KEEPER
Cybersecurity Starts Here

2021
Studie zu den Folgen von Ransomware

Inhalt

Einleitung und Methodik

2021 wird als Jahr der Ransomware in die Geschichte eingehen. Die Häufigkeit der Angriffe steigt rapide an, und zunehmend sorgen aufsehenerregende Lösegeldforderungen für Schlagzeilen. Während Verbraucher in der Vergangenheit von den Auswirkungen relativ verschont blieben, sind auch sie heute von Bestandsausfällen und Problemen beim Zugriff auf bestimmte Dienste betroffen, da die dienstleistenden Unternehmen gezwungen sind, offline zu gehen.

Doch was passiert innerhalb eines Unternehmens nach einem Angriff? Inwiefern werden interne Prozesse beeinträchtigt? Welche Auswirkungen hat das auf die Effizienz und Produktivität der Mitarbeiter? Um dies herauszufinden, befragte Keeper in den USA 2000 Beschäftigte, deren Arbeitgeber in den letzten 12 Monaten von einem Ransomware-Angriff betroffen waren.

Keeper Security beauftragte Pollfish mit der Durchführung dieser Studie unter 2000 US-amerikanischen Vollzeitbeschäftigten. Dabei wurden nur die Unternehmen berücksichtigt, die in den letzten zwölf Monaten Opfer von Ransomware-Angriffen waren. Die Studie wurde im Juni 2021 abgeschlossen.

Die Folgen unzureichender Aufklärung zum Thema Cybersicherheit

Knapp ein Drittel der Mitarbeiter bis zum Angriff nicht ausreichend über Cybersicherheit informiert.

Dabei ist die Sensibilisierung der Beschäftigten für Cybersicherheit entscheidend, um Ransomware-Angriffe zu verhindern, insbesondere weil ein Großteil der Angriffe mittels Social Engineering erfolgen:

- Den Befragten zufolge waren Phishing-E-Mails Auslöser für 42 % der Ransomware-Angriffe.
- Weitere 23 % entfielen auf schädliche Websites.
- 21 % wurden durch kompromittierte Passwörter verursacht.

Trotzdem erklärten 29 % der Befragten gegenüber Keeper, dass sie nicht gewusst hätten, was Ransomware ist, bevor ihre Arbeitgeber betroffen waren. Daraus lässt sich schließen, dass viele, wenn nicht der Großteil der Ransomware-Angriffe durch folgende Maßnahmen verhindert werden könnte:

- Angemessene und routinemäßige Unterweisung der Beschäftigten zum Thema Cybersicherheit, insbesondere in der Vermeidung von Phishing und anderen Social Engineering-Methoden.
- Verpflichtung der Mitarbeitenden zur Nutzung starker, eindeutiger Passwörter für ihre Konten und Aktivierung der Multi-Faktor-Authentifizierung überall dort, wo sie unterstützt wird.

EIN TAG ZU SPÄT UND EIN DOLLAR ZU WENIG?

Die Befragten gaben an, dass 87 % der Unternehmen nach dem Angriff strengere Sicherheitsprotokolle einführten, 90 % ihre Mitarbeiter zusätzlich für Cybersicherheit sensibilisierten und 67 % ihre Ausgaben für Cybersicherheit erhöhten.

Zahlen oder nicht zahlen

Zwar sind sich alle einig, dass die Zahlung von Lösegeld zu weiteren Angriffen ermutigt, doch ob Unternehmen auf Ransomware-Forderungen eingehen sollten, ist selbst in der Sicherheits-Community umstritten. Denn wenn ein Unternehmen aktiv angegriffen wird, wird die Geschäftsführung von Kunden, Unternehmens-Stakeholdern und sogar von Cyber-Versicherern enorm unter Druck gesetzt, das Problem zu lösen und so schnell wie möglich wieder online zu gehen. Besonders hoch ist dieser Druck in Gesundheitseinrichtungen und im öffentlichen Sektor, wo Systemausfälle die Gesundheit und das Leben von Menschen gefährden können.

