriffe. Es ist wichtig anzumerken, dass die Zahl der Beschäftigten im Bereich Cybersicherheit in Deutschland im letzten Jahr deutlich zugenommen hat, und zwar um 165% von knapp über 175.000 auf fast 465.000 innerhalb eines Jahres. Dieser Anstieg wird als Reaktion auf den raschen digitalen Wandel in der deutschen

zugenommen hat, und zwar um 165% von knapp über 175.000 auf fast 465.000 innerhalb eines Jahres.. Dieser Anstieg wird als Reaktion auf den raschen digitalen Wandel in der deutschen Wirtschaft gesehen, der auf die pandemiebedingte Remote-Arbeit und das damit verbundene Wachstum des E-Commerce zurückzuführen ist. Das bedeutet auch, dass Deutschland die meisten Arbeitskräfte im Bereich Cybersicherheit in der Europäischen Union beschäftigt.

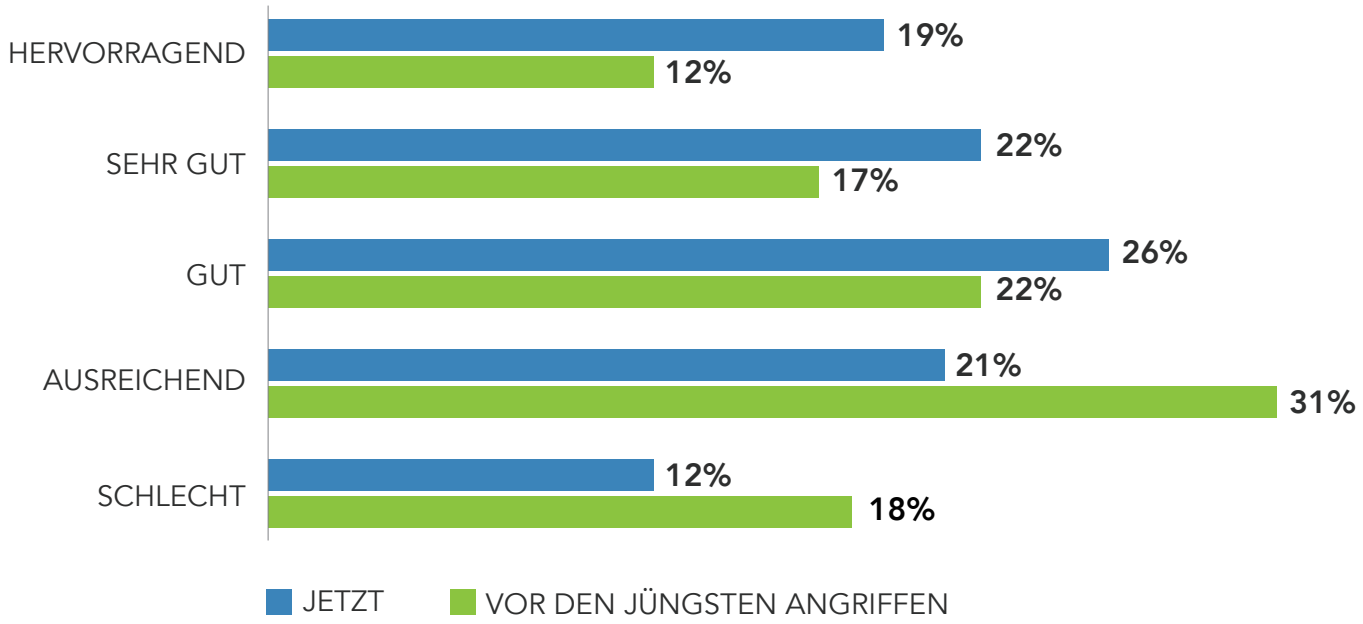
Um besser zu verstehen, wie Ransomware von Führungskräften und leitenden Entscheidungsträgern gesehen wird und wie diese Wahrnehmung Geschäftsentscheidungen, Investitionen und Ressourcen in Bezug auf die aktuelle Bedrohungslandschaft beeinflussen könnte, hat (ISC)^2 eine Studie mit dem Schwerpunkt der Ransomware-Problematik unter Führungskräften in Deutschland durchgeführt.

