Ransomware: Die wahren Kosten

für Unternehmen im Jahr 2024

Unsere jährliche globale Studie über die Geschäftsauswirkungen von Ransomware

Ransomware-Angreifer entwickeln sich weiter. Zu zahlen ist nicht die Lösung.
Es ist an der Zeit, Lösegeldzahlungen abzulehnen.

cybereason©

Vorwort

Wenn ich mir für das Jahr 2024 etwas wünschen dürfte, dann wäre es, dass wir damit aufhören, den Begriff „Ransomware“ zu verwenden.

Dieser Begriff vermag die tatsächlichen Auswirkungen eines Angriffs nicht hinreichend zu beschreiben. Was als simple Idee begann – Daten zu verschlüsseln und Geld zu erpressen, um Zugang zu ihnen zu erhalten – entwickelte sich zu einem komplexen „Schweizer Taschenmesser“, wie es die kombinierten Angriffe in den frühen 2000er Jahren waren.

Jetzt ist ChatGPT auf der Bildfläche erschienen, und es treibt die nächste Evolution von Ransomware voran.

Im Rahmen unserer letztjährigen Umfrage haben wir festgestellt, dass Ransomware-Angreifer in nicht englischsprachigen Ländern (Deutschland, Frankreich, Italien und Japan) erfolgreicher sind. Dieser Trend wird durch generative KI-Tools beschleunigt, die es Angreifern ermöglichen, ihre Aktivitäten schneller und in größerem Umfang zu übersetzen und zu lokalisieren. Diese Tools ermöglichen es ihnen auch, öffentliche Informationen über Personen und Unternehmen auszuspionieren, die sie zur Entwicklung hochgradig personalisierter Social-Engineering-Angriffe nutzen. Generative KI verringert auch die für die Kodierung von Angriffen erforderlichen Fähigkeiten, wodurch die Einstiegshürde sinkt und die Automatisierung beim Entwickeln von Angriffen zunimmt, insbesondere mit Tools wie wormGPT.

Die diesjährige Studie zeigt, dass die meisten Unternehmen zwar über eine Ransomware-Strategie verfügen, diese aber oft Lücken aufweist. Es fehlt entweder an einem dokumentierten Plan oder an den richtigen Personen, die diesen ausführen. Infolgedessen zahlen viele Unternehmen das Lösegeld. Viele davon verfügen zwar über eine Cyberversicherung, wissen aber nicht, ob und in welchem Umfang diese Ransomware-Angriffe abdeckt.

Dies ist in mehrfacher Hinsicht problematisch, denn es gibt keine Garantie dafür, dass Sie Ihre Daten und Systeme unkompromittiert zurückerhalten, dass Angreifer Ihre Daten nicht auf dem Schwarzmarkt verkaufen oder dass Sie nicht erneut angegriffen werden. Und wenn es Beweise dafür gibt, dass Ihre Zahlung zur Terrorismusfinanzierung oder zur Finanzierung von organisierter Kriminalität eingesetzt wurde, müssen Sie sich möglicherweise sogar strafrechtlich dafür verantworten.

Welche Erkenntnis konnten wir also in diesem Jahr gewinnen? Die Bedrohung entwickelt sich ständig weiter, während die Widerstandsfähigkeit der Unternehmen gegenüber Ransomware-Angriffen damit nur schwer Schritt halten kann. Jetzt ist es an der Zeit, Ihre Widerstandsfähigkeit einem Stresstest zu unterziehen, den Rest des Unternehmens einzubeziehen und sicherzustellen, dass Sie ausreichend gegen die Angreifer von heute und morgen geschützt sind.

Greg Day
Global Field CISO, VP Cybereason

Zielsetzung: Von denjenigen lernen, die Opfer von Ransomware-Angriffen geworden sind

Dieser Bericht wurde in Auftrag gegeben, um Sicherheitsexperten dabei zu unterstützen, Erfahrungen auszutauschen und ihre Branchenkolleginnen und -kollegen darüber aufzuklären, wie wichtig es ist, dass Ransomware ganz oben auf der Tagesordnung steht.

Ransomware-Angriffe werden immer häufiger, ausgefeilter und effektiver. In diesem Jahr wollten wir herausfinden, wie sich diejenigen, die Opfer von Ransomware-Angriffen geworden sind, auf künftige Angriffe vorbereiten.

