MANDIANT®

NOW PART OF Google Cloud

Threat Intelligence: eine globale Einschätzung

Aus unserem Bericht „Threat Intelligence: eine globale Einschätzung" geht hervor, dass Sicherheitsteams bezweifeln, ob alle Mitglieder der Führungsriege vollständig verstanden haben, welcher Art von Bedrohungen ihr Unternehmen ausgesetzt ist. Das könnte bedeuten, dass wichtige sicherheitsrelevante Entscheidungen ohne ein ausreichendes Verständnis der Gegner und ihrer Taktiken getroffen werden.

Sandra Joyce
VP, Mandiant Intelligence
Google Cloud

Als erster seiner Art bietet dieser Bericht Einblicke in die Vorgehensweise von Unternehmen beim Umgang mit globalen Cybersicherheitsbedrohungen. Die Ergebnisse beruhen auf umfassenden Interviews mit 1.350 Managern aus Geschäfts- und IT-Abteilungen, die in Unternehmen und Institutionen mit mindestens 1.000 Mitarbeitern sicherheitsrelevante Entscheidungen treffen. Die Umfrageteilnehmer sind in 13 Ländern in drei Regionen ansässig und in 18 Branchen tätig, unter anderem im Finanz- und Gesundheitswesen sowie im öffentlichen Dienst.

Aufgrund ihrer Qualität und globalen Abdeckung stellen die Antworten unserer Umfrageteilnehmer eine gute Momentaufnahme der Analyse und Nutzung von Threat Intelligence durch Führungkräfte großer Unternehmen mit Entscheidungsbefugnis für die Cybersicherheit dar.

Ergebnisse

Die Antworten bestätigen die ursprüngliche Annahme, dass Teams Threat Intelligence schätzen und aus mehreren Quellen beziehen, sich aber bei ihrer unternehmensweiten praktischen Anwendung oft noch schwer tun.

Dabei stehen die Sicherheitsteams der größten Konzerne der Welt nicht nur enorm unter Druck, sondern sind oft auch bei der unternehmensinternen Kommunikation mit Herausforderungen konfrontiert. Und obwohl Sicherheitsprofis nur zu gut wissen, wie nützlich ausführlichere Informationen über die Angreifer wären, müssen viele von ihnen Entscheidungen treffen, ohne genau zu wissen, wer ihre Infrastruktur angreift und warum. Aufgrund dieser fehlenden Informationen entscheiden sie sich möglicherweise für Sicherheitsmaßnahmen, die das angestrebte Ziel verfehlen.

96 % der Umfrageteilnehmer sind mit der Qualität der genutzten Threat Intelligence zufrieden

47 % nannten die effektive Nutzung der Threat Intelligence im gesamten Sicherheitsteam als eine ihrer größten Herausforderungen

67 % sind der Meinung, dass ihre Führungsriege die Cyberbedrohungen, denen ihre Organisation ausgesetzt ist, unterschätze

96 % der Entscheidungsträger im Bereich der Cybersicherheit halten es für wichtig, zu wissen, welche Angreifer oder Angreifergruppen ihre Organisation im Visier haben

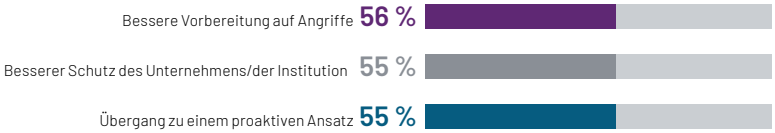
79 % treffen eigenen Aussagen zufolge die meisten Entscheidungen ohne ausreichende Hintergrundinformationen über ihre Gegner

Bedrohungsbewusstsein und Sicherheitsvertrauen der Praktiker

Bei den für diesen Bericht durchgeführten Untersuchungen haben wir weltweit Diskrepanzen zwischen dem selbstsicheren Umgang von Sicherheitsteams mit Cyberangriffen und ihrer Neigung zur Entscheidungsfindung ohne umfassende Informationen über die Bedrohungsurheber und deren Taktiken, Techniken und Prozeduren (TTPs) festgestellt.

Dennoch meinten die meisten (96 %) der befragten Entscheidungsträger im Bereich der Cybersicherheit, dass es wichtig sei, zu wissen, welche Angreifer oder Angreifergruppen ihre Organisation im Visier haben könnten.

Warum halten Sie als Entscheidungsträger im Bereich der Cybersicherheit es für wichtig, zu wissen, welche Akteure Ihre Organisation angreifen könnten?