Diese Studie, für die 250 Führungskräfte in ganz Deutschland befragt wurden, liefert Cybersicherheitsexperten verwertbare Informationen darüber, was die C-Suite über Ransomware wissen möchte. Die Studie zeigt, dass Führungskräfte ein größeres Bewusstsein und Verständnis für Risiken und Bedrohungen benötigen, dass sie einen besseren Fahrplan benötigen, wie sie Personal und Budget richtig einsetzen können, um den aktuellen Bedrohungen zu begegnen, und dass sie eine Anleitung benötigen, um die Fähigkeiten ihrer Unternehmen proaktiv zu stärken, damit sie kurz- bis mittelfristig mit einer erhöhten Bedrohungslage umgehen können. Die Ergebnisse zeigen, dass Ransomware in Deutschland weniger als unmittelbare Bedrohung wahrgenommen wird und dass die Führungskräfte in Deutschland weniger defensiv eingestellt sind als in anderen großen internationalen Volkswirtschaften.

Nur 40% der Befragten stuften sich vor den jüngsten Vorfällen als “sehr bewusst” in Bezug auf Ransomware ein. Eine Zahl, die darauf schließen lässt, dass die verwertbaren Erkenntnisse dieses Bewusstseins gering waren. Das ist deutlich weniger als in den anderen G7-Ländern und lässt sich damit rechtfertigen, dass andere Länder zumindest anfangs als attraktivere Ziele wahrgenommen wurden. Das ändert jedoch nichts an der Tatsache, dass Deutschland als eine der größten Volkswirtschaften der Welt und als strategisch wichtige Finanz-, Produktions- und Handelsnation ein wichtiges Ziel für Ransomware-Angriffe ist, die darauf abzielen, zu betrügen, zu schädigen und zu destabilisieren.

EIN DEFIZIT IN DER KOMMUNIKATION

Bewertung der Ransomware-Kommunikation von Cybersicherheits-Teams



Das Bewusstsein für Ransomware ist bei den Führungskräften in Deutschland gering. Nur 12% bewerteten ihr Bewusstsein für Ransomware vor den jüngsten öffentlichkeitswirksamen Angriffen (Beispiele hierfür sind die Angriffe auf Colonial Pipeline, JBS Foods und Kaseya) als hervorragend. Weitere 17% bezeichneten ihr Bewusstsein als gut, aber fast die Hälfte (49%) bezeichnete es als schlecht oder sehr schlecht.

Die Daten deuten darauf hin, dass der Grund dafür in der Art und Weise liegt, wie Bedrohungen und Probleme bis hinauf zur C-Suite und anderen Führungskräften im Unternehmen kommuniziert werden. Nur 19% halten die Kommunikation, die sie von ihren Cybersicherheitsteams über Ransomware erhalten, für hervorragend, während nur 3% sie als gut bezeichnen. Ein Drittel (33%) hält die Kommunikation für schlecht oder sehr schlecht, und nur ein Viertel (26%) bewertet den Standard der Ransomware-bezogenen Kommunikation als ausreichend. Dies macht deutlich, dass Unternehmen und ihre Cybersicherheitsexperten vor einer großen Herausforderung stehen: Sie müssen sowohl den Umfang als auch die Qualität ihrer Berichte und Warnungen erhöhen, um nicht zu riskieren, dass die Herausforderung, die Ransomware darstellt, fälschlicherweise

heruntergespielt wird und Geschäftsentscheidungen in Bezug auf Investitionen in Cybersicherheit beeinträchtigt werden.

Es ist auch klar, dass trotz der weltweiten Zunahme von Ransomware-Angriffen die Häufigkeit der Kommunikation von Cybersicherheitsteams mit ihren Führungskräften nicht im gleichen Maße zugenommen hat. Nur 20% der Befragten berichteten über einen deutlichen Anstieg, 31% über einen leichten Anstieg. In beiden Fällen ist dies unterdurchschnittlich im Vergleich zu anderen Volkswirtschaften wie den USA und Großbritannien. Ein Viertel der deutschen Führungskräfte berichtete von keiner Veränderung und fast ein weiteres Viertel gab an, dass die Ransomware-bezogene Kommunikation zurückgegangen ist. Bemerkenswert war auch, dass 25% ausdrücklich häufigere Mitteilungen wünschen, während 31% mehr umsetzbare Informationen wünschen.

