EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Unterstützt von: vmware

Ransomware: Zunehmende Angriffe führen zu veränderten Sicherheitsprioritäten und -ausgaben in Unternehmen

EMA Research Report Juni 2022

Christopher M. Steffen, CISSP, CISA Managing Research Director
Ken Buckler, CASP Research Analyst

Informationssicherheit, Risiko- und Compliance-Management

Inhaltsverzeichnis

Einführung

Im Rahmen eines Proof-of-Concept verbreitete sich 1971 der erste selbstreplizierende Virus „Creeper“ im ARPANET. Der Virus sollte keinen Schaden anrichten, sondern lediglich potenzielle Schwachstellen in Großrechnern im Netzwerk aufzeigen. Diese Malware war nicht destruktiv, sie wurde den Betroffenen höchstens lästig. Auf den infizierten Systemen wurde die eher lustige Meldung I'M THE CREEPER, CATCH ME IF YOU CAN angezeigt. Das zerstörerische Potenzial von sich selbst replizierender Malware wurde dadurch aber deutlich.

Leider sind die Zeiten der „Scherz“-Malware vorbei, denn moderne Malware ist nicht zum Lachen. Heute ist Ransomware eine der am schnellsten wachsenden Bedrohungen in der Cybersecurity-Branche. Sie kann sich nicht nur selbst verbreiten, sondern auch alle Dateien oder ganze Systeme in einem Netzwerk verschlüsseln. Mit dieser spezialisierten Malware verfolgen Angreifer vor allem das Ziel, sich direkt zu bereichern.

Wie funktioniert Ransomware? Nach der Erstinfektion versucht Ransomware, das Netzwerk zu durchdringen und alle Computer im LAN oder WAN zu infizieren. Sobald genügend Zeit vergangen ist und eine maximale Verbreitung erreicht wurde, beginnt die Ransomware, Daten und/oder Systeme unbemerkt zu verschlüsseln. Wenn das erledigt ist, erhält der Anwender eine Benachrichtigung, dass die Daten oder das System erst wieder freigeschaltet werden, wenn er ein Lösegeld zahlt. Normalerweise haben diese Lösegeldforderungen eine Frist. Manchmal wird bei rascher Zahlung sogar ein Rabatt angeboten. Die Angreifer fordern in der Regel Kryptowährung. So kann die Zahlung nicht so leicht rückgängig gemacht oder zurückverfolgt werden.

An dieser von Enterprise Management Associates durchgeführten Umfrage nahmen 213 Personen aus Unternehmen mit 250 oder mehr Mitarbeitern aus über 20 verschiedenen Branchen teil. Fast die Hälfte (46,9 %) der befragten Personen gab an, dass ihr Unternehmen schon einmal von einen Ransomware-Angriff betroffen war. Von diesen hat etwa ein Drittel (32,0%) das Lösegeld gezahlt. Diese Umfrage untersucht die Auswirkungen von Ransomware und die Effektivität von Abwehr- und Wiederherstellungsstrategien, die heute eingesetzt werden.

Die wichtigsten Ergebnisse

Budget und Prioritäten

47 % der befragten Unternehmen gaben an, dass ihre IT-Abteilung über das Sicherheitsbudget entscheidet, aber die Abteilung für Informationssicherheit die Sicherheitsprioritäten festlegt.

Schutz vor Ransomware

95,3 % der befragten Unternehmen sind der Meinung, dass die Branche eine bessere Technologie zum Schutz vor Ransomware benötigt. 93,4 % sind überzeugt, dass ihr derzeitiger Schutz ausreichend ist.

56 % der Unternehmen sind der Meinung, dass eine einfache Antivirensoftware für den Schutz vor Ransomware nicht ausreichend ist.

Auswirkungen und Wiederherstellung

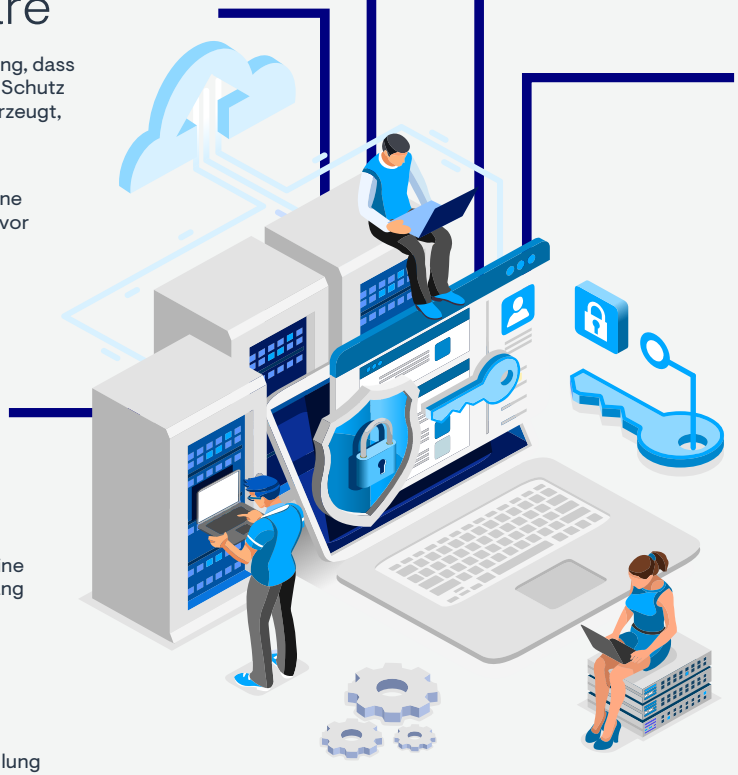
46,9 % der befragten Unternehmen waren schon einmal von einem Ransomware-Angriff betroffen.

69 % der Ransomware-Angriffe erfolgten über eine Phishing-E-Mail mit einem bösartigen Anhang oder bösartigen Link.

69 % der Unternehmen waren in der Lage, ihre Systeme innerhalb von sechs Tagen nach dem Angriff wiederherzustellen.

76,5 % der Unternehmen planen die Wiederherstellung nach einem Ransomware-Angriff mit vollständigen System-Backups oder Daten-Backups (69 %).

53,5 % der Unternehmen wollen eine Cyberversicherung nutzen oder das Lösegeld mit eigenen Mitteln zahlen (24,5 %).



Versicherungsausgaben

86 % der Unternehmen, die in eine Cyberversicherung investiert haben, gaben an, dass die Prämien sich zumindest leicht erhöht haben. Bei 42,9 % betrug die Erhöhung mindestens 10 %.

62,4 % der befragten Unternehmen mit einer Cyberversicherung haben eine Versicherungssumme von mehr als 500.000 US-Dollar vereinbart.

Zahlung des Lösegelds

32 % der von einem Ransomware-Angriff betroffenen Unternehmen haben das Lösegeld gezahlt.

56 % entschieden sich für die Zahlung des Lösegelds, weil die Remediation-Kosten noch höher gewesen wären.

53 % entschieden sich für die Zahlung, weil die Ausfallzeit eine zu große Belastung für das Unternehmen gewesen wäre.

75 % gaben an, dass sich mit der Zahlung alle erwarteten Probleme lösen ließen, und 21,9 %, dass das Unternehmen durch die Zahlung Kosten gespart hat. Nur 3,1 % waren der Meinung, dass der Lösegeldbetrag höher war als die Kosten, wenn sie nicht gezahlt hätten.

50 % der Unternehmen, die das Lösegeld nicht zahlten, gaben als Grund dafür die Überzeugung an, dass dies nicht der richtige Weg sei.

39,7 % der Unternehmen, die das Lösegeld nicht zahlten, vertrauten nicht darauf, dass die Angreifer ihr Versprechen einhalten würden.

73,2 % der Unternehmen sind der Meinung, dass die Zahlung von Lösegeld bei Ransomware von den Regierungen als illegal eingestuft werden sollte, um Angreifer abzuschrecken.

54,5 % der Unternehmen sind der Meinung, dass Unternehmen das Lösegeld zahlen sollten, um ihren Betrieb wiederaufnehmen zu können.

Zitate und Feedback von Umfrageteilnehmern

Ausgewählte Beispielantworten:

Erläutern Sie in Ihren eigenen Worten den Ansatz Ihres Unternehmens für den Umgang mit Ransomware.

[Ransomware] macht sich die Tatsache zunutze, dass unsere Kulturen nicht auf diese Art von Bedrohungen vorbereitet sind. Wir nutzen zwar Technologien, aber nicht immer mit der erforderlichen Sicherheit.

[Unser Unternehmen] möchte natürlich keinem Ransomware-Angriff zum Opfer fallen, aber auch nicht das nötige Geld ausgeben, um sicherzustellen, dass das auf keinen Fall passiert. Wir erstellen zwar tägliche Backups und senden sie an einen externen Standort, aber wir haben keine gute Möglichkeit, um zu verhindern, dass Ransomware überhaupt in unsere Umgebung gelangt.

Wir waren von einem Ransomware-Angriff betroffen und haben drei Millionen Dollar Lösegeld gezahlt. Seitdem haben wir unsere Cybersecurity-Strategie verbessert und eine zusätzliche Versicherung abgeschlossen.

Wir planen im Voraus. Wir haben einen Plan zur Reaktion auf Vorfälle, der regelt, wie das System auf Vorfälle wie Ransomware-Angriffe überwacht wird, wie sie erkannt werden und wie das Unternehmen darauf reagiert. Wir bieten auch Schulungen für Mitarbeiter zum Thema Sicherheit an. Außerdem testen wir unseren Plan zur Reaktion auf Vorfälle und Wiederherstellung mithilfe von Simulationen und Übungen, in denen wir alle Schritte durchgehen.

Wir verfügen über mehrere Schutzebenen, darunter vollständige System-Images, externe Datenspeicherung und vollständige Verschlüsselung sowie eine Ransomware-Versicherung bei zwei Anbietern. Wir nehmen Ransomware sehr ernst, da wir mit sensiblen Daten arbeiten.

Manchmal ist es günstiger, das Lösegeld zu zahlen, als Geld auszugeben, um das Problem anders zu lösen.

Kommentar:

Wir haben alle Befragten gebeten anzugeben, inwieweit sie verschiedenen Aussagen über Ransomware zustimmen.

Die Ergebnisse zeigen, welche Auswirkungen Ransomware auf Unternehmen in allen Branchen weltweit hat.

Bemerkenswerterweise sind 43 % der Befragten der Meinung, dass eine einfache Antivirensoftware ausreichenden Schutz vor Ransomware bietet. Gleichzeitig haben über 80 % der Unternehmen ihre Cloud-Computing-Strategien sowie ihre Strategien zur Sicherung und Wiederherstellung von Dateien aufgrund der Bedrohung durch Ransomware überdacht.

Während 95,3 % der Unternehmen der Meinung sind, dass die Branche eine bessere Technologie zum Schutz vor Ransomware benötigt, gab eine ähnliche Anzahl (93,4 %) der befragten Personen an, dass ihr derzeitiger Schutz ausreichend ist. Diese Daten mögen widersprüchlich erscheinen. Eine Erklärung könnte darin liegen, dass Unternehmen die beste verfügbare Technologie nutzen, sich aber bewusst sind, dass diese letztendlich nicht ausreicht, um diese wachsende Bedrohung vollständig zu verhindern. Selbst wenn die neuesten Technologien eingesetzt werden, gibt es noch viel Verbesserungspotenzial.