In diesem Zusammenhang erklärten 49 % der Befragten gegenüber Keeper, dass ihre Arbeitgeber das Lösegeld bezahlt hätten. Dieses Geld fiel jedoch nicht einfach vom Himmel: 93 % berichteten, dass nach der Lösegeldzahlung von ihrem Arbeitgeber die Mittel in anderen Bereichen gekürzt wurden.

Die hohen indirekten Kosten von Ransomware

Die Wiederherstellung nach einem Ransomware-Angriff ist mit hohen indirekten Kosten verbunden.

Während in den sozialen Medien stratosphärische Lösegeldforderungen kursieren, müssen sich Unternehmen infolge eines Angriffs mit zahlreichen indirekten Kosten und insbesondere mit Systemausfällen auseinandersetzen. Diese Ausfälle frustrieren nicht nur Kunden und Partner, sondern hindern auch die Beschäftigten daran, ihre Arbeit zu erledigen.

- 77 % der Befragten hatten nach dem Angriff vorübergehend keinen Zugang zu Systemen oder Netzwerken.
- 28 % der Ausfälle dauerten eine Woche oder länger an.
- 26 % der Befragten waren für mindestens eine Woche nicht in der Lage, ihre Aufgaben ungehindert zu erledigen.

Selbst nach der Wiederinbetriebnahme der Systeme sind Unternehmen damit beschäftigt, die nötigen Änderungen vorzunehmen, um weitere Angriffe zu verhindern. Die überwältigende Mehrheit der Befragten (83 %) gab an, dass ihre Unternehmen neue Software installiert oder andere wichtige Aktualisierungen, wie die Migration von Datensätzen in die Cloud, vorgenommen haben.

In den meisten Fällen beeinträchtigte die Einführung dieser Änderungen die Produktivität und brachte indirekte Wiederherstellungskosten mit sich. 71 % der Befragten gaben an, dass der Prozess der Installation neuer Software und Updates umständlich war bzw. die Produktivität beeinträchtigte.

- 64 % der Befragten verloren Zugangsdaten oder Dokumente.
- 38 % berichteten von Programm- oder Anwendungsproblemen.
- 33 % sahen sich mit einem enormen Lernprozess zu neuen Protokollen konfrontiert.
- 40 % verloren Zeit durch häufige Computer-Neustarts und Updates.
- 43 % mussten sich immer wieder neu in Programme/Konten einloggen (konnten also nicht dauerhaft angemeldet bleiben).
- 21 % berichteten, dass ihre normalen Online-Tools und Anwendungen nicht mehr verfügbar waren.

Noch dazu waren die IT-Abteilungen überlastet, gerade als die Mitarbeiter am dringendsten IT-Support benötigten, um ihre Passwörter zurückzusetzen, verlorene Dokumente wiederherzustellen und Hilfestellung bei neuen Anwendungen und Protokollen zu erhalten. Mehr als ein Drittel (36 %) der Befragten gab an, dass sie nach dem Angriff für nicht sicherheitsrelevante Fragen nur begrenzten Zugang zu IT-Support hatten.

Anteil der nicht gemeldeten Angriffe

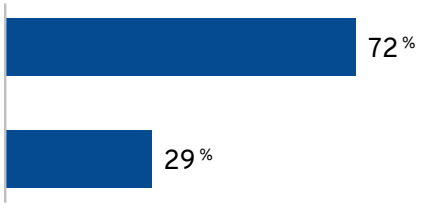
Ransomware-Angriffe sind weiter verbreitet als man denkt, denn häufig wird nicht darüber gesprochen.

Zusätzlich zu dem Druck für die Geschäftsleitung, das Lösegeld zu zahlen, um weiterarbeiten zu können, sind 64 % der Befragten der Meinung, dass ein Ransomware-Angriff negative Auswirkungen auf den Ruf ihres Unternehmens hätte. Ferner gaben 63 % der Beschäftigten an, dass der Angriff auch bei ihnen persönlich zu einem Vertrauensverlust gegenüber ihrem Unternehmen geführt hat.

