KuppingerCole Report

WHITEPAPER

By Martin Kuppinger

June 30, 2022

Vorsprung vor den Cyberkriminellen: Die externen Bedrohungen verstehen

Verantwortliche für Cybersicherheit sehen sich mit wachsenden Herausforderungen konfrontiert, da die Cyberkriminellen immer kreativer werden und mit einem anscheinend unendlichen Arsenal an Ressourcen bewaffnet sind. Die rasante Digitalisierung in der Folge der Pandemie und die unsichere geopolitische Situation zwingen die Verantwortlichen, ihre Cybersicherheitsstrategien zu überdenken. Trotz eines deutlichen Anstiegs bei den Cybersicherheitsbudgets werden Unternehmen weiterhin Opfer von Cyberattacken. „Den Feind und die eigenen Schwachstellen erkennen und verstehen“ ist der Schlüssel zu wirksamen Verteidigungsstrategien und dafür, einen Vorsprung vor den Cyberkriminellen zu bekommen. Organisationen müssen einen vollständigen Einblick in die externe Bedrohungslandschaft haben und wissen, welche potenziellen Angriffe ihnen drohen. Diese vorausblickende Fähigkeit ermöglicht es Organisationen, sich auf die größten Risiken zu fokussieren und zumindest die schwerwiegendsten Schäden durch Angriffe zu vermeiden.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

Im Auftrag von CYFIRMA

1 Überblick

Die Cyberrisiken nehmen zu. Die Zahl der Angriffe nimmt zu. Jeden Tag werden neue Schwachstellen entdeckt. Immer mehr Organisationen werden Opfer von Cyberangriffen. Während die Cybersicherheit in den Fokus der Geschäftsführung gerückt ist und die Ausgaben für Cybersicherheit erhöht wurden, müssen die Effektivität und Effizienz vieler Cybersicherheitsaktivitäten in Frage gestellt werden.

Es gilt drei weitere Aspekte zu berücksichtigen: Die Ausgaben für die Cybersicherheit werden niemals so schnell wachsen können, wie die Angriffe zunehmen. Der bloße Versuch, sich zu verteidigen, reicht nicht aus - Unternehmen müssen den Cyberkriminellen einen Schritt voraus sein und über introspektive Ansätze zur Cybersicherheit hinausgehen, indem sie die externe Bedrohungslandschaft verstehen. Und schließlich das Tempo des Wandels: Die Cybersicherheit muss mit diesem Tempo mithalten. Cybersicherheitsinitiativen müssen daher über den traditionellen, introspektiven Ansatz von Schutz, Erkennung und Reaktion hinausgehen und proaktiv werden.

Dies erfordert ein gründliches Verständnis der Angreifer, ihrer Beweggründe, ihrer Ziele und ihrer Methoden. Um eine Analogie zu verwenden: Erfolgreiche Unternehmen verkaufen gut, weil sie ihre Kunden verstehen. Unternehmen werden auch bei der Cyberabwehr erfolgreicher sein, wenn sie ihre Angreifer verstehen und wissen, wie sie aus der Perspektive eines Hackers aussehen.

Während es immer notwendig ist, die IT-Assets (einschließlich der Schatten-IT) der Organisation und die Angriffsfläche, aber auch die Risiken Dritter entlang der Lieferkette zu kennen, ist es ebenso wichtig zu verstehen, welche Schwachstellen derzeit aktiv von Angreifern ausgenutzt werden und welche Arten von Organisationen, Branchen und Technologiestacks vorrangig Ziel von Angriffen sind. Auch die spezifischen Risiken für das eigene Unternehmen und die eigene Marke müssen berücksichtigt werden, da sie entweder ein bevorzugtes Ziel bestimmter Angreifergruppen sind oder sensible Informationen wie Code, Passwörter oder andere Informationen sich längst im Dark Web verbreiten.