Neue Investitionen und Veränderungen

Entscheidungsträger und Führungskräfte wünschen sich mehr Kommunikation von ihren Cybersicherheitsteams. Sie wünschen sich vor allem klare Anfragen und Erklärungen zu ihren Bedürfnissen und Wünschen. So gaben beispielsweise 32% an, dass sie genau wissen müssen, was im Zusammenhang mit Ransomware im Detail gefordert wird, wie z. B. mehr Budget, mehr Mitarbeiter usw., um effektive Geschäfts- und Budgetentscheidungen zu treffen.

Gleichzeitig sagten 34%, dass die Cybersicherheitsteams quantifizieren müssen, wie mehr Geld oder mehr Ressourcen eine Veränderung oder einen Nutzen bringen. Die größte Sorge bereitet die Rückmeldung, dass 29% der befragten Unternehmensleiter und Entscheidungsträger nach einem größeren Ausbruch von Ransomware zeitnahere Updates benötigen, um zu wissen, ob ihr Unternehmen betroffen ist oder nicht. Dies ist ein signifikanter Anteil der Studienteilnehmer, die das Gefühl haben, von wichtigen Informationen über Ransomware, die die Assets ihres Unternehmens bedroht, abgeschnitten zu sein.

VIER GOLDENE REGELN, BEWUSSTSEIN UND BEREITSCHAFT FÜR RANSOMWARE ZU VERBESSERN

Auch wenn die Entscheidungen, die letztlich die Investitionen und die strategische Ausrichtung bestimmen, bei der Unternehmensleitung liegen, kann das Cybersicherheitsteam selbst viel tun, um das Unternehmen besser vorzubereiten und einige der in dieser Studie aufgezeigten Herausforderungen anzugehen:

Verstärkte Kommunikation und Berichterstattung an die Führung

Das Feedback zeigt deutlich, dass die Führungsebene mehr Kommunikation von den Cybersicherheitsexperten, die sich mit Ransomware innerhalb des Unternehmens befassen, wünscht und benötigt. Außerdem müssen die Berichte und Warnungen detaillierter und ausführlicher sein, damit die Führungskräfte die Situation und die einzelnen Bedrohungen besser verstehen, fundiertere Entscheidungen treffen und die Forderung nach Investitionen in die Cybersicherheit unterstützen können. Implementieren Sie neue Berichterstattungsprozesse und vereinbaren Sie mit den Führungskräften, wie die Berichte aussehen sollen, um eine bessere Detailgenauigkeit zu erreichen, die den Entscheidungsprozess unterstützt.

Ransomware-Prozesse klären

Die Hälfte der befragten Unternehmen hat keine klare Position, ob sie ein Lösegeld zahlen sollen, da sie nicht besprochen haben, was sie in einem solchen Szenario tun würden. Es ist wichtig, Unklarheiten zu vermeiden und sicherzustellen, dass sich alle Beteiligten über die ethische und operative Haltung des Unternehmens im Falle einer Zahlungsforderung durch Cyberkriminelle im Klaren sind, bevor es zu einem solchen Vorfall kommt. Die Führungsebene muss eine klare Richtlinie für Lösegeldzahlungen diskutieren, vereinbaren und umsetzen und diese Entscheidung allen mitteilen, um Unklarheiten zu vermeiden.

Klarstellen, dass Cybersicherheit in der Verantwortung eines jeden liegt

Die Antworten haben gezeigt, dass Verantwortung in deutschen Unternehmen verteilt ist, und zwar gleichmäßig auf die Bereiche Cybersicherheit, IT und Geschäftsführung. Es ist wichtig, dass Unternehmen die Tatsache im Auge behalten, dass die Abwehr von Ransomware