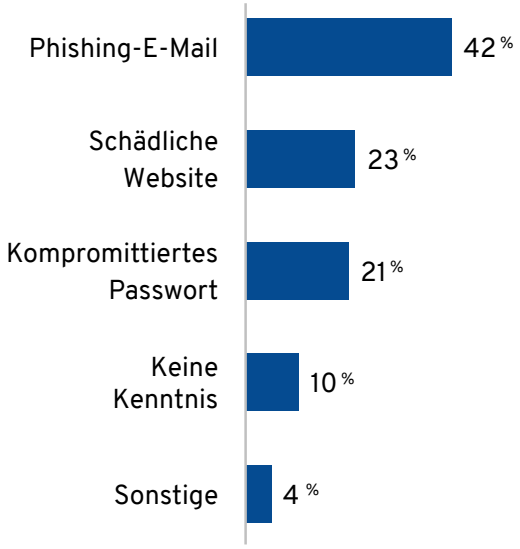
Vor diesem Hintergrund ist es nicht verwunderlich, dass 26 % der Befragten angaben, dass ihre Arbeitgeber über den Angriff nur Partnern und Kunden (und nicht der breiten Öffentlichkeit) gegenüber Auskunft erteilten, während 15 % es ganz und gar für sich behielten. Dies deutet darauf hin, dass Ransomware-Angriffe wahrscheinlich weitaus verbreiteter sind, als man sich vorstellen kann.

Vollständige Daten

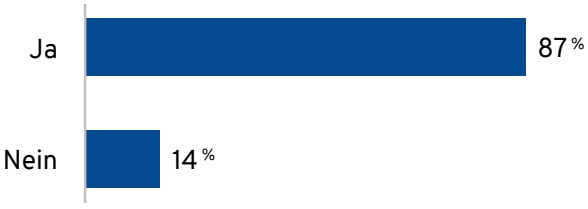
F1. Konnten Sie vor dem Angriff mit dem Begriff Ransomware etwas anfangen?



F2. Was war die Ursache für den Ransomware-Angriff auf Ihr Unternehmen?

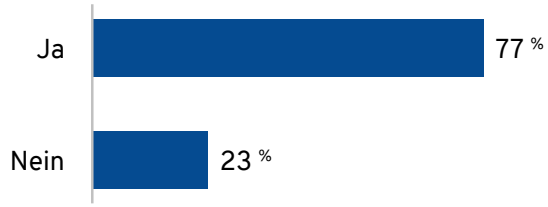


F3. Wurden in Ihrem Unternehmen als Folge des Ransomware-Angriffs strengere Sicherheitsprotokolle eingeführt?

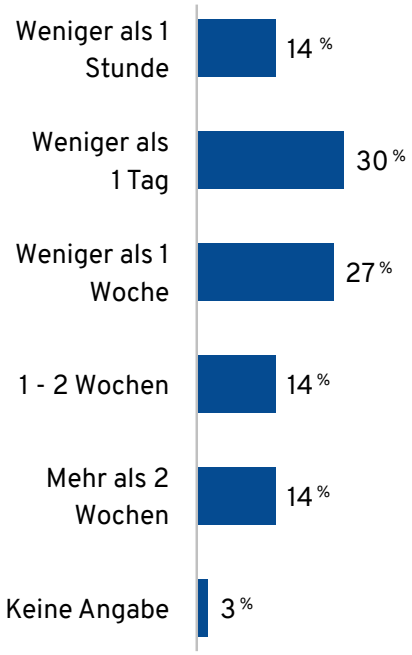


Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

F4. Musste Ihr Unternehmen aufgrund des Ransomware-Angriffs für einen gewissen Zeitraum offline gehen (also den Zugriff auf Systeme oder Netzwerke unterbinden)?

