

März 2023

MARKTBERICHT

2023 Ransomware Einblicke

Die Verbreitung und
Wirkung von Ransomware-
Angriffen auf der ganzen
Welt »

Inhalt

- Einleitung.....3
- Erkenntnis Nr. 1: Die meisten Unternehmen haben bereits einen Ransomware-Angriff erlebt..5
- Erkenntnis Nr. 2: Wiederholte Opfer sind eher bereit, Lösegeld zu zahlen, um die verschlüsselten Daten wiederherzustellen.....7
- Erkenntnis Nr. 3: E-Mail ist der häufigste Ausgangspunkt für die Ransomware-Angriffe.....11
- Erkenntnis Nr. 4: Unternehmen mit Cyberversicherung sind häufiger von Ransomware-Angriffen betroffen.....13
- Erkenntnis Nr. 5: Viele Unternehmen fühlen sich nicht ausreichend auf Ransomware vorbereitet.....14
- Schlussfolgerung.....16
- Über Barracuda.....17
- Über Vanson Borne.....17

Einleitung

Ransomware – eine dauerhafte und sich entwickelnde Bedrohung

Bei [Ransomware](#) handelt es sich um bösartige Software, die so konzipiert ist, dass sie das Netzwerk des Opfers infiziert und bis zum Bezahlen von Lösegeld den Zugang zu Daten und Systemen sperrt. Sie entwickelt sich vielfältig weiter und ist eine Bedrohung, die auch den Diebstahl von sensiblen oder vertraulichen Informationen und die Drohung beinhalten kann, die Daten an die Öffentlichkeit gelangen zu lassen, wenn kein Lösegeld bezahlt wird. Das kriminelle Geschäftsmodell ist äußerst lukrativ – [oft verfügbar als ein Service](#) und zugänglich für alle Widersacher, unabhängig von ihren Ressourcen oder Kenntnissen.

Jedes Unternehmen ist ein potenzielles Ziel. Ransomware-Angriffe können den täglichen Betrieb und die Lieferketten der Kunden lahmlegen und so Chaos und finanzielle Verluste verursachen. Sie können sowohl den Ruf des Unternehmens als auch die Kundenbeziehungen zerstören.

Unsere internationale Umfrage untersuchte die Erfahrungen mit Ransomware-Angriffen auf Unternehmen in den letzten 12 Monaten. Den Ergebnissen zufolge waren fast drei Viertel (73%)

der Befragten im Jahr 2022 von mindestens einem erfolgreichen Ransomware-Angriff betroffen – 38% gaben an, zweimal oder öfter betroffen gewesen zu sein.

Die Wahrscheinlichkeit, ein Lösegeld für die Wiederherstellung verschlüsselter Daten zu zahlen, war bei Unternehmen, die mehrfach von Ransomware betroffen waren, höher. Von denjenigen, die einmal betroffen waren, zahlten 31% das Lösegeld, um die verschlüsselten Daten wiederherzustellen, verglichen mit 34% derjenigen, die zweimal betroffen waren, und 42% derjenigen, die dreimal oder häufiger betroffen waren. Wiederholte Opfer nutzten auch seltener ein System zum Daten-Backup für die Wiederherstellung der Daten.

Die Ergebnisse zeigen, dass bei 69% der Unternehmen der Ransomware-Angriff mit einer bösartigen E-Mail begann, z. B. einer [Phishing E-Mail](#) die auf den Diebstahl von Zugangsdaten abzielt. So können die Cyberkriminellen Zugang zum Netzwerk erhalten, um Assets, Server und Datenbanken zu untersuchen, bevor sie schließlich den Ransomware-Angriff starten. Web-

Applikationen und Web-Traffic stehen an zweiter Stelle und stellen ein wachsendes Risiko im Rahmen einer sich ständig vergrößernden Bedrohungsfläche dar.

Organisationen mit Cyberversicherung waren mit größerer Wahrscheinlichkeit von Ransomware betroffen.

Mehr als drei Viertel (77%) der Unternehmen mit einer Cyberversicherung waren von mindestens einem erfolgreichen Ransomware-Angriff betroffen, verglichen mit 65% der Unternehmen ohne Cyberversicherung. Dies könnte bedeuten, dass Cyberkriminelle eher Unternehmen mit einer Versicherung ins Visier nehmen, weil sie davon ausgehen, dass die Versicherer bereit sind, die Kosten für das Lösegeld zu übernehmen, um die Wiederherstellung zu beschleunigen.

Die Studie ergab auch, dass mehr als ein Viertel (27%) der befragten Unternehmen sich nicht vollständig auf einen Ransomware-Angriff vorbereitet fühlt.

Die Sicherheitsbranche spielt eine wichtige Rolle bei der Unterstützung von Unternehmen im Kampf gegen Bedrohungen durch Ransomware. Dies geschieht mithilfe von tiefgreifenden, mehrschichtigen Sicherheitstechnologien, Bedrohungsjagd und erweiterten Erkennungs- und Reaktionsfähigkeiten (XDR) sowie einer effektiven Incident Response, um Eindringlinge zu erkennen und Lücken zu schließen und Angreifern so den Zugang zu erschweren.

Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer weltweiten Umfrage unter IT-Managern und technischen IT-Fachleuten, leitenden IT-Sicherheitsmanagern und Entscheidungsträgern aus den Bereichen IT und IT-Sicherheit. Es gab 1.350 Umfrageteilnehmer aus einer Vielzahl von Branchen, darunter Landwirtschaft, Biotechnologie, Bauwesen, Energie, Regierungsbehörden, Gesundheitswesen, Fertigung, Einzelhandel, Telekommunikation, Großhandel und andere. Die Umfrageteilnehmer waren aus den USA, Australien, Indien und Europa. Die europäischen Befragten stammten aus dem Vereinigten Königreich, Frankreich, der DACH-Region (Deutschland, Österreich, Schweiz), den Benelux-Staaten (Belgien, Niederlande, Luxemburg) und Skandinavien (Dänemark, Finnland, Norwegen, Schweden). Die Umfrage wurde im Dezember 2022 durchgeführt.

Der Bericht bezieht sich auch auf von Barracuda in Auftrag gegebene Forschungsergebnisse, die 2019 veröffentlicht wurden. Diese Umfrage umfasste Antworten von 660 Führungskräften, einzelnen Mitwirkenden und Teammanagern, die in IT-Sicherheitspositionen in Amerika, EMEA und APAC tätig waren.