Dies erfordert eine Lösung, die einen umfassenderen Einblick in den Stand der Cybersicherheit bietet und Informationen aus all diesen Bereichen miteinander in Beziehung setzt, von den Erkenntnissen über die Absichten und das Verhalten des Hackers bis hin zur konkreten Risikoexposition eines Unternehmens. Dies ist die Grundlage für die gezielte Ausrichtung von Cybersicherheitsinitiativen und die Konzentration auf die kritischsten Schwachstellen zu jedem Zeitpunkt.

CYFIRMA bietet eine umfassende, integrierte Plattform für das Management der externen Bedrohungslandschaft, die dabei hilft, Erkenntnisse sowohl aus dem Unternehmen als auch aus der

externen Welt zu gewinnen, einschließlich der proaktiven und kontinuierlichen Überwachung des Dark Web, des Surface Web und der Social-Media-Plattformen, und die alle diese Informationen miteinander in Beziehung setzen kann, so dass Unternehmen und ihre Cybersecurity-Teams die richtigen Maßnahmen ergreifen und Veränderungen in der Risikoexposition des Unternehmens verstehen können.

2 Wichtigste Erkenntnisse

- Angesichts der Zunahme von Cyberangriffen und der ständig wachsenden Cyberrisiken für Unternehmen müssen Unternehmen sowohl die Effektivität und Effizienz ihrer Ausgaben für die Cybersicherheit als auch ihre Fähigkeiten zur Cyberabwehr überprüfen.
- Das Hinzufügen von weiteren Cybersicherheitswerkzeugen allein reicht nicht aus. Unternehmen müssen ein besseres Verständnis ihrer konkreten Gefährdung durch Cyberangriffe erlangen, um die richtigen Tools auszuwählen, aber auch, um alte Cybersicherheits-Tools, die die Erwartungen nicht mehr erfüllen, abzuschalten.
- Dies erfordert ein tieferes Verständnis der Beweggründe und Ziele ihrer Angreifer. Nur wenn Unternehmen ihre Feinde kennen, können sie den Cyberkriminellen einen Schritt voraus sein.
- Unternehmen müssen die derzeit verwendeten Angriffe und ausgenutzten Schwachstellen, die konkreten Bedrohungen für ihr Unternehmen und ihre Branche sowie ihre Angriffsfläche kennen und diese Informationen miteinander korrelieren, um zu verstehen, worauf sie ihre Gegenmaßnahmen konzentrieren müssen.
- Da sich Schwachstellen, Ziele und Angriffsvektoren ständig ändern, müssen Unternehmen die Bedrohungslandschaft kontinuierlich überwachen, um ihre Maßnahmen anzupassen, und zwar über gelegentliche oder regelmäßige Pen-Tests und Red-Team-Übungen hinaus.
- CYFIRMA bietet eine umfassende Unified External Threat Landscape Management-Plattform, die Unternehmen dabei hilft, Einblick in die Absichten und Aktivitäten ihrer Angreifer zu erhalten und sich auf die kritischsten Schwachstellen in ihrer IT-Umgebung zu konzentrieren.

3 Erkennung von Cyber-Bedrohungen und Cyber-Verteidigung: Wie effektiv und effizient ist sie wirklich?

Während die Budgets für die Cybersicherheit steigen, nimmt auch die Zahl der Angriffe zu, ebenso wie der Erfolg solcher Angriffe und der dadurch verursachte Schaden. Es reicht nicht aus, nur das Budget und die Anzahl der eingesetzten Tools zu erhöhen. Unternehmen müssen die Ursachen für die Lücken in der Effektivität und Effizienz ihrer Investitionen in die Cybersicherheit analysieren.

Bei der Effizienz geht es darum, Dinge richtig zu tun. Bei der Effektivität geht es darum, die richtigen Dinge zu tun. Im Bereich der Cybersicherheit stellt sich heute die offensichtliche Frage, ob das, was getan wird, effizient und effektiv ist. Trotz einer kontinuierlichen Erhöhung der Ausgaben für die Cybersicherheit steigen die Zahl der Cyberangriffe und die Kosten der Cyberkriminalität stetig an. Laut einer aktuellen Umfrage von KuppingerCole Analysts erhöht rund ein Drittel der Unternehmen ihr Cybersecurity-Budget 2022 um mehr als 20 % im Vergleich zu 2021, und weitere 47 % berichten von einem Anstieg im Bereich von 5 % bis 20 %.

