Intelligente Sicherheit: Verwendung von Machine Learning zum Erkennen komplexer Cyberangriffe

Ein fortschrittliches, datengesteuertes Cybersicherheitsmodell beschleunigt die Erkennung und reduziert Risiken.

Microsoft

Angreifer warten nicht, bis Ihre Sicherheitssoftware auf dem neuesten Stand ist. Branchenberichten zufolge können komplexe Cyberangriffe etwa 200 Tage lang unerkannt bleiben. In der heutigen Bedrohungslandschaft benötigen Unternehmen intelligente Sicherheitslösungen, die kontinuierlich weiterentwickelt werden, um mit neuen Bedrohungen Schritt zu halten.

Ist Ihr Unternehmen in der Lage, die wichtigen Bedrohungen im Grundrauschen all Ihrer Daten zu finden? Lesen Sie weiter, um zu erfahren, wie Ihnen ein fortschrittliches Sicherheitsmodell dabei helfen kann, Ihre Risiken zu reduzieren.

Microsoft

INHALT

Microsoft

200 Tage bis zur Erkennung? Branchenberichte zeichnen ein düsteres Bild

Wenn Sicherheitsexperten eine Sicherheitsverletzung erkennen, ist es so gut wie sicher, dass der Angreifer schon seit einiger Zeit in der Umgebung des Opfers aktiv war. Aber wie lange?

Viele in der Branche akzeptierten „200 Tage" als einen Standard zum Formulieren des Durchschnittswerts. Dieser „Standard" ist jedoch aus verschiedenen Gründen auch problematisch.

Zum einen ist es einfach eine lange Zeit. Es bedeutet, dass sich ein erfahrener Cyberangreifer oder eine Gruppe von Angreifern rund sechseinhalb Monate in Ihren Systemen zu schaffen gemacht hat. Während dieser Zeit waren die sensiblen Daten und das geistige Eigentum Ihres Unternehmens potenziell ungeschützt, und mit jedem Tag ist die Kompromittierung Ihrer Daten unvermeidlicher geworden.

Die Angst vor dem, was während dieser 200 Tage geschieht, hat die Statistik für CISOs, CSOs und sogar CEOs zu einem Gradmesser gemacht. Unternehmen, Sicherheitsexperten und die gesamte Technologiebranche fordern heute neue, leistungsfähigere Sicherheitsmaßnahmen, die diese Zahl reduzieren.

In der Praxis sind „200 Tage" nur ein Meilenstein, eine Zahl, die zum Messen und Erörtern der Fortschritte der Branche verwendet wird. CISOs und CSOs wissen, dass die Tagesanzahl nicht der wichtigste Aspekt bei einem Angriff ist. Was uns nachts nicht schlafen lässt, ist die Tatsache, dass bereits ein Tag zu lang und es immer schon zu spät ist, wenn ein Angriff erkannt wird.

Um dies zu erreichen, benötigen Unternehmen einen intelligenteren Ansatz, mit dem sie Bedrohungen früher erkennen und eine Wende im Kampf gegen komplexe Cyberangriffe herbeiführen können. Dieses Whitepaper soll Ihnen einen Einblick geben, wie Angreifer bei komplexen Bedrohungen vorgehen, um Ihre sensiblen Daten zu stehlen, und wie die fortschrittliche Rechenleistung der Cloud in Verbindung mit Data Science und menschlichen Experten dazu beitragen kann, die Erkennung von Angriffen in Ihrem Unternehmen zu beschleunigen.

Doch wie genau und hilfreich ist diese etwas willkürlich erscheinende Zahl? Selbst unter Sicherheitsexperten variieren die Schätzungen. Hier ein kurzer Überblick, wie verschiedene Unternehmen das Problem wahrnehmen:

146 Tage:

M-Trends-Bericht 2016, Mandiant, ein FireEye-Unternehmen

229 Tage:

Aktuelle Advanced Threat Monitoring-Seite von Lockheed Martin

200 Tage:

Advanced Threat Analytics-Seite von Microsoft

Steigt die Zahl wieder?

Der aktuelle Untersuchungsbericht von Verizon zu Datenpannen nennt keine konkrete Zahl, zeigt aber, dass das Defizit nach einer geringfügigen Verbesserung im Jahr 2014 im letzten Jahr tatsächlich zugenommen hat.

