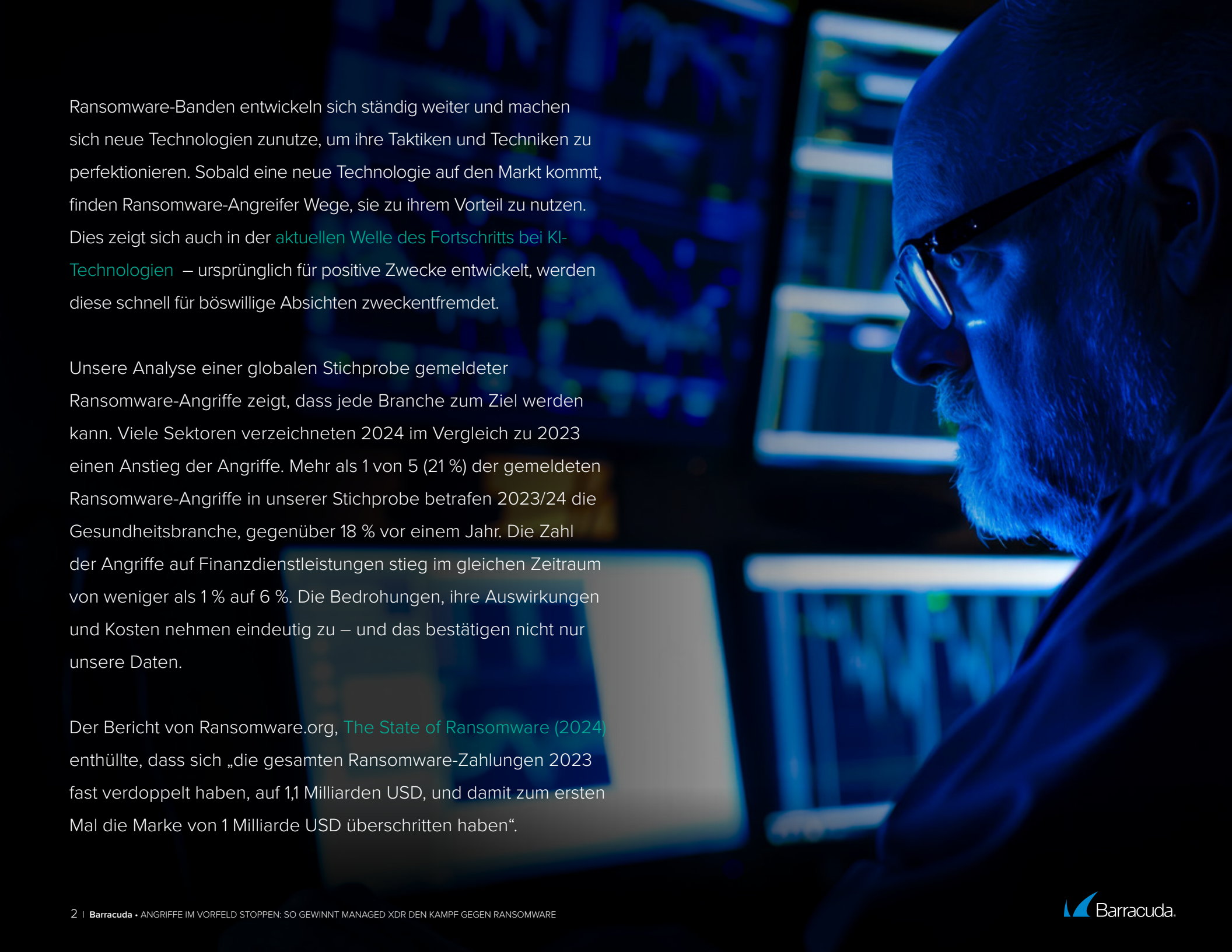
Angriffe im Vorfeld stoppen: So gewinnt Managed XDR den Kampf gegen Ransomware

Barracuda



Ransomware-Banden entwickeln sich ständig weiter und machen sich neue Technologien zunutze, um ihre Taktiken und Techniken zu perfektionieren. Sobald eine neue Technologie auf den Markt kommt, finden Ransomware-Angreifer Wege, sie zu ihrem Vorteil zu nutzen. Dies zeigt sich auch in der aktuellen Welle des Fortschritts bei KI-Technologien – ursprünglich für positive Zwecke entwickelt, werden diese schnell für böswillige Absichten zweckentfremdet.

