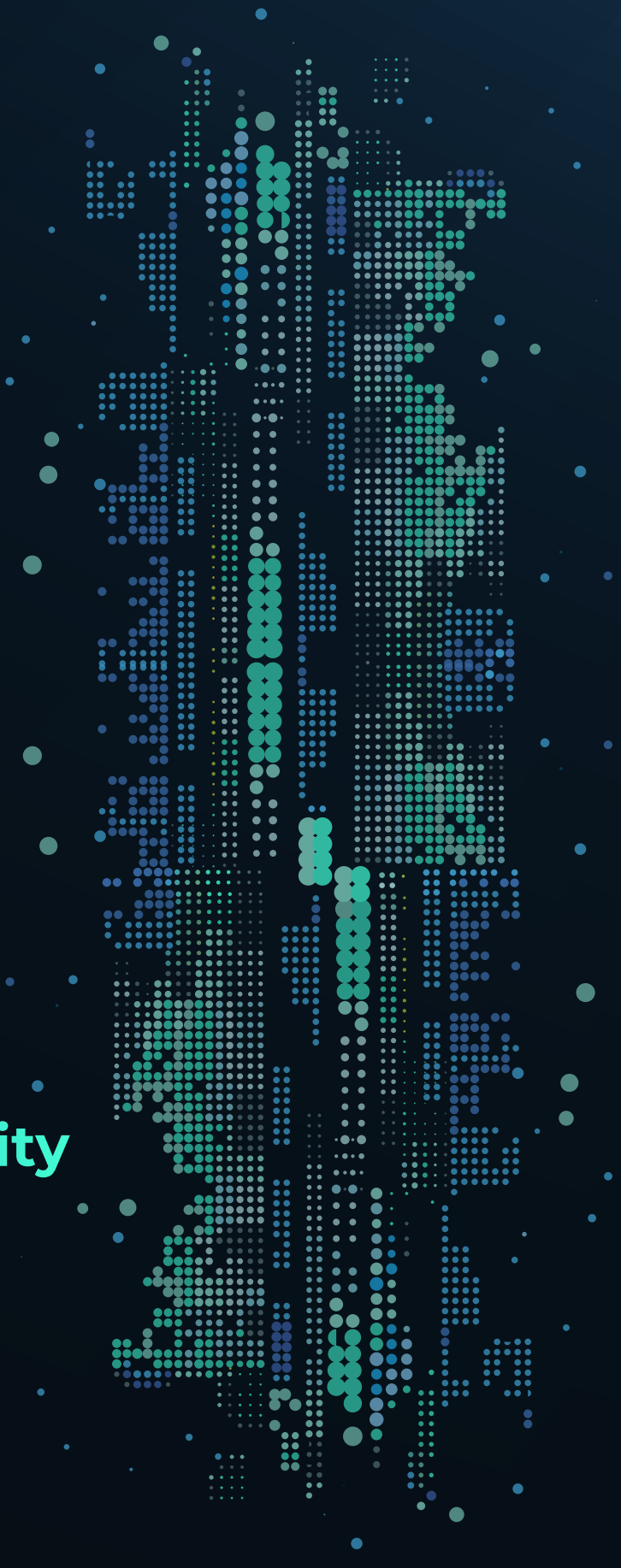
ANOMALI



2022

# Anomali Cybersecurity Insights Report

Der Zustand der Cyber-Resilienz
in Unternehmen

# Inhaltsverzeichnis

# Einführung

Willkommen beim Anomali Cybersecurity Insights Report 2022. In dieser ersten Studie ermitteln und untersuchen wir die Herausforderungen, mit denen Unternehmen bei der Schaffung und Aufrechterhaltung eines belastbaren Cybersicherheitsniveaus konfrontiert sind, das sie benötigen, um sich vor fortgeschrittenen Cyberbedrohungen zu schützen und darauf zu reagieren.

Um grundlegende Daten für diesen Bericht zu sammeln und zu erarbeiten, beauftragte das Team von Anomali Threat Research das Unternehmen The Harris Poll mit der Befragung von 800 Entscheidungsträgern im Bereich Unternehmenssicherheit aus 11 Ländern und von Unternehmen mit 5.000 oder mehr Mitarbeitern. Da COVID-19 solch tiefgreifende Auswirkungen auf das Geschäft und die Cybersicherheit hatte, haben wir bei der Befragung dieser Entscheidungsträger Cybersicherheitsniveaus und Herausforderungen bis zurück ins Jahr 2019 berücksichtigt, um ein besseres Verständnis dafür zu entwickeln, wie die globale Pandemie die Unternehmen beeinflusst hat. Analysten für den Bereich Threat Research im Team von Anomali Threat Research haben die Erkenntnisse mit einer Analyse zu Bedrohungstrends untermauert, sodass Lesern verwertbare Informationen zur Verfügung gestellt werden, mit denen sie Sicherheitsverstöße und Angreifer besser erkennen und besser darauf reagieren können.

Zu den wichtigsten Erkenntnissen gehört, dass **viele Unternehmen trotz erheblicher Investitionen in die Cybersicherheit mit Hindernissen konfrontiert sind, wenn es darum geht, das Maß an Cyber-Resilienz zu erreichen, das erforderlich ist, um vor Angriffen zu schützen, sie zu erkennen und darauf zu reagieren**. Angesichts der Zunahme von Sicherheitsverstößen und Cyberangriffen in den vergangenen Jahren dürfte diese Erkenntnis für die meisten Leser nicht überraschend sein.

**DAS IST CYBER-RESILIENZ**

Die Fähigkeit zum proaktiven und reaktiven Schutz des Unternehmens im Hinblick auf Bedrohungen und Angriffe, zur Anpassung an veränderte Umstände während eines Angriffs und zur Wiederherstellung nach einem Cyberangriff.

# Zusammenfassung

Unsere Untersuchungen haben viele Gründe aufgedeckt, warum es schwierig ist, Cyber-Resilienz zu erreichen. In erster Linie haben Unternehmen mit Leistungs- und Kompetenzlücken zu kämpfen, wenn es um das Maß an Erkennung, Reaktion und Wiederherstellung geht, das erforderlich ist, um mit unmittelbar bevorstehenden und zukünftigen Angriffen und Sicherheitsverstößen umzugehen.

Diese Untersuchungen haben ergeben, dass die Anzahl der Cyberangriffe zunimmt (Anstieg um **15 %** gegenüber dem Niveau von 2019, also vor der Pandemie). Es war daher für uns keine Überraschung, dass etwa drei von vier Unternehmen (**74 %**) ihre Budgets für Cybersicherheit erhöht haben und ihre Cybersicherheitsstrategien neu bewerten (**78 %**).

Auch mit erhöhten Investitionen sind die meisten Unternehmen (**87 %**) in den letzten drei Jahren Opfer erfolgreicher Cyberangriffe geworden, die in ihrem Geschäft zu Schäden, Störungen oder Verstößen geführt haben. Trotz ihrer Bemühungen geben rund zwei Drittel (**67 %**) an, dass sich seit Beginn der Pandemie mehr erfolgreiche Cyberangriffe auf ihr Unternehmen ausgewirkt haben. Allein im Jahr 2020 war einer von sieben (**14 %**) Cyberangriffen erfolgreich und führte zu Sicherheitsverletzungen, Schäden oder Betriebsstörungen. Entscheidungsträger im Bereich Unternehmenssicherheit gehen davon aus, dass diese Zahl ansteigen wird, da ihre Angriffsflächen mit dem zunehmenden und noch nie dagewesenen Umfang der Projekte zur digitalen Transformation ebenfalls immer größer werden. Selbst angesichts dieser zunehmend gefährlichen Bedrohungslandschaft gibt es nur bei 44 Prozent der Unternehmen etablierte Best Practices für die Reaktion auf Vorfälle, die bei einem Angriff angewendet werden können.

Cybervorfälle belasten fast alle Unternehmen finanziell, wobei Verluste durch gezielte Cyberangriffe, Malware-Kampagnen, Phishing, Insider-Bedrohungen und damit verbundene Datenschutzverletzungen eine Höhe von mehreren Hunderttausend Dollar pro Unternehmen erreichen. Fast drei von zehn Unternehmen (**28 %**) weltweit berichteten für das Jahr 2020 von Verlusten in Höhe von 500.000 US-Dollar oder mehr, was gegenüber 2019 fast einer Verdopplung entspricht (Anstieg um **193 %**). Zudem meldeten fast die Hälfte der Unternehmen (**47 %**) Verluste in Höhe von 100.000 US-Dollar oder mehr. Neben erheblichen Verlusten nehmen auch die Angriffe selbst mit einem erstaunlichen Tempo zu.

Abgesehen von Faktoren wie dem schnellen Tempo der digitalen Transformation und den steigenden Angriffszahlen nannten viele Entscheidungsträger im Bereich der Unternehmenssicherheit auch einen Mangel an integrierten Cybersicherheitslösungen als Hindernis bei der Erkennung von Cyberangriffen und Sicherheitsverstößen sowie der Reaktion auf solche Ereignisse und der anschließenden Wiederherstellung.

Viele Befragte geben an, dass ihre Unternehmen angefangen haben, die neuesten technologischen Innovationen im Zusammenhang mit erweiterter Erkennung Reaktion (XDR) und Advanced Threat Intelligence zu nutzen oder Investitionen in diesem Bereich planen, um Schwierigkeiten auszugleichen.

Es ist klar, dass ein Interesse an Cybersicherheitslösungen besteht, die über einen guten Support verfügen (**48 %**), einfach zu bedienen sind (**46 %**) und sich besser in bestehende Frameworks und Architekturen integrieren lassen (**44 %**), wobei mehr als vier von zehn Entscheidungsträgern diese Attribute als unverzichtbar betrachten.