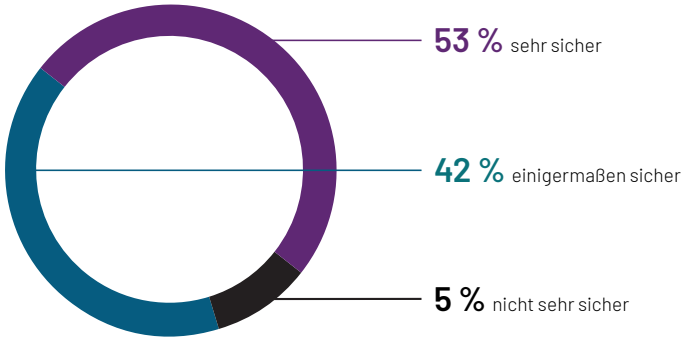


Obwohl fast alle Umfrageteilnehmer Informationen über Bedrohungsurheber für wichtig halten – und 96 % mit der Qualität ihrer Threat Intelligence zufrieden sind – treffen 79 % eigenen Angaben zufolge die meisten Entscheidungen über Cyberangriffe, ohne zu wissen, wer ihre Infrastruktur im Visier haben könnte. Nur 35 % meinten, dass ihr Team eine umfassende Übersicht über verschiedene Angreifergruppen und deren TTPs habe.

Darüber hinaus glauben 67 % der Entscheidungsträger mit Verantwortung für die Cybersicherheit, dass die Cyberbedrohungen für ihr Unternehmen bzw. ihre Institution von der Führungsriege unterschätzt werden. Mehr als zwei Drittel (68 %) stimmten der Aussage zu, dass ihr Team ein besseres Verständnis der Bedrohungslage benötige.

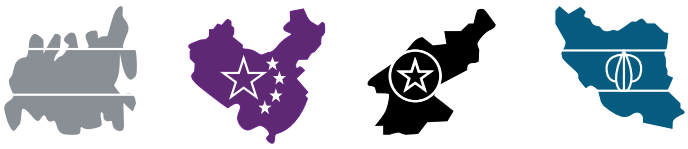
Trotz dieser Bedenken sind die Entscheidungsträger zuversichtlich, dass ihr Team Sicherheitsbedrohungen in Schach halten könnte. Fast alle Umfrageteilnehmer (95 %) sind der Meinung, dass sie ihrer Führungsriege ein nachweisbar moderat bis hochgradig effektives Cybersicherheitsprogramm vorlegen könnten.

Wie sicher sind Sie sich, dass Sie Ihrer Führungsriege (dem Vorstand oder der Unternehmensleitung) beweisen könnten, dass Ihr Team über ein effektives Cybersicherheitsprogramm verfügt?



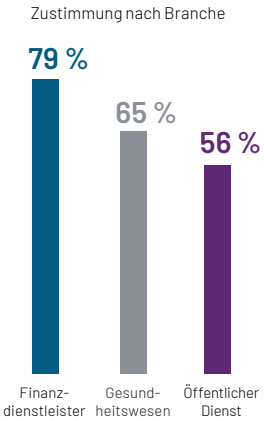
Viele Entscheidungsträger sind sich sicher, dass ihre Teams ausreichend auf die Abwehr eines Cyberangriffs erheblichen Ausmaßes durch finanziell motivierte Cyberkriminelle (91 %), Hacktivisten (89 %) oder staatlich gesponserte Angreifer (83 %) vorbereitet seien.

Gegen staatlich gesponserte Angreifer aus welchem der folgenden Länder könnte Ihr Unternehmen bzw. Ihre Institution sich Ihrer Meinung nach nicht vollständig erfolgreich verteidigen?



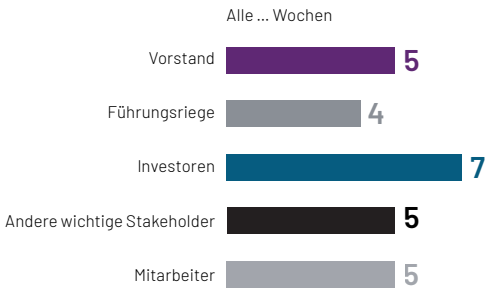
Russland 57 % China 53 % Nordkorea 52 % Iran 44 %

Glauben Sie, dass Ihr Team ein besseres Verständnis der Bedrohungslage benötigt?



Eine mögliche Erklärung für den Mangel an Informationen über Bedrohungsurheber ist der relativ seltene Informationsaustausch zwischen Entscheidungsträgern im Bereich der Cybersicherheit und anderen Teilen der Organisation. Unseren Umfrageteilnehmern zufolge wird die Cybersicherheit im Durchschnitt nur alle vier bis fünf Wochen mit Gruppen außerhalb des Sicherheitsteams – wie dem Vorstand, der Führungsriege und anderen Stakeholdern – diskutiert. Diskussionen mit Investoren finden noch seltener – durchschnittlich alle sieben Wochen – statt.