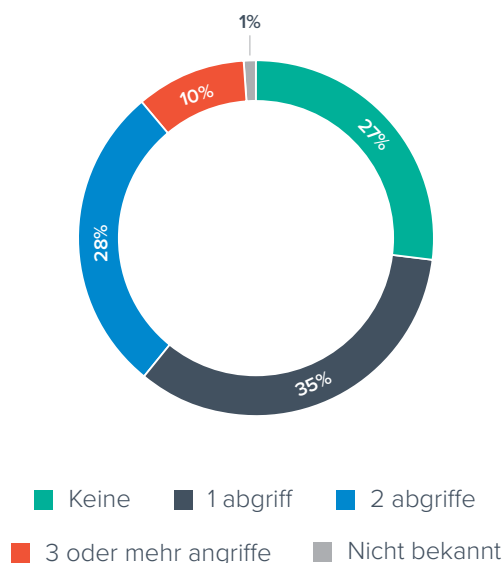
Die meisten Unternehmen haben zumindest einen Ransomware-Angriff erlebt – ein Drittel davon zweimal oder öfter.

Knapp drei Viertel der befragten Unternehmen meldeten mindestens einen erfolgreichen Ransomware-Angriff in den letzten 12 Monaten.

Der hohe Anteil an Unternehmen, die insgesamt von Ransomware betroffen sind, sollte nicht überraschen. Hacker wenden sich zunehmend dem Ransomware-as-a-Service-Modell zu, das es Angreifern leichter – und billiger – macht, Ransomware-Angriffe zu starten, für die oft nur geringe oder gar keine technischen Kenntnisse erforderlich sind. Ransomware-as-a-Service (RaaS) ist eine kostenpflichtige Malware, bei der die Entwickler ihre Ransomware-Infrastruktur an andere Cyberkriminelle vermieten.

Wie viele erfolgreiche Ransomware-Angriffe hat Ihr Unternehmen in den letzten 12 Monaten erlebt?

(n=1,350)



Über ein Drittel (38%) der befragten Unternehmen meldete in demselben Zeitraum zwei oder mehr erfolgreiche Ransomware-Angriffe.

Die Tatsache, dass mehrere erfolgreiche Angriffe möglich sind, deutet darauf hin, dass die Sicherheitslücken nach dem ersten Vorfall nicht vollständig geschlossen werden.

Hierfür kann es mehrere Gründe geben. Fehlende Sicherheitskontrollen, Incident Response und Untersuchungsmöglichkeiten sowie die zunehmende Raffinesse und die bessere Tarnung der Angreifer können beispielsweise dazu führen, dass eingeschleuste Hintertüren oder andere von Angreifern hinterlassene, schwer zu entdeckende Tools nicht erkannt und entfernt werden. Zugangspunkte bleiben möglicherweise offen und Kontokennwörter werden nicht zurückgesetzt, sodass gestohlene Zugangsdaten erneut ausgenutzt werden können.

Die vollständige Neutralisierung eines Angriffs wird dadurch erschwert, dass die Angreifer häufig legitime IT-Verwaltungstools ausnutzen, die auch von IT-Teams für harmlose, alltägliche Geschäftszwecke verwendet werden, sodass ihr Auftauchen im Netzwerk möglicherweise nicht sofort Verdacht erregt.

Variationen nach Branche

Es gab erhebliche Unterschiede bei den von Ransomware betroffenen Branchen. Beispielsweise waren fast alle (98%) Unternehmen für Verbraucherdienstleistungen von mindestens einem Ransomware-Angriff betroffen.

Verbraucherdienstleister haben oft mit vielen persönlichen Kundendaten zu tun und erhalten eine große Menge an Kommunikation von außerhalb ihrer Organisation, was sie zu einem guten Ziel für Ransomware macht. Gleichzeitig fühlten sich nur 22% der Befragten aus dieser Branche unzureichend auf einen Ransomware-Angriff vorbereitet.

Strom-, Öl-/Gas- und Versorgungsunternehmen berichteten ebenfalls von einer überdurchschnittlichen Erfolgsquote von Ransomware-Angriffen — 85 Prozent. Kritische Infrastrukturen werden zu einem beliebten Ziel, angesichts der Menge an Störungen, die Ransomware-Angriffe verursachen können, und der Höhe der potenziellen Auszahlung.

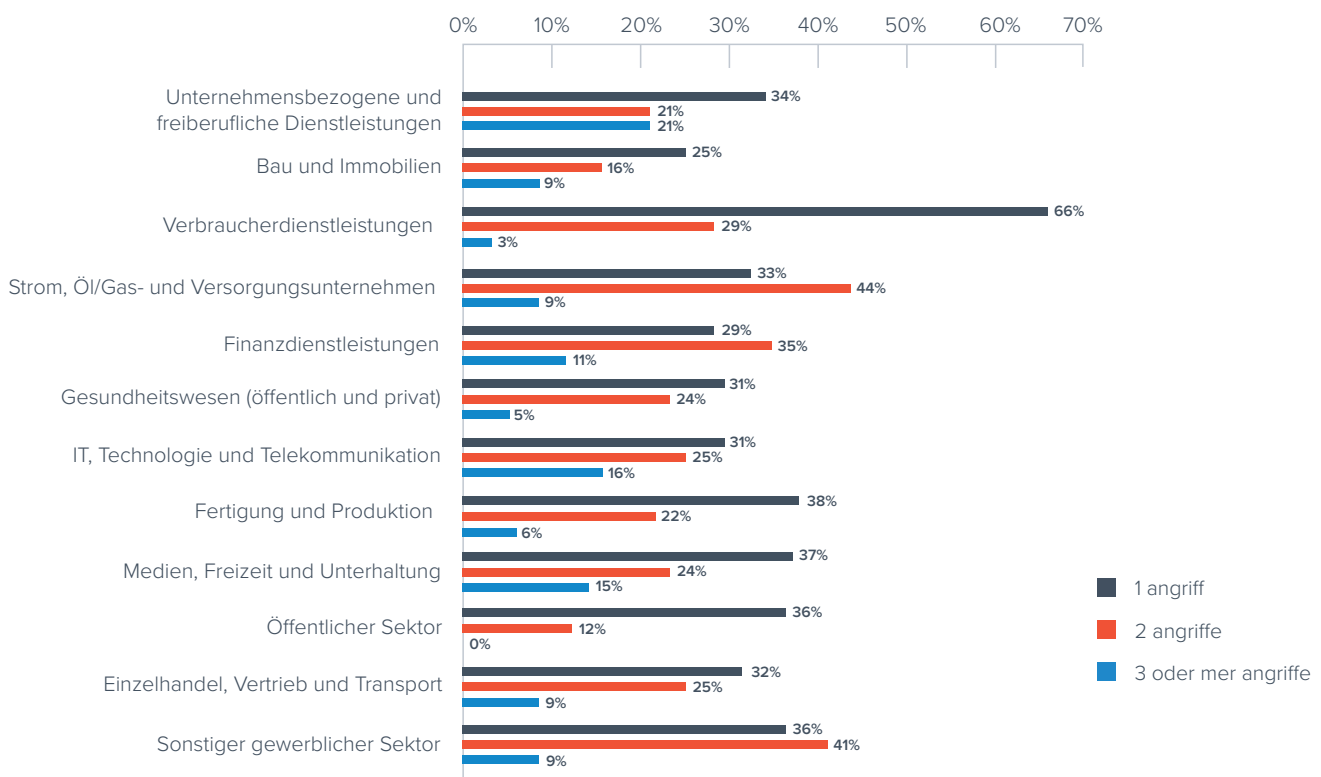
Anzahl erfolgreicher Ransomware-Angriffe in 12 Monaten nach Branche