**87 %**

**der Entscheidungsträger im Bereich Unternehmenssicherheit geben an, dass es bei ihrem Unternehmen in den vergangenen drei Jahren zu einem erfolgreichen Cyberangriff gekommen ist, der zu geschäftlichen Schäden, Störungen oder zu Sicherheitsverstößen geführt hat.**

## DIE GRÖßTEN HERAUSFORDERUNGEN IM HINBLICK AUF CYBER-RESILIENZ

Erkenntnis 1

# Unternehmen sind nur mäßig effektiv bei der Erkennung von und Reaktion auf Cyberbedrohungen und der anschließenden Wiederherstellung

Zweiundvierzig Prozent der Entscheidungsträger im Bereich der Unternehmenssicherheit sind der Ansicht, dass sie nicht das erforderliche Maß an Resilienz haben, um ihre Unternehmen vor Sicherheitsverstößen und Angriffen zu schützen. Weniger als sechs von zehn Entscheidungsträgern (58 %) sind der Meinung, dass ihre Unternehmen über ausreichend Cyber-Resilienz verfügen. Diese Feststellung steht jedoch im Gegensatz zur Tatsache, dass es bei 87 Prozent der Unternehmen in den letzten drei Jahren zu Sicherheitsverstößen kam.

Erkenntnis 2

# Nur knapp die Hälfte der Entscheidungsträger im Bereich Unternehmenssicherheit stimmen der Aussage voll und ganz zu, dass ihre Cybersicherheitsteams Bedrohungen schnell auf der Grundlage von Trends, Schweregrad und potenziellen Auswirkungen priorisieren können

Ein Drittel gibt zu, dass ihre Teams Schwierigkeiten haben, Sicherheitskontrollen zu aktualisieren, damit diese auch mit neuen Angriffen fertig werden (31 %). Weniger als die Hälfte (49 %) der Entscheidungsträger im Bereich Unternehmenssicherheit stimmen der Aussage voll und ganz zu, dass ihre Cybersicherheitsteams Bedrohungen schnell auf der Grundlage von Trends, Schweregrad und potenziellen Auswirkungen priorisieren können. Noch weniger (46 %) sind sehr zuversichtlich, dass ihre Cyberschutztechnologien weiterentwickelt werden können, um auch neue, global identifizierte Bedrohungen zu erkennen. Ein Drittel (32 %) gibt zu, dass die eigenen Teams Schwierigkeiten haben, mit der sich verändernden Bedrohungslandschaft im Hinblick auf die Cybersicherheit Schritt zu halten. Kleinere Unternehmen sind noch stärker gefährdet. Diejenigen mit weniger als 10.000 Mitarbeitenden verfügen seltener über eine Reihe von etablierten Best Practices, die sie bei der Reaktion auf Cyberangriffe einsetzen können (40 %).

Abbildung 1.0
**CYBER-RESILIENZ VON UNTERNEHMEN** (STIMME VOLLSTÄNDIG ZU IN %)

**49 %**
STIMME VOLL UND GANZ ZU

Mein Team kann Bedrohungen schnell basierend auf Trends, Schweregrad und potenziellen Auswirkungen auf unser Unternehmen priorisieren.

**46 %**
STIMME VOLL UND GANZ ZU

Meine Cybersicherheitstechnologien können optimiert werden, sodass auch neue, global identifizierte Bedrohungen erkannt werden.

**32 %**
STIMME VOLL UND GANZ ZU

Mein Team hat Probleme, mit der sich schnell verändernden Bedrohungslandschaft im Hinblick auf die Cybersicherheit Schritt zu halten.

## DIE GRÖßTEN HERAUSFORDERUNGEN IM HINBLICK AUF CYBER-RESILIENZ

Erkenntnis 3

# Unternehmen erreichen ihre Ziele bei der Erkennung und Reaktion auf Cyberbedrohungen nicht

Die Verweildauer ist der Zeitraum zwischen dem Zeitpunkt, zu dem ein Bedrohungsakteur Zugriff auf ein Netzwerk erhält, bis zu dem Punkt, wenn dies erkannt und schließlich unterbunden wird. Die Verweildauer ist direkt proportional zum Ausmaß der Schäden, die ein Angreifer verursachen kann. Je länger sie sich in Ihrem Netzwerk befinden, desto mehr Erkenntnisse gewinnen sie, desto mehr Daten und IP werden gestohlen und desto mehr Systeme können von ihnen mit Ransomware und anderen Bedrohungen infiziert werden. Es wird geschätzt, dass Angreifer die Erkennung im Durchschnitt 140 Tage umgehen können. Diese Metrik bezieht sich jedoch konkret auf die erstmalige Erkennung und Offenlegung einer Bedrohung.

Ein weiterer, genauso heikler Aspekt der Verweildauer ist die Zeit, die benötigt wird, um festzustellen, ob eine neu offengelegte Bedrohung auch in Ihrer Umgebung vorhanden ist. Im Rahmen der Umfrage haben wir Unternehmen gefragt, wie lange es gedauert hat, Angriffe, die bereits zuvor offengelegt wurden, zu erkennen und darauf zu reagieren. Die Ergebnisse waren besorgniserregend, da im Durchschnitt alle Entscheidungsträger im Bereich Unternehmenssicherheit zugaben, dass sie ihre Erkennungs- und Reaktionsziele im Großen und Ganzen nicht erreichen und bei bestimmten Arten von Bedrohungen auch hinterher hinken.

Abbildung 1.1

**DURCHSCHNITTLICHE ZEIT BIS ZUR ERKENNUNG UND REAKTION IM VERGLEICH ZUM ZIEL**

(In Tagen)

| | Datenschutzverletzung | | Netzwerkkom-promittierung | | Cyberangriff | |
|---|---|---|---|---|---|---|
| | Durchschnitt-liche Zeit | Durchschnitt-liches Ziel | Durchschnitt-liche Zeit | Durchschnitt-liches Ziel | Durchschnitt-liche Zeit | Durchschnitt-liches Ziel |
| ERKENNUNG | 3,1 | 2.1 | 2.8 | 2.1 | 2.7 | 2.5 |
| REAKTION | 2.5 | 2.2 | 2,5 | 2.1 | 2.4 | 2.1 |

Leistungsfähige Sicherheitsteams achten beim Aufklären von Vorfällen genau auf ihre MTTR- und MTTD-Kennzahlen. Es ist entscheidend, dass man eifrig darauf hinarbeitet, diese Kennzahlen in Unternehmen zu reduzieren, da eine kürzere Verweildauer das allgemeine Risiko von Schäden und Störungen reduziert. Die Verringerung der Verweildauer (MTTD und MTTR) beginnt mit dem Verständnis von Angriffen und deren Auswirkungen. Unternehmen müssen auch Silos aufbrechen und funktionsübergreifend zusammenarbeiten, um effektive Erkennungs- und Reaktionsprozesse zu gewährleisten.

MTTD

Die durchschnittliche Zeit bis zur Erkennung („Mean Time to Detect“, kurz MTTD) spiegelt die Zeit wider, die Ihr Team benötigt, um eine potenzielle Bedrohung zu entdecken.

MTTR

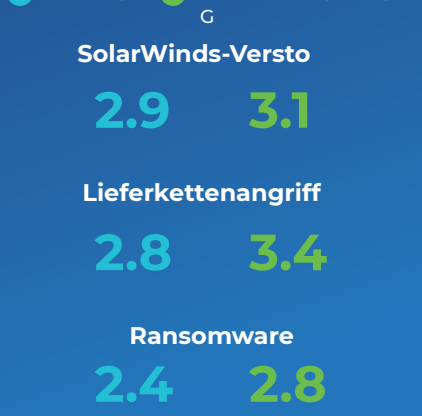
Die durchschnittliche Reaktionszeit („Mean Time to Respond“, kurz MTTR) ist die Zeit, die benötigt wird, um eine Bedrohung zu kontrollieren, zu beheben und/oder zu beseitigen, nachdem sie entdeckt wurde.

Abbildung 1.2

**DURCHSCHNITTLICHE ANZAHL DER TAGE, UM BEKANNTE CYBERANGRIFFE ZU ERKENNEN**

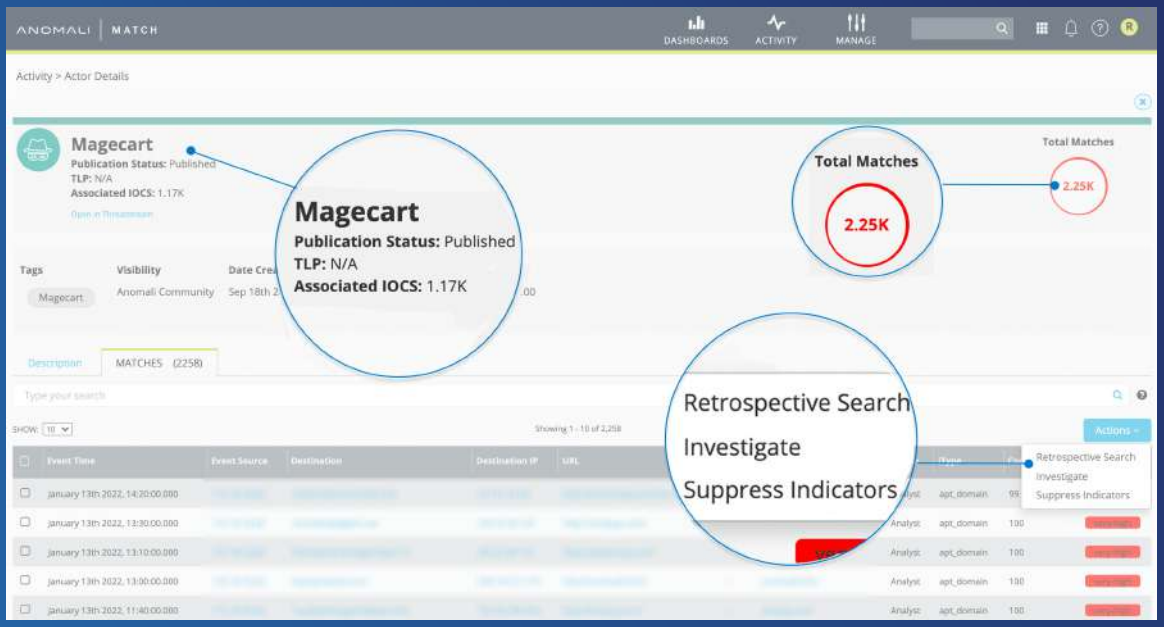

Abbildung 1.3

**DURCHSCHNITTLICHE ANZAHL DER TAGE BIS ZUR REAKTION AUF CYBERANGRIFFE UND BIS ZUR ANSCHLIESSENDEN WIEDERHERSTELLUNG**



# Anatomie der Bedrohungserkennung

**MAGECART: eine Gruppe bösartiger Cyberkrimineller, die E-Commerce-Websites anvisieren, um Zahlungskartendaten zu stehlen und in kriminellen Foren zu verkaufen**




Es gibt viele verschiedene Arten von Bedrohungen, und die Erkennung dieser Bedrohungen ist in der Regel nur ein Aspekt der Abwehr und Reaktion. Die Erfassung weiterer Informationen ist von zentraler Bedeutung für die datengestützte Entscheidungsfindung.