Bewerten Sie die folgenden Aussagen zu Ransomware:

	Stimme voll zu	Stimme eher zu	Stimme eher nicht zu	Stimme überhaupt nicht zu
Die Cybersecurity-Branche braucht bessere Technologien zur Abwehr von Ransomware.	47,4 %	47,9 %	4,7 %	0,0 %
Das Sicherheitsbudget meines Unternehmens reicht aus, um sich vor einem Ransomware-Angriff zu schützen.	34,7 %	51,2 %	13,6 %	0,5 %
Die derzeitigen Schutzmaßnahmen meines Unternehmens gegen Ransomware sind ausreichend.	30,0 %	63,4 %	6,6 %	0,0 %
Regierungen sollten handeln, um die Cybersecurity durch Gesetze und entsprechende Strafverfolgung zu erhöhen.	46,9 %	40,4 %	10,8 %	1,9 %
Die jüngsten Ransomware-Angriffe auf IT-Managementtools haben uns dazu veranlasst, unsere Cloud-Computing-Strategie/Cloud-Managementstrategie zu überdenken.	37,6 %	46,0 %	12,7 %	3,8 %
Die jüngsten Ransomware-Angriffe auf Workstations und Dateifreigaben haben uns dazu veranlasst, unsere Strategie für Backup und Wiederherstellung von Dateien zu überdenken.	32,4 %	49,3 %	16,4 %	1,9 %
Von Ransomware betroffene Unternehmen sollten Lösegeld an die Angreifer zahlen, um ihren Betrieb wiederaufzunehmen.	23 %	31,5 %	21,6 %	23,9 %
Eine einfache Antivirensoftware ist ausreichend für den Schutz vor Ransomware.	14,1 %	29,1 %	22,1 %	34,7 %
Das Zahlen des Lösegelds ermutigt die Ransomware-Angreifer nur, weiterzumachen.	56,3 %	34,7 %	6,6 %	2,3 %
Ransomware-Angreifer halten ihr Versprechen und geben verschlüsselte Dateien gegen Bezahlung frei.	16,9 %	28,6 %	27,7 %	26,8 %

Budget und Prioritäten

Analyse:

In der Regel entscheidet die IT-Abteilung über das Budget für die Informationssicherheit, aber die Abteilung für Informationssicherheit kann ihre eigenen Prioritäten setzen.

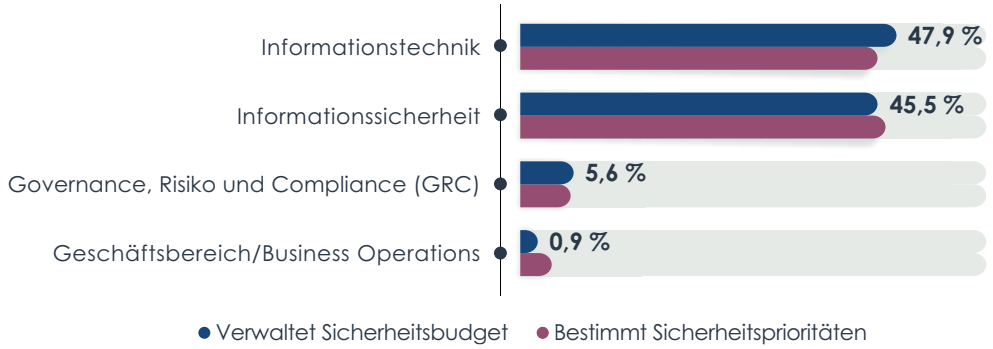
Für die meisten Unternehmen ist die Preisgabe von Kundendaten bei einem Ransomware-Angriff die wichtigste Bedrohung, die Preisgabe von internen Daten und Geschäftsgeheimnissen folgt direkt dahinter an zweiter Stelle.

Kommentar:

Es ist keine Überraschung, dass es für Unternehmen bei einem Ransomware-Angriffen oberste Priorität hat, die Preisgabe von Kundendaten zu verhindern. Die Preisgabe von Kundendaten kann für Unternehmen äußerst kostspielig sein und dazu führen, dass sie für jeden Kunden über Jahre Identitätsüberwachungsdienste anschaffen müssen und möglicherweise loyale Kunden verlieren, was Umsatzeinbußen mit sich bringt.

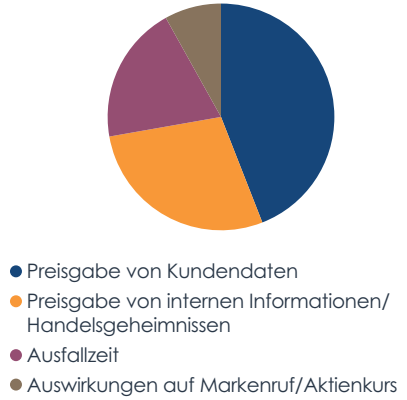
Diese Prioritäten bestimmen zweifelsohne die Sicherheitsausgaben und den Fokus von Unternehmen. Doch auch wenn das Sicherheitsteam diese Prioritäten festgelegt, ist die entsprechende kompensierende Kontrolle immer nur so effektiv, wie es das Sicherheitsbudget erlaubt.

Verantwortung für das Sicherheitsbudget vs. Sicherheitsprioritäten



Bewerten Sie die folgenden Aussagen zu Ransomware:

	1.	2.	3.	4.
Preisgabe von Kundendaten	44,1 %	31,9 %	14,6 %	9,4 %
Preisgabe von internen Informationen/ Handelsgeheimnissen	28,2 %	34,7 %	21,1 %	16,0 %
Ausfallzeit	19,7 %	16,9 %	31,5 %	31,9 %
Auswirkungen auf Markenruf/Aktienkurs	8,1 %	16,7 %	33,3 %	41,9 %



Auswirkungen und Wiederherstellung

Analyse:

Während die Wahrscheinlichkeit eines Ransomware-Angriffs bei allen Unternehmen durchschnittlich 46,9 % beträgt, ist die Wahrscheinlichkeit eines Ransomware-Angriffs bei Unternehmen, deren Abteilung für Informationssicherheit für das Sicherheitsbudget verantwortlich ist, geringer: nur 41,2 % sind von einem Angriff betroffen.

Kommentar:

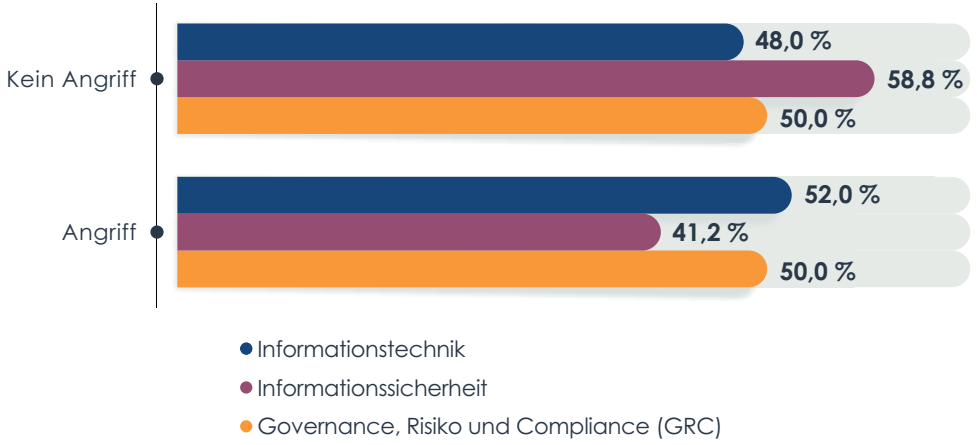
Die geringere Wahrscheinlichkeit eines Ransomware-Angriffs in Unternehmen, bei denen die Abteilung für Informationssicherheit ihr eigenes Budget hat, zeigt: Es ist wichtig, Abteilungen für Informationssicherheit einzurichten und ihnen entsprechende Mittel zuzuweisen. Unterfinanzierte Abteilungen stehen vor zusätzlichen Herausforderungen, wenn es darum geht, Ransomware-Angriffe zu verhindern.

Erwähnenswert ist, dass zwischen Unternehmen, in denen die Abteilung für Informationstechnik das Sicherheitsbudget verwaltet, und Unternehmen, in denen die Abteilung für Governance-, Risiko- und Compliance-Management dafür verantwortlich ist, kein erkennbarer Unterschied bestand. Die Wahrscheinlichkeit eines Ransomware-Angriffs lag jeweils bei etwa 50 %.

Eine weitere Queranalyse im Hinblick auf die Verringerung der Wahrscheinlichkeit, Opfer eines Ransomware-Angriffs zu werden, ergab keine weiteren nennenswerten Ergebnisse. Es gibt jedoch viele wirksame Strategien, um die Ausfallzeit nach einem erfolgreichen Angriff zu verkürzen oder die Zahlung des Lösegelds zu verhindern. Diese Strategien werden im Folgenden untersucht.

Gab es in Ihrem Unternehmen schon einmal einen Ransomware-Angriff?

Wie wirkt sich die Verantwortung für das Sicherheitsbudget auf die Wahrscheinlichkeit aus, einen Ransomware-Angriff zu erleben?



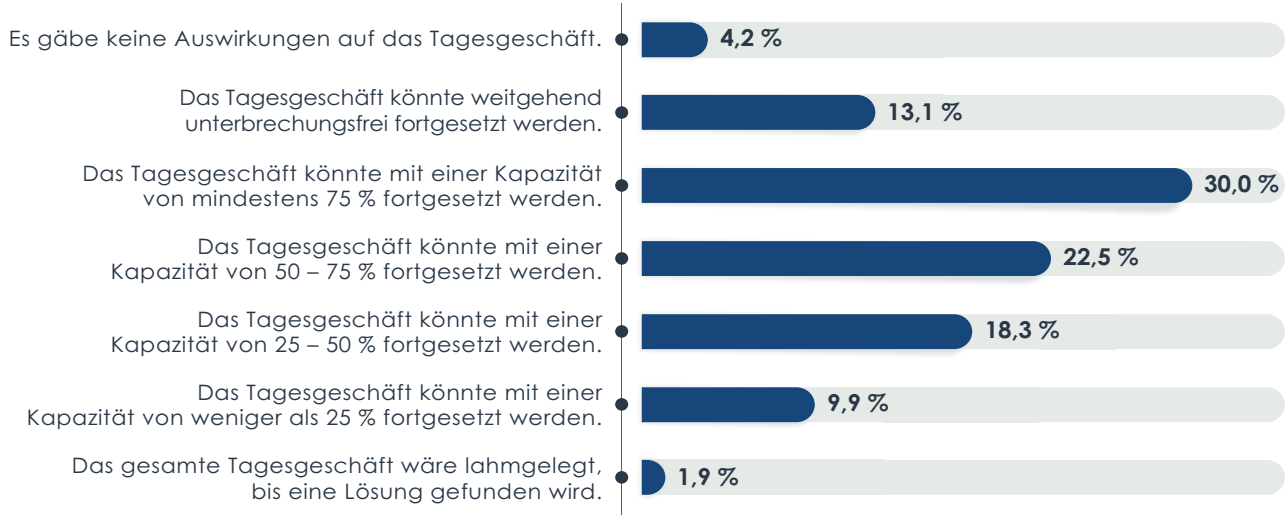
Analyse:

Die meisten Unternehmen rechnen bei einem umfassenden Ransomware-Angriff auf ihr Unternehmen mit Umsatz- und Produktivitätseinbußen von mindestens 25 %. Mindestens einer von zehn Befragten gab an, dass ein umfassender Ransomware-Angriff verheerende Folgen hätte und das Unternehmen mit Umsatz- und Produktivitätseinbußen von mindestens 75 % oder sogar dem völligen Stillstand rechnen müsste.

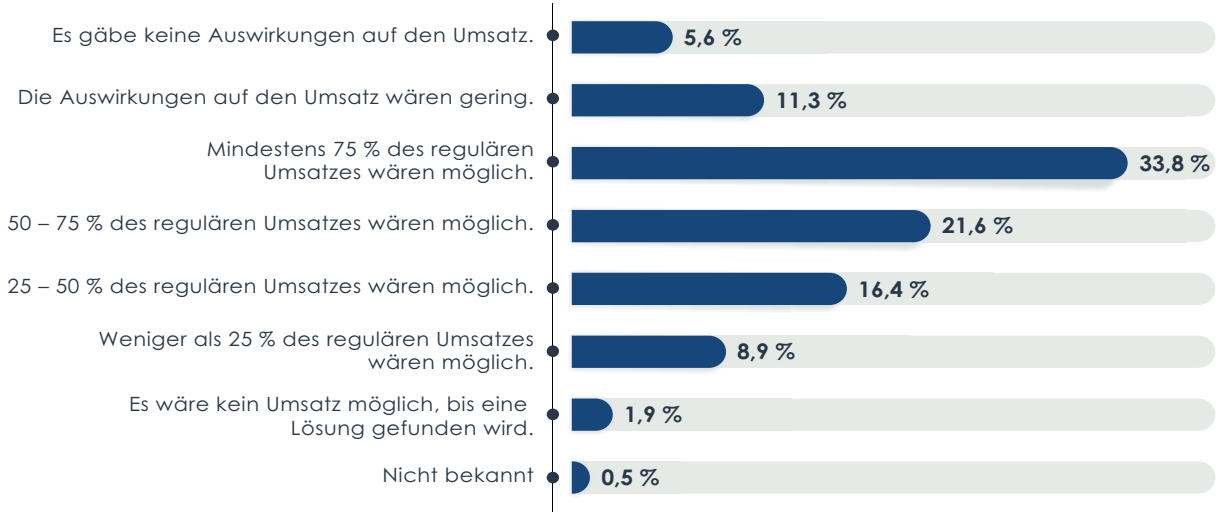
Kommentar:

Es ist erschreckend, dass ein Ransomware-Angriff eines von zehn der Hunderttausenden mittleren und großen Unternehmen in Nordamerika schwer treffen könnte. Das ist jedoch nicht verwunderlich, da die Zahl der Software- und Technologieunternehmen in Nordamerika rasant ansteigt und diese in hohem Maße auf ihre Computersysteme angewiesen sind, um Einnahmen zu erzielen.