Unsere Analyse einer globalen Stichprobe gemeldeter Ransomware-Angriffe zeigt, dass jede Branche zum Ziel werden kann. Viele Sektoren verzeichneten 2024 im Vergleich zu 2023 einen Anstieg der Angriffe. Mehr als 1 von 5 (21 %) der gemeldeten Ransomware-Angriffe in unserer Stichprobe betrafen 2023/24 die Gesundheitsbranche, gegenüber 18 % vor einem Jahr. Die Zahl der Angriffe auf Finanzdienstleistungen stieg im gleichen Zeitraum von weniger als 1 % auf 6 %. Die Bedrohungen, ihre Auswirkungen und Kosten nehmen eindeutig zu – und das bestätigen nicht nur unsere Daten.

Der Bericht von Ransomware.org, The State of Ransomware (2024) enthüllte, dass sich „die gesamten Ransomware-Zahlungen 2023 fast verdoppelt haben, auf 1,1 Milliarden USD, und damit zum ersten Mal die Marke von 1 Milliarde USD überschritten haben“.

Barracuda

Wie dringen Ransomware-Angriffe in Organisationen ein?

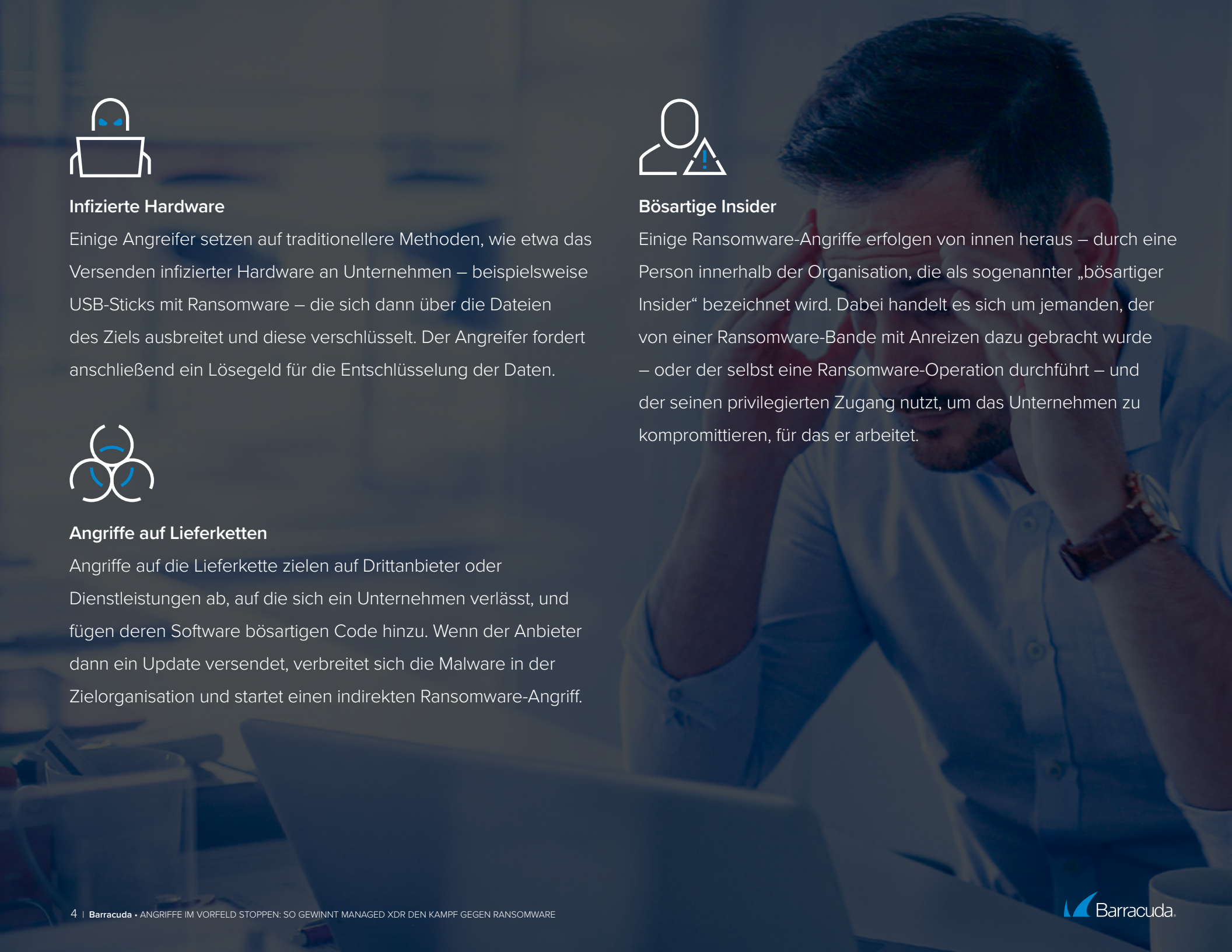
Ransomware-Angreifer nutzen zahlreiche Taktiken und Einstiegspunkte, um in Organisationen einzudringen. Viele Angreifer versuchen gleichzeitig mehrere Ansätze, bis ihnen der Zugriff auf das Zielnetzwerk gelingt. Zu diesen Taktiken gehören:

Phishing/Vishing/Quishing/Smishing

Dabei kommen der Reihenfolge nach E-Mail-Konten, Sprachanrufe und Nachrichten, QR-Codes und SMS-Nachrichten zum Einsatz. Bei diesen Angriffen werden schädliche Links an die Zielperson gesendet, normalerweise an deren Geschäftskonto oder Gerät. Ziel ist es, den Benutzer dazu zu bringen, auf einen Link zu klicken und Anmeldedaten einzugeben, die der Angreifer dann nutzen kann, um ins Netzwerk einzudringen, oder das Opfer dazu zu bringen, bösartige Anhänge herunterzuladen.

Ausnutzen von ungepatchten oder unbekannten (Zero-Day) Software-Schwachstellen

Manchmal gelingt es einem Angreifer, eine Schwachstelle in einer Software zu identifizieren, bevor der Anbieter oder die Organisation sie erkennt. So kann er die ungepatchte Schwachstelle ausnutzen und bösartigen Code einfügen, um Daten zu stehlen. Dies wird als Zero-Day-Angriff bezeichnet. Ransomware-Banden scannen Netzwerke außerdem aktiv nach bekannten Schwachstellen, die noch nicht gepatcht wurden, und greifen diese gezielt an.



Infizierte Hardware

Einige Angreifer setzen auf traditionellere Methoden, wie etwa das Versenden infizierter Hardware an Unternehmen – beispielsweise USB-Sticks mit Ransomware – die sich dann über die Dateien des Ziels ausbreitet und diese verschlüsselt. Der Angreifer fordert anschließend ein Lösegeld für die Entschlüsselung der Daten.

