Kaspersky for Security Operations Centers

Bewertung von Quellen für Threat Intelligence

Ein Artikel von Artem Karasev, Das Kaspersky

kaspersky

Weitere Informationen finden Sie unter kaspersky.de
#bringonthefuture

Angesichts größerer Angriffsflächen und fortschrittlicherer Bedrohungen ist Vorfallsreaktion allein nicht genug. Zunehmend komplexe Umgebungen bieten Angreifern viele Möglichkeiten. Jede Branche und jedes Unternehmen hat ganz eigene individuelle Daten zu schützen und verwendet eigene Programme, Technologien etc. All dies führt dazu, dass in den möglichen Methoden zur Ausführung eines Angriffs sehr viele Variablen bestehen und täglich entstehen weitere neue Angriffsmethoden.

Seit einigen Jahren verschwimmen die Grenzen zwischen den verschiedenen Bedrohungsarten und den verschiedenen Arten von Bedrohungsakteuren. Methoden und Tools, die bisher nur für eine begrenzte Anzahl von Unternehmen eine Bedrohung waren, bedrohen heute eine Vielzahl von Unternehmen. Ein Beispiel dafür ist das Code-Dumping der Gruppe Shadow Brokers, die hochentwickelte Exploits (angeblich von der NSA entwickelt) kriminellen Vereinigungen anbietet, die sonst keinen Zugang zu derart komplexen Codes hätten. Ein weiteres Beispiel dafür ist das Aufkommen von APT-Kampagnen, die nicht auf Cyberspionage, sondern auf Diebstahl ausgerichtet sind – um an Geld zu kommen, mit dem andere Aktivitäten der APT-Gruppe finanziert werden sollen. Und dies sind nur einige Beispiele.

Methoden und Tools, die bisher nur für eine begrenzte Anzahl von Unternehmen eine Bedrohung waren, **bedrohen heute eine Vielzahl von Unternehmen.**

Es bedarf eines neuen Ansatzes

Weil Unternehmen immer häufiger das Ziel von ausgefeilten und zielgerichteten Angriffen sind, brauchen wir neue Methoden zur erfolgreichen Abwehr. Unternehmen müssen zu ihrem eigenen Schutz einen proaktiven Ansatz wählen und dabei ihre Sicherheitskontrollen fortwährend an eine sich stets verändernde Bedrohungsumgebung anpassen. Wer mit diesen Änderungen Schritt halten will, muss über ein effektives Threat Intelligence-Programm verfügen.

Threat Intelligence ist mittlerweile ein zentraler Bestandteil der Sicherheitsmaßnahmen von Unternehmen verschiedenster Größe in allen Branchen und Regionen. Weil Threat Intelligence in menschenlesbaren wie auch maschinenlesbaren Formaten zur Verfügung steht, kann sie die Sicherheitsteams mit sinnvollen Informationen während des gesamten Zyklus des Vorfallsmanagements unterstützen und zur informierten strategischen Entscheidungsfindung beitragen (Abbildung 1).

Allerdings hat die wachsende Nachfrage nach externer Threat Intelligence zu einer wahren Flut an Threat Intelligence-Anbietern geführt, von denen jeder massenhaft verschiedene Leistungen anbietet. Ein großer und wettbewerbsintensiver Markt mit unzähligen komplexen Optionen kann die Wahl der richtigen Lösung für das eigene Unternehmen sehr verwirrend und frustrierend machen.