Und auch das Folgende wollten wir wissen:

- Wie sich Angreifer Zugang zu Netzwerken verschaffen
- Worauf sie es abgesehen haben
- Wie viele Unternehmen, die von einem Ransomware-Angriff betroffen waren, der Zahlung eines Lösegelds zugestimmt haben
- Ob es sich gelohnt hat, das Lösegeld zu zahlen

Wir haben

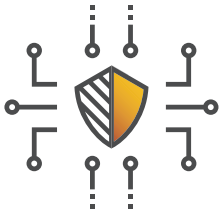
1.008

IT-Fachleute in verschiedenen Unternehmen befragt

waren für die Cybersicherheit verantwortlich

Alle wurden mindestens einmal **Opfer** eines Ransomware-Angriffs in den letzten

24



Monaten.

Die Ergebnisse überraschen uns noch immer.

Wie Sie sehen werden, sind Unternehmen, die in der Vergangenheit bereits Opfer eines Ransomware-Angriffs wurden, nach wie vor gefährdet, und viele von ihnen glauben nicht, dass sie auf einen weiteren Ransomware-Angriff vollständig vorbereitet sind.

Die Ergebnisse im Überblick

Die diesjährigen Ergebnisse zeichnen ein interessantes Bild. Obwohl sie schon einmal Opfer eines Ransomware-Angriffes waren, glauben viele Sicherheitsexperten nicht, dass ihre Unternehmen über die richtigen Mitarbeitenden und Pläne verfügen, um den nächsten Angriff zu bewältigen.

Die Ransomware-Angreifer entwickeln sich ständig weiter

Komplexere Low-and-Slow-Angriffe zielen darauf ab, einen möglichst großen Teil des angegriffenen Netzwerks zu kompromittieren, um bei „RansomOps"-Angriffen ein möglichst hohes Lösegeld zu fordern.

56 % gaben an, dass ihr Unternehmen einen Ransomware-Angriff erst nach **3 bis 12 Monaten** entdeckt hat.

Worauf haben sie es abgesehen?

- **Geistiges Eigentum (IP)/ Geschäftsgeheimnisse**
- **Personenbezogene Daten**
- **Geschützte Gesundheitsdaten**
- **Kundendaten**
- **Konto-Anmeldeinformationen**

Wie haben sie sich Zugang verschafft?

41 % sind über einen **Partner in der Lieferkette** eingedrungen

24 % sind **direkt** eingedrungen

22 % sind mit Hilfe eines **Insiders** eingedrungen

Lösegeldzahlungen sind nicht die Lösung

Obwohl die meisten Opfer bereit waren, das Lösegeld zu zahlen, erhielten weniger als die Hälfte von ihnen ihre Systeme und Daten unkompromittiert zurück. Bei den meisten kam es zudem innerhalb eines Jahres erneut zu einem Ransomware-Angriff.

84 % haben das Lösegeld gezahlt.

Allerdings erhielten nur

47 %

ihre Daten und Dienste unkompromittiert zurück.

Warum haben sie das Lösegeld gezahlt?

- **Die Angreifer haben mit der Weitergabe sensibler Daten gedroht**
- **Es war ein Feiertag/Wochenende und wir waren unterbesetzt**
- **Wir befürchteten Geschäftseinbußen**
- **Es ging um Leben und Tod**
- **Es schien die schnellste Lösung zu sein**
- **Wir hatten keine Sicherungsdateien**

78 %

wurden anschließend erneut Opfer eines Ransomware-Angriffs.

und

63 %

von ihnen wurden beim zweiten Mal zu einer **höheren Zahlung** aufgefordert.

82 % wurden innerhalb eines Jahres **erneut Opfer** eines Angriffs

Bei **36 %** erfolgte dieser durch **dieselben Akteure**

Bei **42 %** ging der Angriff von **anderen Akteuren aus**

Die tatsächlichen Auswirkungen sind erschreckend

Die **Lösegeldgebühren** sind nach wie vor hoch, und sie sind nur **die Spitze des Eisbergs**, wenn es um die **wahren Kosten** für ein Unternehmen geht.

Durchschnittliche Lösegeldzahlungen in den letzten 24 Monaten im Vergleich:

USA: 1,4 Mio. Dollar

Frankreich: 1 Mio. Dollar

Deutschland: 762.000 Dollar

GB: 423.000 Dollar

46 % schätzen die geschäftlichen Verluste auf 1–10 Mio. Euro.