Die 1-Milliarden-Dollar-Schwelle: Das Gefährdungspotenzial ist größer denn je

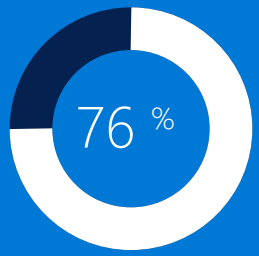
Angreifer, die mit leistungsfähigen Exploits angreifen, sind für jedes Unternehmen eine ständige Sorge. Bei dieser es um weit mehr geht als nur den anfänglichen finanziellen Schaden, der durch einen Angriff entsteht. Dies gilt für kleine Unternehmen im gleichen Maße wie für große. Die Motive der hochqualifizierten, finanziell gut ausgestatteten und sich ständig weiterentwickelnden Cyberangreifer reichen von Diebstahl, über Industriespionage bis hin zu großangelegten Angriffen auf Nationalstaaten.

Zunächst gibt es die finanziellen Beweggründe. Die vielen böswilligen Akteure, die komplexe Angriffe nutzen, wollen heute mit ihren Aktionen Profit machen. Es überrascht daher nicht, dass das Ausmaß der Schäden immer größer wird.

2015 wurde ein neuer Schwellenwert erreicht, als einem technisch versierten Hackerring ein Angriff auf mehr als 100 Banken in 30 Ländern gelang. Die Verluste wurden auf mehr als 1 Milliarde US-Dollar geschätzt. Aufgrund des erhöhten Risikos entwickeln sich Cyber-Versicherungspolicen für viele Unternehmen zu einem neuen Posten in den Betriebskosten. Die Prämien für diese neuen Versicherungen sollen sich bis 2020 verdreifachen und auf bis zu 7,5 Milliarden US-Dollar steigen.

200+

Die durchschnittliche Anzahl von Tagen, die die Angreifer vor der Erkennung in einem Netzwerk aktiv sind.



Bis zu 76 % aller Netzwerkangriffe sind auf Anmeldedaten zurückzuführen.

Durch Cyberkriminalität bedingte Schäden für die Weltwirtschaft:

500 Milliarden US-Dollar

Zudem gibt es die weniger quantifizierbaren und potenziell kostspieligeren Wunden, die erfolgreiche Cyberangriffe verursachen, beispielsweise beschädigtes Markenimage, misstrauische Kunden, stagnierendes Wachstum und beschädigte diplomatische Beziehungen. Obwohl sie sich nicht direkt beziffern lassen, können sich diese Auswirkungen langfristig nachteilig auf ein Unternehmen auswirken. Sie verringern die Kundentreue, erhöhen die Skepsis der Öffentlichkeit und setzen letztlich das für Angriffe zur Verantwortung zu ziehende Sicherheitspersonal unter Druck.

Andere Angriffe sind nicht durch finanzielle Anreize motiviert, sondern durch die Suche nach sensiblen Informationen. Nehmen Sie beispielsweise STRONTIUM. STRONTIUM ist eine bekannte Hackergruppe, zu deren Zielen Regierungsbehörden, diplomatische Vertretungen, Journalisten und Militärangehörige zählen. Ihnen geht es weder um Geld noch um die Größe eines Ziels. Sie suchen die sensibelsten Daten, die sie finden können. In ähnlicher Weise attackierte die 2013 aufgedeckte Hackergruppe Red October mindestens fünf Jahre lang staatliche und diplomatische Einrichtungen.

Dies klingt nicht nur wie eine Geschichte aus einem Spionageroman, das ist es auch. Noch vor zwei Jahrzehnten hätte ein Begriff wie „unsichtbare Kosten durch Sicherheitslücken" in unseren Ohren wie Science Fiction geklungen. Da so viel auf dem Spiel steht, ist es kein Wunder, dass die Budgets steigen und Unternehmen nach neuen Lösungen für das wachsende Problem von komplexen Cyberangriffen verlangen.

Durchschnittliche Kosten von Datenschutzverletzungen für ein Unternehmen:

3,5 Millionen US-Dollar

Eines von fünf kleinen und mittleren Unternehmen ist das Ziel von Cyberangriffen.

Geschätzter Schaden durch Produktivitätsverluste und Wachstumseinbußen infolge von Cyberkriminalität:

3 Billionen US-Dollar

-Ponemon Institute

Modus Operandi: Komplexe Angriffe in Aktion

Was geschieht bei einem komplexen Angriff während der 200 Tage, nachdem sich der Angreifer Zugang zu Ihrem Netzwerk verschafft hat? Angreifer nutzen heute verschiedene Methoden. Sie arbeiten sowohl mit traditionellen als auch neuen Techniken und erforschen ständig neue Wege, um Menschen und Technologien zu instrumentalisieren. Je länger ein Angriff in Ihrem System unentdeckt bleibt, desto mehr Informationen kann der Angreifer sammeln. Eine frühzeitige Erkennung ist daher von größter Bedeutung.