Wie oft diskutiert Ihre Abteilung Cybersicherheitsthemen mit den folgenden Gruppen? (Durchschnitt aller Regionen)

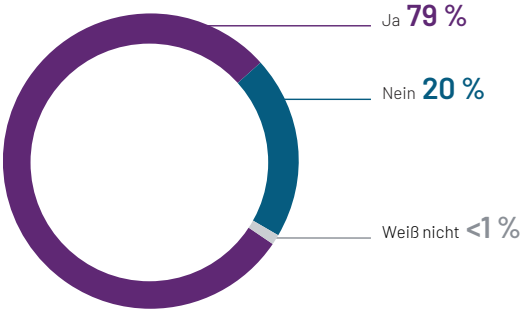


Herausforderungen und Risiken bei der praktischen Nutzung von Threat Intelligence

Die Wichtigkeit von Threat Intelligence ist unbestritten. Die große Mehrheit der Umfrageteilnehmer hielt es für wichtig, Angreifer (85 %), die genutzten Angriffstools und -taktiken (88 %) und die Beweggründe für einen Angriff (87 %) zu identifizieren. Doch obwohl Sicherheitsteams detaillierte Threat Intelligence zu schätzen wissen, gestehen sie Verbesserungsbedarf bei deren konsequenter Nutzung ein. Nur 34 % berücksichtigen eigenen Angaben zufolge beim Testen ihrer Sicherheitsmaßnahmen und -prozesse stets die Urheber potenzieller Angriffe.

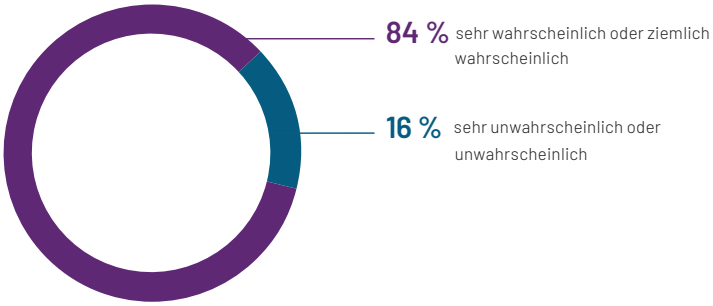
Sicherheitsteams investieren auch nicht genügend Zeit in die Aufdeckung von und Reaktion auf Bedrohungen. Eine beträchtliche Mehrheit der Befragten (79 %) gab zu, dass ihr Team mehr Zeit und Energie in die Erkennung kritischer Cybersicherheitstrends investieren könnte. Fast alle (98 %) meinten, dass sie ihre Cybersicherheitsstrategie schneller ändern müssten, wenn aktuelle Threat Intelligence dies erfordert.

Glauben Sie, dass Ihr Team mehr Zeit und Energie auf die Verfolgung kritischer Cybersicherheitstrends konzentrieren sollte?



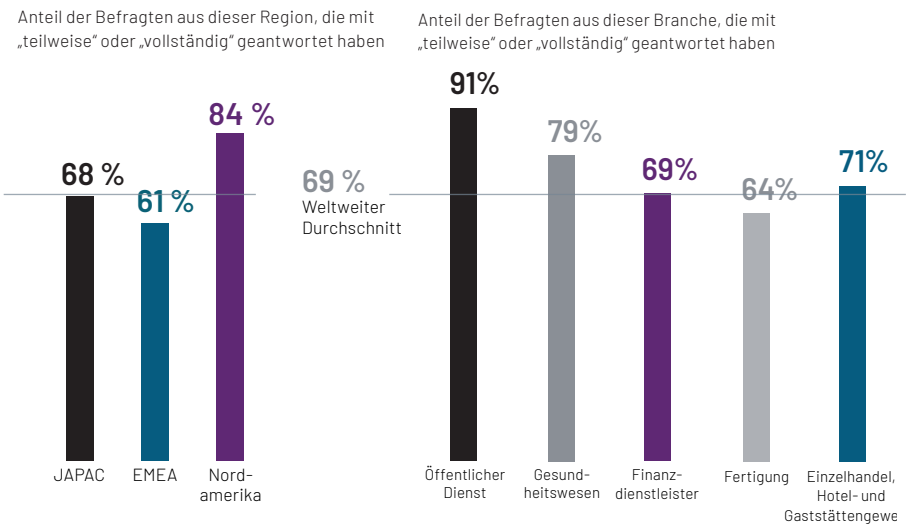
Zur Gewinnung praxistauglicher Threat Intelligence muss ein Sicherheitsteam jeden Tag große Datenmengen verarbeiten. Die große Mehrheit (84 %) der Befragten befürchten, Bedrohungen oder Vorfälle in ihrer Infrastruktur aufgrund der großen Anzahl der zu analysierenden Warnmeldungen und Daten zu übersehen. Diese überwältigende Informationsflut beeinträchtigt auch das Wohlbefinden des Personals: Mehr als zwei Drittel (69 %) der Mitarbeiter von Sicherheitsteams fühlen sich eigenen Angaben zufolge überfordert.