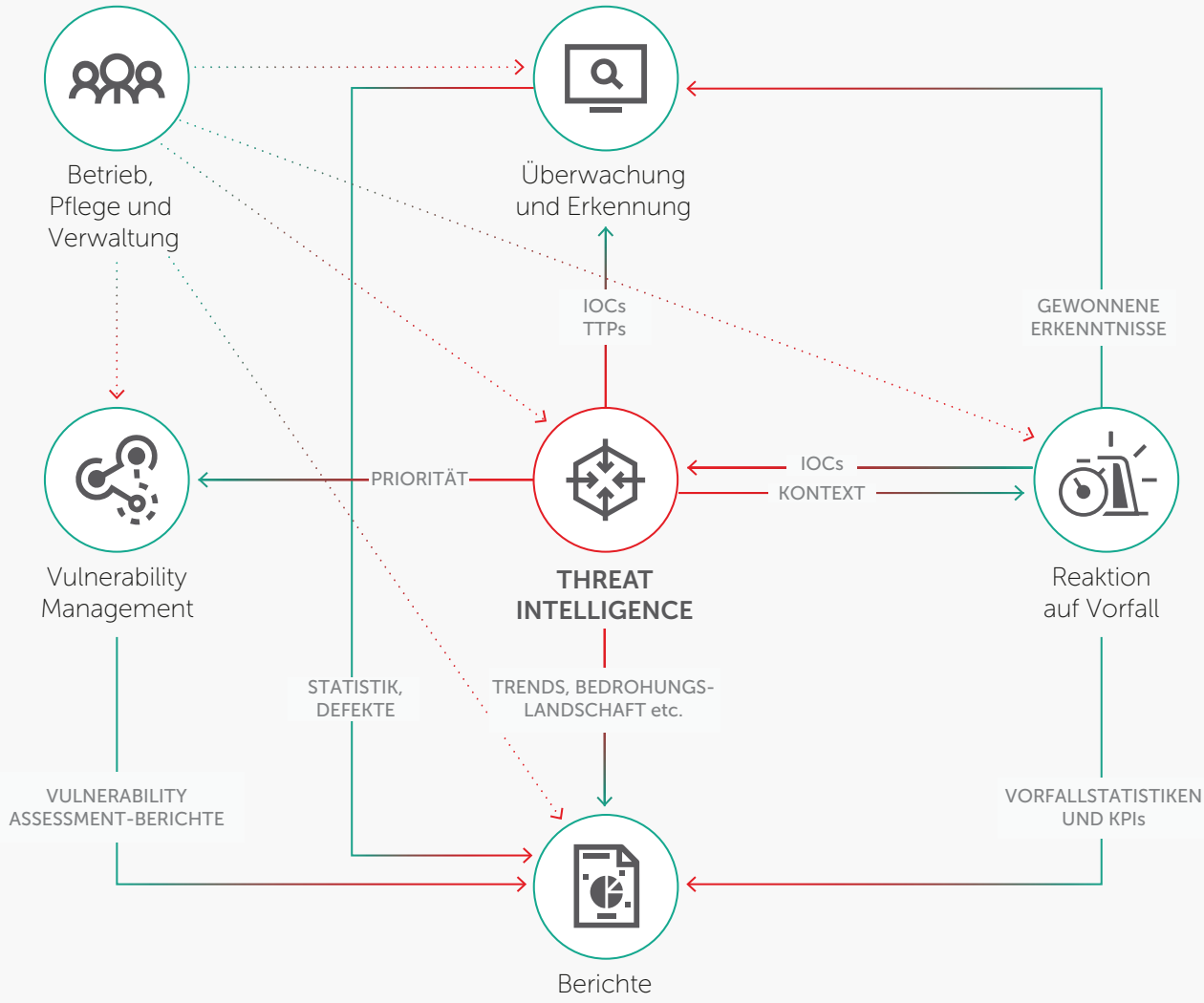

Abbildung 3
Threat Intelligence-getriebene Sicherheitsmaßnahmen

Threat Intelligence, die nicht an die Besonderheiten Ihres Unternehmens angepasst ist, kann die Situation verschlimmern. In vielen Unternehmen verbringen die Sicherheitsanalysten heute mehr als die Hälfte ihrer Arbeitszeit damit, False Positives auszusortieren, anstatt proaktiv dem Threat Hunting nachzugehen und Abwehrmaßnahmen durchzuführen. Dadurch steigt die Erkennungszeit deutlich an. Wenn Ihre Sicherheitsmaßnahmen irrelevante oder ungenaue Informationen erhalten, steigt die Anzahl der Fehlalarme noch weiter. Dies kann zu ernsthaften negativen Folgen für Ihre Abwehrfunktionen führen – und für die allgemeine Sicherheit Ihres Unternehmens.