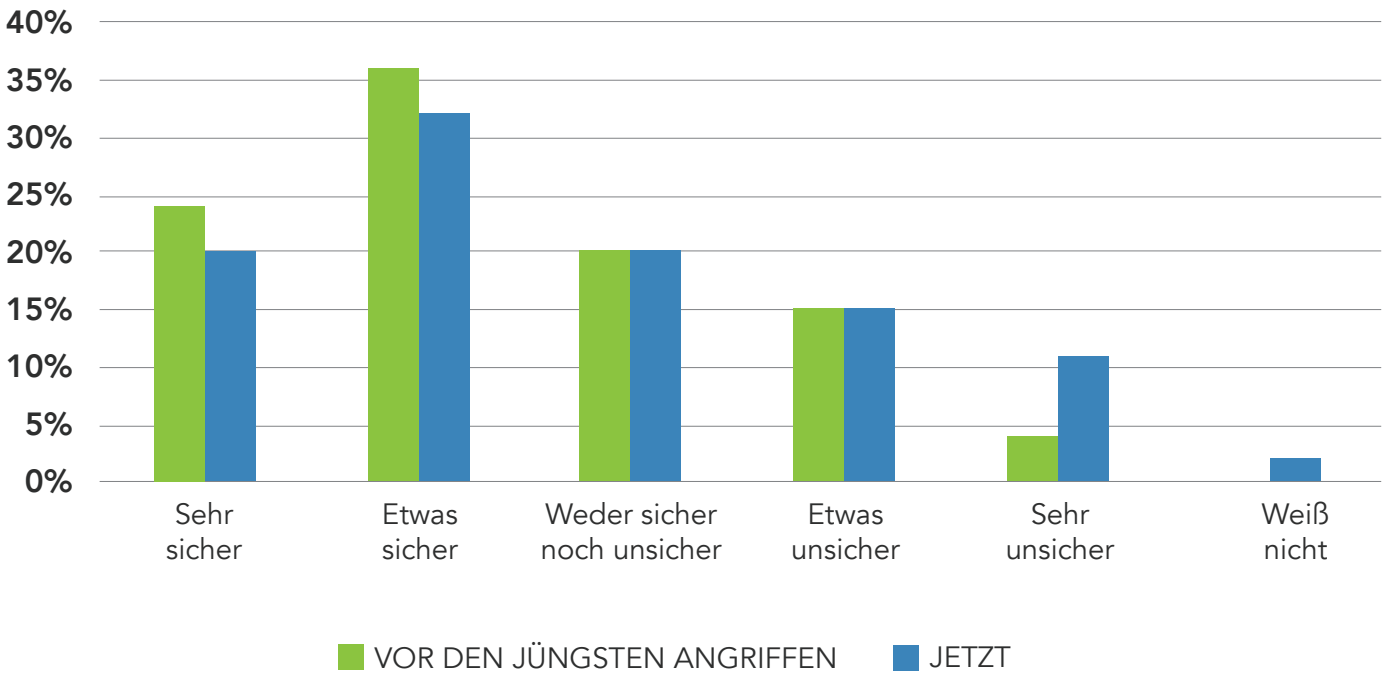
in der Verantwortung aller liegt, und eine Aufteilung von Verantwortung und Transparenz für Ransomware-Wissen, Richtlinien und Prozessen vermeiden. Nur 30% der Befragten gaben an, dass die letzte Verantwortung bei der Geschäftsleitung liegt. Letztlich muss die Führung in allen Fällen von der Unternehmensspitze ausgehen, allerdings mit dem Vorbehalt, dass die IT-Abteilung, die Cybersicherheit und alle anderen Teams für die Umsetzung der Richtlinien, die Berichterstattung und die Reaktion auf erkannte Bedrohungen oder ein erhöhtes Ransomware-Risiko verantwortlich sind.

Die regulatorische Landschaft verstehen

Die Daten zeigen, dass der Grad an Bewusstsein und Besorgnis über die regulatorischen Auswirkungen eines Ransomware-Angriffs geringer sind. Ein Ransomware-Angriff auf ein Unternehmen löst wahrscheinlich DSGVO-Protokolle aus, wie die Meldung des Vorfalls, den Nachweis, dass alle angemessenen Schritte zum Schutz der Daten vor und während des Vorfalls unternommen wurden, sowie die Compliance der Handlungen des Unternehmens (einschließlich der Entscheidung, ein Lösegeld zu zahlen). Die Lösegeldforderungen sind gestiegen, um von der Tatsache zu profitieren, dass eine DSGVO-Geldstrafe noch höher ausfallen könnte. Eine Forderung der DSGVO ist, dass der Verantwortliche bestimmte Datenschutzverletzungen an die Aufsichtsbehörde in seiner Region melden muss. Die Entscheidung, Lösegeld an Cyberkriminelle zu zahlen, um eine Meldung an die Aufsichtsbehörde zu vermeiden, wäre bereits ein Verstoß gegen die Verordnung. Wenn das Unternehmen erwischt wird, drohen ihm Strafen für den Verstoß und die Nichtmeldung. Informieren Sie sich über die regulatorischen Anforderungen in Bezug auf Ransomware und handeln Sie bei der Handhabung und Meldung ethisch und rechtlich.