16 % schätzen die Verluste auf über 10 Mio. Euro.

Die tatsächlichen Kosten sind viel **höher** und umfassen:

- Markenschäden
- Umsatzverluste
- Vorübergehende Schließung
- Rücktritte auf Führungsebene
- Entlassungen

Unternehmen müssen mehr tun

Die meisten Unternehmen haben **ihre Investitionen in die Cybersicherheit nach einem Angriff erhöht**, doch das **Risiko bleibt bestehen**.

Weniger als die Hälfte der Sicherheitsexperten sagen, dass sie auf den nächsten Angriff angemessen vorbereitet sind.

87%

haben ihre Ausgaben für die Cybersicherheit erhöht.

Nur

41%

sind jedoch der Meinung, dass sie über die richtigen Mitarbeitenden und einen geeigneten Plan verfügen, um den nächsten Angriff zu bewältigen.

37%

haben **das richtige Personal**, aber nicht den richtigen Plan.

18%

haben **den richtigen Plan**, aber nicht das richtige Personal.

Sie investieren in die folgenden Bereiche:

1. Fachkräfte im Bereich Cybersicherheit
2. Schulungen zum Sicherheitsbewusstsein
3. Neue Technologien (z. B. Endgerätetechnologie und Identitätsdienste)
4. Verbesserte Einhaltung interner Vorschriften/Lieferketten-Compliance
5. Cyberversicherungen
6. Krypto-Wallets

Was passiert und wie man sich darauf vorbereitet

Angreifer nutzen generative KI und maschinelles Lernen, um neue Wege in Netzwerke zu finden und ihre Aktivitäten auszuweiten. Gleichzeitig werden Unternehmen durch verschiedene Herausforderungen behindert.

Wir haben **sechs zentrale Herausforderungen** identifiziert. Obwohl keine davon leicht zu bewältigen ist, geben wir Ihnen einige Tipps, wie Sie Ihr Unternehmen auf jede einzelne davon vorbereiten können.

1/ Angreifer werden immer effektiver, unter anderem dank generativer KI

Die Situation:

Überall arbeiten Unternehmen daran, wie sie generative KI am besten nutzen können, um in großem Umfang effektiver und effizienter zu werden. Und dasselbe gilt für böswillige Akteure. Sie nutzen Tools wie ChatGPT 4.0, um personenbezogene Daten zu sammeln, professionell aussehende Nachrichten zu verfassen und sie effektiver in jede Sprache zu übersetzen.

So können Sie sich vorbereiten:

Stellen Sie sicher, dass sich alle Mitarbeitenden des erhöhten Risikos bewusst sind, dass böswillige Akteure diese Tools nutzen, um weniger verdächtig erscheinende Nachrichten zu erstellen. Zeigen Sie ihnen, worauf sie achten müssen, und führen Sie regelmäßig Übungen durch. Vergewissern Sie sich, dass alle Teams die grundlegenden bewährten Sicherheitspraktiken einhalten. Und arbeiten Sie mit einem Cybersicherheitsanbieter zusammen, um kritische Systeme und Daten zu sichern. Einige Anbieter setzen inzwischen KI ein, um die Erkennung von und den Schutz vor Ransomware zu automatisieren.

Ist generative KI gefährlich?

> Im Februar 2023 entdeckten Forscher des Sicherheitsunternehmens Checkpoint, dass es böswilligen Akteuren gelungen war, einen Chatbot durch Veränderung seiner API in die Lage zu versetzen, Malware-Code zu generieren, und die Virenerstellung in die Hände nahezu jedes Möchtegern-Hackers zu legen.

Mehr dazu in dieser Folge unseres Malicious Life-Podcasts.

2/ Der Fachkräftemangel wächst weiter

Die Situation:

Die Zahl der Beschäftigten im Bereich der Cybersicherheit mag weltweit einen Rekordstand erreicht haben, doch die Nachfrage nach bestimmten Kompetenzen übersteigt das Angebot an qualifizierten Arbeitskräften bei Weitem. Die Einstellung von Fachkräften im Bereich Cybersicherheit war die wichtigste Investition der Befragten. Sie können allerdings einfach nicht im erforderlichen Tempo mithalten.