Wo es die beste Threat Intelligence gibt...

Wie also bewertet man die zahlreichen Quellen für Threat Intelligence, wie ermittelt man die für das eigene Unternehmen relevante Threat Intelligence und wie setzt man sie wirksam ein? Wie findet man sich angesichts der vielen Werbeanzeigen zurecht, in denen fast jeder Anbieter behauptet, über die beste Threat Intelligence zu verfügen?

Dies Fragen sind zwar berechtigt, sollten aber nicht die ersten sein, die Sie sich stellen. Viele Unternehmen lassen sich von den auffälligen Botschaften und vollmundigen Versprechen zu der Annahme verführen, dass sie ein externer Anbieter mit einem Superpower-Röntgen-Blick ausstatten kann. Dabei wird jedoch vollkommen außer Acht gelassen, dass sich die wertvollsten Informationen innerhalb des eigenen Unternehmensnetzwerks befinden...

Daten aus Intrusion Detection Systemen und aus Präventionssystemen, Firewalls, Programmprotokolle und Protokolle aus anderen Sicherheitskontrollen können viel Auskunft darüber geben, was im Inneren eines Unternehmensnetzwerks los ist. Sie können für das Unternehmen spezifische Muster von schädlichen Aktivitäten ermitteln. Außerdem können sie zwischen einem normalen Nutzer und einem Netzwerkverhalten unterscheiden und zur Aufrechterhaltung einer Aktivitätenspur zum Datenzugriff beitragen.