(n=1,350)

Unsere Recherchen zu öffentlich gemeldeten Ransomware-Angriffen im vergangenen Jahr haben gezeigt, dass sich [Cyberangriffe im Zusammenhang mit Infrastrukturen vervierfacht haben](#), was darauf hindeutet, dass Cyberkriminelle größeren Schaden zufügen möchten, der über die Auswirkungen auf das unmittelbare Opfer hinausgeht.

Strom-, Öl-/Gas- und Versorgungsunternehmen waren auch am häufigsten von mehreren Angriffen betroffen: 53% meldeten zwei oder mehr erfolgreiche Ransomware-Vorfälle, verglichen mit einer Gesamtzahl von 38%.

46% der Finanzdienstleistungsunternehmen gaben an, zweimal oder häufiger betroffen gewesen zu sein. Hochrangige Ziele von Ransomware, wie das Gesundheitswesen, waren weniger häufig von Mehrfachangriffen betroffen: Nur 29% der Befragten aus diesem Sektor berichteten von zwei oder mehr erfolgreichen Angriffen.



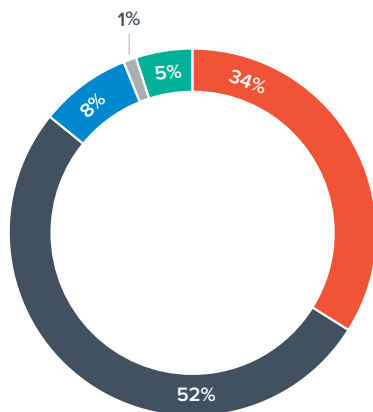
Opfer von wiederholten Angriffen zahlen viel eher Lösegeld zur Wiederherstellung verschlüsselter Daten

Bei einem erfolgreichen Ransomware-Angriff werden in der Regel wertvolle Daten innerhalb eines Unternehmens verschlüsselt. Ganze 95% der befragten Unternehmen, die in den letzten 12 Monaten einen erfolgreichen Ransomware-Angriff erlebt haben, berichteten von verschlüsselten Daten, was zu erheblichen Störungen ihres Geschäfts führte.

Insgesamt verlor nur 1% die verschlüsselten Daten, 34% zahlten das Lösegeld, und 52% nutzten ihre Backup-Systeme zur Wiederherstellung der Daten.

Ist es Cyberkriminellen gelungen, die Daten Ihres Unternehmens während des größten Ransomware-Angriffs der letzten 12 Monate zu verschlüsseln?

(n=982)



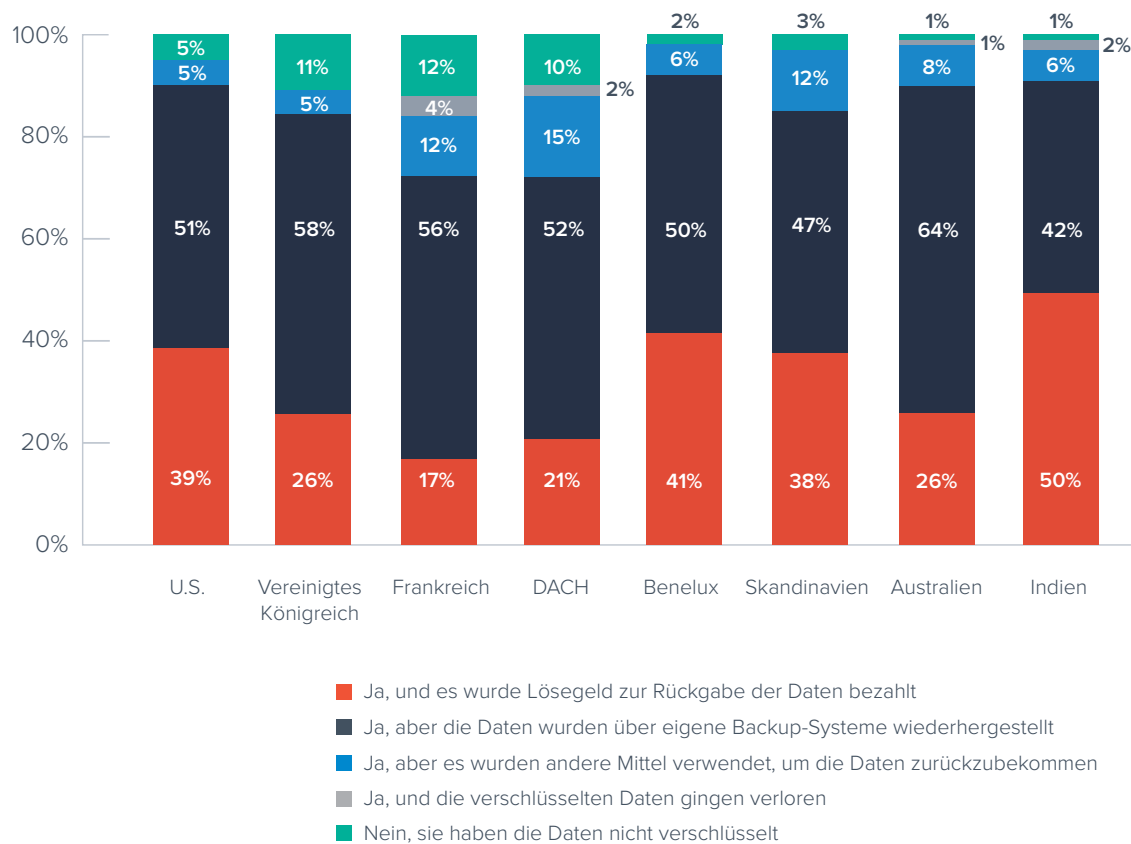
- Ja, und es wurde Lösegeld zur Rückgabe der Daten bezahlt
- Ja, aber die Daten wurden über eigene Backup-Systeme wiederhergestellt
- Ja, aber es wurden andere Mittel verwendet, um die Daten zurückzubekommen
- Ja, und die verschlüsselten Daten gingen verloren
- Nein, sie haben die Daten nicht verschlüsselt

Die Bereitschaft, unabhängig von der Anzahl der Angriffe ein Lösegeld zu zahlen, war je nach Land und Branche sehr unterschiedlich.