Fast 80 Prozent aller Angriffe beginnen mit einem guten altmodischen Betrug. Benutzer werden durch Spear-Phishing-Angriffe mit raffinierten Tricks dazu gebracht, ihre Informationen offenzulegen. Wie der Sicherheitsanbieter McAfee kürzlich bestätigte, wird es künftig noch raffiniertere Angriffe geben, darunter neue Integritätsangriffe, die interne Prozesse ändern und Daten bei der Übertragung im Netzwerk umleiten können. (Diese Methode wurde beim oben erwähnten 1-Milliarden-Dollar-Bankraub genutzt.)

Angreifer entwickeln ständig neue Formen von Schadsoftware, die besser verborgen werden oder sich selbst löschen können. Auch die Angriffsvektoren ändern sich: Ziel der Angreifer sind nicht mehr Inhalte auf PCs und Servern in den Firmenzentralen, sondern Außenstellen, private Computer von Mitarbeitern und sogar die Software in Mobiltelefonen, tragbaren Geräten und Fahrzeugen.

Die Cyber Kill Chain®

Angriffe umfassen im Allgemeinen sechs eindeutige Phasen, die unter Security Intelligence-Experten als die Cyber Kill Chain® (ein durch Lockheed Martin markenrechtlich geschützter Ausdruck) bekannt sind. Diese Phasen können nacheinander, gleichzeitig oder in einer anderen Reihenfolge stattfinden, und jede von ihnen bietet auch die Möglichkeit, Informationen zur Abwehr von Angriffen zu gewinnen:

Erkundung

Der Angreifer späht sein Ziel aus. Dazu setzt er technische Verfahren ein oder erkundet einfach die Website des Unternehmens. Häufig bleibt diese Phase unerkannt. Es ist jedoch möglich, einen Zusammenhang zwischen scheinbar harmlosen Verhaltensmustern herzustellen und daraus eine Frühwarnung abzuleiten.

Die Bewaffnung

Der Angreifer erstellt eine Shell, um eine schädliche Nutzlast zu verbergen. Es ist nicht immer möglich, die spezifische „Waffe" zu erkennen, die bei einem Angriff eingesetzt wird. Wird sie jedoch erkannt und mittels Reverse Engineering untersucht, so wird sie zu einem eindeutigen Fußabdruck für spätere ähnliche Angriffe.

Die Bereitstellung des Codes

Der Angreifer infiziert das System mit schädlichem Code oder verleitet einen Benutzer dazu, den Code herunterzuladen. Dies ist die kritische Phase, in der der Angreifer sich Zugang verschafft und mit seiner Arbeit beginnt.

Der Datenmissbrauch

Der Code schädigt das System. Manchmal beginnt der bereitgestellte Code sofort, die Befehle des Angreifers auszuführen. In anderen Fällen erfolgt der Angriff in mehreren Phasen, z. B. wenn das ursprüngliche Paket mit dem Download von anderem Code beginnt und erst dadurch entdeckt werden kann.

Steuerung und Kontrolle (C2)

Der Angreifer und der Code arbeiten zusammen, um Schwachstellen im System auszunutzen. Dies kann in Form von lateralen Bewegungen erfolgen, um Anmeldedaten mit höheren Berechtigungen zu erlangen, oder durch direktes Durchsuchen des Netzwerks nach den gewünschten Datenressourcen.

Vorsätzliche Aktionen

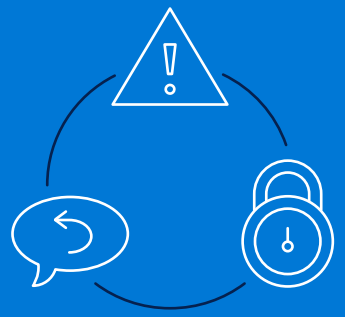
Sensible Daten werden gestohlen. An diesem Punkt war der Angriff erfolgreich. Ob finanzielle Informationen Ihrer Kunden, streng geheime Dokumente oder Blaupausen für ein neues Produkt – sie befinden sich jetzt in den Händen des Angreifers.

Quelle: Lockheed Martin

Einen Schritt voraus sein: Umstieg auf ein proaktives Sicherheitsmodell

Da sich komplexe Angriffe gut tarnen, müssen Unternehmen den Wechsel zu einem proaktiveren Sicherheitsmodell vollziehen, das ihre Fähigkeit verbessert, den Angreifer zu erkennen und sofort zu stoppen.