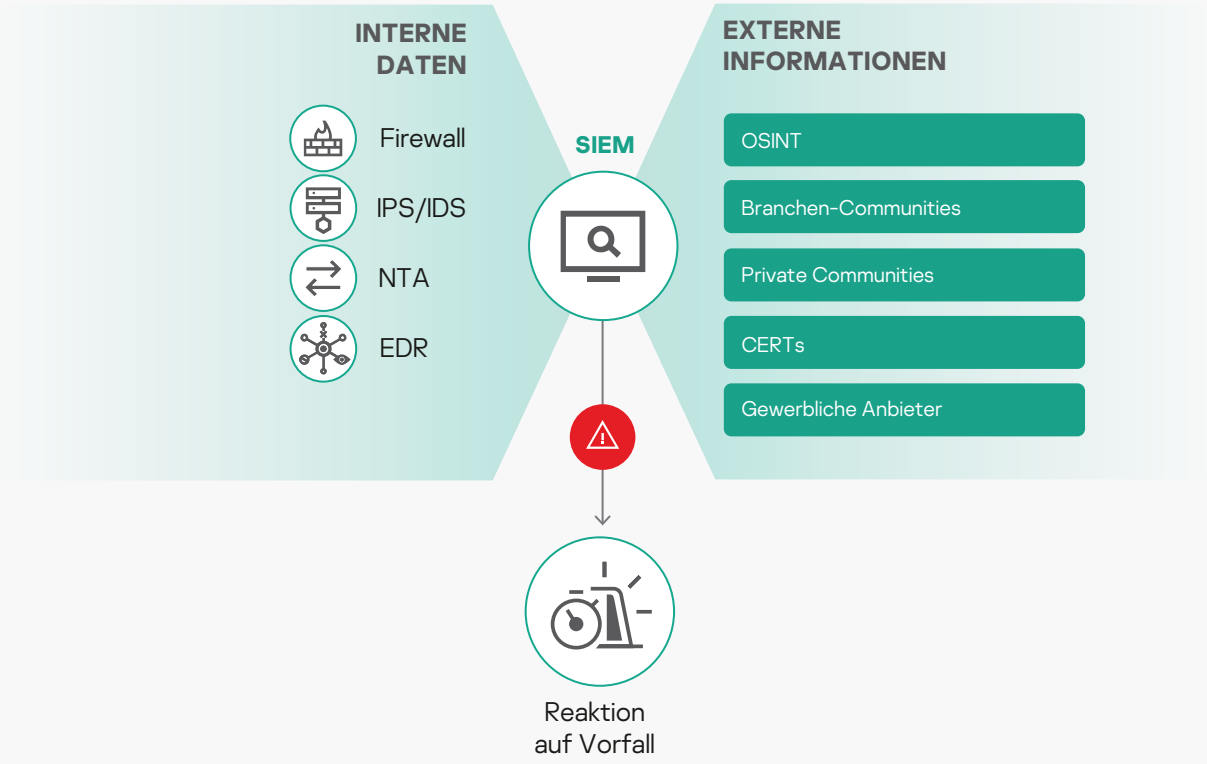

Abbildung 3
Operationalisierung externer Bedrohungsinformationen

Wie ein Angreifer denken

Um ein wirksames Threat Intelligence-Programm erstellen zu können, müssen Unternehmen – auch die mit einem Security Operations Center – wie ein Angreifer denken. So lassen sich die wahrscheinlichsten Ziele ermitteln und schützen. Um den vollen Mehrwert aus einem Threat Intelligence-Programm ziehen zu können, ist ein sehr klares Verständnis davon erforderlich, welche die zentralen Assets sind und welche Datensätze und Geschäftsprozesse für die Erreichung der Unternehmensziele kritisch sind. Die Ermittlung dieser „Kronjuwelen" ermöglicht es den Unternehmen, um diese herum Datenerfassungspunkte einzurichten und mit extern verfügbaren Bedrohungsinformationen weiter abzugleichen. Angesichts der begrenzten Ressourcen, über die die Abteilungen für Informationssicherheit üblicherweise verfügen, ist das Profiling eines ganzen Unternehmens ein immenses Unterfangen. Die Lösung besteht darin, einen risikobasierten Ansatz zu wählen und sich so zuerst auf die empfindlichsten Ziele zu konzentrieren.

Sobald die Quellen für Threat Intelligence definiert und operationalisiert wurden, kann das Unternehmen damit beginnen, über die Aufnahme externer Informationen in seine bestehenden Arbeitsabläufe nachzudenken.

Eine Frage des Vertrauens

Externe Quellen für Threat Intelligence unterscheiden sich im Vertrauensgrad:

- Offene Quellen stehen kostenlos zur Verfügung. Allerdings mangelt es ihnen oftmals an Kontext, und sie bringen viele False Positives hervor.
- Eine gute Wahl für den Anfang ist ein Zugang zu branchenspezifischen Communities zum Austausch von Informationen, wie das Financial Services Information Sharing and Analysis Center (FS-ISAC). Diese Communities liefern sehr wertvolle Informationen, jedoch haben oftmals nur Mitglieder Zugang dazu.
- Kommerzielle Quellen für Threat Intelligence sind viel verlässlicher, möglicherweise aber mit hohen Kosten verbunden.

Der Leitgrundsatz für die Auswahl externer Quellen für Threat Intelligence sollte lauten: Qualität geht vor Quantität. Einige Unternehmen glauben möglicherweise, dass es für eine möglichst gute Transparenz möglichst vieler Quellen für Threat Intelligence bedarf. Das mag in manchen Fällen sogar zutreffen – beispielsweise in Bezug auf sehr vertrauenswürdige Quellen, einschließlich kommerzieller Quellen, sofern die Threat Intelligence auf das konkrete Bedrohungsprofil des Unternehmens zugeschnitten ist. Andernfalls besteht das erhebliche Risiko, dass Ihre Sicherheitsteams mit irrelevanten Informationen überflutet werden.

Die Überlappung der von spezialisierten Threat Intelligence-Anbietern bereitgestellten Informationen kann sehr gering sein. Weil sich ihre Informationsquellen und Erfassungsmethoden unterscheiden, sind die von ihnen gelieferten Erkenntnisse in gewisser Hinsicht einzigartig. Beispielsweise kann es sein, dass ein Anbieter aufgrund seiner größeren Präsenz in einer bestimmten Region mehr Einzelheiten zu den von dieser Region ausgehenden Bedrohungen hat, während ein anderer Anbieter mehr Einzelheiten zu konkreten Bedrohungsarten hat. Ein Zugang zu beiden Quellen kann also vorteilhaft sein – und in Kombination können beide zu einem größeren Bild beitragen und das Threat Hunting sowie die Reaktion auf Vorfälle wirksamer steuern. Bedenken Sie jedoch, dass diese Arten von vertrauenswürdigen Quellen ebenfalls eine sorgfältige vorherige Bewertung erfordern. Nur so kann sichergestellt werden, dass die erhaltenen Informationen für die konkreten Anforderungen und Anwendungsfälle Ihres Unternehmens geeignet sind, wie Sicherheitsmaßnahmen, Reaktion auf Vorfälle, Risikomanagement, Schwachstellenmanagement, Einsatz von Red Teams etc.