Im Vereinigten Königreich, in Frankreich, den DACH-Ländern und Australien gab es weniger Fälle, in denen Unternehmen Lösegeld zahlten, um ihre Daten zurückzubekommen, während in Indien in 50% der Fälle Lösegeld gezahlt wurde. Aber fast überall war die Wiederherstellung aus dem Backup die beste Wiederherstellungsmethode.

Ist es Cyberkriminellen gelungen, die Daten Ihres Unternehmens während des größten Ransomware-Angriffs der letzten 12 Monate zu verschlüsseln?

(n=982)

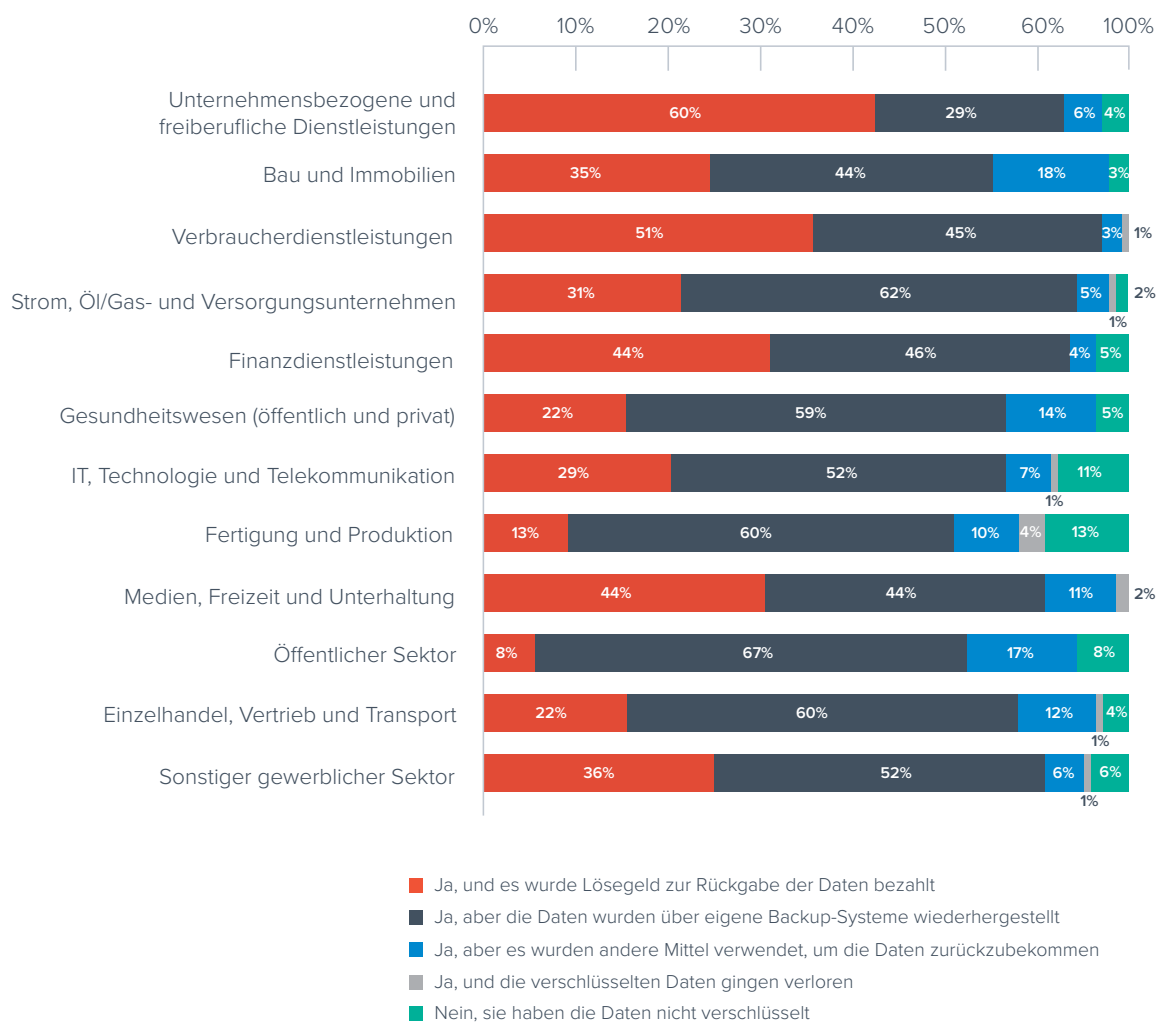


Unternehmen aus dem Bereich der Unternehmens- und Dienstleistungsbranche waren am ehesten bereit, das Lösegeld zu zahlen, um die Daten zurückzubekommen, und zwar in 60% der Fälle. Unternehmen für Verbraucherdienstleistungen zahlten das Lösegeld in 51% der Fälle, während sowohl Finanzdienstleister als auch Medien-, Freizeit- und Unterhaltungsunternehmen in 44% der Fälle zahlten.

Gesundheitsorganisationen zahlten das Lösegeld seltener und taten dies nur in 22% der Fälle.

Ist es Cyberkriminellen gelungen, die Daten Ihres Unternehmens während des größten Ransomware-Angriffs der letzten 12 Monate zu verschlüsseln?

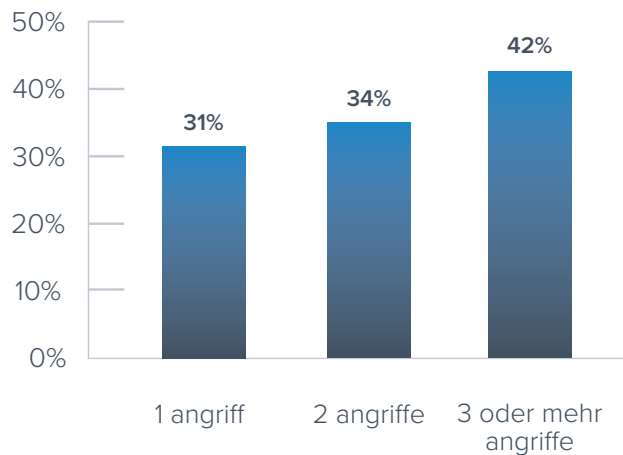
(n=982)



Die Umfrage ergab, dass Unternehmen, die am häufigsten von Ransomware betroffen waren, auch eher Lösegeld zahlten, um verschlüsselte Daten wiederherzustellen: 42% derjenigen, die drei oder mehr Angriffe erlebten, zahlten das Lösegeld. Sie nutzten auch seltener ein System zum Backup von Daten für die Wiederherstellung der Daten.