Figure 1: Cyberangriffe haben 2021 im Vergleich zu 2020 stark zugenommen (Quelle: CYFIRMA).

Dieser Anstieg der Ausgaben ist im Vergleich zur Zunahme der Angriffe immer noch gering. Angesichts der Zunahme von Angriffen und von neuen Angriffsvektoren stellt sich die Frage, ob die Herausforderung aus einem Mangel an Ausgaben für die Cybersicherheit oder aus einem Mangel an Effektivität und Effizienz resultiert. Einfach mehr Geld für traditionelle Cybersicherheitslösungen auszugeben, wird das Problem nicht lösen. Unternehmen müssen darüber nachdenken, worauf sie ihre Ausgaben für Cybersicherheit konzentrieren, um Angriffe erfolgreich abzuwehren und ihren Angreifern einen Schritt voraus zu sein.

Eine bloße Erhöhung der Ausgaben für Cybersicherheit reicht nicht aus - die Zunahme von Cyberangriffen übersteigt ohnehin den Anstieg der Ausgaben, die Unternehmen tätigen können

---

Dies ist in einer sich entwickelnden Bedrohungslandschaft noch wichtiger. Die Cybersicherheit muss sich weiterentwickeln, wenn sich die Bedrohungen weiterentwickeln. Was in der Vergangenheit effektiv und effizient war (falls dies überhaupt der Fall war), ist möglicherweise nicht mehr der richtige Ansatz für die heutige Bedrohungslandschaft. Noch wichtiger: Unternehmen müssen von einem reaktiven, defensiven Ansatz zu einem proaktiven Modell übergehen, mit dem sie auf die sich ständig weiterentwickelnde Bedrohungslandschaft vorbereitet sind. Nur dann können Maßnahmen ergriffen werden, die gegen die neuen Bedrohungen wirksam sind.

Die Entwicklung der Bedrohungslandschaft ist vielfältig. Kinetische Cyberangriffe, die sich auf die

Verursachung physischer Schäden konzentrieren, z. B. im Bereich der Produktionstechnologie, die Zunahme staatlich gesponserter Angriffe, die durch geopolitische Spannungen ausgelöst werden, die Eskalation der Ransomware-Bedrohung, die durch ein gut funktionierendes Geschäftsmodell angetrieben wird, oder neue Technologien wie Deepfake zur Verbreitung von Fehlinformationen sind symptomatisch für diese Entwicklung.

Im Zusammenhang mit dieser Entwicklung der Bedrohungen verändert sich auch die Risikolandschaft von Unternehmen zum Schlechteren. Die Angreifer haben es auf ein breites Spektrum von Daten abgesehen, von Finanzunterlagen über Produktdaten und Plänen bis hin zu Softwarekonfigurationen und mitarbeiterbezogenen Informationen. Andere Angriffe zielen nur darauf ab, Systeme zu beschädigen oder Lösegeld zu erpressen. Kritische Infrastrukturen und betriebliche Produktionsumgebungen, Finanzsysteme, Lieferketten (und deren Unterbrechung), aber auch KMU (kleine/mittlere Unternehmen) sind Ziel von Angriffen.

Unternehmen müssen besser verstehen, welche Tools sie zur Abwehr von Cyberangriffen benötigen, basierend auf den konkreten Bedrohungen für das Unternehmen und seine IT-Ressourcen

---

Mit dem bloßen Hinzufügen von mehr oder "besseren" Werkzeugen lässt sich diese Herausforderung nicht lösen. Solange nicht die richtigen Werkzeuge vorhanden sind, um dem zu begegnen, was Angreifer nicht nur heute tun, sondern auch morgen tun werden, sind Maßnahmen nicht wirksam. Effizienz erfordert einen klaren Fokus auf die wirklichen Risiken und Werkzeuge, mit denen die Herausforderungen der Cybersicherheit mit vernünftigem Aufwand angegangen werden können, insbesondere im Zeitalter des Fachkräftemangels im Bereich der Cybersicherheit.