So können Sie sich vorbereiten:

Steigern Sie die Effizienz, um das vorhandene Cybersecurity-Personal voll auszuschöpfen. Dies kann die Konsolidierung, Automatisierung und Auslagerung verschiedener Teile Ihrer Sicherheits- und Incident-Response-Funktionen bedeuten. Mehr über MalOp™ und Cybereasons betriebszentrierten Ansatz finden Sie hier:

cybereason.com/platform#malop

3/ Veraltete Systeme erhöhen die Anfälligkeit des Netzwerks

Die Situation:

Während die meisten Teile des Netzes in die Cloud migriert werden, bleiben viele kritische Systeme offline. Diese scheinen zwar weniger anfällig für Angriffe zu sein, sind aber auch weniger geschützt. Und ihr kritischer Charakter macht sie zu idealen Zielen für Social Engineers, die nur einmal das schwächste Glied finden müssen, um an Passwörter zu gelangen oder sich physischen Zugang zu verschaffen.

So können Sie sich vorbereiten:

Ignorieren Sie Offline- oder geschlossene Systeme nicht. Kontrollieren Sie den Zugang, stellen Sie sicher, dass sie passwortgeschützt sind, und klären Sie Ihre Mitarbeitenden über die Gefahren des Social Engineering auf. Sichern Sie diese Systeme, indem Sie mit einem Anbieter von Cybersicherheitslösungen zusammenarbeiten, der leichtgewichtige, nicht-intrusive Sicherheitslösungen einsetzen kann.

Bei der Aufdeckung des Hackerangriffs auf das Kernkraftwerk Sellafield fanden die Ermittler mehrere Schwachstellen, darunter die Tatsache, dass externe Auftragnehmer unbeaufsichtigt Speichersticks in das System einstecken konnten.

4/ Eine Versicherung federt nur einen Teil des Angriffs ab

Die Situation:

Obwohl fast alle Befragten eine Cyberversicherung abgeschlossen haben, sind sich nur 40 % sicher, dass ein Ransomware-Angriff abgedeckt wäre. Nur etwa die Hälfte derjenigen, die nach einem Angriff ihre Versicherung in Anspruch nahmen, erhielten die vollen Kosten zurück.

So können Sie sich vorbereiten:

Cyberversicherungen mildern einen Teil der Gesamtauswirkungen eines Angriffs ab. Nehmen Sie sich also die Zeit, die Cyberversicherungspolice(n) Ihres Unternehmens vollständig zu lesen und zu verstehen, um sich gegen die tatsächlichen Kosten eines Ransomware-Angriffs abzusichern.

5/ Sicherheitsexperten brauchen Hilfe bei der Planung für den nächsten Angriff

Die Situation:

Trotz der hohen Wahrscheinlichkeit, Opfer eines weiteren Angriffs zu werden, sind nur 41 % der Unternehmen auf den nächsten Angriff vorbereitet, und die größte Lücke besteht in der Planung.

So können Sie sich vorbereiten:

Konzentrieren Sie sich auf das, was Sie mit den Ihnen aktuell zur Verfügung stehenden Mitteln kontrollieren können. Der beste Weg, damit zu beginnen, ist ein Belastungstest in Bezug auf Ihren aktuellen Notfallplan. Ziehen Sie die Zusammenarbeit mit einem Partner für Cybersicherheit in Betracht, um eine Ransomware-Risikobewertung durchzuführen. Die Bewertung sollte aus „Tabletop-Übungen" bestehen, die einen Ransomware-Angriff simulieren und die personellen, verfahrenstechnischen und technologischen Aspekte Ihres Plans testen. Die Ergebnisse werden Ihnen zeigen, wie Sie Ihre Ressourcen bestmöglich einsetzen können.

6/ Es lohnt sich immer noch nicht, zu zahlen

Die Situation:

84 % der Befragten gaben an, dass ihr Unternehmen das Lösegeld gezahlt hat. Das ergibt Sinn, da wir festgestellt haben, dass die Eröffnung einer Krypto-Wallet eine beliebte Investition ist. Leider haben die meisten derjenigen, die gezahlt haben, ihre Systeme und Daten nicht unkompromittiert zurückerhalten. Und 78 % wurden erneut zur Kasse gebeten, wobei 63 % angaben, dass sie beim zweiten Mal ein höheres Lsegeld zahlen mussten.