Geschätzte Auswirkungen eines erfolgreichen Angriffs auf die Produktivität



Geschätzte finanzielle Auswirkungen eines erfolgreichen Angriffs



Analyse:

Phishing-E-Mails mit bösartigen Anhängen oder bösartigen Links waren der häufigste Einstiegspunkt, wobei 69 % der Angriffe über Phishing-E-Mails erfolgten.

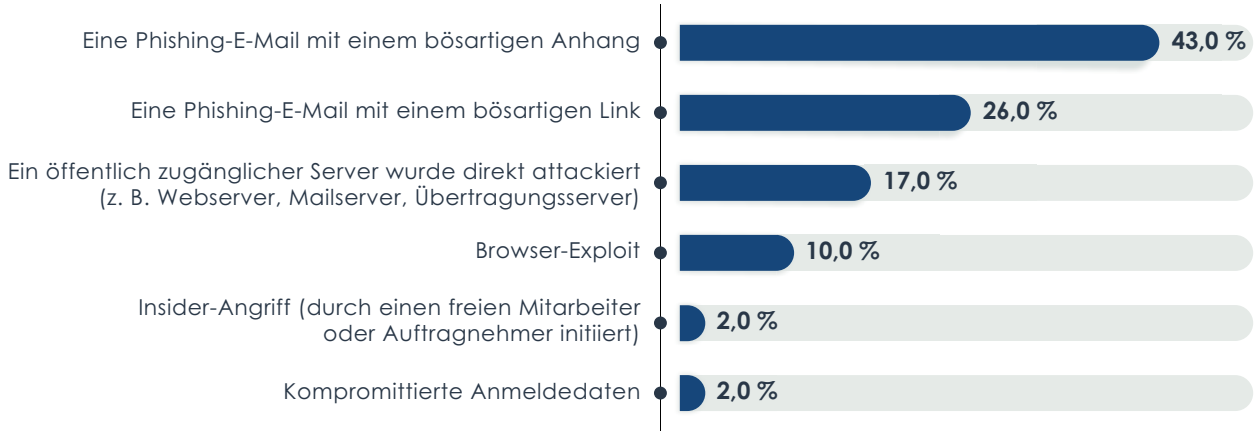
Es ist wichtig anzumerken, dass die meisten Unternehmen die Angriffe zwar innerhalb von weniger als einem Tag erkannten, es sich dabei aber um die Entdeckung des eigentlichen Angriffs und nicht der ersten Infektion handelt.

Kommentar:

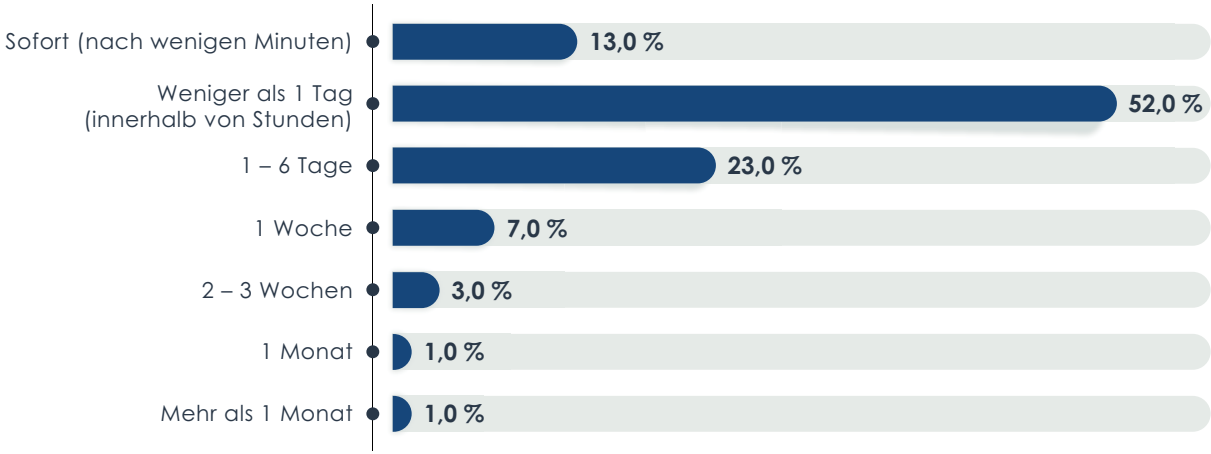
Dass Phishing die häufigste Angriffsmethode ist, überrascht nicht, da es sich um einen Angriffsvektor mit kleinem Aufwand und großer Wirkung handelt. Für Hacker ist es relativ einfach, einen Phishing-Angriff vorzubereiten, und oft sind sogar nicht zielgerichtete Phishing-Angriffe erfolgreich.

Viele Ransomware-Infektionen sind so konzipiert, dass sie interne Netzwerke durchlaufen, sobald ein Computer infiziert ist, und dann den Angriff auf allen Geräten gleichzeitig starten, um eine maximale Wirkung zu erzielen. Ein Netzwerk kann Tage, Wochen oder sogar Monate infiziert sein, bevor der Angriff tatsächlich ausgeführt wird.

Was war der Einstiegspunkt?



Wie lange hat es gedauert, bis Ihr Unternehmen den Angriff erkannt hat?



Analyse:

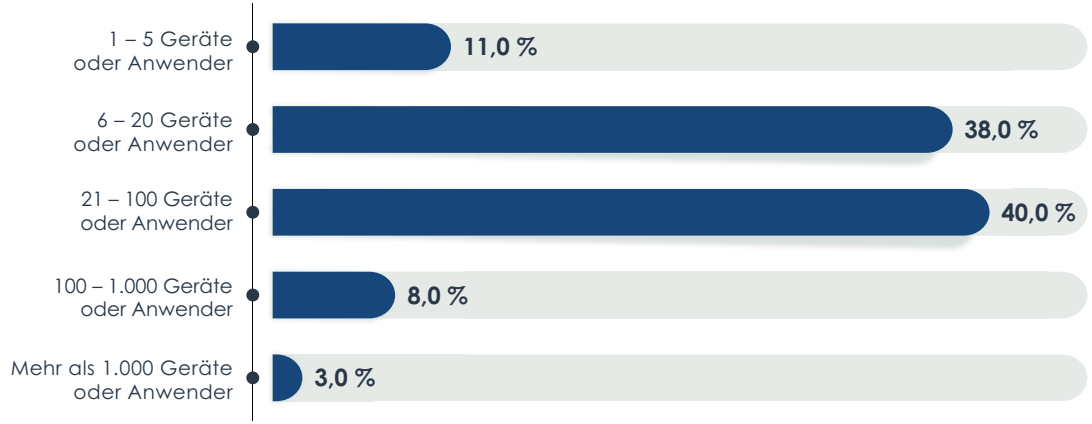
In den meisten Fällen waren weniger als 100 Geräte oder Anwender betroffen. Bei einem von zehn Angriffen waren es jedoch Hunderte oder sogar Tausende von Geräten oder Anwendern.

Die meisten Unternehmen waren nicht in der Lage, ihre Systeme noch am selben Tag des Ransomware-Angriffs wiederherzustellen.

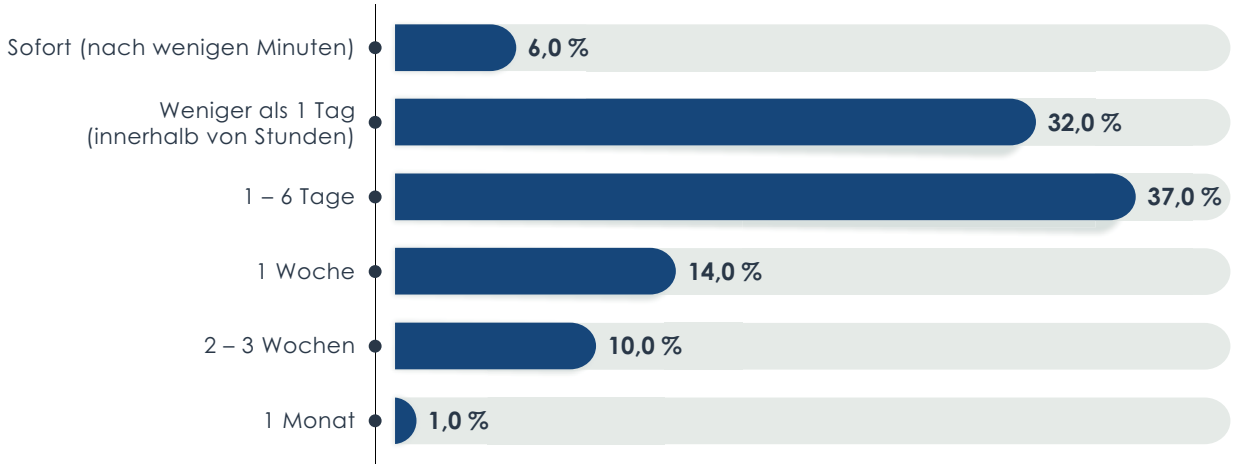
Kommentar:

Die Tatsache, dass bei den meisten Angriffen mehrere Geräte oder Anwender betroffen waren, bestätigt, dass Ransomware sich meist über interne Netzwerke verbreitet, um eine größere Wirkung zu erzielen. Die EMA hofft, dass Netzwerksegmentierung und Zero-Trust-Networking, die sich in der Branche immer mehr durchsetzen, einen besseren Schutz vor Ransomware bieten, indem diese schon am Punkt der Erstinfektion isoliert wird und so das Netzwerk nicht mehr durchqueren kann.

Wie viele Geräte oder Anwender waren von dem Angriff betroffen?



Wie lange hat es gedauert, bis alle Daten wiederhergestellt waren und der Betrieb vollständig wiederaufgenommen werden konnte?



Analyse:

Trotz der Empfehlungen der Branche, das Lösegeld nicht zu zahlen, haben 32 % der Unternehmen gezahlt.

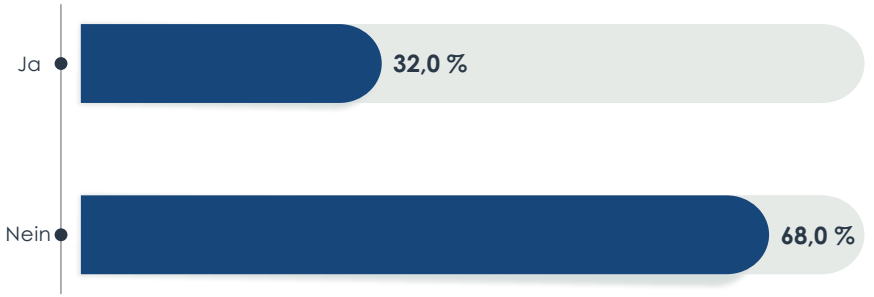
53 % der Unternehmen, die das Lösegeld nicht gezahlt haben, hatten eine Ausfallzeit von mindestens einem Tag. Von den Unternehmen, die das Lösegeld gezahlt haben, hatten hingegen 83,1 % eine Ausfallzeit von mindestens einem Tag zu verzeichnen.

