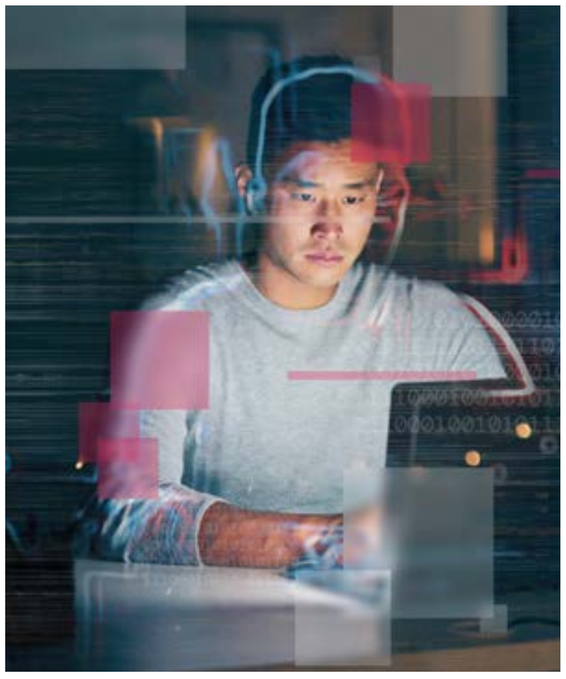
Ransomware-Angreifer nehmen Führungskräfte ins Visier

THREATLABZ RESEARCH

Die Berichterstattung über Ransomware-Angriffe konzentriert sich oft auf die betroffenen Unternehmen, die gestohlenen Daten, die Malware-Tools und die Höhe der Lösegeldzahlungen. Hingegen liegen kaum Daten darüber vor, welche Personen innerhalb der Unternehmen Bedrohungsakteure konkret ins Visier nehmen. Eine neue Studie von ThreatLabz schließt diese Lücke und untersucht, welche Rollen und Geschäftsfunktionen am häufigsten unter den anvisierten Opfern vertreten sind. Die Ergebnisse zeigten, dass Ransomware-Angreifer keineswegs wahllos Einzelpersonen in Unternehmen aufs Korn nehmen. Im Gegenteil haben sie es auf bestimmte Mitarbeitende mit privilegierten Rollen und geschäftskritischen Funktionen abgesehen, um ihre Chancen zu erhöhen, sich im Netzwerk einzunisten und auszubreiten, vertrauliche Daten zu exfiltrieren und ihren Zugriff zu monetarisieren.

Methodik

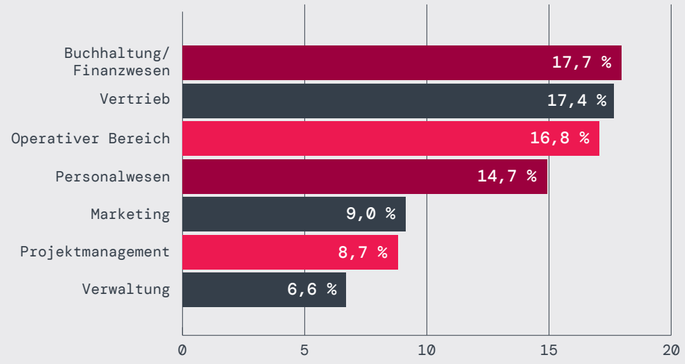
Innerhalb eines Monats identifizierte ThreatLabz 351 kompromittierte Opfer in 334 Unternehmen in Verbindung mit einem Bedrohungsakteur, der sich darauf spezialisiert hat, sich Erstzugriff zu verschaffen, um große Mengen an Unternehmensdaten zu stehlen und kritische Systeme selektiv zu verschlüsseln.



Haupterkenntnisse

62 % der Opfer waren leitende Angestellte (mittlere Führungsebene oder höher)