Unternehmen, die das Lösegeld zur Wiederherstellung verschlüsselter Daten bezahlt haben

(n=982)



Der Anteil an Unternehmen, die Lösegeld trotz oder aufgrund von zwei oder mehr erfolgreichen Ransomware-Angriffen bezahlen, stimmt mit den Erkenntnissen anderer Studien überein. Beispielsweise ergab [eine Studie von 2022](#) über Lösegeldzahlungen, dass 80% der Ransomware-Opfer, die bezahlen, ein zweites Mal angegriffen werden – und häufig ein zweites Mal Lösegeld zahlen.

Eine mögliche Erklärung für eine Verbindung zwischen mehreren Angriffen und Ransomware-Zahlungen ist, dass andere Angreifer dasselbe Opfer anvisieren, sobald sie wissen, dass ein Unternehmen bereit ist zu bezahlen.

Underground-Marktplätze und Initial Access Broker (IAB) zahlen wahrscheinlich extra für die Zugangsdaten von Opfern, von denen bekannt ist, dass sie zur Zahlung bereit sind und sie weiter anfällig sind. In einigen [gemeldeten Fällen](#) kehren dieselben Angreifer zurück und fordern mehr.

Wenn Sie in eine Data Protection-Lösung investieren, die beim Backup und der Wiederherstellung von Daten hilft, können Sie eine Lösegeldzahlung vermeiden, die Cyberkriminelle andernfalls zu erneuten Angriffen verleiten könnte.

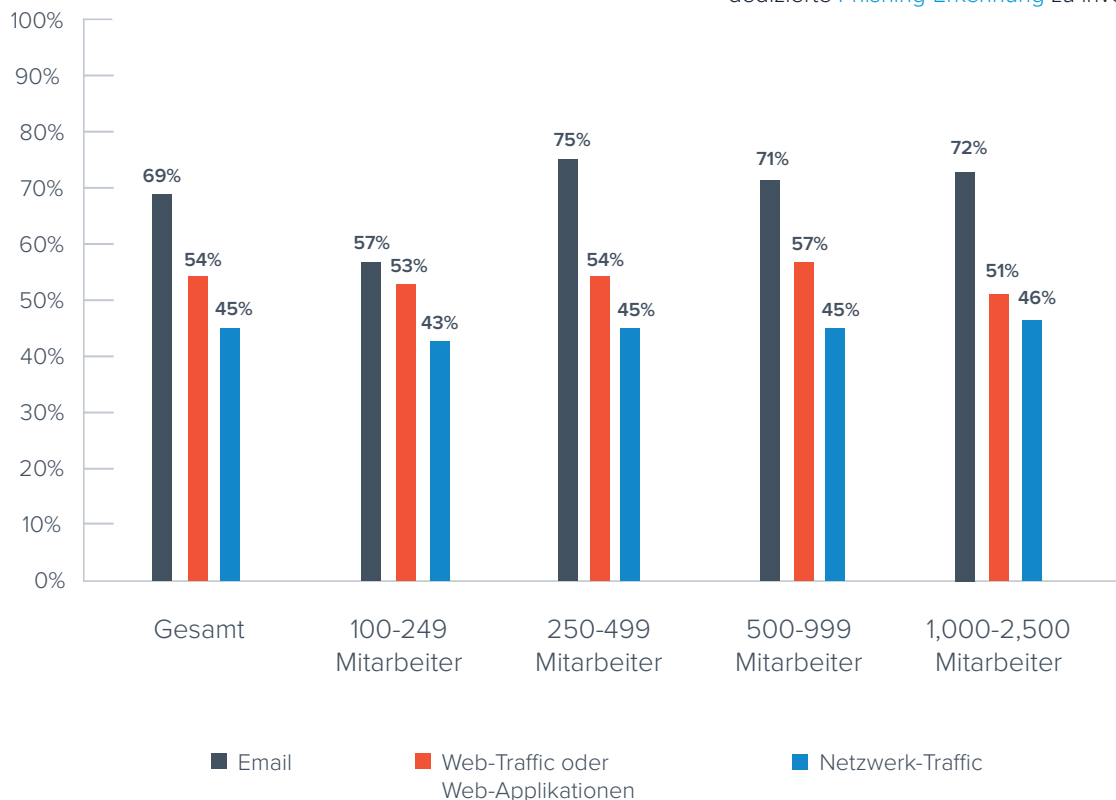
E-Mail ist der häufigste Ausgangspunkt für Ransomware-Angriffe

Für 69% der Unternehmen beginnt ein Ransomware-Angriff mit einer bösartigen E-Mail.

Bei etwas größeren Unternehmen mit über 250 Mitarbeitern liegt dieser Prozentsatz über dem Durchschnitt (75%). Das Senden einer E-Mail ist viel einfacher als das Eindringen in das Netzwerk einer Organisation.

Woher stammen die Ransomware-Angriffe auf Ihr Unternehmen?

(n=982)



Traditionell hängen Hacker ein Dokument mit einer bösartigen Payload oder einer URL an, die zu einer gefälschten Website führt, die Malware verbreiten kann. Als Unternehmen Advanced Threat Protection wie Sandboxing und URL-Schutz zum Zeitpunkt des Anklickens implementierten, setzten Cyberkriminelle [Social Engineering-Taktiken](#) ein, um nach den Zugangsdaten der Benutzer zu phishen. Kompromittierte Konten können ein einfaches Sprungbrett für Ransomware-Angriffe sein, sodass sich Cyberkriminelle seitlich innerhalb des Unternehmens bewegen können, ohne entdeckt zu werden. Unternehmen, die ihre Abwehr gegen Ransomware verbessern möchten, sollten damit beginnen, in ihre E-Mail-Sicherheit und insbesondere in die dedizierte [Phishing-Erkennung](#) zu investieren.