Kommentar:

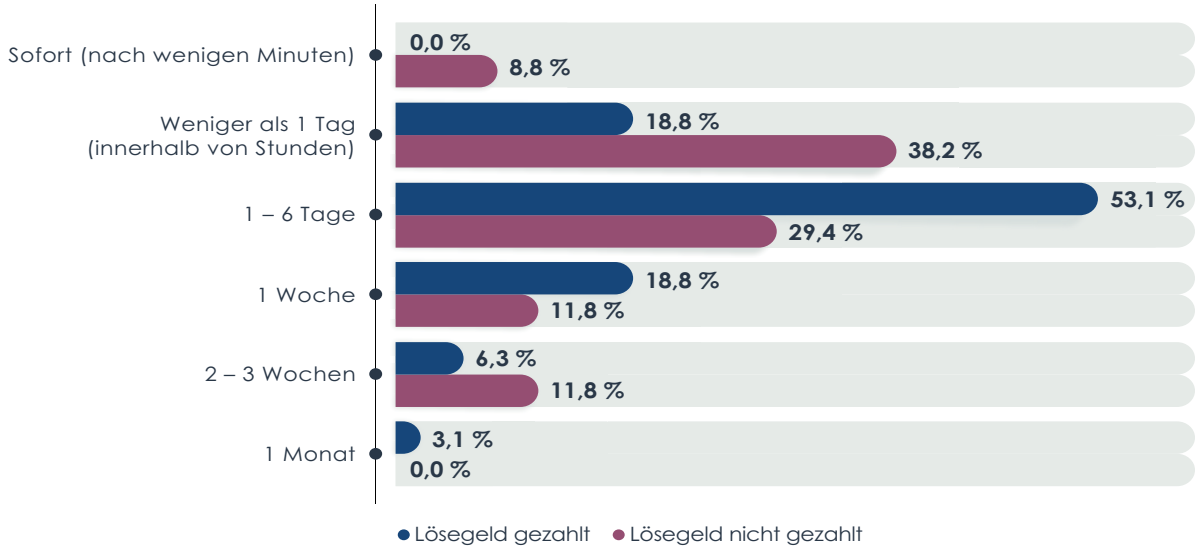
Während die Lösegeldzahlung in der Regel als kostensparende Methode zur Verringerung der Ausfallzeit gedacht ist, zeigt sich ein interessanter Trend, wenn man die tatsächliche Ausfallzeit der Unternehmen vergleicht: Bei den Unternehmen, die das Lösegeld zahlten, war die Ausfallzeit trotzdem tendenziell länger.

Dies ist jedoch im jeweiligen Zusammenhang zu sehen. Es kann sein, dass diese Unternehmen so entschieden haben, um weitaus längere Wiederherstellungszeiten zu vermeiden. Die eigentliche Ursache könnte eine unzureichende Planung für den Fall eines Ransomware-Angriffs sein, z. B. zeitnahe Backups, oder das Ausmaß des Angriffs und die Anzahl der betroffenen Geräte.

Hat Ihr Unternehmen das Lösegeld gezahlt?



Wie steht die Zahlung des Lösegelds damit in Zusammenhang, wie lange ein Unternehmen braucht, um alle Daten wiederherzustellen und den Betrieb wieder aufzunehmen?



Analyse:

Die häufigsten Gründe für die Zahlung eines Lösegelds waren Remediation-Kosten und eine drohende lange Ausfallzeit. Bemerkenswert ist, dass 21,9 % der Unternehmen, die das Lösegeld zahlten, dies aufgrund fehlender Backups taten. Und das hätte sehr wahrscheinlich verhindert werden können.

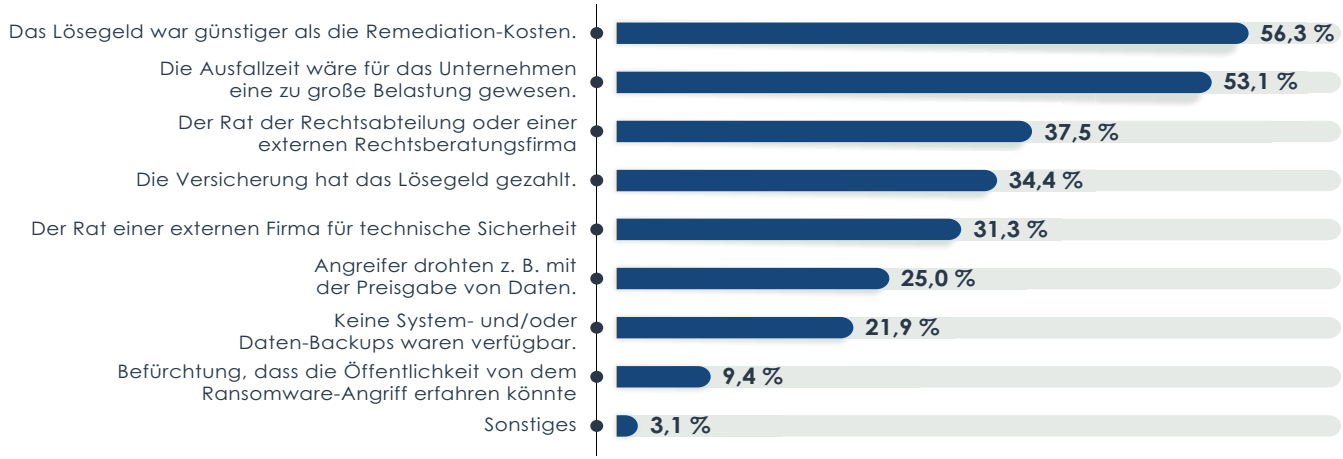
Die Hälfte der von Ransomware betroffenen Unternehmen wählten als Grund für die Nichtzahlung, dass ihrer Meinung nach Lösegelder grundsätzlich nicht gezahlt werden sollten. Der zweithäufigste Grund für die Nichtzahlung war das mangelnde Vertrauen, dass die Angreifer ihren Teil der Abmachung einhalten würden.

Kommentar:

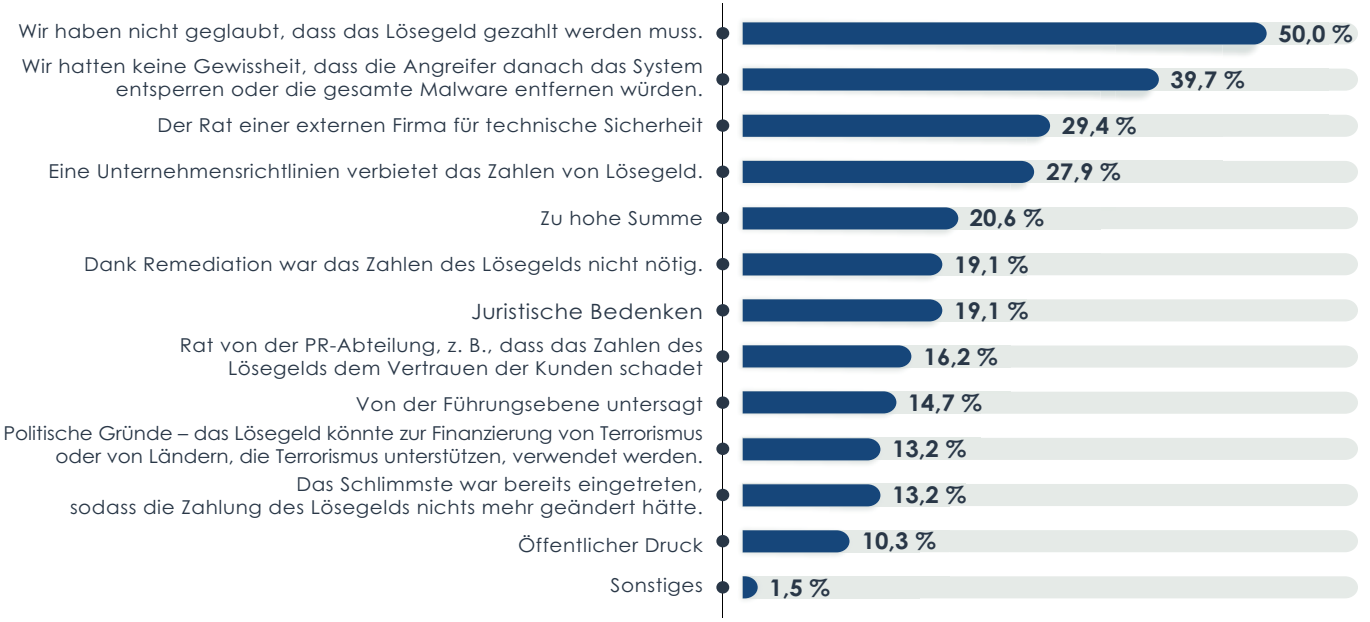
Interessant ist, dass Unternehmen, die das Lösegeld gezahlt haben, häufig eine längere Ausfallzeit hatten als die Nichtzahler, wie in den vorherigen Diagrammen dargestellt.

Viele Nichtzahler gaben als Grund ihre Zweifel an, dass die Angreifer sich an die Abmachung halten würden. Die statistischen Ergebnisse zeigen jedoch, dass diese Angst unbegründet ist. Mehr dazu auf der nächsten Seite.

Was hat Sie dazu bewegt, das Lösegeld zu zahlen?



Was hat Sie dazu bewegt, das Lösegeld nicht zu zahlen?



Analyse:

Es gibt einen klaren Trend: Je mehr Anwender oder Geräte von einem Ransomware-Angriff betroffen sind, desto wahrscheinlicher ist es, dass das Lösegeld gezahlt wird.

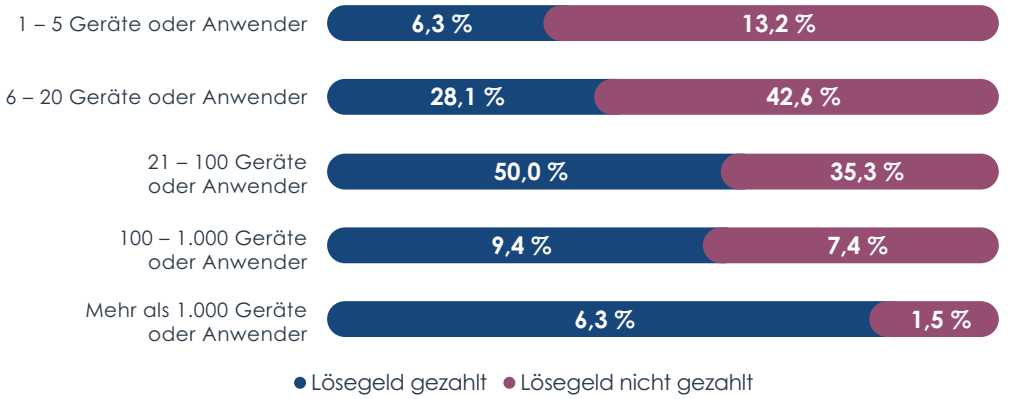
75 % der Unternehmen, die gezahlt haben, erhielten im Gegenzug genau das, was sie erwartet hatten, nämlich die Lösung der Probleme, die sie sich davon versprochen hatten. Nur 3,1 % der Unternehmen gaben an, dass ihnen nach Zahlung des Lösegelds höhere Kosten entstanden sind, als wenn sie nicht gezahlt hätten.

Kommentar:

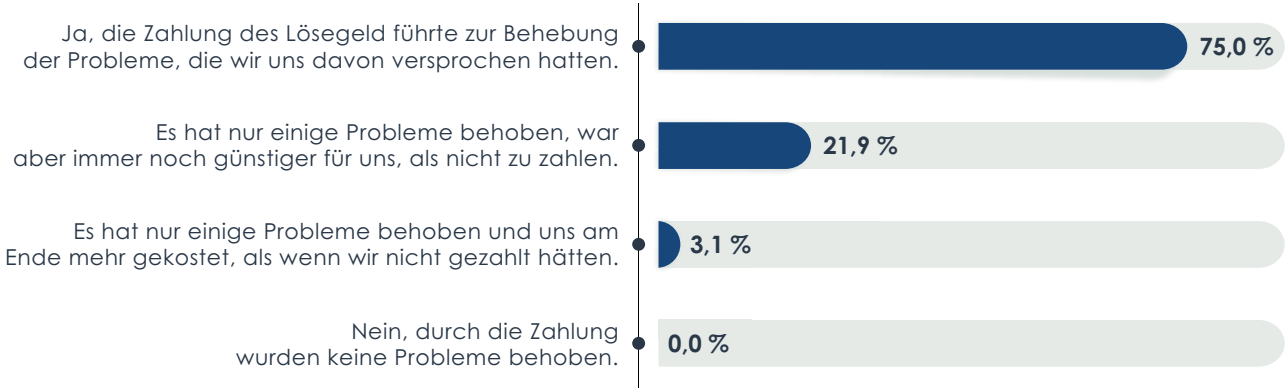
Je mehr Anwender oder Geräte von einem Ransomware-Angriff betroffen sind, desto größer die Auswirkungen und desto länger die Wiederherstellungszeit. Damit erhöht sich auch die Wahrscheinlichkeit, dass ein Unternehmen das Lösegeld zahlt.