Während das traditionelle Modell der Unternehmenssicherheit beim Schutz der Netzwerkgrenzen ansetzte, empfehlen Experten heute einen proaktiveren Ansatz, der mit der Erkennung durch stabile Sicherheitsanalysen beginnt. Ab diesem Punkt verläuft bei diesem Modell alles Weitere in einem kontinuierlich verbesserten Zyklus, da vor einem Angriff greifende Abwehrmaßnahmen laufend anhand neuer Informationen verbessert werden. Diese werden aus der Erkennung und Abwehr von Angriffen gewonnen.



Das Erkennen

Durch die Erkennung auf Grundlage von Analysen sind Unternehmen in einer besseren Position, um sich vor komplexen Angriffen und neuen Angriffsstrategien zu schützen.

Das Reagieren

Die Reaktionsphase dient nicht nur dazu, eine Sicherheitslücke zu schließen, sondern sie liefert auch wertvolle neue Informationen.

Der Schutz

Die in den Erkennungs- und Reaktionsphasen gewonnenen Daten werden genutzt, um Abwehrtechnologien, die vor einem Angriff greifen, kontinuierlich zu verbessern.

In den letzten Jahren haben CISOs und CSOs mit der Implementierung von Security Intelligence-Maßnahmen, die Daten und Analysen zur schnellen Erkennung des nächsten Angriffs nutzen und die Abwehr insgesamt verbessern, an der Umsetzung dieses neuen Modells gearbeitet. Dazu sind beispielsweise folgende Schritte erforderlich:

- Investition in erweiterte Sicherheitssoftware und sichere Hardware
- Schulung von Mitarbeitern in Sicherheitserfordernissen und -risiken
- Bereitstellung einer Security Intelligence Event Management (SIEM)-Lösung
- Abonnieren von (oft mehreren) Threat Intelligence-Feeds
- Entwicklung von Prozessen, die Bedrohungsdaten korrelieren, und sogar Einstellung von Data Scientists zum Analysieren der Daten

Bisher umfassten diese Tools und Prozesse den Großteil der Branchenreaktionen auf komplexe Angriffe. Und wie bei vielen der ersten Bemühungen in der Technologiebranche fielen die Ergebnisse gemischt aus.

Der Punkt ist nicht, dass die Tools nicht effektiv sind. Dem M-Trends-Bericht 2016 von Mandiant zufolge wird die Dauer eines komplexen Angriffs drastisch verkürzt, wenn Unternehmen die Erkennung mit ihren eigenen Systemen gelingt. Doch es gibt auch Klagen – unter anderem in Bezug auf die Kosten, die zeitraubende Integration und den ineffizienten manuellen Prozess der Korrelation von Bedrohungsdaten und ihrer Einspeisung in das System.

Nachdem Sie Ihre SIEM-Lösung bereitgestellt und implementiert haben, stellt sich zudem ein weiteres großes Problem – irrelevante Daten. Selbst für die fortschrittlichsten Unternehmen sind die Anzahl von Warnungen und die Menge an Daten zu groß, um sie alle zu verstehen.

Wenn das Ziel all dieser Bemühungen, die Reduktion der besagten 200 Tage auf nahezu Echtzeit ist, so ist das Trennen des Wichtigen vom Unwichtigen mittlerweile eines der größten Hindernisse und einer der Gründe dafür, weshalb die Erkennung den Angreifern noch immer einen (kostspieligen) Schritt hinterherhinkt.

Um mit komplexen Angriffen Schritt zu halten, sollten Unternehmen weiter in ihre SIEMs und die zugehörigen Prozesse investieren. Nur die Cloud kann in der heute benötigten Größenordnung Schutz, Erkennung und Wartung der nächsten Generation (einschließlich über Plattformsensoren integrierter Warnmechanismen) bieten und garantieren, dass Schutzmechanismen mit echter Security Intelligence ständig weiterentwickelt werden.

Verbessern der Erkennung: Die Bedeutung eines eindeutigen Signals

Bei dem Versuch, die Erkennung von Angriffen zu beschleunigen, kämpfen Unternehmen mit einem widersprüchlichen Dilemma: Sie haben zu viele sicherheitsbezogene Daten, die verarbeitet werden müssen, und doch nicht genügend Informationen, um das Wichtige vom Unwichtigen zu trennen, und einen Vorfall schnell zu verstehen.