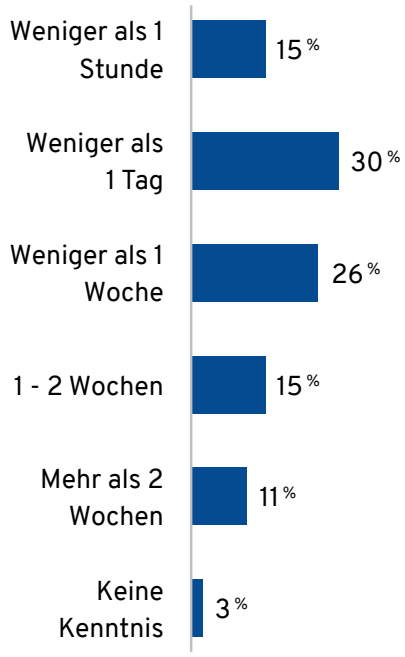


F5. Wenn ja, wie lange musste Ihr Unternehmen vom Netz gehen?

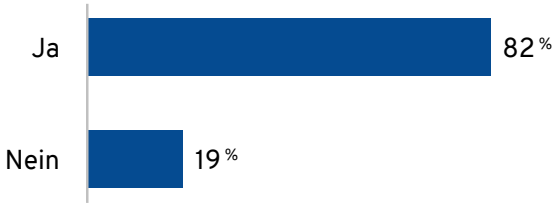


Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

F6. Wenn ja, wie lange konnten Sie Ihre Arbeit nicht ungehindert ausüben?



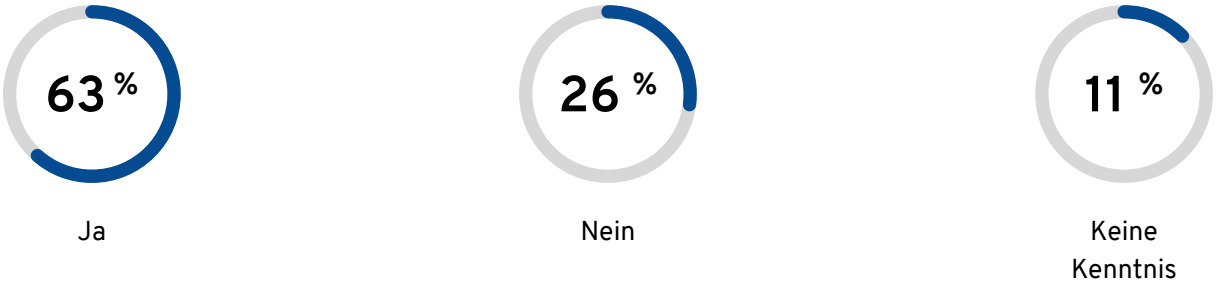
F7. Haben Sie den Eindruck, dass die Geschäftsleitung Ihres Unternehmens nach dem Ransomware-Angriff effektiv mit den Beschäftigten kommuniziert hat?



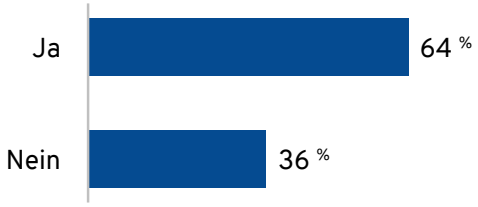
F8. Hat Ihr Unternehmen Kunden und Partner über den Angriff informiert?

Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

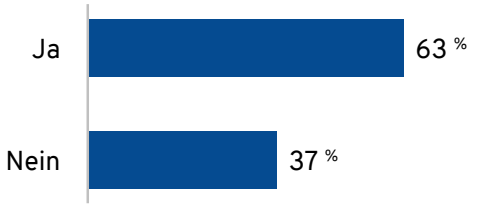
F9. Hat Ihr Unternehmen eine öffentliche Stellungnahme zu dem Angriff abgegeben?



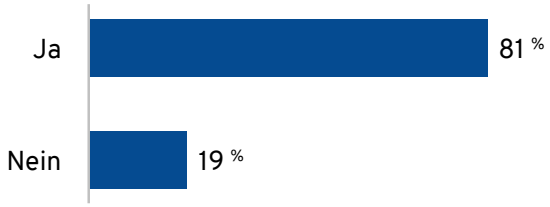
F10. Haben Sie den Eindruck, dass sich der Ransomware-Angriff negativ auf den Ruf Ihres Unternehmens ausgewirkt hat?



F11. Hat der Ransomware-Angriff Ihr Vertrauen in Ihr Unternehmen beeinträchtigt?