Interessant ist, dass die Zahlung des Lösegelds statistisch gesehen eine wirksame Maßnahme ist, um Kosten zu sparen, dass aber trotzdem zahlreiche Unternehmen aufgrund des mangelnden Vertrauens in Angreifer nicht zahlen. Für die Angreifer ist es schließlich von Vorteil, wenn sie sich an ihr Versprechen halten und Systeme und Dateien nach der Zahlung freigeben. Andernfalls werden sie als nicht vertrauenswürdig eingestuft und noch weniger Unternehmen zahlen das geforderte Geld. Die Angreifer haben also nichts davon, wenn sie ihren Teil der Abmachung nicht einhalten.

Wie wirkt sich die Anzahl an betroffenen Geräten oder Anwendern auf die Wahrscheinlichkeit aus, dass das Lösegeld gezahlt wird?



Hatte die Zahlung des Lösegelds die erwartete Wirkung?



Reaktion auf Ransomware

Analyse:

Die bloße Bedrohung durch Ransomware ist für die meisten Unternehmen – selbst für die nicht von einem Angriff betroffenen – ausreichend, um die Beziehungen zu ihren Serviceanbietern neu zu bewerten und dem Kauf neuer oder anderer Sicherheitslösungen Priorität einzuräumen.

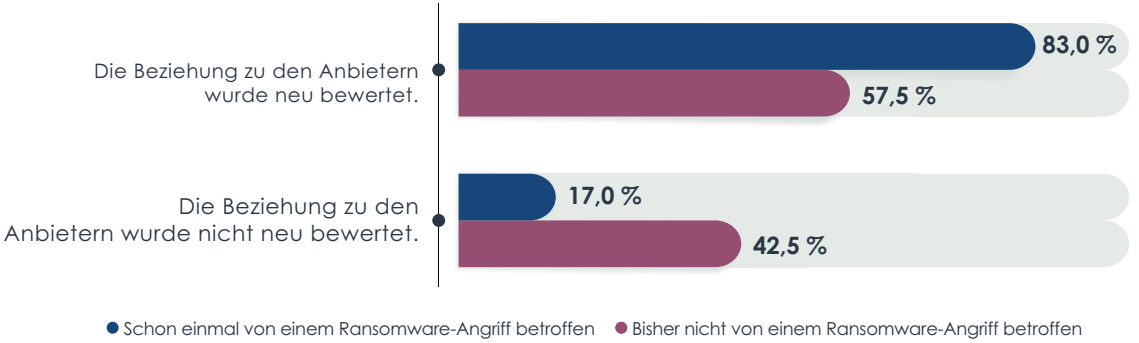
Für die tatsächlich von einem Ransomware-Angriff betroffenen Unternehmen ist die Motivation, die Beziehungen zu Lösungsanbietern neu zu bewerten und neue oder andere Sicherheitslösungen zu kaufen, sogar noch größer.

Kommentar:

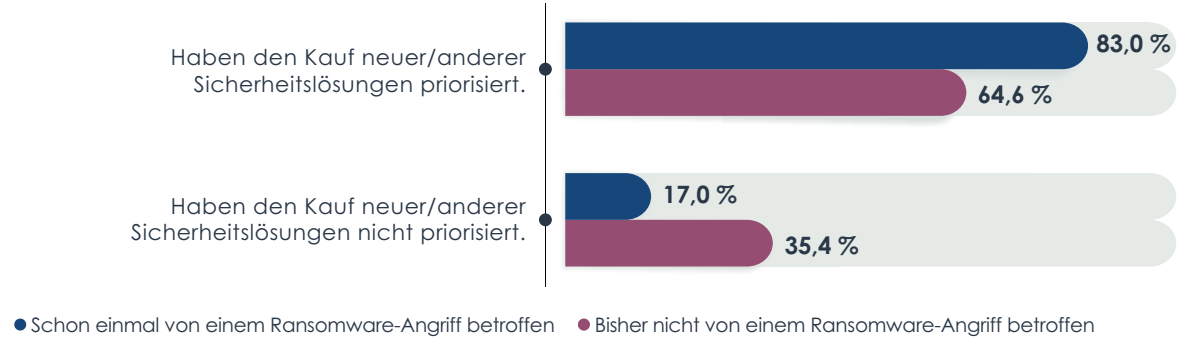
83 % der Unternehmen, die Ransomware-Angriffe zu verzeichnen hatten, bewerten die Beziehungen zu Serviceanbietern neu und priorisieren den Kauf neuer oder anderer Sicherheitslösungen. Das bedeutet, dass die Bedrohung durch Ransomware bei Kaufentscheidungen von Unternehmens durchaus eine wichtige treibende Kraft sein kann.

Serviceanbieter und Anbieter von Sicherheitslösungen müssen wissen, dass Kunden Alternativen in Betracht ziehen, wenn sie glauben, dass das Produkt oder der Service des entsprechenden Anbieters für einen Ransomware-Angriff auf ihr Unternehmen verantwortlich ist.

Wie wirkt sich die Tatsache, Opfer eines Ransomware-Angriffs geworden zu sein, auf die Beziehungen eines Unternehmens zu seinen Serviceanbietern aus?



Wie wirkt sich die Tatsache, Opfer eines Ransomware-Angriffs geworden zu sein, auf den Kauf von Sicherheitslösungen aus?



Analyse:

Anti-Malware und Software zur Abwehr von Eindringversuchen sind mit 91,5 % die in Unternehmen am häufigsten eingesetzten Strategien zum Schutz vor Ransomware, gefolgt von Anti-Phishing-Technologien und -Schulungen (71,8 %).

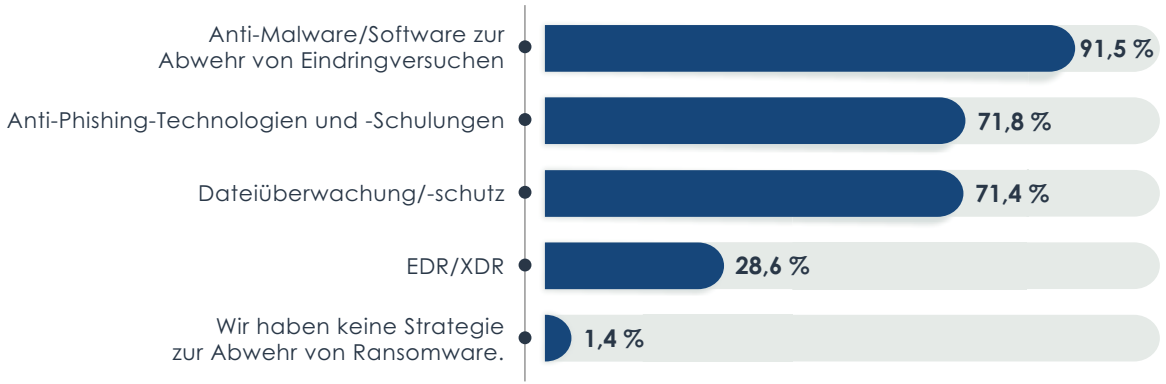
Die häufigsten Wiederherstellungsstrategien sind vollständige System-Backups (76,5 %) und Daten-Backups (69 %). 53 % der Unternehmen haben auch in eine Cyberversicherung investiert.

Kommentar:

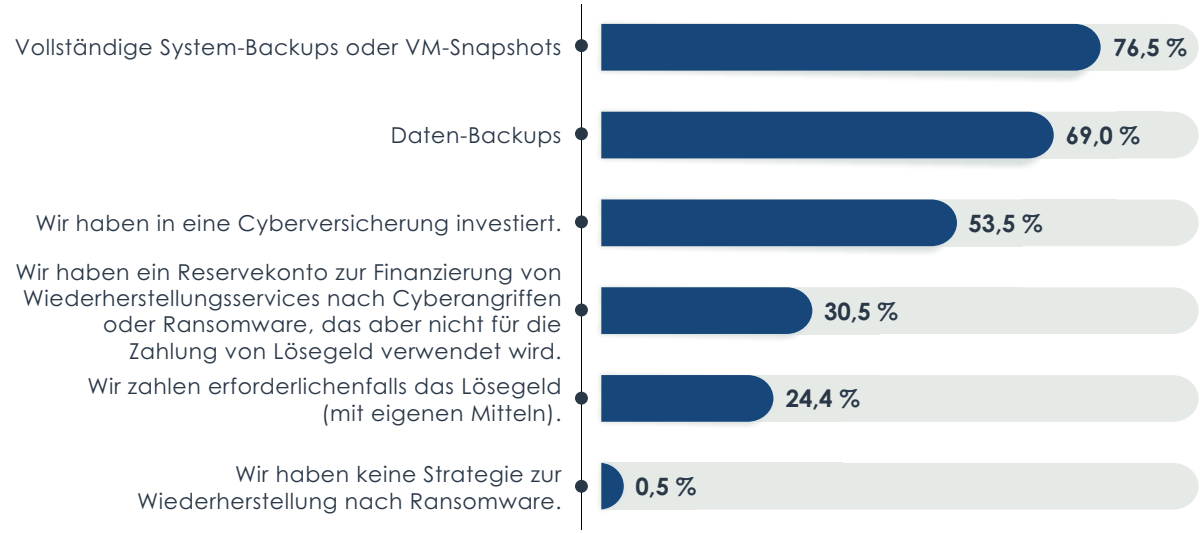
Da es sich bei EDR/XDR um eine neuere Technologie handelt, ist die Akzeptanzrate mit nur 28,6 % noch gering. Wie jedoch später in diesem Bericht erörtert wird, bietet EDR/XDR laut statistischer Ergebnisse Vorteile durch eine schnellere Entdeckung/Wiederherstellung.

Mehr als die Hälfte der Unternehmen hat in eine Cyberversicherung investiert, eine Möglichkeit, die noch vor zehn Jahren kaum jemand kannte. Wachsende Cyberbedrohungen, insbesondere Ransomware, haben den Bedarf an Cyberversicherungen und Strategien für die Reaktion auf Cybervorfälle drastisch erhöht.

Welche Strategie hat Ihr Unternehmen momentan zur Abwehr von Ransomware?



Welche Strategie hat Ihr Unternehmen momentan zur Wiederherstellung nach Ransomware?



Analyse:

Insgesamt wurden die Prämien bei den meisten Unternehmen mit Cyberversicherung im letzten Jahr zumindest leicht erhöht. Das ist zweifellos auf die zunehmende Verbreitung von Ransomware als Cyberbedrohung zurückzuführen.

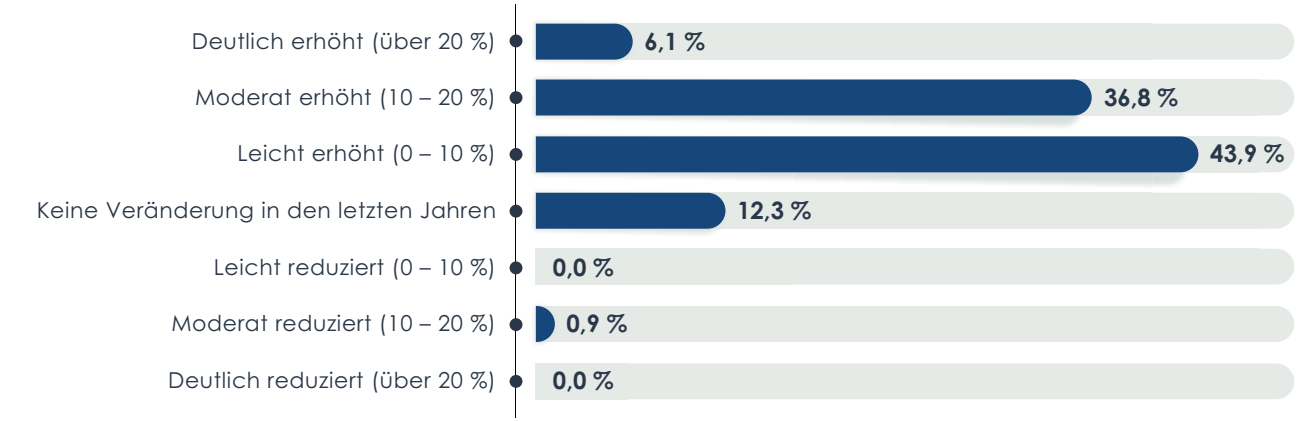
Das Lösegeld richtet sich in der Regel nach der Anzahl der Geräte oder der Menge der verschlüsselten Daten. Deshalb ist es nicht verwunderlich, dass über 62 % der Unternehmen Cyberversicherungspolicen in Höhe von mindestens einer halben Million US-Dollar abgeschlossen haben.