Cybersicherheitsexperten nutzen jetzt Big-Data-Analysen (große Datenmengen aus mehreren Quellen), um Bedrohungen zu ermitteln, bevor sie auftreten. Mit den richtigen Technologien können diese Daten analysiert werden, um Einblicke in menschliches Verhalten zu gewinnen, zukünftige Trends vorherzusagen oder Sicherheitsverstöße zu verhindern.

Das obige Beispiel zeigt, wie Tools, die große Mengen an Big Data integrieren, unter anderem auch Gefährdungsindikatoren (IoCs), beobachtete Verhaltensweisen, Wissen über Bedrohungsakteure und Bedrohungsmodelle, von Analysten verwendet werden können, um sofort zu wissen, ob es in ihren Umgebungen Bedrohungen wie Magecart gibt und wenn ja, wie lange diese Bedrohungen dort schon vorhanden sind. Wenn Unternehmen Zugang zu solch unmittelbarer Intelligence haben, können sie schnell und entschieden reagieren, was für die Einrichtung einer proaktiven und widerstandsfähigen Sicherheitsstrategie von entscheidender Bedeutung ist.

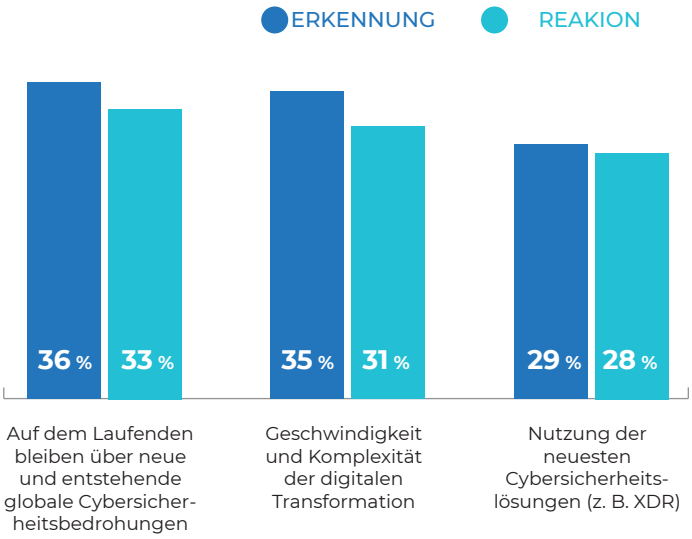
Erkenntnis 4

## Über neue und entstehende globale Cybersicherheitsbedrohungen auf dem Laufenden zu bleiben sowie die Geschwindigkeit und Komplexität der digitalen Transformation gehören zu den größten Herausforderungen

Unternehmen stehen bei der Erkennung vor vielen Herausforderungen. Zu den größten davon gehört einerseits, über neue und entstehende globale Cybersicherheitsbedrohungen auf dem Laufenden zu bleiben (36 %) und andererseits auch die Geschwindigkeit und Komplexität der digitalen Transformation (35 %) sowie die Einführung von Fortschritten im Bereich der Cybersicherheit, beispielsweise XDR (29 %). Für die Reaktion auf und die Wiederherstellung infolge von Bedrohungen wurden nahezu identische Herausforderungen festgestellt.

Abbildung 1.4

**HERAUSFORDERUNGEN IM ZUSAMMENHANG MIT CYBERANGRIFFEN, NETZWERKKOMPROMITTIERUNGEN UND DATENSCHUTZVERLETZUNGEN**




Erkenntnis 5

## Die fehlende Möglichkeit, Threat Intelligence über interne Ressourcen hinweg zu teilen, behindert die Bemühungen zur Abwehr

Über neue und entstehende globale Cybersicherheitsbedrohungen auf dem Laufenden zu bleiben sowie die Geschwindigkeit und Komplexität der digitalen Transformation zählen ebenfalls zu den von Entscheidungsträgern im Bereich Unternehmenssicherheit genannten Herausforderungen. Doch mehr als alles andere ist es wohl der Mangel an integrierten Lösungen und einer Möglichkeit, Threat Intelligence funktionsübergreifend zu teilen, der die Bemühungen zur Erkennung von Cyberangriffen, zur Reaktion darauf und zur anschließenden Wiederherstellung behindert. Etwas mehr als die Hälfte (53 %) der Entscheidungsträger sind der Ansicht, dass ihre Unternehmen Threat Intelligence über interne Ressourcen hinweg sehr effektiv teilen.

## DIE GRÖßTEN HERAUSFORDERUNGEN IM HINBLICK AUF CYBER-RESILIENZ

Threat Intelligence ist komplex und es gibt zahlreiche Variablen, die oft anders beschrieben werden. Damit der Informationsaustausch erfolgreich verläuft, wurden Standards wie beispielsweise MITRE, NIST und STIXX entwickelt, die die Prozesse verbessert haben.

Um zu verstehen, wie der Austausch funktioniert, müssen Unternehmen auch wissen, welche Informationen sie zu teilen versuchen. Um die Komplexität weiter zu reduzieren, kann Threat Intelligence in zwei Kategorien unterteilt werden: IOCs und Bedrohungsakteure. Diese Kategorien können Sicherheits- und Risikoexperten dabei helfen, zu verstehen, wie die Intelligence einzusetzen ist.

Abbildung 1.5

**EFFEKTIVITÄT DER WEITERGABE VON THREAT INTELLIGENCE ÜBER INTERNE RESSOURCEN HINWEG**


### IOCs

- OSINT-Feeds (Open Source Intelligence) können ein Kinderspiel sein, wenn Prozesse vorhanden sind, um Daten entsprechend zu verarbeiten und zu kennzeichnen.
- Threat Intelligence Platforms (TIPs) können einen großen Teil dieser Arbeit für Sie erledigen, indem sie Threat-Intelligence-Feeds aus Ihren Intelligence-Quellen (sowohl kostenlos als auch kommerziell) zusammenführen.
- IoC-Datenbanken und -Repositorys wie beispielsweise AlienVault (OTX), Hybrid Analysis, MalwareBazaar, PolySwarm, VirusTotal, VirusBay, VirSCAN, URLhaus und URLScan sind hervorragende Tools, um Kontext zu sammeln und datengestützte Entscheidungen zu treffen.
- Sandboxes wie beispielsweise AnyRun, Hatching, Hybrid Analysis, Inquest, Joe und Valkyrie Comodo sind hilfreich, um allgemeine Trends und TTPs zu erkennen und Signaturen für gängige Malware-Taktiken zu erstellen.
- OSINT-Erkennungssprachen-Repositorys für Yara, SIGMA, Snort u. a. sind eine großartige Möglichkeit, um häufige schädliche Verhaltensweisen abzudecken.

### BEDROHUNGSAKTEURE

- OSINT-Quellen wie ThaiCERT, MITRE-Gruppen, Malpedia und Maltego sind ausgezeichnete Referenzen für Bedrohungsdaten.
- Auf TIPs sollte es viele dokumentierte Bedrohungsakteure und IOC-Verknüpfungen in Echtzeit geben, um im Hinblick auf produktive Gruppierungen den Überblick zu behalten.
- Zu wissen, welche Art von Malware verschiedene Gruppen einsetzen – also SaaS, modifizierte Commodity Malware, seriöse Tools oder individuelle Malware –, ermöglicht es, eine proaktive Haltung einzunehmen, wenn es darum geht, Abwehrmaßnahmen für diese Bedrohungen einzurichten.

Durch die Kategorisierung von Intelligence-Arten können Angreifer und Sicherheitsverstöße besser erkannt werden und die Reaktion darauf ist einfacher. Unternehmen setzen auf Innovationen, mit denen sich Threat Intelligence über mehrere Sicherheitsinfrastrukturen hinweg automatisieren und operationalisieren lässt, um den Wert dieser Intelligence noch zu steigern. Aktuelle Berichte von führenden Branchenanalysten zeigen, dass die Nachfrage nach Lösungen auf dem Markt für Threat Intelligence, zu dem auch Plattformen für das Bedrohungsmanagement gehören, in den kommenden drei Jahren um bis zu 16 Prozent pro Jahr steigen wird.