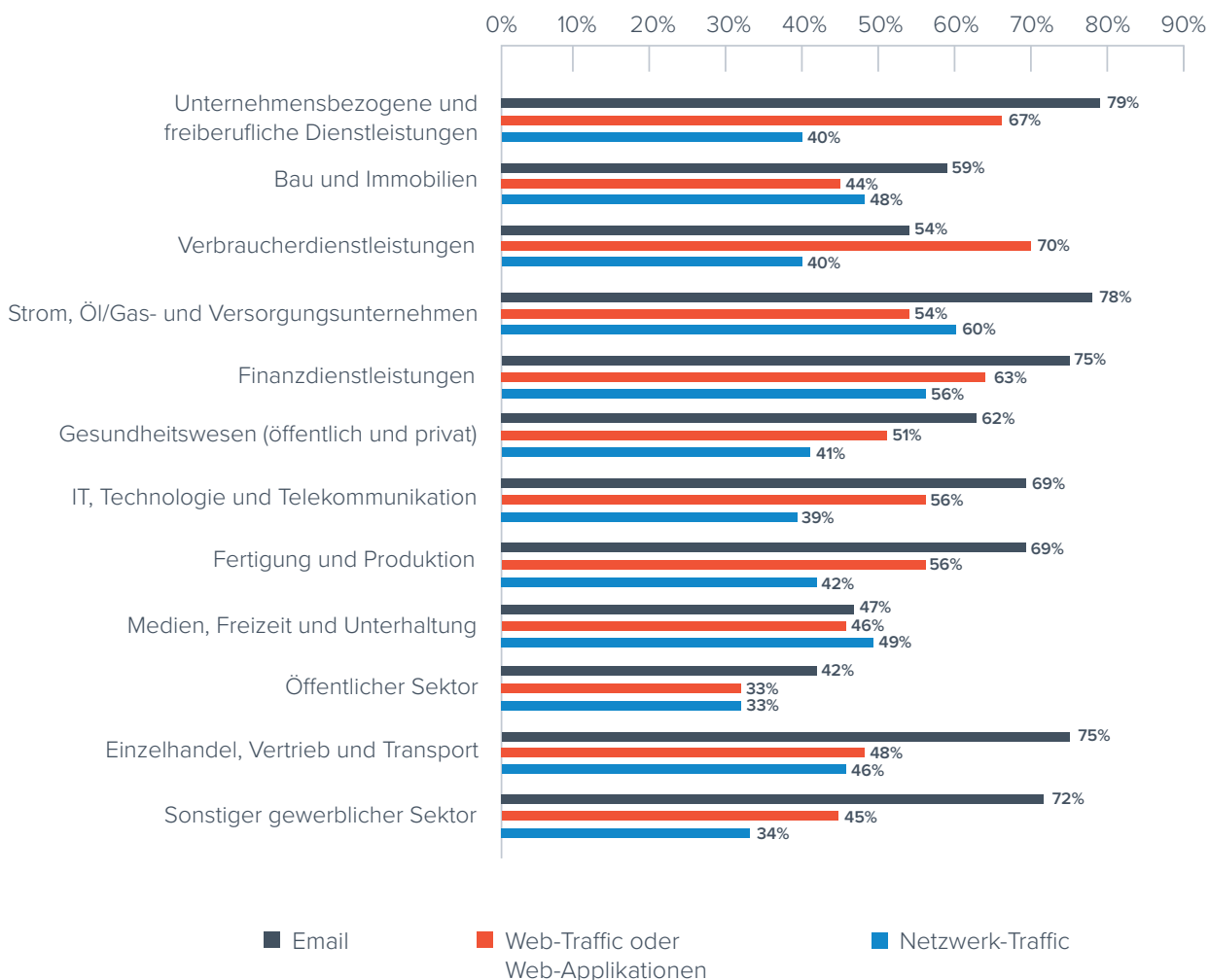
E-Mail ist jedoch nicht für jede Branche der Ransomware-Bedrohungsvektor

Nr. 1. So stammen die meisten Ransomware-Angriffe im Bereich der Verbraucherdienstleistungen aus dem Web-Traffic und aus Web-Applikationen.

Online-Applikationen wie File-Sharing-Dienste, Webformulare und E-Commerce-Websites können von Angreifern kompromittiert werden. Web-Applikationen werden über die Benutzeroberfläche oder eine API-Schnittstelle angegriffen. Oft umfassen diese Angriffe Credential Stuffing, Brute-Force-Angriffe oder [OWASP-Schwachstellen](#). Sobald die Anwendung kompromittiert wurde, kann der Angreifer Ransomware und andere Malware in das System einschleusen. Diese kann dann das gesamte Unternehmensnetzwerk sowie das der Anwendungsnutzer weiter infizieren.

Woher stammen die Ransomware-Angriffe auf Ihr Unternehmen?

(n=982)



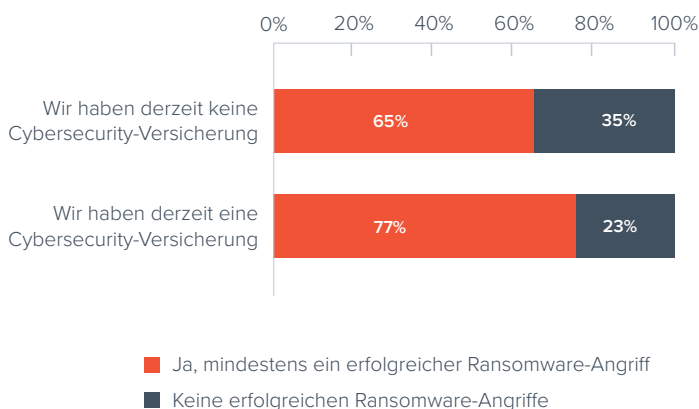
Unternehmen mit Cyber-Versicherungen sind häufiger von Ransomware betroffen

63% der befragten Unternehmen haben in eine Cybersecurity-Versicherung investiert, um die mit jeder Art von Datenverletzung verbundenen Kosten zu minimieren. Cyberversicherungen können zwar bei der Aushandlung von Lösegeldzahlungen helfen oder sogar die Mittel für die Zahlung bereitstellen, doch die zahlreichen Ausschlüsse in ihren Policen bedeuten oft, dass Unternehmen trotzdem eine sehr hohe Rechnung erwartet.

Unternehmen, die über eine Cyberversicherung verfügen, waren im vergangenen Jahr mit größerer Wahrscheinlichkeit von einem erfolgreichen Ransomware-Angriff betroffen. **Bei 77% der Unternehmen mit Cyberversicherung kam es zu einem erfolgreichen Ransomware-Angriff, verglichen mit 65% ohne Cyberversicherung.** Dies könnte bedeuten, dass Cyberkriminelle eher Unternehmen mit Versicherungen ins Visier nehmen, in der Annahme, dass die Versicherer bereit sind, die Lösegeldzahlungen zu übernehmen, um die Wiederherstellung zu beschleunigen.

Wurde Ihr Unternehmen in den letzten 12 Monaten Opfer von mindestens einem erfolgreichen Ransomware-Angriff?