GESCHÄFTSKRITISCHE POSITIONEN WURDEN ANVISIERT

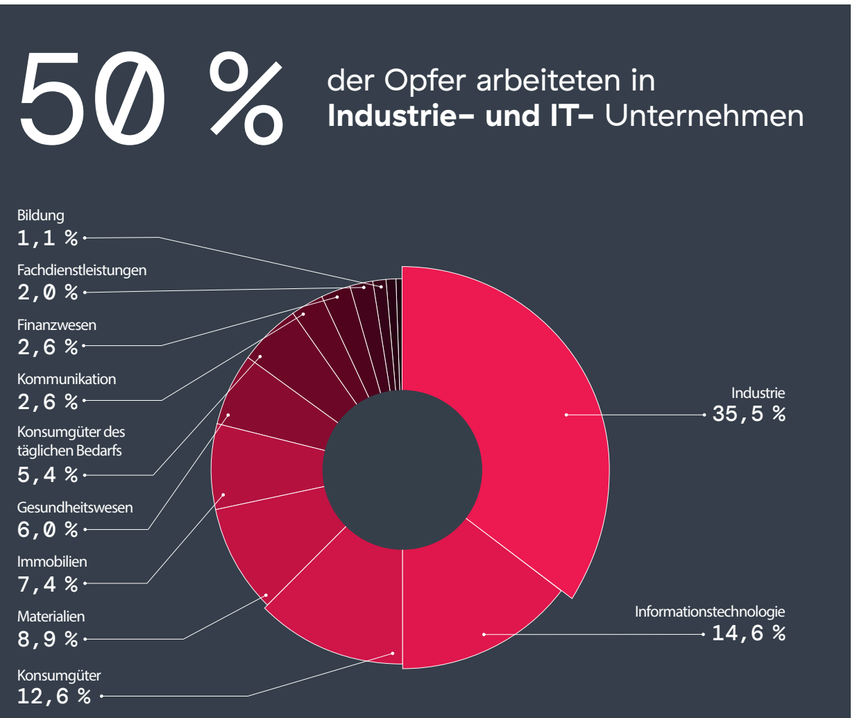


Die Generation X stellte den **größten Anteil der Opfer:**

44 %

Durchschnittsalter: 46
Millennials: **33 %**
Gen Z: **14 %**
Babyboomer: **9 %**

50 % der Opfer arbeiteten in **Industrie- und IT-** Unternehmen



4,6 % Unternehmen mit mehr als einem kompromittierten Mitarbeiter

Ransomware -Opfer im Überblick

- Die Opfer dieses Ransomware-Angreifers **waren überwiegend leitende Angestellte auf mittlerer Führungsebene oder höher.** Dies deutet darauf hin, dass die Angreifer Angestellte ins Visier nehmen, die über privilegierten Zugriff auf Kundendaten, Finanzunterlagen, Verträge und operative Systeme verfügen.
- **Mehr als 75 % der Opfer stammten** aus fünf Abteilungen: Buchhaltung/Finanzwesen, Vertrieb, operativer Bereich, Personalwesen und Marketing.
- Die Opfer kamen aus verschiedenen Altersgruppen, von 23 bis 70 Jahren, **konzentrierten sich aber auf die Altersgruppe Mitte bis Ende 40, wobei die Generation X** 43,9 % der Opfer ausmachte.
- Auf Organisationsebene **stammten 50 % der betroffenen Unternehmen aus nur zwei Sektoren:** Industrie (35,5 %) und Informationstechnologie (14,6 %).
- Bei mehr als einem Dutzend Unternehmen waren **mehrere Mitarbeiter betroffen.**

Typische Opferprofile

Diese Profile liefern Beispiele aus der realen Welt für Ransomware-Opfer und erklären, warum diese möglicherweise ins Visier geraten.

Regionaler Vertrieb Manager

Branche: Industrie

Warum für Angreifer attraktiv: Zugriff auf Kundenkonten, laufende Geschäfte, Verträge, Preisinformationen und Umsatzdaten

Leiter der Kreditorenbuchhaltung

Branche: Informationstechnologie

Warum für Angreifer attraktiv: Zugriff auf Zahlungsdaten, Rechnungen, Finanzgenehmigungen und Lieferantendatensätze

Immobilienverwalter

Branche: Immobilien

Warum für Angreifer attraktiv: Zugriff auf Mietverträge, Lieferantenrechnungen, Verträge, Kundendaten und Finanzinformationen

Leitender Projektmanager

Branche: Konsumgüter des täglichen Bedarfs

Warum für Angreifer attraktiv: Zugriff auf Projektbudgets, Lieferantenverträge und vertrauliche Dateien oder Dokumente

Lektion für Unternehmen: Hochrisiko-User schützen

Diese Kampagne unterstreicht eine entscheidende Priorität der Ransomware-Abwehr: die Stärkung der Kontrollen rund um die User und Arbeitsabläufe mit Zugriff auf vertrauliche Geschäftsdaten. Wenn Angreifer Mitarbeiter in den Bereichen Vertrieb, Finanzen, Buchhaltung oder Betrieb ins Visier nehmen, kann ein einziges kompromittiertes Konto ein unternehmensweites Risiko darstellen.

Die Angreifer nutzen Dringlichkeit, IT-Imitation und vertraute Tools wie Microsoft Teams und Quick Assist, um Vertrauen zu gewinnen. Von dort aus eskaliert das Risiko schnell zu Diebstahl von Zugangsdaten, Fernzugriff, lateraler Bewegung, Datendiebstahl, potenzieller Dateiverschlüsselung und letztendlich Erpressung.

Die Prävention von Ransomware darf nicht mit der Malware-Erkennung enden. Sie muss auch die Mitarbeitenden berücksichtigen, deren Zugriffsrechte im Falle einer Kompromittierung das größte Geschäftsrisiko darstellen.

Um dieses Risiko zu verringern, empfehlen wir folgende Maßnahmen:

- Implementieren Sie Segmentierung mittels einer Zero-Trust-Architektur, um laterale Bewegungen zu verhindern und die Angriffsfläche zu verringern.
- Schulen Sie die Mitarbeiter darin, Anfragen von „IT-Mitarbeitern“ anhand der im Firmenverzeichnis bereitgestellten Informationen zu überprüfen.
- Blockieren Sie externe Sofortnachrichten und Anrufe auf Kooperationsplattformen wie Microsoft Teams und Slack.
- Zugriffsrechte sollten nach dem Prinzip der minimalen Rechtevergabe so weit wie möglich eingeschränkt werden, um den Zugriff auf vertrauliche Systeme und Daten zu begrenzen.
- Setzen Sie KI-gestützten Inline-Bedrohungsschutz und Endgerätesicherheit ein, um Angriffe zu erkennen und zu stoppen.
- Die Aktivitäten von Usern, Geräten und Anwendungen sollten kontinuierlich auf Anzeichen einer Gefährdung überwacht werden.

© 2026 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.