VERTRAUENSEBENEN

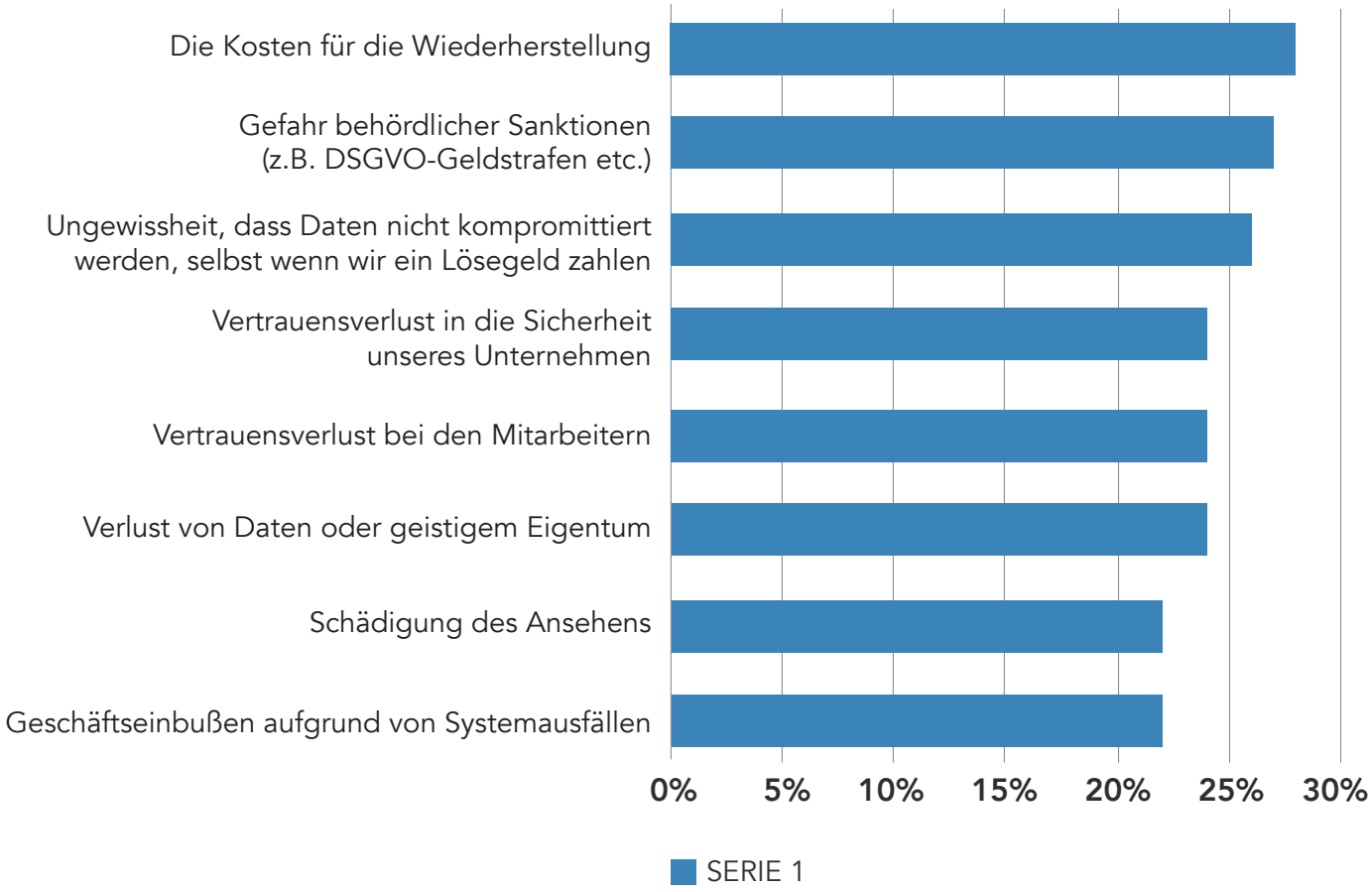
Haben Sie Vertrauen, dass Ihr Unternehmen auf einen Ransomware-Angriff vorbereitet ist?



Es ist auffallend, dass die Vertrauensebenen der Befragten deutlich geringer ist als die ihrer Kollegen in anderen Ländern. Nur 20% sind sehr sicher, dass ihr Unternehmen auf die Abwehr eines Ransomware-Angriffs vorbereitet ist oder sich davon erholen kann. Ein Drittel (32%) ist etwas sicher, während mehr als ein Viertel (26%) etwas oder sehr unsicher ist. Weitere 22% wissen es nicht oder haben keine klare Meinung. Selbst als die gleiche Frage im Zusammenhang mit den genannten Beispielen für weltweite Ransomware-Ausbrüche gestellt wurde, blieb das Vertrauen in Deutschland gering, mit einer Abweichung von nur 2 - 4% bei den Antworten.