Kommentar:

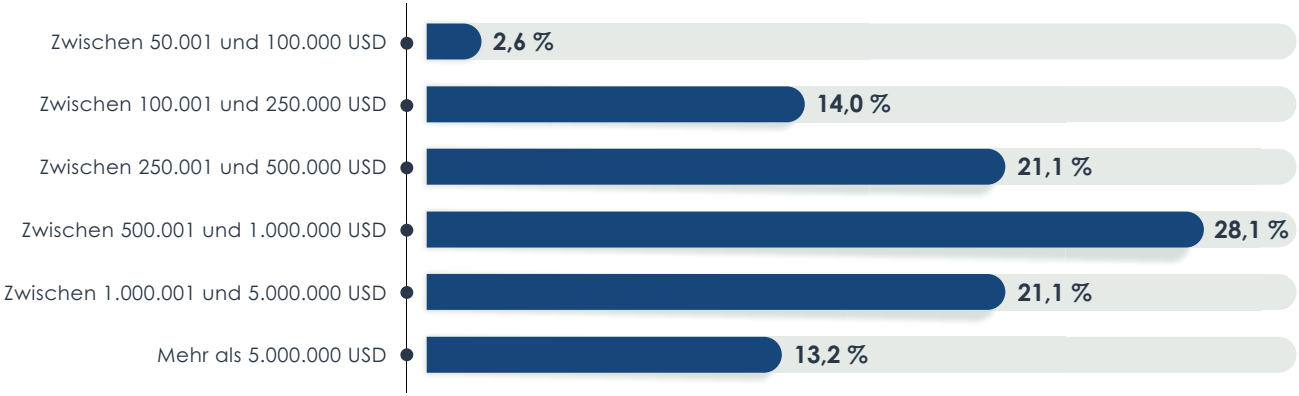
Da die Bedrohung durch Ransomware weiter zunimmt, werden Versicherungsunternehmen zweifellos weiterhin ihre Tarife erhöhen, wenn Kunden keine zusätzlichen Härtungsmaßnahmen nachweisen können.

Die meisten gefährlichen Angreifer verlangen inzwischen Zahlungen in Kryptowährungen, da diese schwer zurückzuverfolgen sind, und konzentrieren sich auf Unternehmen außerhalb ihres Heimatlandes. Mit dieser Angriffsmethode ist das Risiko geringer und sie erbeuten oft Summen in Millionenhöhe.

Wurden die Cyberversicherungsprämien Ihres Unternehmens im letzten Jahr erhöht/reduziert?



Bis zu welcher Summe ist Ihr Unternehmen cyberversichert?



Analyse:

Unternehmen, die EDR/XDR verwenden, erkannten und erholten sich von Ransomware-Angriffen etwas schneller als Unternehmen mit anderen Strategien. Insgesamt waren die Erkennungs- und Wiederherstellungszeiten bei den anderen Unternehmen weitgehend gleich, mit Ausnahme der Unternehmen ganz ohne Abwehrstrategie.

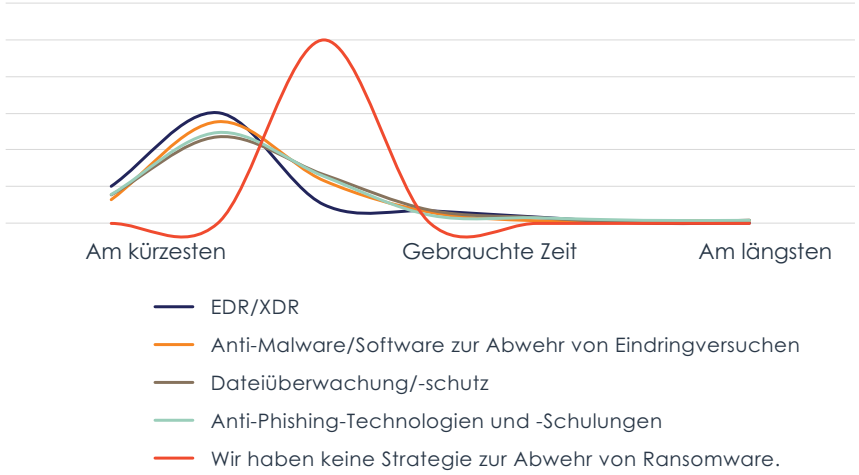
Kommentar:

Während die Ransomware-Abwehrstrategie keinen erkennbaren Einfluss auf die Verhinderung von Ransomware-Angriffen hat, scheint sie doch eine Rolle bei der Erkennungs- und Wiederherstellungszeit zu spielen.

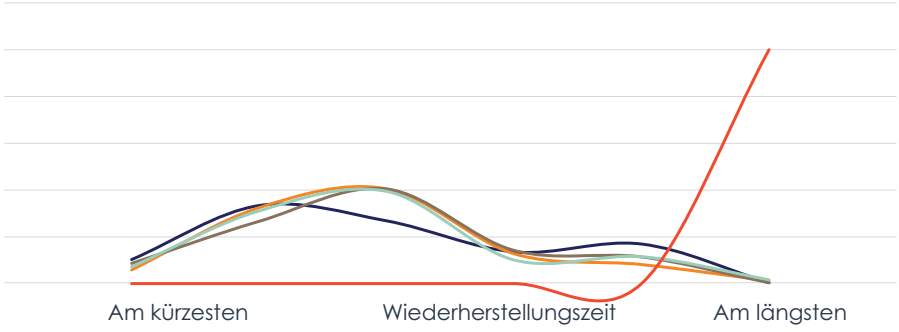
EDR/XDR bietet aufgrund der kürzeren Erkennungs- und Wiederherstellungszeit eindeutig einen Wettbewerbsvorteil gegenüber anderen Verteidigungsstrategien, da Unternehmen damit Angriffe etwas schneller erkennen und Systeme schneller wiederherstellen können als mit anderen Strategien.

Unternehmen, die keine Strategie zur Abwehr von Ransomware hatten, mussten deutlich längere Wiederherstellungszeiten in Kauf nehmen als alle anderen.

Wie wirkt sich die Abwehrstrategie darauf aus, wie lange ein Unternehmen braucht, um einen Ransomware-Angriff zu erkennen?



Wie wirkt sich die Abwehrstrategie darauf aus, wie lange ein Unternehmen für die Wiederherstellung nach Ransomware braucht?



Analyse:

Unternehmen mit Daten-Backups oder vollständigen System-Backups zahlten weniger häufig Lösegeld als der Durchschnitt, während Unternehmen, die Lösegeldzahlungen mit eigenen Mitteln als Strategie angaben, viel häufiger zahlten.

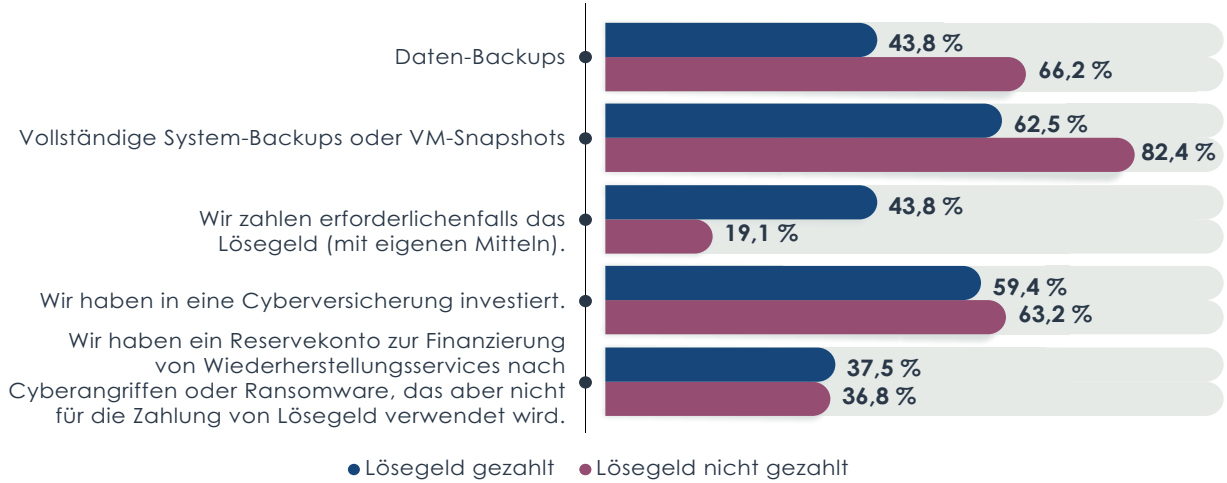
Statistisch gesehen machen Daten-Backups oder vollständigen System-Backups bei den Wiederherstellungszeiten einen erheblichen Unterschied aus und Wiederherstellungszeiten von weniger als einem Tag sind häufiger.

Kommentar:

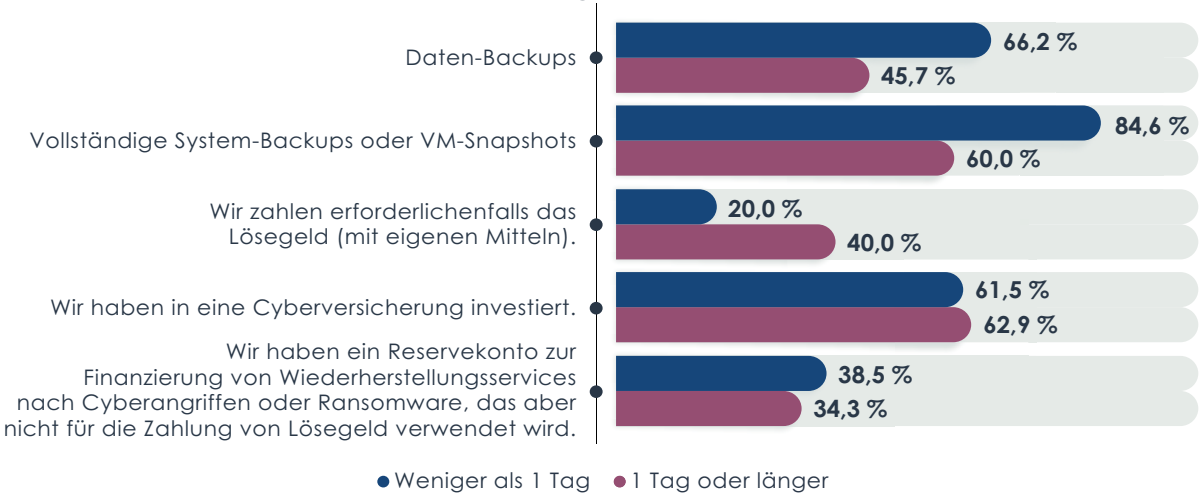
Ein interessanter Datenpunkt ist, dass Unternehmen mit Cyberversicherung weniger häufig Lösegeld zahlen als der Durchschnitt. Das kann darauf zurückzuführen sein, dass sie höhere Versicherungsprämien vermeiden wollen oder dass für die Cyberversicherungspolicen zusätzliche Härtungsmaßnahmen erforderlich sind.

Durch Cyberversicherungen und die Zahlung des Lösegelds mit eigenen Mitteln versuchen Unternehmen, Ausfallzeiten zu reduzieren. Häufig sind diese Strategien jedoch mit längeren Wiederherstellungszeiten von mindestens einem Tag verbunden.

Wie wirkt sich die Strategie zur Wiederherstellung nach Ransomware eines Unternehmens auf die Wahrscheinlichkeit aus, dass es das Lösegeld zahlt?



Wie wirkt sich die Strategie zur Wiederherstellung nach Ransomware darauf aus, wie lange ein Unternehmen braucht, um alle Daten wiederherzustellen und den Betrieb vollständig wiederaufzunehmen?



Analyse:

Es überrascht nicht, dass Backup und Wiederherstellung bei den Strategien zur Wiederherstellung nach Ransomware überwiegen. Remediation und Wiederherstellung von Endpunkten folgen dicht dahinter. Die am wenigsten beliebte Möglichkeit ist die Zahlung des Lösegelds.