Erkenntnis 6

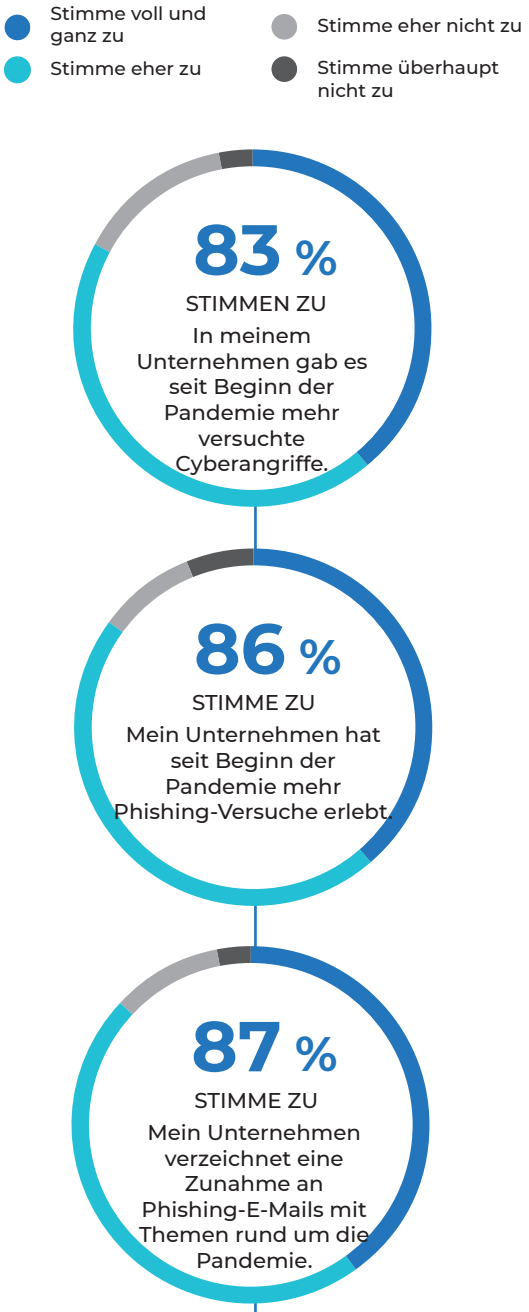
# Cybervorfälle sind weit verbreitet und ihre Anzahl hat sich seit Pandemiebeginn erhöht

Die meisten Entscheidungsträger im Bereich Unternehmenssicherheit stimmen zu, dass es in ihren Unternehmen seit Beginn der Pandemie zu mehr versuchten Cyberangriffen (83 %) und mehr Phishing-Versuchen (86 %) kam. Konkret erhalten diese Unternehmen auch vermehrt Phishing-E-Mail mit Themen rund um die Pandemie (87 %). Im Jahr 2020 berichteten Unternehmen mit 5.000 oder mehr Mitarbeitenden durchschnittlich 30 Cyberangriffe. Im Vorjahr lag diese Zahl bei nur 26. Einer von sieben dieser Cyberangriffe (14 %) war erfolgreich und führte in den Netzwerken, in der Infrastruktur und auf den Geräten zu Schäden, Störungen oder Sicherheitsverstößen.

Abbildung 2.2
**DURCHSCHNITTLICHE ANZAHL VON CYBERANGRIFFEN AUF UNTERNEHMEN**


Unternehmen mit 10.000 oder mehr Mitarbeitenden haben sowohl 2019 als auch 2020 im Vergleich zu Organisationen mit 5.000 bis 9.999 Mitarbeitenden mehr versuchte Cyberangriffe abgewehrt (2019: 29,1 im Vergleich zu 23,3; 2020: 32,4 im Vergleich zu 27,8).

Abbildung 2.1
**ANSTIEG BEI DEN ARTEN VON CYBERANGRIFFEN SEIT BEGINN DER PANDEMIE**



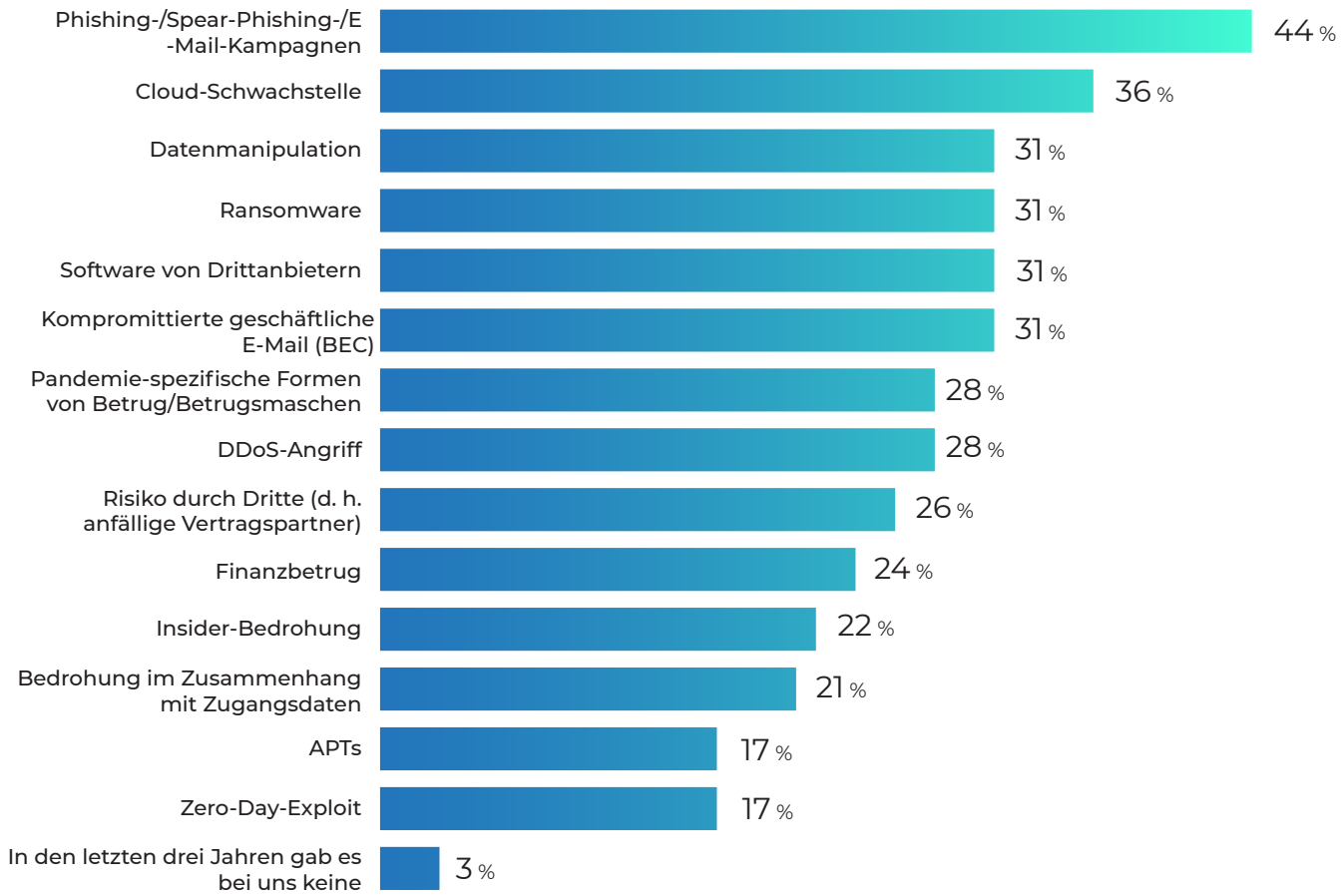
Erkenntnis 7

# E-Mails mit Phishing-Versuchen sind die am häufigsten vorgefundene Bedrohung

Bei 44 Prozent aller Unternehmen gab es in den vergangenen drei Jahren Phishing-Angriffe, womit dies die Art von Angriff ist, die am häufigsten vorkam. Bedrohungsakteure aus allen Raffinesse-Gruppen nutzen Phishing aufgrund der verfügbaren Standardtools und des ständig wachsenden Zielpools. Mit Commodity-Phishing-Kits können Bedrohungsakteure mit geringer Raffinesse potenziell schädliche Kampagnen durchführen, die Commodity Malware verbreiten. Die schädlichen Dokumente („Maldocs“) selbst werden auch durch Tools wie **EtterSilent** standardisiert. Bedrohungsakteure und ihre Gruppen kompromittieren außerdem die E-Mail-Konten von Zielkunden, um ihre schädlichen Aktivitäten weiter auszudehnen. Diese Aktivitäten beinhalten häufig seriöse Dokumente, um die Tätigkeit authentischer aussehen zu lassen. Unsere Untersuchungen haben ergeben, dass seriöse Dokumente in Kampagnen von **Gamaredon** (Primitive Bear) und **Mustang Panda** verwendet werden, wobei erstere wahrscheinlich private Dokumente verwenden, bevor sie veröffentlicht werden.

Abbildung 2.3

**CYBERBEDROHUNGEN IN DEN LETZTEN DREI JAHREN**



Erkenntnis 8

# Cyberkriminelle Unternehmen werden als größte Bedrohung für die Cybersicherheit angesehen (44 %), gefolgt von einzelnen Hackern (21 %)

## Es dauert durchschnittlich 3-4 Tage nach Offenlegung, bis Unternehmen Angriffe von diesen Einheiten erkennen

44 Prozent der Entscheidungsträger für Unternehmenssicherheit sind der Meinung, dass cyberkriminelle Gruppen die größte Bedrohung für ihre Unternehmen darstellen. Für uns war dies nicht überraschend, da die meisten der heutzutage auftretenden Angriffe und Sicherheitsverstöße von dieser Art von Bedrohungsakteuren kommen. Fünfzehn Prozent der Entscheidungsträger für Unternehmenssicherheit sind der Ansicht, dass staatlich unterstützte Akteure die größte Cybersicherheitsbedrohung für ihre Unternehmen darstellen, wobei Russland (39 %) und China (33 %) an der Spitze stehen. Weniger Unternehmen machen sich Sorgen über Bedrohungen aus dem Iran (10 %) oder aus Nordkorea (8 %). Entscheidungsträger im Bereich Unternehmenssicherheit mit weniger als 10.000 Mitarbeitenden verstehen die Motive dieser Akteure tendenziell weniger als Entscheidungsträger bei größeren Unternehmen mit 10.000 oder mehr Mitarbeitenden.