Für wie wahrscheinlich halten Sie es, dass echte Bedrohungen/Vorfälle in Ihrer Infrastruktur aufgrund der großen Anzahl der zu analysierenden Warnmeldungen und Daten übersehen werden?



Das größte Burnout-Risiko durch die schiere Menge an Daten und Warnmeldungen zur Threat Intelligence wurde von Umfrageteilnehmern aus Nordamerika gemeldet. Schlüsselt man die Antworten nach Branche auf, ist die Wahrscheinlichkeit einer diesbezüglichen Überforderung im öffentlichen Dienst am größten.

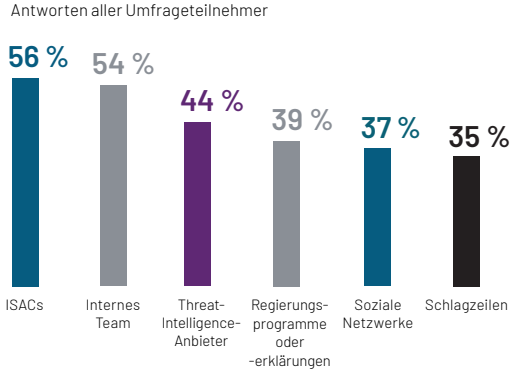
Wie sehr sind die Mitarbeiter Ihrer IT-Sicherheitsteams Ihrer Meinung nach von der Menge der Daten und/oder Warnmeldungen überwältigt, die sie bearbeiten müssen?



Die überwältigende Informationsflut stellt eine Herausforderung für nahezu alle Organisationen dar. Zusätzlich nannte fast die Hälfte (47 %) der Umfrageteilnehmer auch die effektive unternehmensweite Nutzung der Threat Intelligence als eine ihrer größten Herausforderungen und 38 % wissen eigenen Angaben zufolge nicht immer, was sie mit den verfügbaren Informationen tun sollten. Mehr als die Hälfte (53 %) meinten, dass der weltweite Fachkräftemangel in der Cybersicherheit ihre Fähigkeit, mit den neuesten Trends Schritt zu halten, gefährde. 42 % erwähnten in diesem Zusammenhang auch die konstante Weiterentwicklung der Bedrohungen.

Obwohl viele Teams die Nutzung von Threat Intelligence noch perfektionieren müssen, tragen sie weiterhin Informationen aus zahlreichen Quellen zusammen.

Welche Quellen nutzt Ihr Team, um sich über die Bedrohungslage auf dem Laufenden zu halten?



Zu viele Sicherheitsprofis teilen die zusammengetragenen Informationen jedoch nicht mit Kollegen außerhalb ihres Teams. 61 % der Befragten teilen Threat Intelligence entweder mit IT-Teams, zur Behebung von Infrastruktur- oder Anwendungsschwachstellen, oder mit IT-Sicherheitsmanagern, zur Priorisierung von Sicherheitsmaßnahmen. Ein viel kleinerer Teil (38 %) teilen Threat Intelligence auch mit anderen Mitarbeitern, um sie für Sicherheitsrisiken zu sensibilisieren.

Arbeiten Sie die folgende Liste durch, um Threat Intelligence (und die in sie investierten Mittel) effektiv zu nutzen:

Stellen Sie sicher, dass Ihre Daten vertrauenswürdig, aktuell und praxistauglich sind

Erstellen Sie als Ausgangspunkt ein belastbares Threat-Intelligence-Programm mit einer soliden Basis.

Verschaffen Sie sich eine Übersicht über die für Ihr Unternehmen bzw. Ihre Institution und Ihre Branche besonders relevanten aktiven Bedrohungen

Machen Sie sich dabei auch ein klares Bild der hinter diesen Bedrohungen stehenden Angreifer, ihrer Motive, Taktiken, Techniken und Prozesse (TTPs) und passen Sie Ihre Sicherheitsmaßnahmen entsprechend an.