Die Herausforderung hierbei ist nicht nur die schiere Datenmenge, sondern auch die Separation der Daten. Viele Angriffsindikatoren erscheinen allein betrachtet harmlos oder sind nach Branchen, Regionen und Zeitrahmen getrennt. Ohne genauen Einblick in sämtliche Daten wird die frühzeitige Erkennung zu einem Glücksspiel. Diese Einschränkungen gelten selbst für die größten Unternehmen:

- Echte Threat Intelligence erfordert mehr Daten als die meisten Unternehmen selbst erfassen können.
- Die Ermittlung und Verwertung von Mustern in diesem riesigen Datenpool erfordert erweiterte Verfahren wie Machine Learning und eine immense Rechenleistung.
- Die Verwendung neuer Informationen zur kontinuierlichen Verbesserung von Sicherheitsmaßnahmen und -technologien erfordert menschliche Experten, die die Daten verstehen und die Erkenntnisse umsetzen können.

Diese Einschränkungen versucht Microsoft aufzuheben. Als Plattform- und Serviceanbieter hat Microsoft Zugang zu Bedrohungs- und Aktivitätsdaten von sämtlichen Punkten in der Technologiekette, aus allen vertikalen Branchen und der ganzen Welt.

Die Sicherheitsprodukte und Cloud-Technologien von Microsoft arbeiten zusammen, um Bedrohungsdaten zu melden, wenn Unregelmäsigkeiten auftreten. Sie fungieren als eine Art „Flugdatenschreiber", der es möglich macht, Angriffe zu diagnostizieren, komplexe Bedrohungstechniken mittels Reverse Engineering zu untersuchen und diese Informationen auf der gesamten Plattform anzuwenden.

Das Spektrum der Threat Intelligence von Microsoft umfasst im wahrsten Sinne des Wortes Milliarden von Datenpunkten:

35 Milliarden
überprüfte Nachrichten pro Monat

600,000
bekannte Spam-E-Mail-Adressen, die nachverfolgt werden

250 Millionen
Windows Defender-Benutzer weltweit

600 Millionen
Computer, von denen jeden Monat Berichte erstellt werden

Mehr als 8,5 Milliarden
Bing-Webseitenüberprüfungen pro Monat

1 Milliarde
Kunden in den Unternehmens- und Consumersegmenten

200+
Cloud Services

Quelle: Microsoft Security Intelligence Report (SIR)

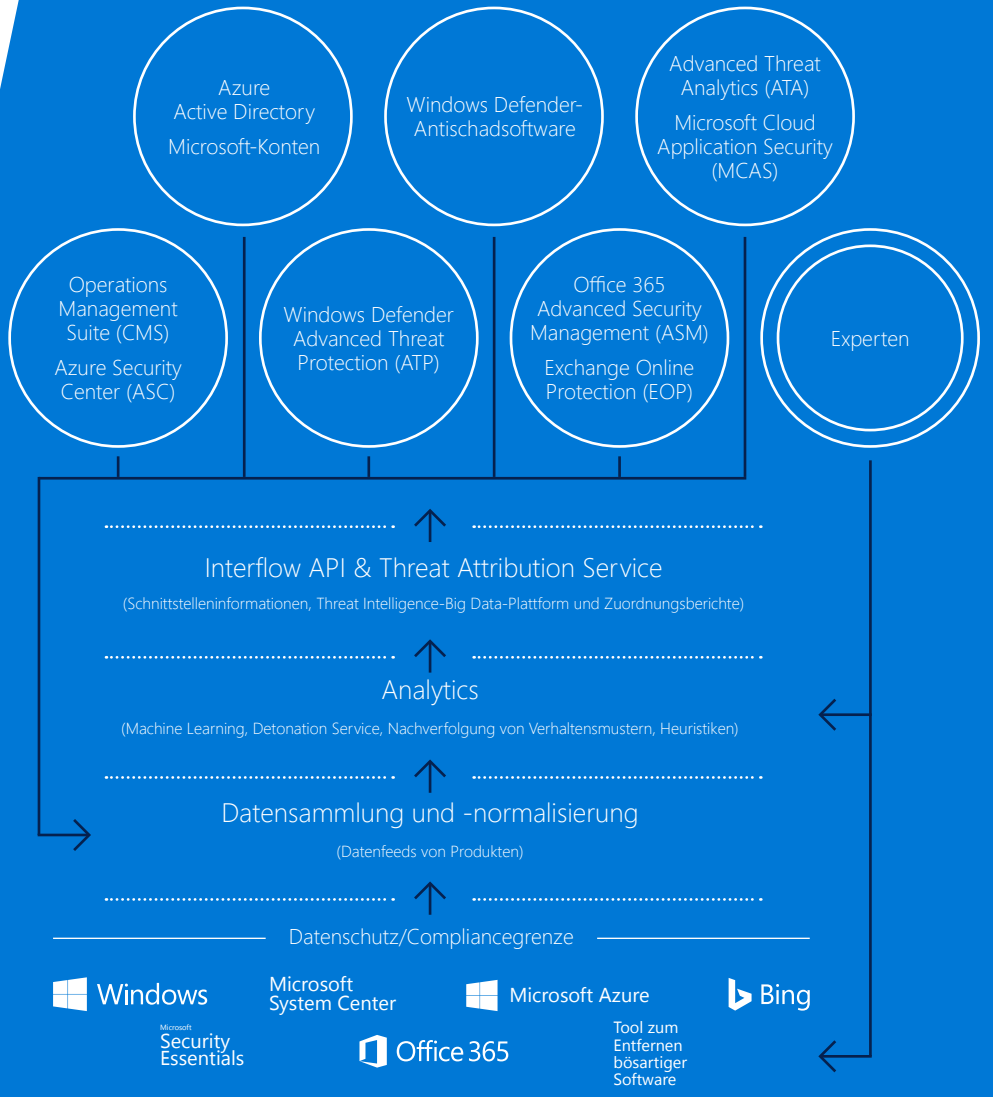
Von Monaten zu Minuten: Angewandte Analytics und deren kontinuierliche Verbesserung