Bei der Beurteilung kommerzieller Threat Intelligence-Angebote zu beachtende Aspekte

Es gibt nach wie vor keine allgemein gültigen Kriterien für die Beurteilung verschiedener kommerzieller Threat Intelligence-Angebote. Nachstehend werden jedoch einige Aspekte aufgezählt, die dabei beachtet werden sollten:

- Suchen Sie nach Informationen mit globaler Reichweite. Angriffe kennen keine Grenzen – ein Angriff auf ein Unternehmen in Lateinamerika kann seinen Ursprung in Europa haben oder umgekehrt. Bezieht der Anbieter seine Informationen weltweit und gleicht er scheinbar getrennte Aktivitäten in kohäsiven Kampagnen ab? Mit solchen Informationen können Sie besser die geeigneten Maßnahmen treffen.
- Wenn Sie nach strategischeren Inhalten für Ihre langfristige Sicherheitsplanung suchen, wie:
  - Umfassende Sicht auf Angriffstrends
  - Von Angreifern angewandte Techniken und Methoden
  - MOTIVATION
  - Attributionen etc.,

dann suchen Sie nach einem Threat Intelligence-Anbieter mit einer nachweislichen Erfolgsbilanz bei der dauerhaften Aufdeckung und Untersuchung komplexer Bedrohungen in Ihrer Region oder Branche. Außerdem ist es wichtig, dass der Anbieter seine Recherche-Ressourcen an die Besonderheiten Ihres Unternehmens anpassen kann.

- Der Kontext macht Daten zu Informationen. Bedrohungsindikatoren ohne Kontext sind wertlos – Sie sollten nach Anbietern suchen, die Ihnen sagen können, ob und inwiefern bestimmte Daten für Sie relevant sind. Beziehungskontext (z. B. mit den ermittelten IP-Adressen oder URLs, von denen die jeweilige Datei heruntergeladen wurde, verbundene Domänen) liefert einen Mehrwert. Dadurch wird die Vorfallsuntersuchung gefördert und eine bessere „Sondierung" des Vorfalls durch die Aufdeckung neu erhaltener verbundener Gefährdungsindikatoren in dem Netzwerk unterstützt.
- Es wird angenommen, dass Ihr Unternehmen bereits über bestimmte Sicherheitskontrollen mit den dazugehörigen definierten Prozessen verfügt und dass es für Sie wichtig ist, Threat Intelligence mit den Tools zu verwenden, die Sie bereits verwenden und kennen. Suchen Sie also nach Liefermethoden, Integrationsmechanismen und Formaten, die eine reibungslose Integration der Threat Intelligence in Ihre bestehenden Sicherheitsmaßnahmen unterstützen.

Bei Kaspersky konzentrieren wir uns schon seit zwanzig Jahren auf die Untersuchung von Bedrohungen. Mit Petabytes an aussagekräftigen Bedrohungsdaten, fortschrittlichen Machine Learning-Technologien und einem Pool weltweit agierender Experten unterstützt Sie Kaspersky mit der neuesten Threat Intelligence aus der ganzen Welt. S halten Sie Ihre Cyber-Immunität auch gegen bisher unbekannte Cyberangriffe aufrecht.

Weitere Informationen finden Sie auf:
https://www.kaspersky.de/enterprise-security/security-operations-center-soc

Cyber Threats News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
Cybersicherheit für KMUs: kaspersky.de/business
Cybersicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven. Transparent. Independent.