Angriffe auf Lieferketten

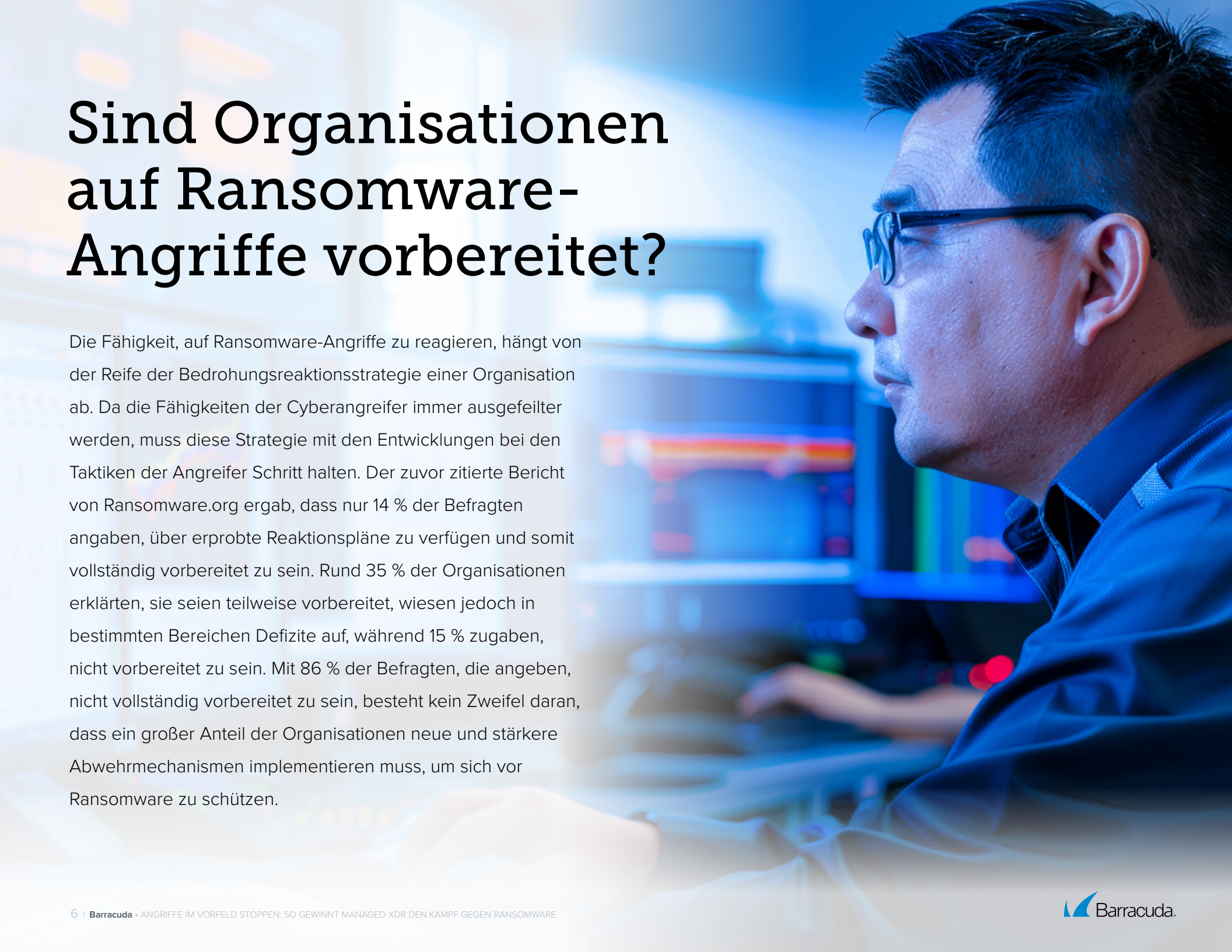
Angriffe auf die Lieferkette zielen auf Drittanbieter oder Dienstleistungen ab, auf die sich ein Unternehmen verlässt, und fügen deren Software bösartigen Code hinzu. Wenn der Anbieter dann ein Update versendet, verbreitet sich die Malware in der Zielorganisation und startet einen indirekten Ransomware-Angriff.

Bösartige Insider

Einige Ransomware-Angriffe erfolgen von innen heraus – durch eine Person innerhalb der Organisation, die als sogenannter „bösartiger Insider“ bezeichnet wird. Dabei handelt es sich um jemanden, der von einer Ransomware-Bande mit Anreizen dazu gebracht wurde – oder der selbst eine Ransomware-Operation durchführt – und der seinen privilegierten Zugang nutzt, um das Unternehmen zu kompromittieren, für das er arbeitet.