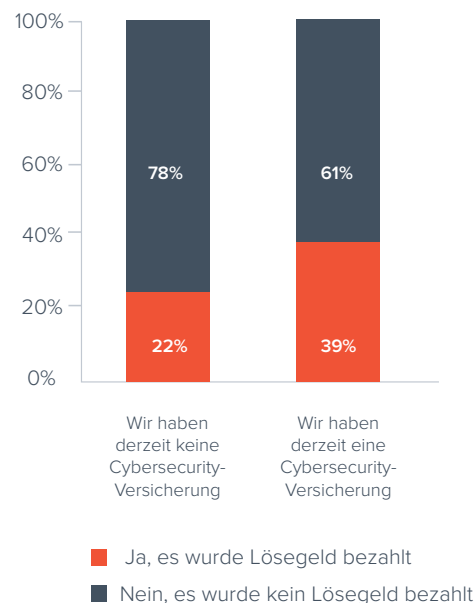
(n=1,350)



Die Umfrageergebnisse zeigen beispielsweise, dass **Unternehmen mit einer Cyberversicherung eher das Lösegeld zahlen, um ihre Daten zurückzubekommen (39% gegenüber 22% der Unternehmen ohne Cyberversicherung).** Und obwohl keine Verbindung hergestellt werden kann, ist es auch erwähnenswert, dass **Unternehmen, die von zwei oder mehr Ransomware-Angriffen betroffen waren, mit größerer Wahrscheinlichkeit auch eine Cyberversicherung abgeschlossen hatten (70%).**

Wurde Lösegeld bezahlt, um die Daten zurückzubekommen?

(n=982)



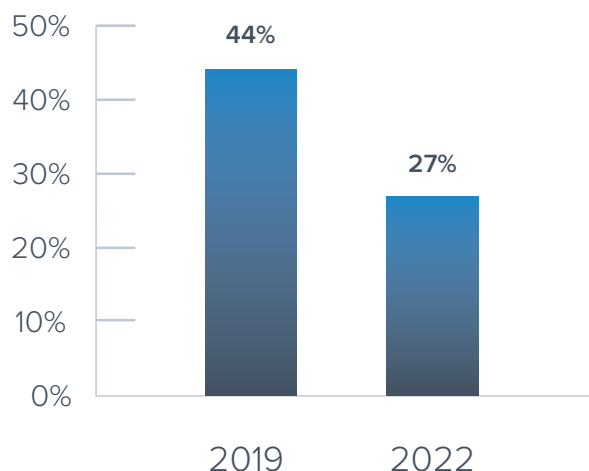
Viele Unternehmen fühlen sich nicht vollständig auf Ransomware vorbereitet

Über ein Viertel (27%) der befragten Unternehmen gab an, dass sie nicht vollständig darauf vorbereitet sind, mit einem Ransomware-Angriff umzugehen.

Dies ist eine Verbesserung gegenüber einer früheren Studie aus dem Jahr 2019, bei der fast die Hälfte (44%) sagte, sie wären nicht auf einen Ransomware-Angriff vorbereitet. Seit 2019 haben wir einige sehr medienwirksame Ransomware-Angriffe beobachtet, die zu erheblichen finanziellen Verlusten geführt haben. Die große Öffentlichkeitswirkung dieser Angriffe hat wahrscheinlich dazu geführt, dass viele Unternehmen in ihre Sicherheit investieren und sich auf mögliche Ransomware-Angriffe vorbereiten.

Nicht vollständig auf den Umgang mit Ransomware vorbereitet

(n=660 für 2019; n=1.350 für 2022)

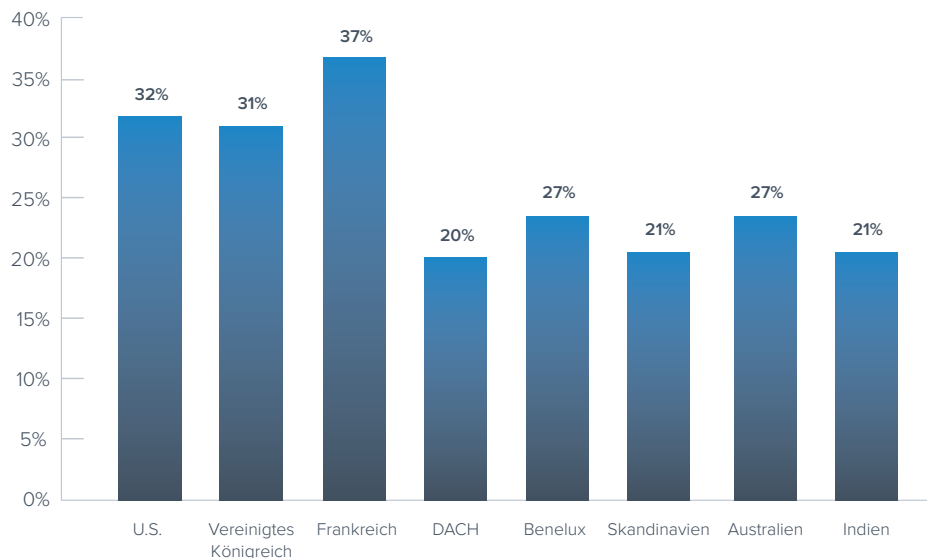


Frühere Untersuchungen von NordLocker ergaben, dass die USA, das Vereinigte Königreich, Kanada und Frankreich weltweit die meisten Ransomware-Angriffe verzeichnen. Unsere Untersuchungen haben ergeben, dass sich Befragte aus den USA, dem Vereinigten Königreich und Frankreich ebenfalls weniger darauf vorbereitet fühlen, mit Ransomware umzugehen.

Höchstwahrscheinlich fühlt sich die Anzahl der Angriffe überwältigend an, und die Unternehmen sind besorgt, dass das hohe Volumen die Erfolgchancen der Bedrohungsakteure erhöht. Größere Unternehmen fühlen sich auch weniger gut vorbereitet, da sie eine große Menge an Daten zu schützen haben und eine viel größere Angriffsfläche bieten.

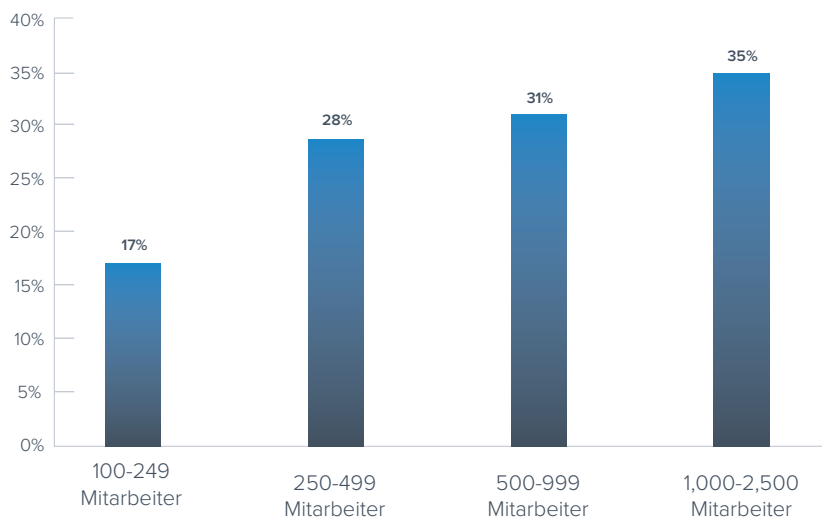
Nicht vollständig auf den Umgang mit Ransomware vorbereitet

(n=1,350)



Nicht vollständig auf den Umgang mit Ransomware vorbereitet

(n=1,350)



Weitere Informationen und praktische Hinweise zum Schutz vor Ransomware finden Sie in [Zahlen Sie kein Lösegeld – ein dreistufiger Leitfaden zum Ransomware-Schutz](#), der eine herunterladbare Checkliste zum Schutz vor Ransomware enthält, um Ihnen den Einstieg zu erleichtern.