WAS FÜHRUNGSKRÄFTE BEUNRUHIGT

Die größten Sorgen, wenn das Unternehmen von Ransomware betroffen ist



Die Bereiche, die bei einem Ausbruch von Ransomware in einem Unternehmen die größten Sorgen bereiten, sind wenig überraschend. Die größte Sorge neben den Gesamtkosten für die Wiederherstellung (28%) ist die Gefahr von Geldstrafen und Rechtsstreitigkeiten (27%), dicht gefolgt von der Gefährdung des geistigen Eigentums (24%). Die Tatsache, dass Geldstrafen das geistige Eigentum übertrumpfen, zeigt auch, dass 37% der befragten Unternehmen bereit wären, ein Lösegeld zu zahlen, wenn dies der effektivste Weg wäre, sich von dem Angriff zu erholen. Für diese Unternehmen ist die Zahlung des Lösegelds entweder der schnellste Weg zu einer Lösung oder der billigste. Ein Punkt, der vielen Entwicklern von Ransomware-Angriffen sehr bewusst ist, insbesondere wenn sie auf europäische Unternehmen abzielen.

SIND SIE VORBEREITET?

Was hält Ihr Unternehmen heute für den Fall eines erfolgreichen Ransomware-Angriffs bereit? (Mehrfachauswahl)

Cyber-Versicherung mit Ransomware-Deckung	25%
Kontakt(e) zu Strafverfolgungsbehörden	27%
Ransomware-Taskforce/-Team	30%
Juristische(n) Kontakt(e)	29%
Ransomware-Reaktionsplan	25%
Bitcoin-Konto für Ransomware-Zahlungen	21%
Disaster Recovery Site	25%

Unternehmen in Deutschland haben einige Maßnahmen ergriffen, um einen Ransomware-Angriff abzuwehren oder darauf zu reagieren, aber diese Maßnahmen sind uneinheitlich und im Vergleich zu anderen Volkswirtschaften unterdurchschnittlich.

Unternehmen müssen ein klares Audit durchführen, um zu verstehen und zu dokumentieren, über welche Maßnahmen das Unternehmen verfügt, und um Bereiche, die mangelhaft sind, zu identifizieren und zu beheben.

Zu den präventiven Maßnahmen gehören Investitionen in den Versicherungsschutz (und die Sicherstellung einer ausreichenden Deckung), die Einrichtung eines Teams, das bei der Reaktion auf einen Vorfall die Führung übernimmt, die Dokumentation eines Ransomware-Reaktionsplans und die Umsetzung physischer Wiederherstellungsmaßnahmen, um die Wiederherstellung nach einem Angriff zu unterstützen (getestete Backups, Standorte für die Notfallwiederherstellung, Remote-Arbeitsinfrastruktur, Redundanz der Ausrüstung usw.)

Mehr als ein Fünftel (21%) der Führungskräfte von Unternehmen gaben an, dass es für die Vorbereitung auf die Abwehr von Ransomware am wichtigsten ist, zu wissen, dass die Pläne zur Sicherung und Wiederherstellung von Daten nicht durch Ransomware-Angriffe beeinträchtigt werden. 36% müssen wissen, was nötig ist, um einen minimalen Betrieb wiederherzustellen, wenn das Unternehmen kompromittiert wird. Dazu gehört die Gewissheit, dass Backups verfügbar sind und funktionieren, die Identifizierung von Systemen mit hoher Priorität, die Wiederherstellung grundlegender Dienste zur Deckung grundlegender betrieblicher Bedürfnisse usw. Weitere 27% verlassen sich darauf, dass ihre Cybersicherheitsteams ihnen sagen, wie das Unternehmen funktionieren kann und wird, wenn wichtige Systeme durch Ransomware außer Gefecht gesetzt werden. Neben diesem Ergebnis benötigen 31% eine klarere Bewertung des Unternehmensrisikos, damit fundierte Entscheidungen über die Ransomware-Strategie getroffen werden können.