Abbildung 2.4
**GRÖSSTE BEDROHUNG FÜR DAS UNTERNEHMEN**

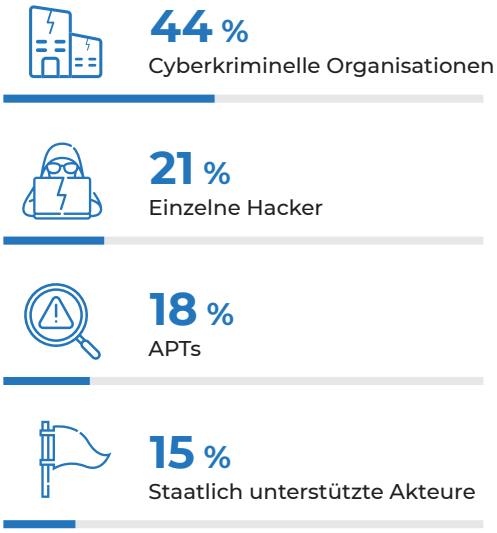
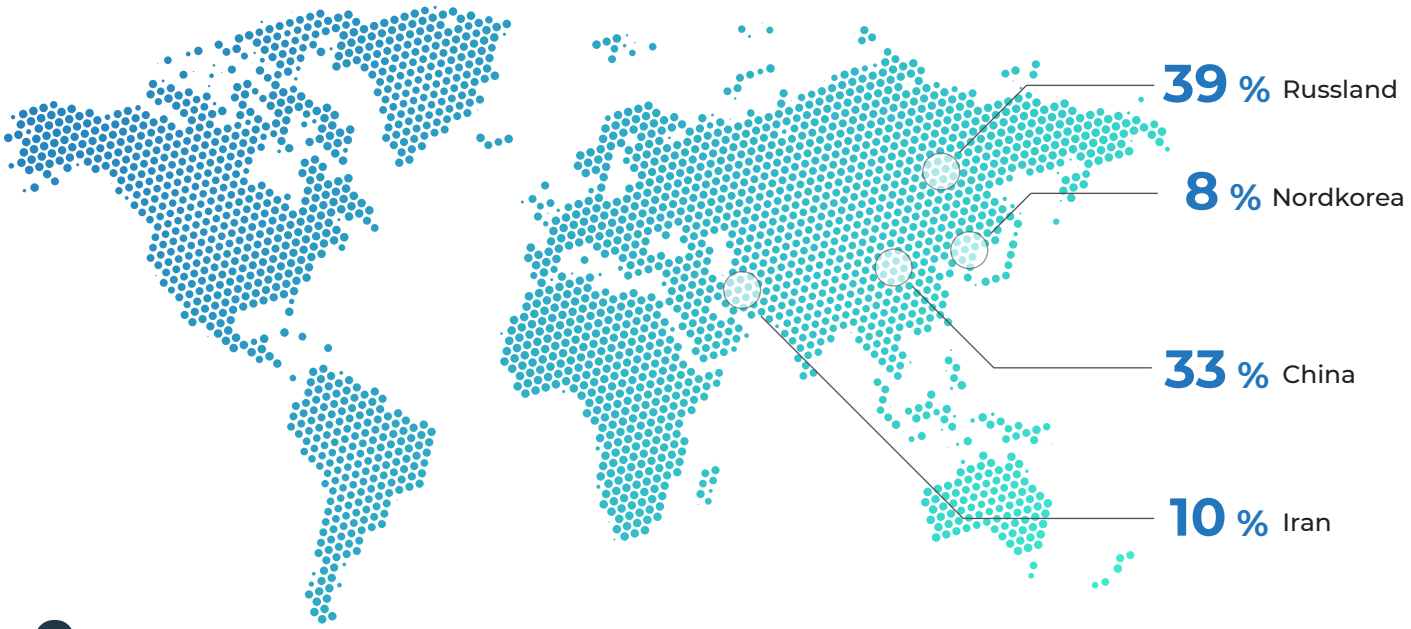



Abbildung 2.5
**LAND, DAS DIE GRÖSSTE CYBERSICHERHEITSBEDROHUNG DARSTELLT**



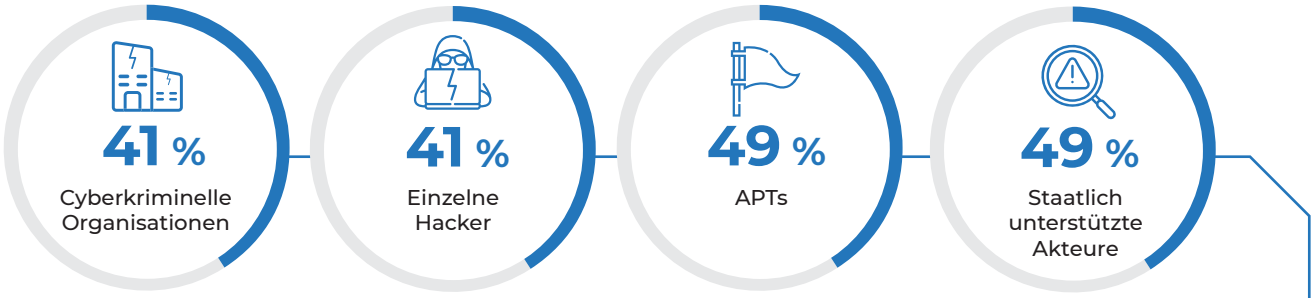
Erkenntnis 9

# Fast die Hälfte der Entscheidungsträger im Bereich Unternehmenssicherheit gibt zu, die Motive der Bedrohungsakteure nicht wirklich gut zu verstehen

In Anbetracht der ständigen Störungen von Bedrohungsakteuren mit niedriger bis mittlerer Raffinesse können Gefährdungsindikatoren (IoCs) wie ein Tropfen auf den heißen Stein erscheinen. Während all dieser Störungen können ausgefeiltere Gruppen von Bedrohungsakteuren unentdeckt im Hintergrund individuelle Tools oder Malware entwickeln oder seriöse Software missbrauchen, um gezielte Angriffe durchzuführen. Daher ist es entscheidend, die Motive der Bedrohungsakteure zu verstehen, um sich eine Vorstellung davon zu verschaffen, wie diese Gruppen arbeiten und welche davon es möglicherweise auch auf Ihr Unternehmen abgesehen haben.

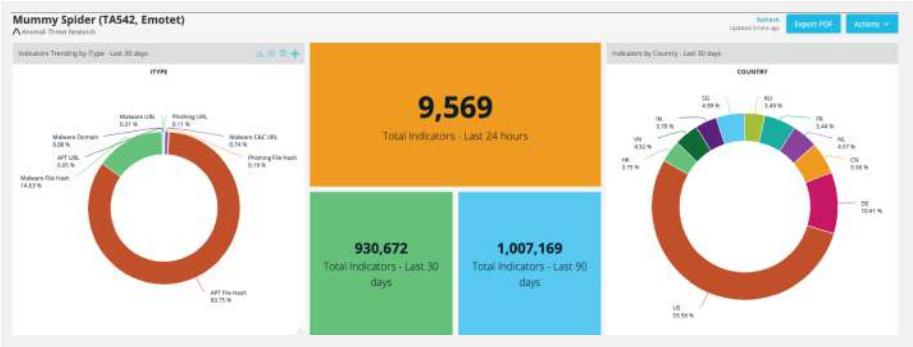
Abbildung 2.6

**PROZENTSATZ DER ENTSCHEIDUNGSTRÄGER IM BEREICH UNTERNEHMENSSICHERHEIT, DIE DIE MOTIVE, TAKTIKEN, TECHNIKEN UND VERFAHREN VON BEDROHUNGSAKTEUREN NICHT SEHR GUT VERSTEHEN**




Die Befragten bei Finanz- und Unternehmensdienstleistern sind am ehesten der Meinung, dass sie die Motivation von Cyberkriminellen sehr gut verstehen (64 % bzw. 65 %), während dieses Verständnis bei den Befragten von Unternehmen aus dem Gesundheitsbereich am wenigsten ausgeprägt ist (45 %).

**BEDROHUNGSAKTEURE: ZUNEHMEND PRÄZISE**



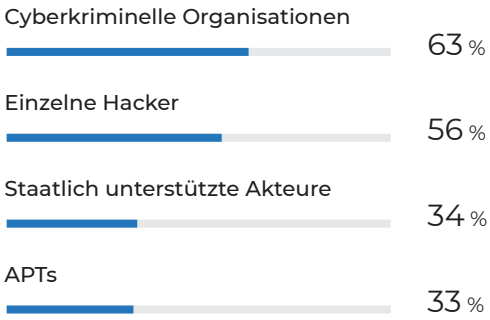

Anomali Threat Research hat dieses Dashboard entwickelt, um zu zeigen, wie Threat Intelligence verwaltet wird, um ein breites Anfangsnetz zu erstellen und Daten zusammenzufassen. Mit diesem Maß an Präzision ist es einfacher, die Motive und Ziele von Bedrohungsakteuren zu verstehen. In diesem Fall haben wir das Dashboard auf **Mummy Spider** angewendet, eine Gruppe Cyberkrimineller, die mit der Entwicklung der als „Emotet“ oder „Geodo“ bekannten Malware in Verbindung steht.

Erkenntnis 10

## Fast neun von zehn (87 %) Unternehmen waren in den vergangenen drei Jahren Opfer einer Art von Cyberangriff

In dieser Gruppe war mehr als die Hälfte von Angriffen durch cyberkriminelle Organisationen oder einzelne Hacker betroffen. Ein Drittel sind staatlich unterstützten Akteuren und Angriffen durch hoch entwickelte, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs) zum Opfer gefallen.

Abbildung 2.7
**ERFOLGREICH VERÜBTE CYBERANGRIFFE AUF UNTERNEHMEN**




Erkenntnis 11

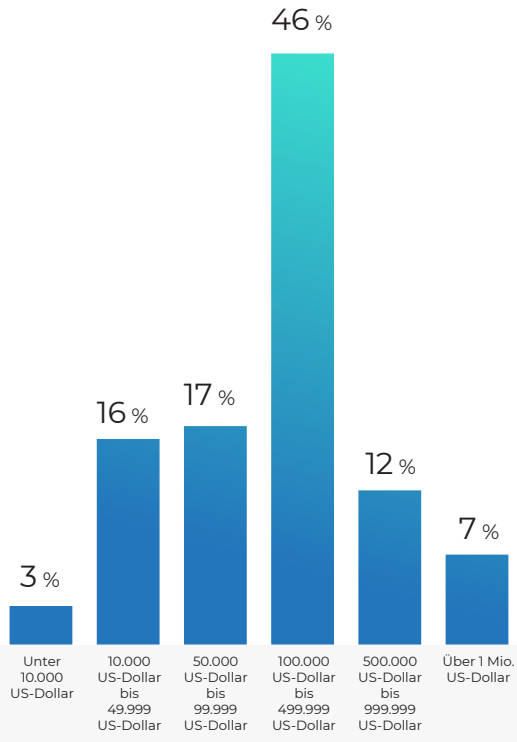
## Etwa die Hälfte aller Unternehmen (52 %) sah sich in den letzten drei Jahren mit Ransomware-Angriffen konfrontiert

Etwa 40 Prozent der betroffenen Organisationen zahlten ein Lösegeld (39 %), wobei eines von fünf (19 %) Unternehmen hier 500.000 US-Dollar oder mehr ausgab. Obwohl Ransomware eine der am weitesten verbreiteten und bekanntesten Bedrohungen ist, richtet diese Art der Bedrohung bei den Organisationen nach wie vor verheerenden Schaden an. Um sich vor dieser Art von Angriff zu schützen, müssen Unternehmen wissen, wo sich ihre Schwachstellen befinden, Netzwerke richtig segmentieren, Benutzerberechtigungen einschränken und überwachen, Sicherungskopien erstellen und sich die Fähigkeit aneignen, Ransomware zu erkennen und darauf zu reagieren, bevor diese ins Netzwerke gelangt.