Dies sind nur einige der Möglichkeiten, wie Ransomware-Angreifer in Organisationen eindringen können. Dabei entwickeln Angreifer ständig neue Methoden. Ein hilfreicher Vergleich zur Verdeutlichung des Schutzes gegen all diese Eintrittspunkte ist die Sicherheit eines Hauses. Ein umfassendes Security-System mit Überwachungskameras, Einbruchmeldeanlagen, fortschrittlichen Schließsystemen und automatisierten Warnmeldungen bietet einen wesentlich besseren Schutz als ein System, das sich nur auf verschlossene Türen verlässt. Die Kombination aus Erkennung und Reaktion in Ihrem Security-Konzept, zusätzlich zu den eher traditionellen Abwehrmethoden, sorgt für einen deutlich besseren Schutz.

Sind Organisationen auf Ransomware-Angriffe vorbereitet?



Die Fähigkeit, auf Ransomware-Angriffe zu reagieren, hängt von der Reife der Bedrohungsreaktionsstrategie einer Organisation ab. Da die Fähigkeiten der Cyberangreifer immer ausgefeilter werden, muss diese Strategie mit den Entwicklungen bei den Taktiken der Angreifer Schritt halten. Der zuvor zitierte Bericht von Ransomware.org ergab, dass nur 14 % der Befragten angaben, über erprobte Reaktionspläne zu verfügen und somit vollständig vorbereitet zu sein. Rund 35 % der Organisationen erklärten, sie seien teilweise vorbereitet, wiesen jedoch in bestimmten Bereichen Defizite auf, während 15 % zugaben, nicht vorbereitet zu sein. Mit 86 % der Befragten, die angeben, nicht vollständig vorbereitet zu sein, besteht kein Zweifel daran, dass ein großer Anteil der Organisationen neue und stärkere Abwehrmechanismen implementieren muss, um sich vor Ransomware zu schützen.

Barracuda.

Einführung von Managed Extended Detection and Response (XDR)

Die Stärkung der Erkennungs- und Reaktionssysteme Ihres Unternehmens ist eine verlässliche Methode, um die Wirksamkeit Ihrer Ransomware-Schutzstrategie zu erhöhen. Oft merken Unternehmen monatelang nicht, dass sie kompromittiert wurden, was den Schaden und die Wiederherstellungszeit erheblich erhöht

Wie lange dauert die Behebung in der Regel?

	Ohne XDR	Mit XDR
Typische BEC-Behebung (nur Gateway)	1 - 2 Monate	**1 - 2 Stunden**
Behebung von Identitätsdiebstahl	3-4 Wochen	**1 - 2 Stunden**
Behebung von Malware-Infektionen	3-4 Wochen	**Ungefähr 1 Stunde**
Lösung von Insider-Bedrohungen	3–6 Monate	**~ 4 Stunden**
Behebung von Erpressungsversuchen ohne XDR	Variabel	**< 24 Stunden**

Barracuda

Doch die Security-Teams vieler Unternehmen stehen bereits unter Zeitdruck und hoher Arbeitsbelastung und können ihren immer länger werdenden Aufgabenlisten keine weiteren Aufgaben hinzufügen.

Eine Umfrage von Cybersecurity Insiders aus dem Jahr 2022, The State of Extended Detection and Response, ergab, dass 52 % der Organisationen den Mangel an qualifiziertem Security-Personal als größte Herausforderung für ihre Cybersecurity nannten. Die Lösung, laut Ransomware.org: „Erweitern Sie Ihre internen Fähigkeiten zur Reaktion auf Ransomware mit ausgelagerten und/oder verwalteten Diensten von vertrauenswürdigen Partnern." Die Implementierung einer verwalteten XDR-Lösung ist ein äußerst effektiver Weg, um die umfassenden Erkennungs- und Reaktionsfähigkeiten einzuführen, die Organisationen benötigen, um ihre Cybersicherheitsarchitektur zu stärken – insbesondere bei einem Mangel an Fachkräften.