4 Die Ursache: Nicht ein Mangel an Werkzeugen, sondern der Fokus

Viele Unternehmen suchen sofort nach Tools, wenn eine neue Cyber-Bedrohung auftaucht oder wenn sie von einem Angriff betroffen sind. Tools sind jedoch nur ein Element der Lösung. Es geht um Menschen, Prozesse und Werkzeuge und um einen ganzheitlichen Ansatz. Aber es geht auch darum, die Angreifer besser zu verstehen.

Die traditionellen Modelle für die Cybersicherheit mit ihren bekannten und definierten zyklischen Modellen, die mit der Ermittlung von Risiken und der Vorbereitung auf Angriffe beginnen, sind nicht falsch. Leider wird dabei vorausgesetzt, dass die Risiken gut bekannt sind. Dies würde voraussetzen, dass man sowohl die eigene Angriffsfläche als auch die Absichten des Angreifers versteht. Wer könnte das Unternehmen angreifen und welche Angriffsvektoren auf welchen Teil Ihrer IT- oder OT-Umgebung verwenden? Eine Risikoanalyse, die sich nur darauf stützt, was für ein Unternehmen am wichtigsten ist oder welche Angriffsvektoren am häufigsten vorkommen oder am kritischsten sind, reicht nicht aus, weil dabei die Perspektive des Angreifers außer Acht gelassen wird, die sich auf die Wahrscheinlichkeit eines Angriffs und, im Falle eines erfolgreichen Angriffs, auf den Umfang der Schäden auswirkt.