**39 %**

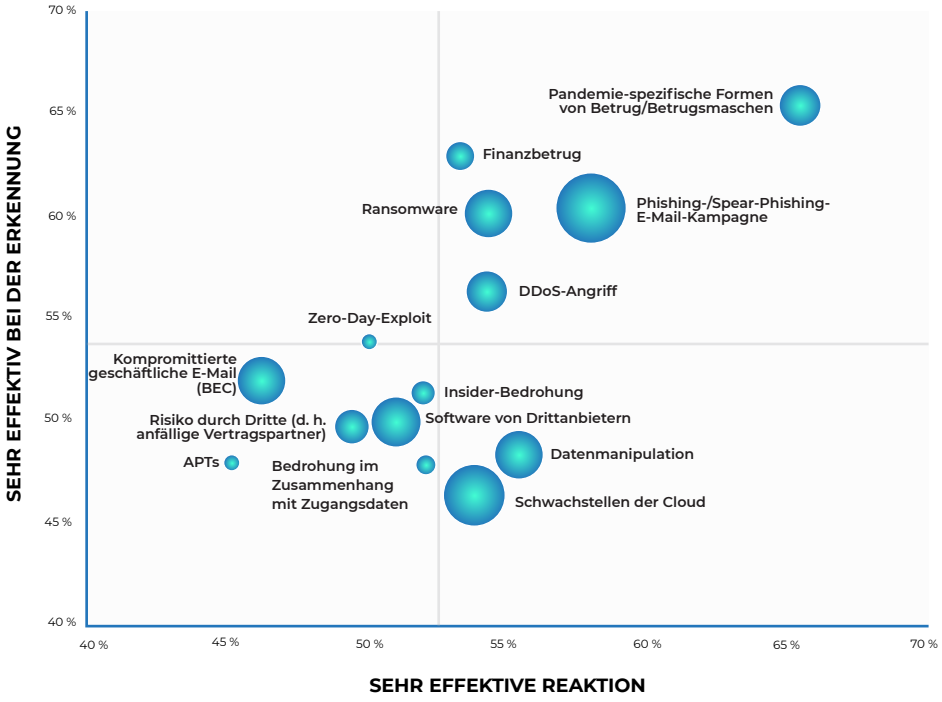
**Gezahltes Lösegeld für Ransomware-Angriffe in den letzten 3 Jahren**

Abbildung 2.8
**ALS LÖSEGELD BEZAHLTER BETRAG**
(US-WÄHRUNGSÄQUIVALENT)



## DIE MODERNE BEDROHUNGSLANDSCHAFT

Abbildung 2.9
**BEREICHE MIT POTENZIELLEN SCHWACHSTELLEN**




**HINWEIS:** Die Größe des Kreises stellt die Häufigkeit der Bedrohung in den letzten drei Jahren dar.

Siebzehn Prozent der Unternehmen haben in den letzten drei Jahren einen APT-Angriff erlebt und ungefähr der gleiche Anteil (18 %) hält APTs für die größte Bedrohung für die Cybersicherheit des eigenen Unternehmens. Entscheidungsträger im Bereich Unternehmenssicherheit fühlen sich für diese Bedrohungen weniger gut gerüstet als für andere Arten von Cyberangriffen, wobei vergleichsweise wenige Unternehmen sagen, dass sie APTs sehr effektiv erkennen (45 %) und sehr effektiv darauf reagieren (48 %).

Am Anfang der Pandemie erkannten die Anomali-Analysten im Bereich Threat Intelligence **6.200 Gefährdungsindikatoren (IoCs) und mindestens 15 unterschiedliche Kampagnen**. Diese wurden mit elf Bedrohungsakteuren oder Gruppen in Verbindung gebracht, die 39 verschiedene Malware-Familien mit 80 verschiedenen MITRE ATT&CK-Techniken verteilten. Anomali kam schon früh zu der Einschätzung, dass die Bedrohung durch COVID-19-bezogene Phishing-Kampagnen gegen öffentliche und private Unternehmen weiter zunehmen würde. Die Erkenntnisse 6 und 7 zeigen, dass solche Angriffe verstärkt auftreten.

Erkenntnis 12

# Die Pandemie hat Organisationen dazu gezwungen, Strategien zur Cybersicherheit neu zu bewerten

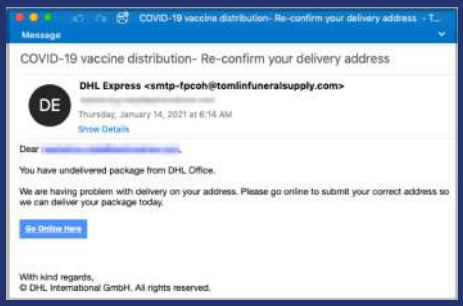
Mehr als 3 von 4 Entscheidungsträgern (78 %) im Bereich Unternehmenssicherheit geben an, dass sie aufgrund der Pandemie ihre Cybersicherheitsstrategien überdenken mussten. Aus unserer Sicht hat dies mehrere Gründe. Projekte zur digitalen Transformation, eine steigende Anzahl an aus der Ferne arbeitenden Mitarbeitenden und die damit zusammenhängende Erweiterung der Cloud-Infrastruktur haben dazu geführt, dass die Angriffsfläche noch schneller gewachsen ist als vor der Pandemie. Diese Faktoren haben Unternehmen dazu gezwungen, die Transparenz innerhalb ihrer Systeme zu erhöhen. Unter anderem auch dadurch lässt sich erklären, warum Investitionen in Bereichen wie XDR, MITRE ATT&CK und Threat Intelligence geplant sind bzw. bereits Systeme in diesen Bereichen eingesetzt werden (Erkenntnis 13). Darüber hinaus hat COVID-19 Bedrohungsakteuren ein Thema mit einem hohen Wiedererkennungswert für Phishing-Kampagnen und andere schädliche Aktivitäten geliefert, denn die Pandemie hat sich als gutes Mittel erwiesen, um Verwirrung Angst, Neugier und andere Emotionen zu erzeugen und Menschen so dazu zu bewegen, auf schädliche Links zu klicken. Da immer neue Varianten des Coronavirus auftreten, müssen Unternehmen ihre Anpassungsfähigkeit verbessern, insbesondere im Hinblick auf häufige Angriffe wie Phishing-E-Mail-Kampagnen.

Abbildung 3.1

**AUSWIRKUNGEN DER PANDEMIE AUF DIE CYBERSICHERHEITS STRATEGIE**


## DIE GLOBALE PANDEMIE VERSCHAFFT ANGREIFERN EINEN VORTEIL

Anomali Threat Research hat seit Anfang der COVID-19-Pandemie viele bösartige Kampagnen ausmachen und erkennen können, bei denen die globale Pandemie als Köder genutzt wurde. Das Bild rechts zeigt ein Beispiel für eine Fake-App für Mobilgeräte im Zusammenhang mit COVID-19, die bereits im Juni 2020 in Umlauf war. Um die Sicherheitsgemeinschaft und die Verbraucher vor solchen betrügerischen Versuchen zur Verbreitung von Malware zu schützen, haben die Anomali-Analysten im Bereich Threat Intelligence einen detaillierten Blog-Post zu diesem Thema veröffentlicht: **„Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data“.**


Neben Fake-Apps zur Kontaktnachverfolgung im Zusammenhang mit COVID-19 haben Anomali-Analysten im Bereich der Threat Intelligence auch Phishing-E-Mail-Kampagnen identifiziert, die sich die Pandemie zunutze gemacht haben. Die folgende E-Mail wurde im Februar 2021 entdeckt.

**Quelle: „Threat Actors Capitalize on COVID-19 Vaccine News to Run Campaigns, AWS Abused to Host Malicious PDFs“** über Anomali Threat Research

Erkenntnis 13

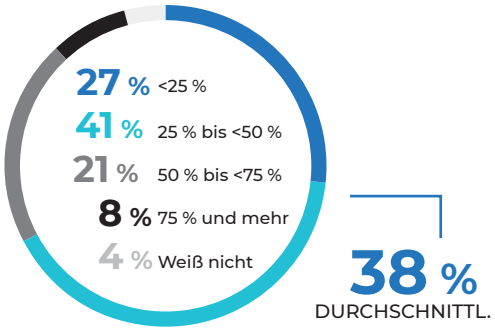
# Die finanziellen Auswirkungen von Cyberbedrohungen lassen sich sowohl durch die steigenden Budgets für Cybersicherheit als auch durch die direkten Verluste durch Cybervorfälle und Ransomware-Angriffe messen

Organisationen müssen eine robuste Sicherheitsarchitektur pflegen, um sich vor einer Vielzahl von Cyberbedrohungen zu schützen, die von Phishing-E-Mail-Kampagnen über Cloud-Schwachstellen und Ransomware bis hin zu APTs reichen. Die Unternehmen widmen mittlerweile fast 40 Prozent ihrer IT-Budgets der Cybersicherheit (38 %) und drei von vier Entscheidungsträgern im Bereich Unternehmenssicherheit (74 %) gaben an, dass die Budgets im letzten Jahr gestiegen sind.