Schon seit fast zwei Jahrzehnten leitet Microsoft aus Bedrohungen nützliche Informationen ab, die dazu beitragen, seine Plattform sicherer zu machen und Kunden zu schützen. Seit der Entstehung des Security Development Lifecycle beim Bekanntwerden der ersten Wurmangriffe wie Blaster, Code Red und Slammer bis zur Einführung moderner, in Plattformen und Services integrierter Sicherheitsdienste, hat das Unternehmen kontinuierlich Prozesse, Technologien und Know-how zur Erkennung und Abwehr neuer Bedrohungen entwickelt.

Heute findet das Unternehmen dank der immensen Vorteile von Cloud Computing neue Wege, um seine hochwertigen, auf Threat Intelligence basierenden, Analysemodule zum Schutz seiner Kunden einzusetzen. Durch eine Kombination von automatisierten und manuellen Prozessen, Machine Learning und menschlichen Experten können wir einen **Intelligent Security Graph** erstellen, der eigenständig lernt, sich in Echtzeit weiterentwickelt und so unseren Zeitaufwand für die Erkennung und Abwehr neuer Bedrohungen in all unseren Produkten reduziert.

Intelligente Sicherheit

Mit diesem **Intelligent Security Graph** schafft Microsoft den branchenweit umfassendsten und flexibelsten Mechanismus zur Weitergabe von Threat Intelligence, dem Anwenden von Analysen und Verbessern der Erkennung für sein gesamtes Produkt- und Serviceportfolio – nicht in 200 Tagen, sondern heute.



Weitere Informationen zu Security Intelligence bei Microsoft

Wie die Bedrohungslandschaft selbst, entwickelt sich auch der Security Intelligence-Ansatz von Microsoft ständig weiter. Kunden stehen verschiedene Ressourcen zur Verfügung, um mehr Informationen zu erhalten und sich über neue Entwicklungen auf dem Laufenden zu halten:

Microsoft Secure Blog

Microsoft-Experten legen hier ihre Gedanken zur Entwicklung der Bedrohungslandschaft und dazu, wie Microsoft und die Branche daran arbeiten, Angreifern immer einen Schritt voraus zu sein, dar.

Azure Active Directory Identity Protection

Azure AD Identity Protection ist eines der Produkte, die laufend mit aktuellen Sicherheitsinformationen aktualisiert werden. Kunden können sich in der Vorschauversion ansehen, wie die Daten genutzt werden, um sicherzustellen, dass Sicherheitsprotokolle auf dem neuesten Stand sind.

The Microsoft Security Intelligence Report (SIR)

Zweimal im Jahr veröffentlicht Microsoft einen detaillierten Bericht über Sicherheitstrends und den ihm zugrunde liegende Daten. Kunden können sich im SIR darüber informieren, welchen Sicherheitsmaßnahmen Priorität eingeräumt werde sollte.