So können Sie sich vorbereiten:

Wie wir in den letzten beiden Jahren gesehen haben, lohnt es sich immer noch nicht, Lösegeld zu zahlen. Vorbeugen ist immer besser als Schadensbehebung. Machen Sie Ransomware-Angriffen ein Ende, indem Sie sich mit einem führenden Anbieter von Cybersicherheitslösungen zusammenschließen, der über eine spezielle Technologie zum Schutz vor Ransomware verfügt. Wenn potenzielle Verluste in Millionenhöhe absehbar sind, können Sie es sich nicht leisten, Ihr Unternehmen schutzlos zu lassen.

Schlussfolgerung: Es ist an der Zeit, Lösegeldzahlungen abzulehnen

Einmal mehr zeigt sich, dass die Zahlung von Millionen von Dollar an Ransomware-Angreifer nicht immer die beste Lösung ist. Es gibt keine Garantie dafür, dass Sie alle Ihre Systeme und Daten unkompromittiert zurückerhalten, dass Ihre Daten nicht auf dem Schwarzmarkt verkauft werden oder dass Sie nicht wieder angegriffen werden. Unsere Umfrage hat vielmehr ergeben, dass man mit hoher Wahrscheinlichkeit erneut angegriffen wird, sobald erst einmal eine Schwachstelle entdeckt wurde.

Ein wesentlich besserer Ansatz gegen die Plage der Ransomware besteht darin, Ihr Unternehmen unangreifbar zu machen. Und das ist möglich. Doch zunächst müssen Sie dem Unternehmen helfen, das wahre Risiko und die Auswirkungen eines Angriffs zu verstehen.

Helfen Sie Ihrem Unternehmen, das tatsächliche Risiko eines Angriffs zu erfassen

Sie können die Ergebnisse dieser Umfrage nutzen, um Ihrem Unternehmen zu helfen, das wahre Risiko und die Kosten einer erfolgreichen Sicherheitsverletzung durch Ransomware-Angreifer zu verstehen. Dies sollte das Thema schnell an die Spitze der Prioritätenliste katapultieren und Ihnen die Sicherstellung eines ausreichenden Investitionsbudgets zur Stärkung der Sicherheitsposition des Unternehmens erleichtern.

Investitionen in Ransomware-Fachkräfte, -Planung und -Technologie

Die im vorigen Abschnitt dieses Berichts empfohlenen Tabletop-Übungen werden Ihnen helfen, die Schwachstellen in Ihrer Schutz- und Reaktionsplanung zu ermitteln. Wir empfehlen die Zusammenarbeit mit einem Anbieter von Cybersicherheitslösungen, um alle Bereiche abzudecken. Im Folgenden finden Sie jedoch schon einmal einige Empfehlungen für den Anfang:

Personal

Stellen Sie eine Cybersecurity-Fachkraft mit Erfahrung im Schutz vor Ransomware ein und befähigen Sie diese, mit weniger mehr zu erreichen, indem Sie den Schutz Ihrer Daten und Systeme automatisieren. Erwägen Sie die Auslagerung von Teilen Ihrer Sicherheitsaktivitäten, um eventuelle Lücken zu schließen, z. B. die Überwachung außerhalb der Geschäftszeiten oder Dienste zur Erkennung von und Reaktion auf Bedrohungen, die Rechner in den frühesten Stadien eines Angriffs automatisch isolieren können.

Prozess

Arbeiten Sie mit dem Unternehmen zusammen, um sicherzustellen, dass es Ressourcen für eine angemessene Planung bereitstellt. Achten Sie darauf, alle Aspekte des Unternehmens einzubeziehen, einschließlich des Vorstands (klären Sie, wer für die Entscheidungsfindung zuständig ist und dass die entsprechende Person auch nach Geschäftsschluss erreichbar ist), der PR- und Marketingabteilung (für Krisenmanagement und Kundenkommunikation) usw. Überprüfen Sie Ihre Pläne regelmäßig.