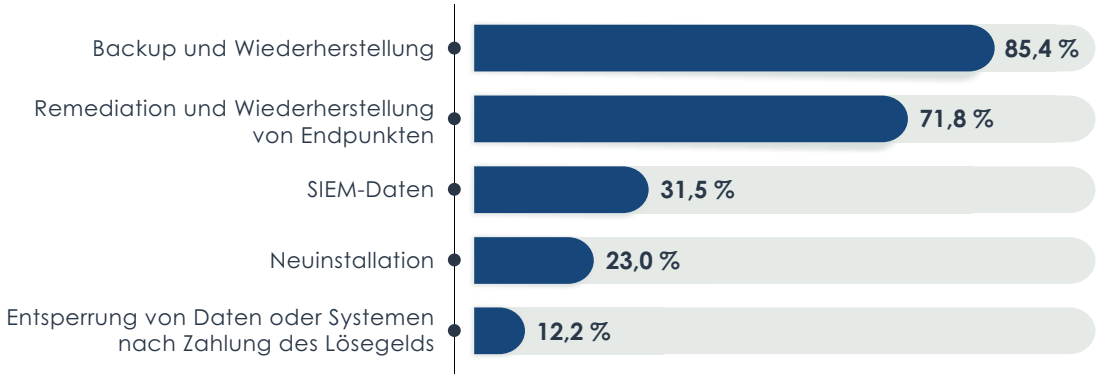
Die Entfernung des Angreifers aus der Umgebung erfolgt bei den meisten Unternehmen durch EDR-Bedrohungsbekämpfung, entweder durch ein internes Team oder durch Beauftragung eines externen Unternehmens. Nur 5,2 % der Unternehmen vertrauen darauf, dass sich die Angreifer nach Zahlung des Lösegelds selbst aus dem Netzwerk zurückziehen.

Kommentar:

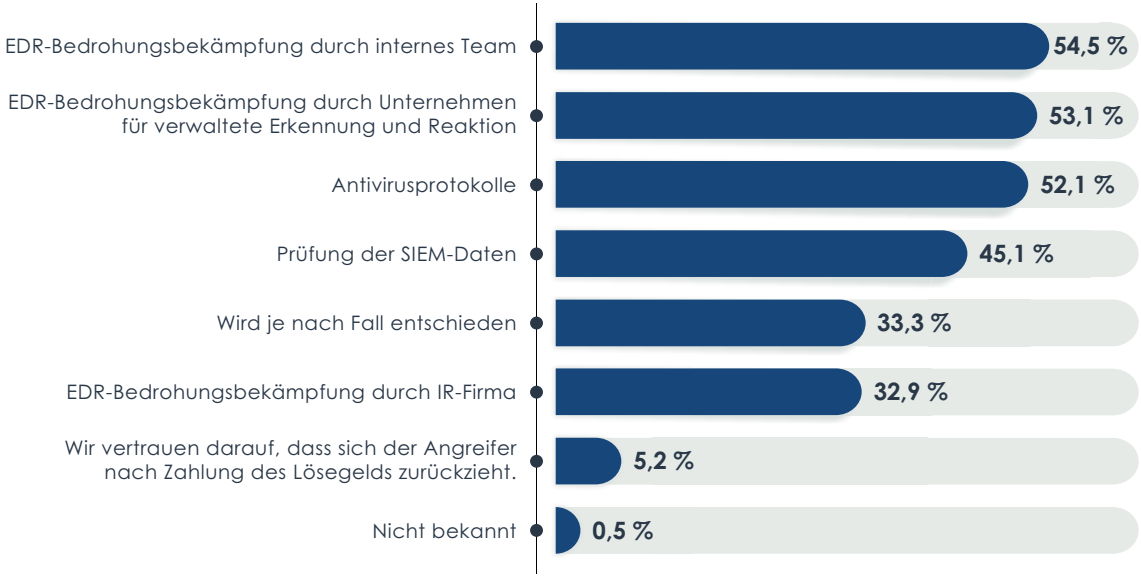
Zweifelsohne sind Backup und Wiederherstellung die besten Wiederherstellungsstrategien im Falle eines Ransomware-Angriffs. Dass die Geräte aber manchmal schon Monate vor dem Angriff infiziert werden, macht die Sache etwas komplizierter. Auch wenn die Remediation und Wiederherstellung von Endpunkten effektiv sein kann, ist eine Neuinstallation mit anschließender Wiederherstellung aller Daten möglicherweise die sicherste Option.

Obwohl EDR eine der am wenigsten verbreiteten Strategien zur Abwehr von Ransomware ist, ist die Lösung bei vielen Unternehmen Teil des Plans zur Reaktion auf Vorfälle. Unternehmen täten gut daran, ihre bestehenden EDR/XDR-Implementierungen zu nutzen, um sich nicht nur von Vorfällen zu erholen, sondern auch sicherzustellen, dass proaktive Maßnahmen ergriffen werden, um die Auswirkungen künftiger Ransomware-Angriffe durch rechtzeitige erste Reaktionen zu verringern.

Wie planen Sie basierend auf Ihrer aktuellen Cybersecurity-Strategie die Wiederherstellung nach einem Ransomware-Angriff?



Wie planen Sie basierend auf Ihrer aktuellen Cybersecurity-Strategie die Entfernung des Angreifers aus Ihrer Umgebung?



Analyse:

Die meisten Unternehmen glauben, dass die Erkennungszeit bei künftigen Ransomware-Angriffen weniger als einen Tag und die Wiederherstellungszeit ein bis sechs Tage betragen wird.

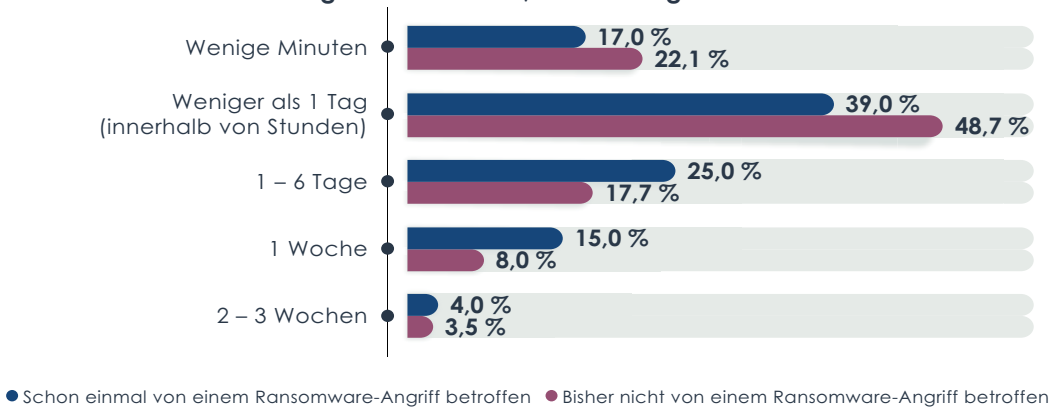
Bei einer genaueren Untersuchung dieser Daten im Hinblick auf Trends zeigt sich, dass Unternehmen, die einen Angriff erlebt haben, eine etwas längere Erkennungszeit und eine etwas kürzere Wiederherstellungszeit vermuten.

Kommentar:

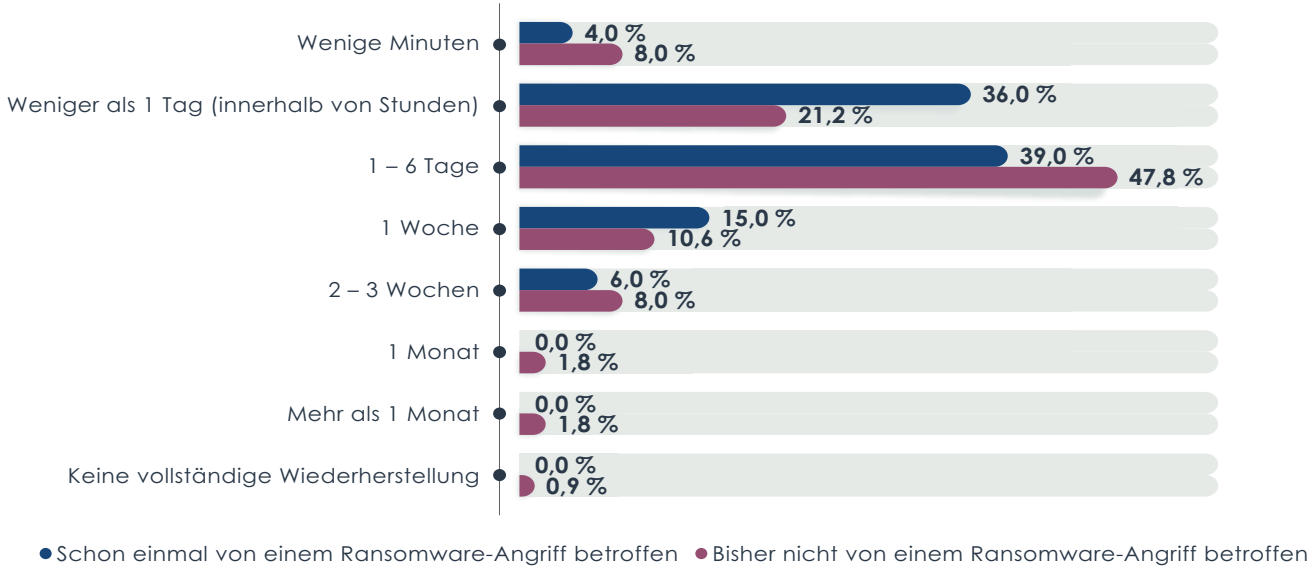
Vermutlich schätzen Unternehmen, die bereits einen Ransomware-Angriff erlebt haben, die Erkennungszeit realistischer ein, gehen aber von einer kürzeren Wiederherstellungszeit aus, da sie Backups als Folge des Angriffs priorisieren.

Die Tatsache, dass 4,5 % der Unternehmen, die bisher keinen Ransomware-Angriff erlebt haben, von Wiederherstellungszeiten von einem Monat oder mehr ausgehen oder davon, dass sie sich möglicherweise nie wieder vollständig erholen, zeigt deutlicher das Problem von Ransomware. Die meisten Unternehmen nehmen Ransomware zwar ernst, aber die wenigsten wissen, wie sie damit umgehen sollen.

Wenn alle Abteilungen Ihres Unternehmens jetzt von einem umfassenden Ransomware-Angriff betroffen wären, wie lange würden Sie Ihrer Meinung nach brauchen, um den Angriff zu erkennen?



Wenn alle Abteilungen Ihres Unternehmens jetzt von einem umfassenden Ransomware-Angriff betroffen wären, wie lange würden Sie Ihrer Meinung nach brauchen, um alle Daten wiederherzustellen und den Betrieb vollständig wiederaufzunehmen?



Perspektive (EMA)

Ransomware war einst ein sehr kleines Problem, das nur wenige Branchen betraf, hat sich aber zu einem lukrativen Geschäft für die organisierte Cyberkriminalität entwickelt und zählt heute in fast allen Branchen zu den häufigsten Cyberangriffen.

Angreifer setzen ihre Lösegelder absichtlich unter den geschätzten Kosten für Remediation und Wiederherstellung an und spekulieren darauf, dass sich die meisten Unternehmen die Ausfallzeit nicht leisten können. Da etwa ein Drittel aller Lösegelder gezahlt wird, manchmal in Millionenhöhe, lohnt sich das für die Angreifer allemal. Bei diesem lukrativen kriminellen Geschäft gibt es aufgrund des geringen Aufwands, der zur Infizierung von Unternehmen erforderlich ist, und des hohen Gewinns bei einem erfolgreichen Angriff kaum einen Grund, damit aufzuhören.

Für einen maximalen Gewinn versuchen Angreifer, so viele Geräte oder Dateien in einem Unternehmen wie möglich zu verschlüsseln, wahrscheinlich durch sich selbst verbreitende Malware, die das Netzwerk durchquert.

Eine der wichtigsten Erkenntnisse dieser Studie: Die Strategie zur Abwehr von Ransomware spielt keine große Rolle dabei, ob ein Unternehmen Opfer eines Ransomware-Angriffs wird. Umso wichtiger ist die Rolle der Abwehrstrategie bei der zeitnahen Erkennung und Reaktion. Da sich die Wahrscheinlichkeit, dass ein Unternehmen Lösegeld zahlen muss, mit der Anzahl der betroffenen Anwender oder Geräte erhöht, sind rechtzeitige Erkennung und Reaktion von entscheidender Bedeutung. Daten-Backups oder vollständige System-Backups sind ebenfalls wichtig, um schnell eine Lösung zu finden und die Zahlung von Lösegeld zu vermeiden.