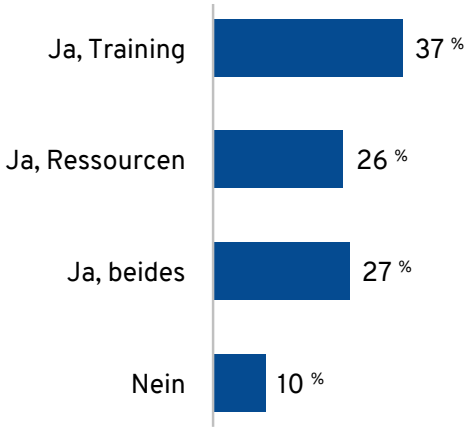


F12. Haben Sie vor dem Ransomware-Angriff regelmäßig Software-Updates installiert, wenn Sie dazu aufgefordert wurden?

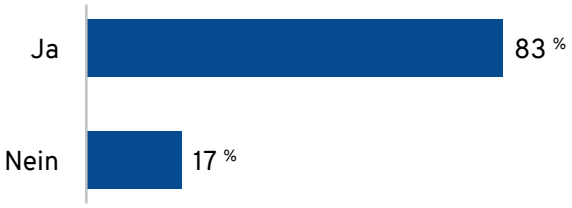


Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

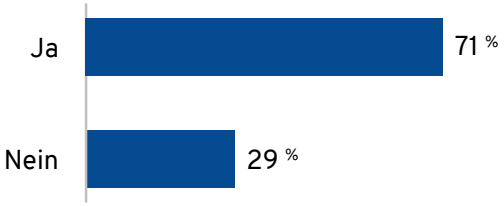
F13. Wurden Sie von Ihrem Unternehmen nach dem Angriff über Cybersicherheit aufgeklärt bzw. diesbezüglich mit Tools ausgestattet?



F14. Wurden in Ihrem Unternehmen nach dem Angriff spezielle Anwendungen installiert oder wichtige technische Aktualisierungen vorgenommen (z. B. Verschieben von Datensätzen in die Cloud)?

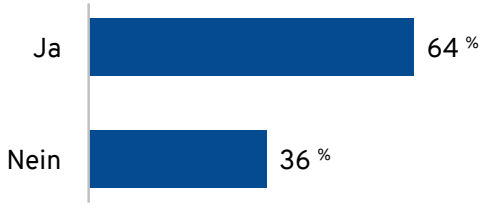


F15. Wenn ja, haben Sie festgestellt, dass durch die Installation der neuen Software bzw. durch die Aktualisierungen irgendwelche Unannehmlichkeiten entstanden sind oder die Produktivität beeinträchtigt wurde?

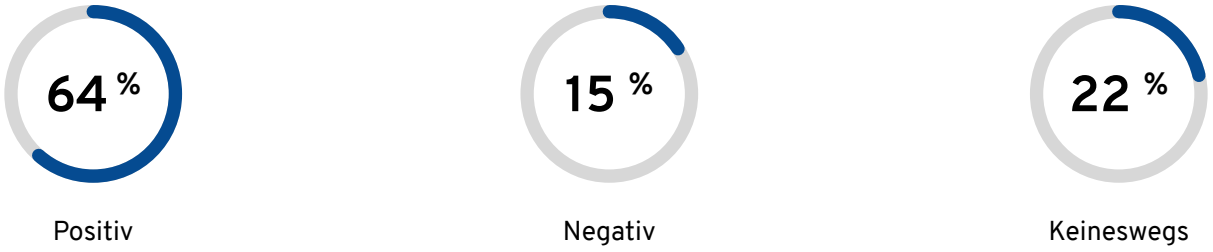


Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

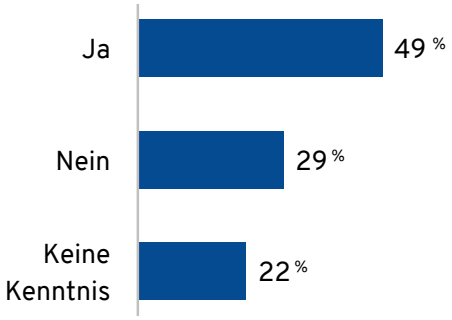
F16. Wenn ja, haben Sie bei der Aktualisierung Ihrer Geräte Informationen, wie Zugangsdaten oder Dokumente, verloren?