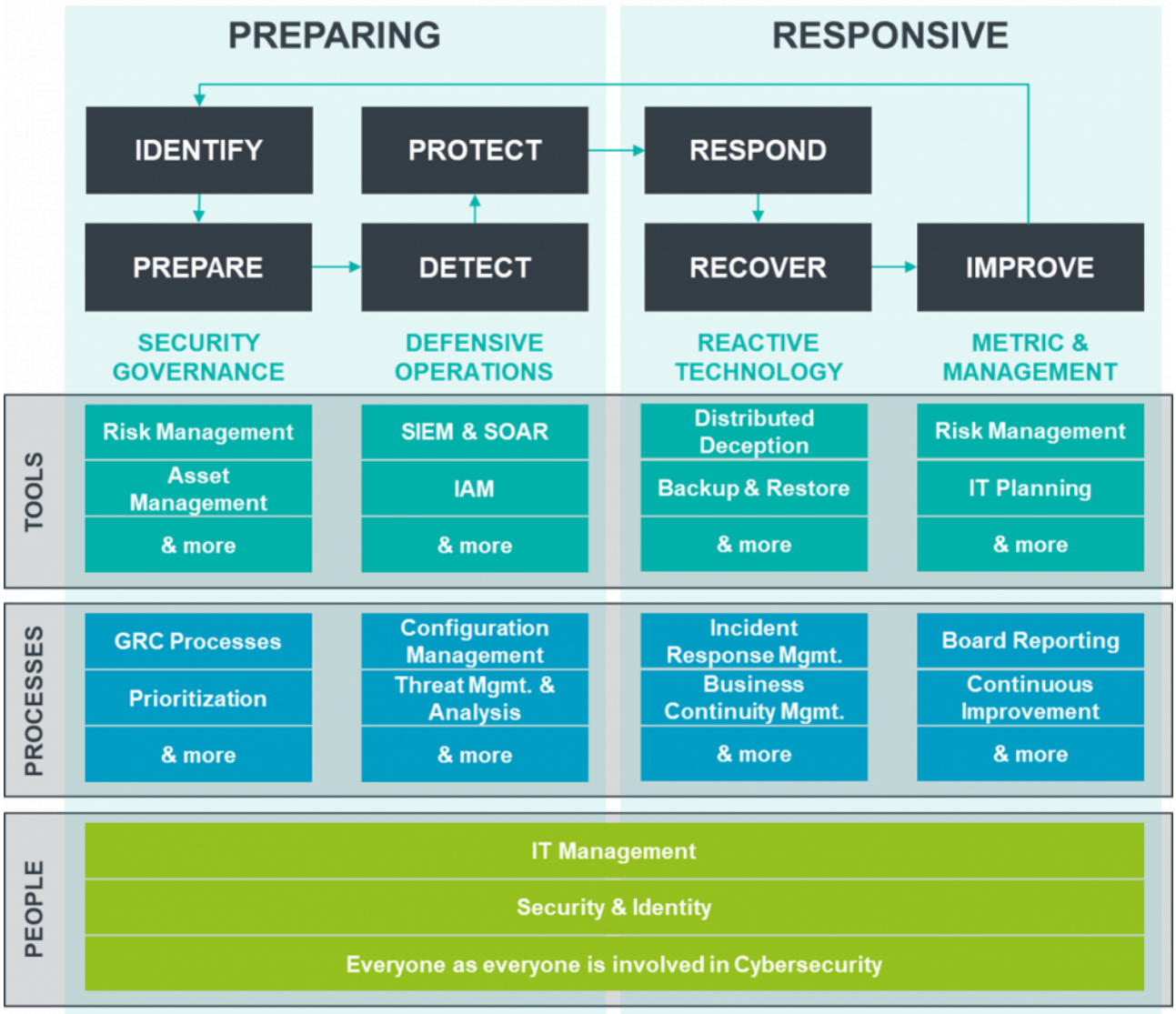

Figure 2: Das KuppingerCole-Modell für das Management von Cyberrisiken.

Wenn man sich eingehender damit befasst, wie man Risikoanalyse richtig macht, stellt man fest, dass es sieben große Herausforderungen gibt:

- Fokus auf Werkzeuge: Viele Cybersicherheitsteams bestehen aus zu wenigen Personen, die sich mit allen technischen Aspekten der Cybersicherheit befassen müssen. Häufig fehlt es an Zeit und methodischem Wissen für eine gründliche Risikoanalyse. Diese Situation zeigt sich auch in zu vielen Fehlalarmen, keiner klaren Priorisierung der Cybersecurity-Bemühungen und einer Tendenz, sich auf Abhilfemaßnahmen mit geringem Aufwand, aber auch geringer Wirkung zu konzentrieren.
- Schatten-IT: Die bekannten Teile der IT sind sicherlich mehr als nur die Spitze des Eisbergs, aber die meisten Unternehmen haben eine erhebliche Menge an Schatten-IT, die im Zeitalter der Remote-

Arbeit weiter zunimmt. Was nicht bekannt ist, kann auch nicht geschützt werden.

- Die Komplexität der IT: Die Komplexität der IT-Umgebungen trägt zu diesem Problem bei. Jedes System und jede Anwendung kann zu einem Ziel oder zu einem Einstiegspunkt für Angreifer werden. Der Schutz komplexer IT-Umgebungen erfordert eine enge Zusammenarbeit mehrerer Beteiligter und ausgefeilte Methoden und Prozesse.
- Angeschlossene Systeme von Drittanbietern: Darüber hinaus müssen sich Unternehmen nicht nur um ihre eigene IT kümmern, sondern sind auch Risiken ausgesetzt, die über angeschlossene Drittsysteme eintreten. Risiken in der Lieferkette sind zu einem der wichtigsten Themen der Cybersicherheit geworden.
- Wachsende Angriffsfläche: Im digitalen Zeitalter und in Multi-Hybrid- und Multi-Cloud-Umgebungen wächst die Angriffsfläche durch das Hinzufügen neuer Cloud-Dienste, neuer digitaler Dienste und die Agilität der heutigen IT ständig.
- Interne Perspektive: Praktisch alle Ansätze für das Risikomanagement nehmen eine interne Perspektive ein und konzentrieren sich darauf, die kritischsten Anlagen und potenziellen Schwachstellen in der eigenen IT zu identifizieren, nehmen aber nicht die Perspektive der Angreifer ein.
- Mangelndes Verständnis für die Angreifer: Dies führt dazu, dass man nicht weiß, was die Angreifer wahrscheinlich tun werden, und dass es an Kontext für isolierte Ereignisse fehlt, die erkannt werden. Ohne den Feind zu kennen und ihn kontinuierlich zu analysieren - abgesehen von gelegentlichen Pen-Tests und Red-Team-Übungen - ist es schwierig, den Feind zu bekämpfen.