Ein interessanter in dieser Studie aufgezeigter Trend ist auch, dass sehr viele Unternehmen nicht darauf vertrauen, dass Angreifer sich an die Abmachung halten, die statistischen Ergebnisse aber etwas ganz anderes ergeben. Das mangelnde Vertrauen in die Angreifer war ein häufiger Grund, aus dem Unternehmen das Lösegeld nicht gezahlt haben. Gleichzeitig gaben 96,9 % der zahlenden Unternehmen als Grund an, dass sie Kosten sparen wollten.

Obwohl die große Mehrheit der Unternehmen der Meinung ist, dass sich die Lösegeldzahlung gelohnt hat, hatten die Unternehmen, die gezahlt haben, laut Statistik die längeren Wiederherstellungszeiten. Diese längeren Wiederherstellungszeiten sind möglicherweise nicht direkt auf die Zahlung des Lösegelds zurückzuführen, sondern eher auf das Fehlen einer angemessenen Wiederherstellungsplanung, wie z. B. Daten- oder System-Backups.

Die beste Lösung für das Ransomware-Problem besteht anscheinend letztlich darin, die Backup-Strategien zu stärken und gleichzeitig die Erkennungs- und Reaktionszeiten zu verbessern. Aufgrund ihres Vorteils bei den Erkennungs-, Reaktions- und Wiederherstellungszeiten sollten Unternehmen verstärkt auf EDR- und XDR-Lösungen setzen, um Bedrohungen so früh wie möglich zu erkennen und die Verbreitung im Netzwerk zu vermeiden. Derzeit besteht einer der Hauptgründe für die Zahlung des Lösegelds darin, die Wiederherstellungskosten zu reduzieren. Erst wenn Unternehmen ihre Umgebung zu geringeren Kosten wiederherstellen können als durch die Zahlung des Lösegelds, werden Ransomware-Angriffe weniger attraktiv für kriminelle Akteure.

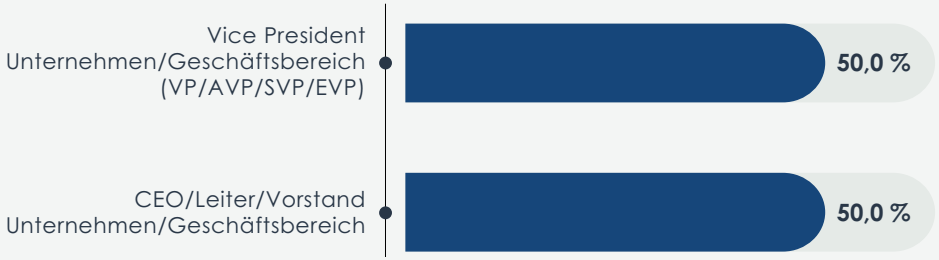
Es sieht nicht so aus, als würde Ransomware in absehbarer Zeit verschwinden. Nur durch richtige Planung und Investitionen können Unternehmen das Risiko verringern, die Reaktions- und Wiederherstellungszeiten verbessern und die Kosten für Lösegeldzahlungen vermeiden.

Forschungsmethodik und Demografie

Welche der folgenden Bezeichnungen beschreibt Ihre Rolle AM BESTEN? IT-Fachkräfte

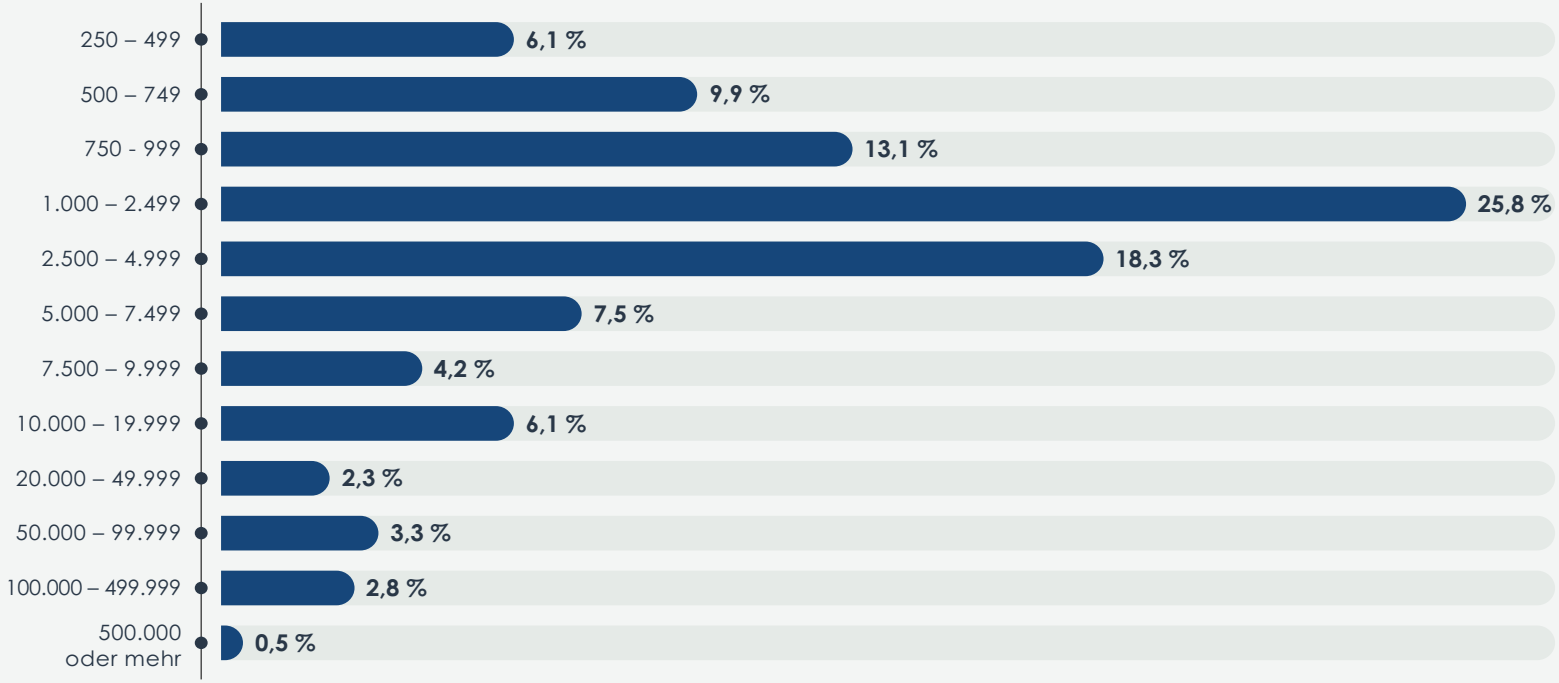
Erhebungsumfang = 199

Welche der folgenden Bezeichnungen beschreibt Ihre Rolle AM BESTEN? Führungskräfte



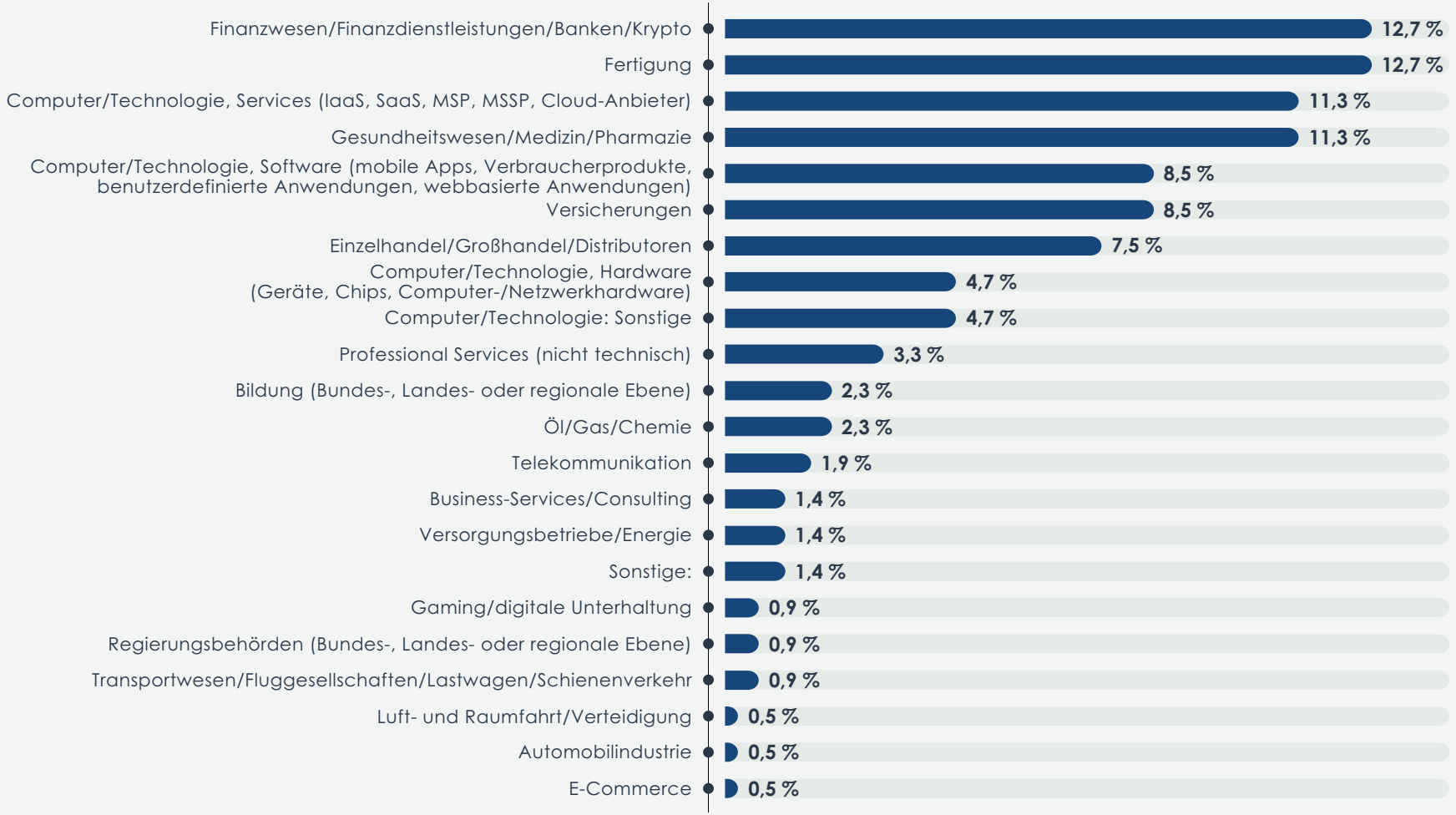
Erhebungsumfang = 14

Wie viele Mitarbeiter sind derzeit in Ihrem Unternehmen beschäftigt?



Erhebungsumfang = 213

Welche der folgenden Bezeichnungen beschreibt am besten die Branche, in der Ihr Unternehmen primär tätig ist?



Erhebungsumfang = 213

Über den Sponsor

VMware

VMware ist ein führender Anbieter von Multi-Cloud-Services für alle Anwendungen und unterstützt digitale Innovationen bei gleichzeitiger Kontrolle der Enterprise-Klasse. VMware-Software fungiert als zuverlässige Grundlage für schnellere Innovationen und bietet Unternehmen die notwendige Flexibilität und Wahlfreiheit, um ihre Zukunft zu gestalten. VMware hat seinen Hauptsitz in Palo Alto, Kalifornien, und setzt sich mit seiner Agenda 2030 für eine bessere Zukunft ein.

Weitere Informationen finden Sie auf der VMware-Seite mit Lösungen zum Schutz vor Ransomware:
https://www.vmware.com/de/solutions/ransomware-protection.html


MALWARE
MALWARE
MALWARE
MALWARE
MALWARE
MALWARE

Über Enterprise Management Associates, Inc.

Enterprise Management Associates (EMA) wurde 1996 gegründet und ist ein führendes Branchenanalyseunternehmen, das umfassende Einblicke in das gesamte Spektrum der IT- und Datenmanagementtechnologien liefert. EMA-Analysten nutzen eine einzigartige Kombination aus praktischer Erfahrung, Erkenntnissen zu branchenspezifischen Best Practices und fundiertem Fachwissen über aktuelle und geplante Anbieterlösungen, um EMA-Kunden beim Erreichen ihrer Ziele zu unterstützen. Weitere Informationen zu den Forschungs-, Analyse- und Consulting-Services von EMA für geschäftliche Anwender, IT-Experten und IT-Anbieter finden Sie auf **www.enterprisemanagement.com** Folgen Sie zudem EMA auf **Twitter** oder **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4189.060322