Fazit

Unternehmen benötigen integrierte und mehrschichtige Sicherheitslösungen, um ihre immer größer werdende Angriffsfläche vor neuen Bedrohungen wie Ransomware zu schützen. Hier sind die wichtigsten Cybersecuritybereiche, auf die Sie sich konzentrieren sollten, um Ihr Risiko und Ihre Gefährdung durch Ransomware und andere Cyberbedrohungen zu minimieren.

- **Schützen Sie Ihre Zugangsdaten.** Der Schutz von Zugangsdaten erfordert einen zweigleisigen Ansatz: Investieren Sie zunächst in Erkennungs- und Reaktionstools und konzentrieren Sie sich dann auf die Schulung Ihrer Benutzer.
 - Die E-Mail-Schutztechnologie sollte in der Lage sein, bösartige Payloads zu erkennen, die über Links oder Anhänge übermittelt werden, und auch erkennen, wenn Angriffe fortgeschrittene [social engineering](#) Taktiken verwenden, die darauf abzielen, die Filtertechnologie zu umgehen und die Benutzer zum Handeln zu bewegen. Achten Sie auf E-Mail-Sicherheitslösungen, die [maschinelle Lerntechnologie](#) integriert, da diese Social-Engineering-Angriffe mit einem höheren Grad an Genauigkeit erkennen und nach den kleinsten Abweichungen von den üblichen Kommunikationsmustern suchen.
 - Außerdem ist es wichtig, dass Mitarbeitende wissen, wie sie verdächtige E-Mails erkennen und melden können. Verwenden Sie Tools wie [Phishing-Simulationen](#) und testen Sie die Effektivität von Schulungen.
- **Schützen Sie den Zugriff auf Konten, Applikationen und Netzwerke.** Die Multifaktor-Authentifizierung (MFA) ist nach wie vor eine Best Practice und sollte von jedem Unternehmen übernommen werden. Angreifer haben jedoch Wege gefunden, um MFA zu umgehen. Erwägen Sie die Implementierung einer fortschrittlicheren [Zero Trust](#) Zugriffsstrategie, die Benutzer und Geräte kontinuierlich überprüft und nur den richtigen Benutzern den Zugriff auf die richtigen Ressourcen ermöglicht.
- **Schützen Sie Ihre Web-Applikationen.** Online-Applikationen wie File-Sharing-Dienste, Webformulare und E-Commerce-Seiten können von Angreifern kompromittiert werden. Applikationen werden dabei oft über die Benutzeroberfläche oder eine API-Schnittstelle angegriffen.
- **Ziehen Sie die Implementierung** von API-basierter Anwendungssicherheit und einer Web Application Firewall in Betracht, die dank mehrschichtiger Security Advanced Threats blockiert, einschließlich Zero-Day-Angriffen, Verhindern von Eindringlingen und Sandboxing von Malware sowie leistungsstarke Netzwerksegmentierung, um eine laterale Ausbreitung innerhalb des Netzwerks zu verhindern.
- **Sichern Sie Ihre Daten.** Um Ihr Unternehmen vor den vollen Auswirkungen eines Ransomware-Angriffs zu schützen, müssen Daten ordnungsgemäß gesichert und isoliert werden – selbst wenn sie sich in der Cloud befinden. Ihr Daten-Backup muss auch die Wiederherstellung der Daten in einem angemessenen Zeitrahmen ermöglichen. Testen Sie daher regelmäßig Ihren Backup-Wiederherstellungsprozess zur Bestätigung seiner Funktionsweise.
- **Bauen Sie eine tiefgreifende Verteidigung mit Threat Intelligence, Incident Response und XDR auf.** Die Freisetzung von Ransomware ist häufig das letzte Stadium eines Angriffs und kann beispielsweise durch seitliche Bewegungen, Datenexfiltration, die Installation zusätzlicher Tools und mehr vorantreiben. Wenn Sie den Angriff in diesen frühen Stadien erkennen und abwehren können, sind Sie möglicherweise in der Lage, die vollen Auswirkungen der Ransomware zu verhindern.
- Hier kommen Dienste wie [XDR](#) ins Spiel. XDR (Extended Detection and Response) bietet Transparenz über eine gesamte IT-Umgebung, unterstützt durch kontinuierlich aktualisierte Bedrohungsinformationen. XDR und andere [automatisierte Incident Response-Lösungen](#) helfen Ihnen, Vorfälle zu identifizieren, einzudämmen und zu neutralisieren, bevor sie eskalieren.
- Außerdem ist es wichtig, dass Sie sich über die Entwicklung der Bedrohungslandschaft auf dem Laufenden halten, einschließlich der neuesten Verhaltensweisen und Tools der Angreifer, damit Sie wissen, worauf Sie achten und wie Sie reagieren müssen. Sie sollten alles untersuchen, was verdächtig aussieht oder sich nicht richtig anfühlt. Wenn Sie befürchten, dass Ihnen dazu die Ressourcen fehlen, sollten Sie die Dienste eines [ausgelagerten Security Operations Center](#), als Teil Ihrer XDR-Plattform in Betracht ziehen, das Ihr Netzwerk rund um die Uhr überwacht und anomales oder verdächtiges Verhalten untersucht.

About Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Meinung, dass jedes Unternehmen Zugang zu Cloud-basierten Sicherheitslösungen auf Unternehmensebene verdient, die einfach zu erwerben, bereitzustellen und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit der Entwicklung unserer Kunden wachsen und sich anpassen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Daher können Sie sich darauf konzentrieren, Ihr Unternehmen auf die nächste Stufe zu heben.

Weitere Informationen finden Sie unter barracuda.com.

About Vanson Bourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Der Ruf des Unternehmens für robuste und glaubwürdige forschungsbasierte Analysen beruht auf strengen Forschungsprinzipien und der Fähigkeit, die Meinungen hochrangiger Entscheidungsträger in allen technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und allen wichtigen Märkten einzuholen.

Weitere Informationen finden Sie unter vansonbourne.com.