FAZIT

Ransomware ist ein globales Problem und stellt eine erhebliche finanzielle, betriebliche und datenbezogene Bedrohung für Unternehmen dar, unabhängig von Größe, Sprache und Standort. Obwohl Ransomware für Unternehmen und andere Entscheidungsträger in Deutschland von besonderem Interesse ist, ist es bemerkenswert, dass Fokus- und Bewusstseinsebene und Informationsqualität deutlich geringer ist als in anderen großen Volkswirtschaften weltweit. Führungskräfte wollen und müssen mehr wissen, um wirksame Entscheidungen zu treffen und die Anforderungen an Investitionen in die Entwicklung von Kompetenzen, Technologien und Prozessen zum Schutz vor dem erhöhten Risiko durch Ransomware vollständig zu verstehen. Obwohl Unternehmen in Deutschland einige neue Investitionen in die Abwehr von Ransomware getätigt haben, gibt es noch Spielraum für weitere Investitionen, um mit den Wettbewerbern in anderen Volkswirtschaften Schritt zu halten. Investitionen beschränken sich nicht nur auf die Technologie. Investitionen in die Mitarbeiterzahl und in die Weiterbildung sind ebenso wichtig, um Ransomware-Bedrohungen mit technischen Gegenmaßnahmen zu bekämpfen.

Der Schlüssel zur Implementierung und Aufrechterhaltung einer robusteren Verteidigungsposition gegen Ransomware-Angriffe ist Kommunikation. Entscheidungsträger müssen wissen, welchen Bedrohungen das Unternehmen ausgesetzt ist, und sie müssen wissen, welche Ressourcen benötigt werden, um einem Angriff vorzubeugen und wie mit einem Angriff umzugehen ist, der Systeme und Daten erfolgreich kompromittiert. Cybersicherheitsexperten müssen mehr Wert darauf legen, rechtliche und regulatorische Fragen zu verstehen und hervorzuheben, ihre Fähigkeiten kontinuierlich weiterzuentwickeln und zu schulen, mit den Strafverfolgungsbehörden zusammenzuarbeiten, Reaktionspläne zu entwickeln und zu dokumentieren und sicherzustellen, dass jeder, der diese Pläne kennen muss, darüber informiert ist und Zugang dazu hat.

Letztlich deuten die Ergebnisse der Studie darauf hin, dass jetzt ein guter Zeitpunkt für Cybersicherheitsexperten ist, um die Kommunikation über Ransomware in ihren Unternehmen zu verstärken. Dazu gehört auch, dass sie jetzt mit dem Führungsteam darüber sprechen, welche weiteren Investitionen in Mitarbeiter, Technologie und Prozesse erforderlich sind. Angesichts der Tatsache, dass Ransomware auch andernorts in den Köpfen der Führungskräfte so präsent ist, ist der Zeitpunkt für Unternehmen in Deutschland ideal, um sich verstärkt mit der Abwehr und dem Schutz von/vor Ransomware sowie der Einhaltung von Vorschriften zu befassen.

Methodik

Die (ISC)² Ransomware-Studie war eine blinde Umfrage, die von (ISC)² und Opinion Matters im September 2021 durchgeführt wurde. Befragt wurden insgesamt 250 C-Suite-Führungskräfte (CEO, CFO, CIO, COO, Chefjustiziar/CLO, President) in Deutschland aus Unternehmen mit mehr als 500 Mitarbeitern. Die Fehlermarge beträgt plus oder minus 6,2% bei einer statistischen Sicherheit von 95%.

Über (ISC)²

(ISC)² ist ein international tätiger gemeinnütziger Mitgliederverband, der sich für ein sicheres Internet einsetzt. (ISC)² ist besonders für sein hoch gelobtes "Certified Information Systems Security Professional" (CISSP®) Zertifikat bekannt und bietet ein Portfolio an anderen Zertifikaten, die Teil einer ganzheitlichen pragmatischen Strategie für mehr Sicherheit sind. Die mehr als 160.000 Mitglieder bestehen aus zertifizierten Fachkräften im Bereich IT-, Informations-, Software- und Infrastruktursicherheit, die sich für Fortschritte in der Industrie einsetzen. (ISC)² engagiert sich mit seiner gemeinnützigen Stiftung The Center for Cyber Safety and Education™ zudem für mehr Aufklärung der Allgemeinheit. Mehr Informationen über (ISC)² finden Sie auf www.isc2.org oder folgen Sie (ISC)² auf Twitter, Facebook oder LinkedIn.