Trotz dieser Ausgaben nehmen die direkten Verluste aufgrund von Cybervorfällen jedoch weiter zu. Im Jahr 2019 meldete nur ein Drittel aller Unternehmen weltweit (36 %) Verluste in Höhe von 100.000 US-Dollar oder mehr (US-Währungsäquivalent). Im Jahr 2020 stieg dieser Anteil auf fast die Hälfte (47 %). Im selben einjährigen Zeitraum haben sich die ausgewiesenen Verluste in Höhe von 500.000 US-Dollar oder mehr bzw. 1 Mio. US-Dollar oder mehr verdoppelt (Verluste in Höhe von 500.000 US-Dollar oder mehr: 15 % im Jahr 2019 im Vergleich zu 28 % im Jahr 2020; Verluste in Höhe von 1 Mio. US-Dollar oder mehr: 5 % im Jahr 2019 im Vergleich zu 11 % im Jahr 2020). Zahlen für das Jahr 2021 standen zum Zeitpunkt der Umfrage noch nicht zur Verfügung.

Abbildung 3.2
**BUDGET FÜR CYBERSICHERHEIT**

Prozentsatz des IT-Budgets für Cybersicherheit




Budgetänderung im letzten Jahr

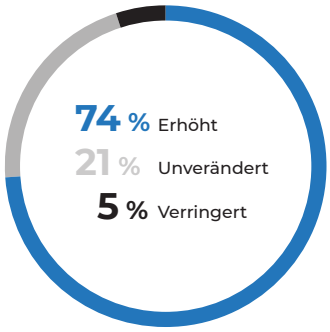
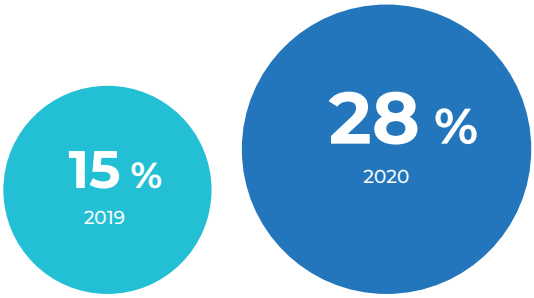



Abbildung 3.3
**UNTERNEHMEN VERLOREN ÜBER 500.000 US-DOLLAR AUFGRUND VON CYBERANGRIFFEN**
(US-WÄHRUNGSÄQUIVALENT)




Ransomware-Angriffe sind auch sehr kostspielig geworden. Von den etwa zwei von fünf Unternehmen (39 %), die von einem Ransomware-Angriff betroffen waren und sich für die Zahlung eines Lösegelds entschieden haben, zahlten fast zwei Drittel (65 %) einen Betrag von umgerechnet 100.000 US-Dollar oder mehr.

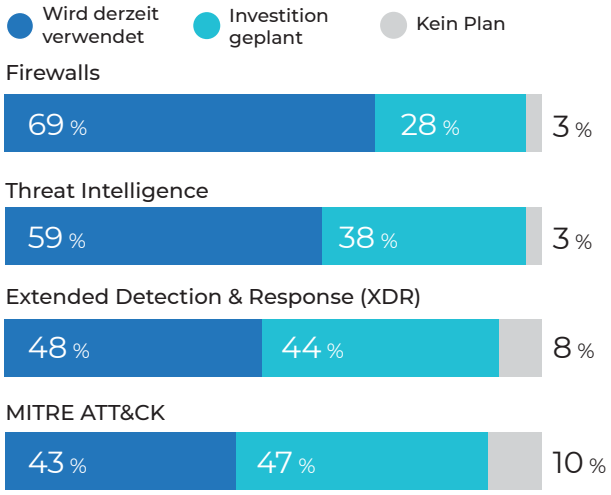
Erkenntnis 14

## Unternehmen setzen weiterhin veraltete Technologien ein, lassen sich aber auf neue Innovationen ein

Sieben von zehn (69 %) Unternehmen nutzen weiterhin Firewalls, um Bedrohungen im Netzwerk zu erkennen. 59 Prozent setzen jedoch Threat Intelligence ein (38 % planen hier Investitionen), 48 Prozent verwenden XDR (44 % planen hier Investitionen) und 43 Prozent nutzen das MITRE ATT&CK-Framework (47 % planen hier Investitionen). Wir sind der Ansicht, dass dieser Wandel hin zur Nutzung von neuen Tools und zu Investitionen in diesem Bereich auf der Erkenntnis beruht, dass veraltete Lösungen zwar weiterhin eine Rolle bei defensiven Strategien spielen werden, man sich aber nicht mehr ausschließlich auf diese Lösungen verlassen kann, wenn es darum geht, neu aufkommende Bedrohungen zu erkennen und darauf zu reagieren.

Abbildung 4.1

**AKTUELL GENUTZTE INNOVATIONEN**




Erkenntnis 15

## Neue Cybersicherheitslösungen müssen in bestehende Frameworks und Architekturen integriert werden

Um mit den Cyberbedrohungen umzugehen, denen sie jeden Tag ausgesetzt sind, suchen Entscheidungsträger im Bereich Unternehmenssicherheit nach neuen Lösungen, die guten Support bieten und benutzerfreundlich sind und in andere Cybersicherheitssysteme und verschiedene Teile ihrer Unternehmen integriert sind.

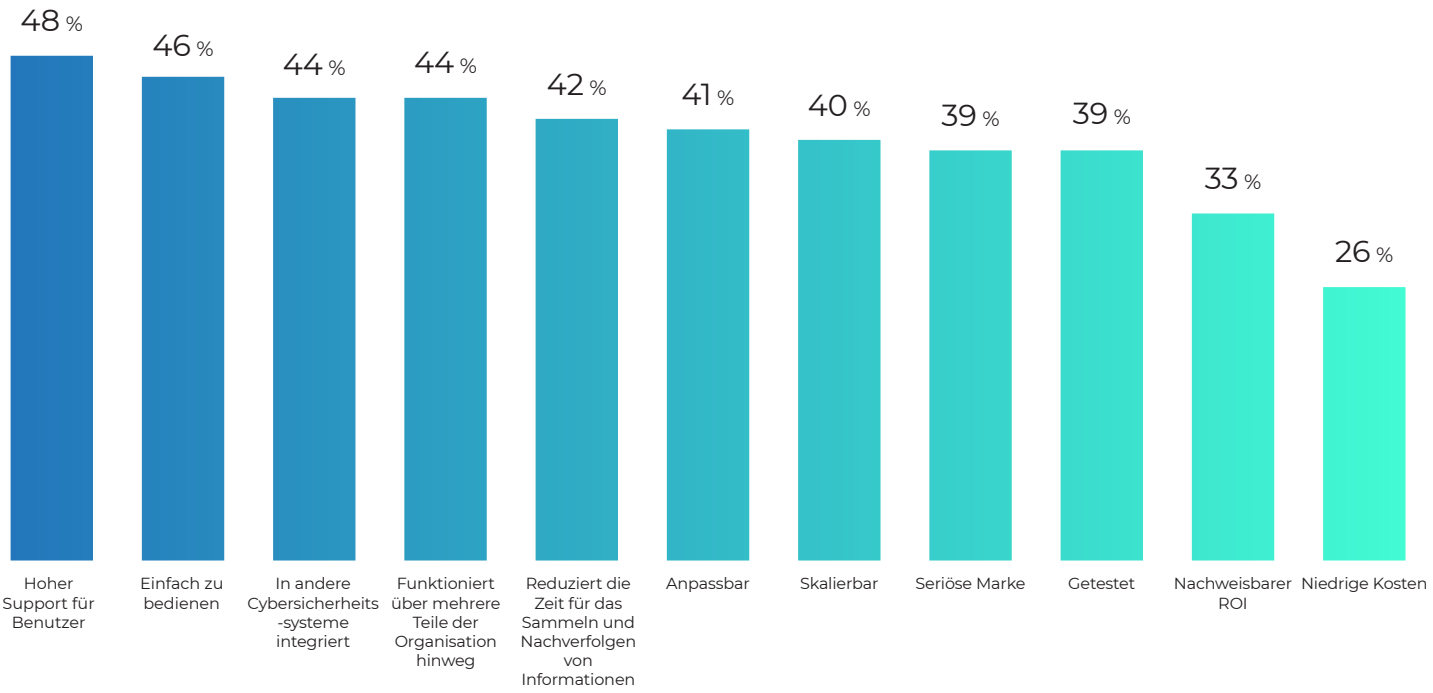
Für mindestens vier von zehn Entscheidungsträgern (41 %) gelten auch die Möglichkeit zur Anpassung und Skalierbarkeit als wesentliche Attribute bei der Bewertung neuer Cybersicherheitstools. Fast genauso viele von ihnen (39 %) wünschen sich Lösungen von namhaften Marken, die gründlich getestet wurden.

Interessanterweise ist nur ein Drittel der Unternehmen (33 %) der Meinung, dass eine neue Cybersicherheitslösung sich auch im Hinblick auf den ROI unter Beweis stellen muss. Niedrige Kosten sind für die Entscheidungsträger am wenigsten ausschlaggebend und nur ein Viertel der Befragten (26 %) führt dies als wesentliche Anforderung an.

## REAKTION AUF CYBERANGRIFFE

Abbildung 4.2

**WESENTLICHE MERKMALE BEI DER BEWERTUNG VON CYBERSICHERHEITSLÖSUNGEN**




Obwohl die Ergebnisse teilweise eine anhaltende übermäßige Abhängigkeit von veralteten Technologien zeigen, war es ermutigend, festzustellen, dass Unternehmen derzeit entweder bereits Innovationen einsetzen oder planen, in Innovationen wie das MITRE ATT&CK-Framework, XDR und Threat Intelligence zu investieren, um dieses Problem anzugehen.

Erkenntnis 16

# Um mit der Entwicklung der Bedrohungslandschaft Schritt zu halten, verwenden die meisten Unternehmen Tools und Technologien, die zur Überwachung globaler Bedrohungen entwickelt wurden

Die Operationalisierung von Threat Intelligence spielt eine immer entscheidendere Rolle, wenn es darum geht, wie gut ein Unternehmen mit Cyberrisiken umgehen und Cyber-Resilienz aufbauen kann. Oftmals kann es sein, dass Sicherheitsteams von der Menge der gesammelten Daten oder der Anzahl der Warnmeldungen, die sie erhalten, überwältigt sind. Wenn sie in der Lage sind, auf Bedrohungen zu reagieren, die für ihre spezifische digitale Präsenz relevant sind, werden sie effektiver und effizienter.