Werkzeuge allein helfen nicht weiter. Sie mögen den Eindruck erwecken, dass die erforderlichen Maßnahmen ergriffen worden sind. Aber die Tatsache, dass wachsende Investitionen in die Cybersicherheit nicht zu einem Rückgang der Zahl der Angriffe oder der Kosten von Cybervorfällen führen, zeigt, dass es nicht nur um Werkzeuge geht.

Die Herausforderungen bei der Umsetzung einer starken Cybersicherheitsstrategie sind vielfältig. Die größten Herausforderungen sind die Übersicht über die eigenen IT-Ressourcen und deren Verwundbarkeit sowie das Verständnis der Ziele von Angreifern

---

Es gibt auch keine Lücke in der Anzahl der Sicherheitstools, die in den meisten Unternehmen eingesetzt werden. Es geht darum

- Die richtigen Werkzeuge zu haben

- Keine unnötigen Werkzeuge zu haben, die keinen Mehrwert zu anderen Tools liefern
- Werkzeuge effizient und effektiv zu nutzen
- Tools zu integrieren

Die Auswahl der richtigen Werkzeuge, ihre Integration und ihr Einsatz funktionieren nur, wenn die Risiken richtig verstanden werden. Dies erfordert einen anderen, umfassenderen Ansatz für das Cyber-Risikomanagement, der über die interne Perspektive hinausgeht. Nur wenn die Angreifer, ihre Techniken und ihre Ziele verstanden werden, können die richtigen Maßnahmen ergriffen werden.

5 Einblick in die externe Bedrohungslandschaft - Predictive Threat Intelligence, um Cyberkriminellen einen Schritt voraus zu sein

Kein erfolgreiches Unternehmen wird den Kunden ignorieren. Die Anforderungen des Kunden zu verstehen, ist der Schlüssel zum Erfolg im Vertrieb. Ähnlich verhält es sich mit der Cybersicherheit: Wenn Unternehmen die Angreifer nicht verstehen, können sie keine gezielten Gegenmaßnahmen ergreifen. Es besteht die Notwendigkeit einer vorausschauenden Bedrohungsanalyse, die Einblick in die Absichten und Handlungen der Hacker gibt.

Der traditionelle introspektive Ansatz der Cybersicherheit reicht nicht mehr aus. Die Cybersicherheit hat sich in den letzten Jahren erheblich weiterentwickelt. Sie hat sich von einem hauptsächlich schützenden Fokus zu einem mehrschichtigen Modell gewandelt, wie in Abbildung 2 dargestellt. Sie hat sich von einem netzwerkzentrierten Ansatz zu einem Zero-Trust-Modell entwickelt, das viele Ebenen abdeckt, von der Identität und den Endpunkten bis hin zu Netzwerken und Daten. Dennoch ist es der Cybersicherheit nicht gelungen, den Cyberkriminellen einen Schritt voraus zu sein, sondern sie bleibt reaktiv.

Ein wichtiges, wenn nicht das wesentliche fehlende Element für gute Cybersicherheit ist das Verstehen des Feindes:

- Was ist deren Ziel?
- Welche Art von Angriffen wird derzeit genutzt?
- Worüber unterhalten sie sich?
- Wie betrifft das die eigene Organisation?
- Was kann gegen mich eingesetzt werden?
- Wie kann ich angegriffen werden?