Technologien

Drehen Sie den Spieß um, indem Sie in die allerneuesten Technologie investieren. Stellen Sie sicher, dass sie sowohl Online- als auch Offline-Netze abdeckt. Suchen Sie außerdem nach Ransomware-spezifischen Lösungen, die Schutz in jeder Phase eines Angriffs bieten und als letzte Verteidigungslinie ein Rollback für alle betroffenen Dateien vorsehen. Arbeiten Sie mit Ihrem Anbieter zusammen, um verwaltete Erkennungs- und Reaktionsdienste mit 24x7x365-Überwachung zu implementieren, die helfen, Angriffe innerhalb weniger Augenblicke zu erkennen, zu stoppen und sogar zu beheben, unabhängig davon, wann sie auftreten.

Machen Sie Ihr Unternehmen unbezwingbar

mit KI-gestütztem Schutz

Mit mehrschichtigem Schutz, KI-gesteuerten Endgeräten, Transparenz vom Kernel bis zur Cloud und dem einzigen verfügbaren prädiktiven Ransomware-Schutz ist Cybereason ein unbezwingbarer Gegner der Angreifer von heute und bereit für jene von morgen. Sie können auf eine leistungsstarke Kombination von Lösungen und Diensten zurückgreifen, die rund um die Uhr Sicherheit, optimierte Sicherheitsabläufe und die schnellste Erkennung, Einordnung und Behebung von Problemen auf dem Markt bieten.

Finde mehr heraus

Kontaktiere uns

Über Cybereason

Cybereason ist ein XDR-Unternehmen, das sich gemeinsam mit Defenders der Abwehr von Angriffen auf Endgeräteebene, in der Cloud und im gesamten Unternehmens-Ökosystem verschrieben hat. Nur die KI-gestützte XDR-Plattform von Cybereason bietet vorausschauende Prävention, Erkennung und Reaktion für bisher unerreichten Schutz gegen moderne Ransomware und fortschrittliche Angriffstechniken. Cybereason MalOp™ liefert sofort und mit unvergleichlicher Geschwindigkeit und Genauigkeit kontextreiche Angriffsinformationen über jedes betroffene Gerät, jeden Benutzer und jedes System. Cybereason verwandelt Bedrohungsdaten in umsetzbare Entscheidungen, die mit der Dynamik von Geschäftsprozessen Schritt halten können. Cybereason ist ein internationales Unternehmen in Privatbesitz mit Hauptsitz in Boston und Kunden in mehr als 40 Ländern.

Ransomware-Schutzfähigkeiten von Cybereason

Cybereason bietet seinen Kunden einzigartige Fähigkeiten, die sicherstellen, dass sie im Kampf gegen Ransomware unbezwingbar bleiben. Unsere einzigartige Kombination aus neun Schichten für den Endgeräteschutz (EPP), mit integrierten Technologien zur Endgeräteerkennung (EDR) von Cybereason und unserem MDR-Service (Managed Detection and Response) bildet eine Rundumschutz-Lösung für unsere Kunden in jeder Phase der fortschrittlichsten Ransomware-Angriffe.

Das Ergebnis: Die Kunden sind geschützt. Eine Minute für die Erkennung, fünf Minuten für die Einstufung und 30 Minuten für die Behebung des Angriffs. Den ganzen Tag, die ganze Woche, das ganze Jahr über – auch außerhalb der Geschäftszeiten und an den Wochenenden (wenn Angreifer bevorzugt zuschlagen).

Erhebungsmethode

Diese Untersuchung wurde von Censuswide im Auftrag von Cybereason durchgeführt. An der Online-Umfrage nahmen zwischen dem 25. September und dem 6. Oktober 2023 insgesamt 1.008 Cybersicherheitsexperten aus Unternehmen mit 500 oder mehr Mitarbeitern teil. Die Teilnehmer kommen aus den Vereinigten Staaten, dem Vereinigten Königreich, Frankreich und Deutschland. Die Repräsentativerhebung umfasst Antworten aus einer Vielzahl von Branchen. IT und Telekommunikation waren mit 31 % am stärksten vertreten, gefolgt von Fertigung und Versorgung (13 %) und Einzelhandel, Gastronomie und Freizeit (10 %). Weitere Branchen sind z. B. Architektur, Ingenieurwesen und Bauwesen, Kunst und Kultur, Bildung, Gesundheitswesen, Recht, Verkehr und mehr. Es wurden nur Unternehmen mit mindestens 500 Mitarbeitern befragt. Die Unternehmen mit 500–999 Beschäftigten machten 87 % der Gruppe aus, die restlichen 13 % entfielen auf Unternehmen mit mehr als 1.000 Beschäftigten.

cybereason©