Kommunizieren Sie mit Stakeholdern

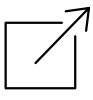
Leiten Sie relevante taktische, operative und strategische Informationen regelmäßig an die richtigen Stakeholder-Gruppen weiter, damit alle, bis hinauf auf die oberste Führungsebene und in den Vorstand, fundierte Sicherheits- und Geschäftsentscheidungen treffen können.

Setzen Sie Ressourcen dort ein, wo sie am dringendsten benötigt werden

Nutzen Sie Ihre Threat Intelligence, um zu beurteilen, welche Bedrohungen derzeit die größte Gefahr für Ihr Unternehmen darstellen. Beurteilen Sie Schwachstellen und potenzielle Einfallstore, weisen Sie ihnen eine auf dem Schweregrad basierte Risikobewertung zu und gehen Sie sie in der richtigen Reihenfolge an.

Testen Sie Ihre Abwehr

Testen Sie die Reaktion Ihres Unternehmens bzw. Ihrer Institution auf typische Angriffstaktiken der als relevant identifizierten Angreifer proaktiv. Bewerten Sie Ihren Schutz vor diesen Angreifern und Angreifergruppen und messen Sie Verbesserungen in Ihrem Programm im Verlauf der Zeit.



Handeln Sie proaktiv

Nutzen Sie die Threat Intelligence aus Ihren Sicherheitssystemen und -prozessen, um sich proaktiv vor potenziellen Bedrohungen zu schützen.

Fazit

Vor dem Hintergrund einer äußerst dynamischen Bedrohungslandschaft müssen Sicherheitsteams ihre Unternehmen bzw. Institutionen nicht nur vor finanziell motivierten Cyberkriminellen, sondern auch vor staatlich gesponserten Hackern schützen, deren Motive von Sabotage über Spionage bis hin zu Angriffen auf kritische Infrastrukturen reichen können.

In diesem Kontext können Entscheidungsträger Threat Intelligence nutzen, um Bedrohungen vorherzusehen und ihnen einen Riegel vorzuschieben, bevor sie Probleme verursachen. Unsere Ergebnisse zeigen, dass sich die überwältigende Mehrheit der Entscheidungsträger im Bereich Cybersicherheit der Bedeutung von Threat Intelligence bewusst ist und mit ihr bessere Entscheidungen treffen kann.

Trotz der nahezu einstimmig geäußerten Wertschätzung für Threat Intelligence wird sie bei der Bedrohungsabwehr jedoch nicht von allen Sicherheitsteams konsequent genutzt. Fast die Hälfte aller sicherheitsrelevanten Entscheidungen werden ohne Threat Intelligence zu den potenziellen Angreifern getroffen.

Sicherheitsteams befürchten, echte Bedrohungen zu übersehen, weil ihre Mitglieder mit der schieren Menge der zu sichtenden Daten überfordert sind. Mancherorts fehlt es zudem an qualifiziertem Personal, sodass die vorhandenen Mitarbeiter nicht immer wissen, wie sie die verfügbaren Informationen nutzen können. Bis es Sicherheitsteams gelingt, Threat Intelligence zu Bedrohungsurhebern besser zu nutzen, bleiben ihre Unternehmen bzw. Institutionen anfällig für die stetig steigende Anzahl von Cyberangriffen und die damit einhergehenden Störungen und Schäden.

Umfragemethodik: Die Umfrage für den Bericht „Threat Intelligence: eine globale Einschätzung" wurde im August und September 2022 im Auftrag von Mandiant von der global agierenden Marktforschungsagentur Vanson Bourne durchgeführt. Befragt wurden 1.350 Entscheidungsträger im Bereich IT-Sicherheit in Unternehmen und Institutionen mit mindestens 1.000 Mitarbeitern in den Regionen EMEA, Nordamerika und JAPAC.

Weitere Informationen finden Sie unter www.mandiant.de

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
Virginia 20190, USA Tel.: +1 703 935 1700
+1 833 3MANDIANT (362 6342)
info@mandiant.com

Über Mandiant

Mandiant ist als führender Anbieter von dynamischen Cyberabwehrlösungen, Threat Intelligence und Incident-Response-Services bekannt. Mandiant nutzt seine jahrzehntelange Praxiserfahrung, um Unternehmen und Institutionen bei der souveränen Prävention und Abwehr von Cyberbedrohungen zu unterstützen. Mandiant gehört nun zu Google Cloud.

MANDIANT
NOW PART OF Google Cloud