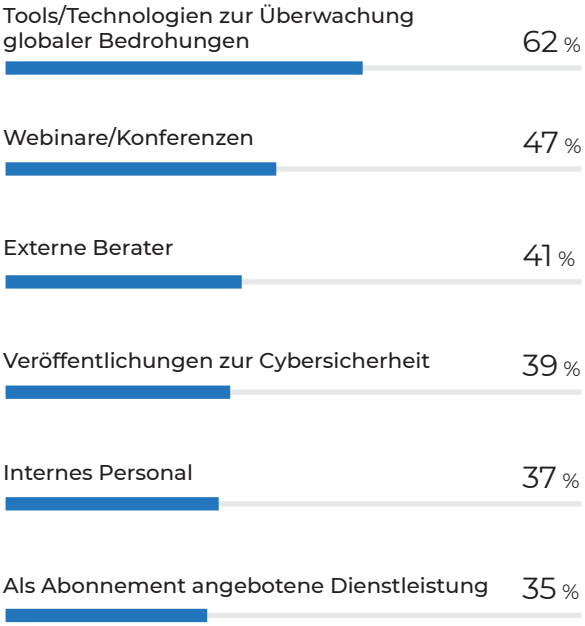
Laut der Studie verwenden 62 % der Unternehmen Tools und Technologien, um globale Bedrohungen im Auge zu behalten und ihre Performance im Bereich Threat Intelligence zu beschleunigen. Diese Ergebnisse stehen im Einklang mit den Branchenkennzahlen, denen zufolge die Nachfrage nach Plattformen für Bedrohungsmanagement, die globale Intelligence zur Erkennung von Bedrohungen einsetzen, und auch nach anderen Technologien, die die Erfassung und Korrelation von Daten automatisieren, sodass sie von anderen Sicherheitsteams verwendet werden können, steigt.

Diese Tools stellen Intelligence-Experten auch Prozesse zur Verfügung, mit denen sie die Anforderungen von Interessengruppen verwalten, den Nutzen der Datenanalyse durch das Verständnis der Intention und Ziele von Angreifern maximieren und die Entscheidungsfindung prognostizieren und verbessern können.

Cybersicherheit ist heute eine wichtige Geschäftsstrategie.  Um Cybersicherheitsbedrohungen zu verstehen und abzuwehren, sind die richtigen Tools, das richtige Wissen und die richtigen Fachkenntnisse erforderlich. Ein effektives Threat-Intelligence-Programm hilft Unternehmen dabei, Bedrohungen frühzeitig zu erkennen und schnell darauf zu reagieren.

Abbildung 4.3

**ARTEN, WIE UNTERNEHMEN MIT DER SICH SCHNELL VERÄNDERNDEN BEDROHUNGSLANDSCHAFT SCHRITT HALTEN**



SCHLUSSFOLGERUNG

# Das Maß an Cyber-Resilienz, das Unternehmen erreicht haben

In dieser Umfrage haben wir Cyber-Resilienz als die Fähigkeit zum proaktiven und reaktiven Schutz des Unternehmens im Hinblick auf Bedrohungen und Angriffe, zur Anpassung an veränderte Umstände während eines Angriffs und zur Wiederherstellung nach einem Cyberangriff definiert. Wir haben festgestellt, dass Unternehmen zwar ihre Budgets für Cybersicherheit erhöhen, innovative Sicherheitsebenen hinzufügen und den Fokus auf Effizienz statt auf die Kosten legen, aber trotzdem noch viel Arbeit vor sich haben, wenn sie in Zukunft erfolgreich sein möchten.

Nach fast zwei Jahren voller noch nie dagewesener Herausforderungen und Störungen in unserem Arbeits- und Privatleben sind einige Entscheidungsträger im Bereich Unternehmenssicherheit der Überzeugung, dass sie Fortschritte machen. Wir können jedoch nicht erkennen, dass dies der Fall ist. Zwar stimmen sechs von zehn Entscheidungsträgern (58 %) voll und ganz zu, dass ihre jeweiligen Unternehmen Cyber-Resilienz erlangt haben, doch waren 87 Prozent in den vergangenen drei Jahren Opfer eines erfolgreichen Cyberangriffs, der in Ihrem Geschäft zu Schäden oder Störungen oder zu Sicherheitsverstößen geführt hat. Die 42 Prozent, die das Gefühl haben, noch nicht das erforderliche Maß an Resilienz erreicht zu haben, beurteilen das Sicherheitsniveau ihres Unternehmens möglicherweise treffender. Etwa die Hälfte der Entscheidungsträger im Bereich Unternehmenssicherheit – und auch jene, die angaben, Cyber-Resilienz entwickelt zu haben – äußerten sich dahingehend, dass die Ausweitung von Projekten zur digitalen Transformation und die andauernde Arbeit aus der Ferne
die Wahrscheinlichkeit erhöhen,
Opfer eines Angriffs zu werden.

Abbildung 5.1
**CYBER-RESILIENZ DES UNTERNEHMENS**
(STIMME VOLL UND GANZ ZU)

## ÜBER ANOMALI

Anomali ist der führende Anbieter für Cybersicherheitslösungen zur Intelligence-basierten Erkennung und Reaktion (XDR). Die Anomali-Plattform basiert auf Big-Data-Management und wird ergänzt durch künstliche Intelligenz und maschinelles Lernen. Sie bietet proprietäre Funktionen, die ein außergewöhnliches Telemetrievolumen aus vom Kunden bereitgestellten Sicherheitslösungen mit dem größten Repository globaler Intelligence korrelieren. So können Sicherheitsteams Bedrohungen präzise erkennen, die Reaktion optimieren, Resilienz erreichen und Angreifer und Sicherheitsverstöße stoppen. Unsere Cloud-First-Lösungen auf SaaS-Basis lassen sich problemlos in bestehende Sicherheitstechnik integrieren und gestatten eine hybride Bereitstellung. Anomali wurde 2013 gegründet und bedient Organisationen des öffentlichen und privaten Sektors, ISACs, MSSPs und Global-1000-Kunden weltweit in allen wichtigen Branchen. Führende Venture-Unternehmen wie Google Ventures, General Catalyst und IVP unterstützen Anomali. Weitere Informationen finden Sie unter www.anomali.com.

## SO HILFT ANOMALI

Cyberkriminelle, staatlich unterstützte Akteure und Hacktivisten schieben Überstunden, um Unternehmen als Ausnutzungsziele auszuwählen. Unternehmen benötigen Daten und Einblicke zur Threat Intelligence, um ihre Schwachstellen vollständig zu verstehen, Bedrohungen einen Schritt voraus sein und schnell auf Ereignisse reagieren zu können.

Die Intelligence-basierte Extended Detection and Response Lösung (XDR) von Anomali bietet Sicherheitsteams den erforderlichen Kontext, um Bedrohungen schneller und effektiver zu verhindern und abzuwehren. Dadurch, dass interne und externe Daten, Informationen und Intelligence zu Bedrohungen automatisiert erfasst und analysiert werden, können Sicherheitsteams Bedrohungen schnell verstehen, die Auswirkungen ermitteln und auf Basis dieser Erkenntnisse eine optimale Reaktion festlegen.

## PRODUKTE VON ANOMALI

**Anomali ThreatStream**
Threat Intelligence-Management, das die Erfassung und Verarbeitung von Rohdaten automatisiert und diese in nutzbare Threat Intelligence verwandelt, um die Erkennung zu beschleunigen, Untersuchungen zu optimieren und die Produktivität von Analysten zu steigern.

**Anomali Match**
Intelligence-basierte Extended Detection and Response Lösung (XDR), mit der Unternehmen Bedrohungen schnell erkennen und in Echtzeit darauf reagieren können. Match gleicht automatisch ALLE Sicherheitstelemetriedaten mit der gesamten Threat Intelligence ab, sodass über 190 Billionen Bedrohungsereignisse pro Sekunde geprüft und bekannte und unbekannte Bedrohungen erkannt werden können, um Sicherheitsverstöße und Angreifer zu stoppen.

**Anomali Lens**
Natural Language Processing (NLP) ist eine leistungsstarke Erweiterung, die das Erfassen von Threat Intelligence ermöglicht. Dabei werden webbasierte Inhalte automatisch gescannt, um relevante Bedrohungen zu ermitteln und die zugehörige Recherche und Berichterstellung zu optimieren.

Um herauszufinden, wie Anomali Ihr Unternehmen dabei unterstützen kann, Cyber-Resilienz zu erreichen, besuchen Sie uns unter **anomali.com.**

# Methodik

Anomali beauftragte The Harris Poll mit der Durchführung von Online-Umfragen unter Entscheidungsträgern im Bereich Unternehmenssicherheit in Unternehmen mit 5.000 oder mehr Mitarbeitenden. Die Umfrage wurde zwischen dem 9. September und dem 13. Oktober 2021 in den folgenden Ländern durchgeführt:


* Australien, Singapur, Hongkong, Indien und Neuseeland
** Mexiko und Brasilien

**QUALIFIZIERUNGSKRITERIEN**

- **18** Jahre oder älter
- **Vollzeitbeschäftigung**
- In den Bereichen **Finanzdienstleistungen, Pharmazie, Gesundheitswesen, Telekommunikation Fertigung und Unternehmensdienstleistungen**
- In einer **IT-Rolle**
- **Technologieperspektive:** auf Managerebene oder höher und mit Einfluss auf Lösungen zur Datensicherheit
- **Geschäftsperspektive:** auf Direktorebene oder höher und mit Einfluss auf die Strategie zur Datensicherheit

Die Rohdaten wurden nach Bedarf nach der Anzahl der Unternehmen innerhalb einer auf der Mitarbeiteranzahl basierenden Größenklasse gewichtet, sodass sie die tatsächlichen Anteile an der Gruppe der Unternehmen mit 5.000 oder mehr Mitarbeitenden in den ausgewählten Branchen wie Fertigung, Telekommunikation, Finanzdienstleistungen, Gesundheitswesen, Pharmazie sowie Unternehmens-, Wissenschafts- und Technikdienste widerspiegeln, und zwar für jedes Land separat. Die Länder wurden dann mit einer Postgewichtung kombiniert, um sie gleichmäßig in der Summe zu verteilen.