Managed XDR bietet ein zentrales Repository für Sicherheitsdaten und Telemetrie sowie eine Analysefunktion, um diese Daten zu interpretieren und die Bedrohungserkennung zu beschleunigen. Managed XDR bietet außerdem automatisierte Reaktionen auf Vorfälle auf Grundlage zuvor vereinbarter Leitfäden und Pläne. Darüber hinaus überprüfen und sammeln Netzwerkerkennungs- und Reaktionssysteme Protokolle von Netzwerkgeräten und analysieren den Datenverkehr, der in das Unternehmensnetzwerk eintritt, es verlässt und es durchquert.

Managed XDR integriert Sicherheitsdaten aus all diesen Quellen – und weiteren. Security-Analysten können diese Daten dann auswerten, Bedrohungen eindämmen oder den Unternehmen Anleitungen für Abhilfemaßnahmen zur Verfügung stellen, um die Erkennung zu beschleunigen und die Reaktionszeiten zu verkürzen. Dies ermöglicht bessere Einblicke und hilft, echte Bedrohungen von falschen Alarmen zu unterscheiden. Rund 72 % der Befragten der Cybersecurity Insiders-Umfrage stimmten zu, dass Managed XDR eine wichtige grundlegende Plattform ist.

Wie XDR Ihre Security verbessert

Die Erkennungsfunktion von XDR verschafft Unternehmen einen besseren Überblick über den Zustand ihres Netzwerks und alle Bedrohungen – ob Ransomware oder andere Angriffsformen –, die versuchen, in das Netzwerk einzudringen. Das lässt sich mit einer Überwachungskamera im Bereich der Haussicherheit vergleichen: Man hat stets im Blick, was im digitalen Umfeld passiert. Diese „Kamera“ zeichnet sich durch höhere Genauigkeit und bessere Analysefähigkeiten aus als ein Mensch, der Bedrohungen manuell überprüft. XDR kann Bedrohungen wie IP-Adressen, Domains und Datei-Hashes blockieren, die als bösartig identifiziert werden – ähnlich wie ein zuverlässiges Schließsystem Eindringlinge vom Zugang abhält.

Automatisierung ist ein zentraler Bestandteil von XDR und beschleunigt die Reaktion auf Vorfälle erheblich. Automatisierte Reaktionen und Warnmeldungen, vergleichbar mit einem Alarmsystem für Ihr Zuhause, ermöglichen eine schnelle Reaktion auf Sicherheitsbedrohungen und informieren die zuständigen Personen. Ein weiterer wichtiger Vorteil ist die Vereinfachung: Sie benötigen nicht mehrere Einzellösungen verschiedener Anbieter für die Erkennung von und Reaktion auf Bedrohungen, wenn Sie eine verwaltete XDR-Lösung haben. Außerdem vereinfacht sie das Reporting sowohl für die Datenanalyse als auch für die Compliance, denn sie protokolliert alle potenziellen Bedrohungen, Warnungen und automatischen Reaktionen mit einem zentralisierten Berichtssystem, genau wie die Ereignisprotokolle, die von Haussicherheitssystemen erstellt werden. Mehr über die Funktionsweise von XDR und die Vorteile für Unternehmen erfahren Sie in unserem eBook, XDR erklärt: A Stretegischer Ansatz für Threat Management.

Um mehr darüber zu erfahren, wie Managed XDR die Cybersecurity Ihres Unternehmens stärken könnte, besuchen Sie unsere Website. Sie können auch erfahren, wie Barracuda die Erkennung beschleunigen und Ihre Reaktionszeit mit einem rund um die Uhr verwalteten XDR-Service verkürzen kann.

Barracuda

Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu erwerben, zu implementieren und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen. Hunderttausende Unternehmen weltweit vertrauen auf den Schutz und die Unterstützung von Barracuda, damit sie sich ganz auf ihr Wachstum konzentrieren können. Weitere Informationen finden Sie auf de.barracuda.com.

Barracuda