F17. Wenn ja, wie haben sich die Aktualisierungen auf Ihren Arbeitsalltag ausgewirkt?

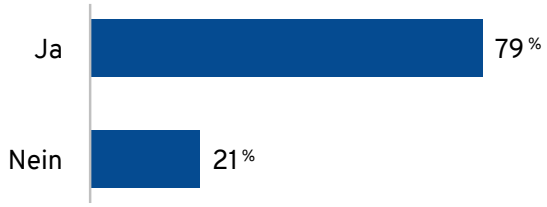


F18. Wurde das Lösegeld von Ihrem Unternehmen gezahlt?



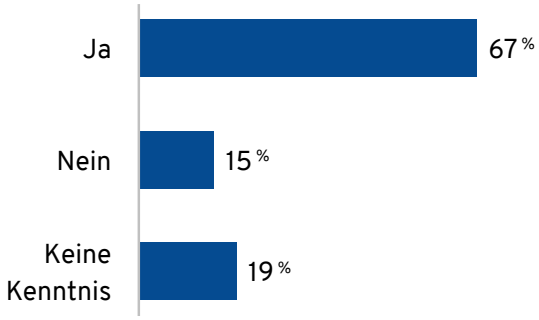
Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

F19. Wenn ja, wurde der Betrag den Beschäftigten gegenüber offengelegt?



F20. Wenn ja, ist Ihnen aufgefallen, dass nach der Zahlung in Ihrem Unternehmen die Budgets in anderen Bereichen gekürzt wurden?

F21. Wurden die Aufwendungen für Cybersicherheit nach dem Angriff in Ihrem Unternehmen erhöht?



Anmerkung zu den Befragungsergebnissen: durch Aufrunden können einige Antworten leicht über 100% liegen.

Über Keeper

Keeper schützt Unternehmen vor Ransomware-Angriffen mit robuster Administration, Kontrolle und Transparenz durch eine hohe Passwortsicherheit und Dark Web-Echtzeitmonitoring.

Die Zero Knowledge-Passwortsicherheits- und Verschlüsselungsplattform von Keeper hilft Tausenden von Unternehmen auf der ganzen Welt, passwortbezogene Cyberangriffe zu verhindern, die Produktivität zu verbessern und Compliance durchzusetzen.

Keeper gewährt IT-Administratoren eine vollständige Übersicht über die Passwortpraktiken der Mitarbeiter und ermöglicht es ihnen, die Umsetzung der Passwortvorgaben zu überwachen und Passwort-Sicherheitsrichtlinien unternehmensweit durchzusetzen, einschließlich starker, eindeutiger Passwörter und Multi-Faktor-Authentifizierung (2FA). Fein abgestufte Zugriffskontrollen ermöglichen es Administratoren, die Zugriffsrechte von Mitarbeitern je nach Funktion und Zuständigkeit festzulegen und gemeinsame Ordner für einzelne Teams, z. B. für Aufgabenbereiche oder Projektteams, einzurichten.

Zusätzliche Sicherheit erzielen Unternehmen durch den Einsatz praktischer Add-ons, wie Keeper Secure File Storage, mit dem Mitarbeitende Dokumente, Bilder, Videos und sogar digitale Zertifikate und SSH-Schlüssel sicher speichern und austauschen können, und BreachWatch™, das Dark Web-Foren scannt und IT-Administratoren benachrichtigt, wenn die Passwörter von Mitarbeitern bei einem öffentlichen Datenbruch kompromittiert wurden.

Keeper ist nach SOC-2, FIPS 140-2 und ISO 27001 zertifiziert und für die Nutzung durch die US-Bundesregierung über das System for Award Management (SAM) gelistet. Keeper schützt Unternehmen jeglicher Größe in allen wichtigen Wirtschaftszweigen.

Mehr Informationen erhalten Sie unter **keeper.io/ransomware-impact**.