Die Cybersicherheit muss hier eine andere Perspektive einnehmen, wie es auch in vielen anderen Bereichen des Unternehmens üblich ist. Produktmanagement und Vertrieb handeln aus der Kundenperspektive. Wer ist der Kunde? Wer ist der Käufer beim Kunden? Was braucht er? Dies sind grundlegende Fragen, die in erfolgreichen Unternehmen immer gestellt werden.

Wenn Sie Ihren Feind nicht kennen, können Sie Ihre Organisation nicht erfolgreich schützen.

Erfolgreiche Cybersicherheit erfordert einen ähnlichen Ansatz, um die Angreifer zu verstehen. Wer sind die

Angreifer? Wer steckt dahinter, was ist ihr Plan und was sind ihre Ziele? Was wollen sie erreichen? Wer die Angreifer versteht, versteht auch besser, welche Gegenmaßnahmen ergriffen werden müssen.

Im Bereich der Cybersicherheit trägt der ständige Wandel zur Komplexität bei:

- Es werden ständig neue Sicherheitslücken entdeckt, wie die große Zahl der monatlich veröffentlichten Patches zeigt.
- Es werden ständig neue Angriffsvektoren entwickelt, manchmal Tausende von Varianten solcher Vektoren.
- Die Angriffsziele ändern sich häufig, insbesondere bei staatlich gesponserten Angriffen.
- Die "Geschäftsmodelle" der Angreifer ändern sich häufig - sobald eine bestimmte Art von Angriffen erfolgreich verhindert wurde, kommen neue Ansätze "auf den Markt".

Das bedeutet, dass die Analyse der Angreifer keine einmalige oder in langen Abständen durchgeführte Aufgabe ist, sondern zu einer ständigen Übung werden muss.

Die Analyse externer Bedrohungen, das Management von Angriffsflächen und die Verwaltung von Schwachstellen erfordern ständige Aktualisierungen - alle Bereiche sind einem ständigen Wandel unterworfen.

Die externe Bedrohungslandschaft und das Verständnis der Angreifer müssen dann auf den Zustand der IT in der eigenen Organisation abgebildet werden. Das Verständnis der konkreten Bedrohungen und der vorhandenen Angriffsfläche hilft bei der Festlegung konkreter Gegenmaßnahmen, die sich auf den Schutz der Schwachstellen der IT des Unternehmens vor den konkreten, aktuellen Bedrohungen konzentrieren.

6 Der Ansatz von CYFIRMA für Predictive Threat Intelligence

CYFIRMA hat eine umfassende Plattform für Unified External Threat Landscape Management entwickelt. Diese Plattform integriert eine Reihe von Funktionen wie das Attack Surface Management, die Erkennung digitaler Risiken und verschiedene andere Funktionsbereiche und ist die Grundlage für eine vorausschauende Bedrohungsanalyse.

CYFIRMA bietet hierfür eine umfassende Lösung, die Unified External Threat Landscape Management Platform. Diese Lösung deckt sechs Funktionsbereiche ab:

- Erkennung der externen Angriffsfläche (External Attack Surface Discovery(: Trotz der Fokussierung auf die Angreifer ist das Verständnis der eigenen Angriffsfläche von entscheidender Bedeutung und darf nicht auf die bekannten Angriffsflächen beschränkt sein. Schatten-IT und Risiken von Drittanbietern entlang der Lieferkette müssen ebenfalls in diese Analyse einbezogen werden.
- Informationen über Schwachstellen (Vulnerability Intelligence): Bestehende Schwachstellen müssen bekannt sein und verstanden werden, und zwar nicht nur im Hinblick auf ihren technischen Schweregrad, sondern auch auf den aktuellen Status der Ausnutzung durch Angreifer. Dies hilft bei der gezielten Behebung von Schwachstellen mit hoher Auswirkung.
- Marken-Analyse (Brand Intelligence): Marken, Produkte und Dienstleistungen können ein aktuelles Ziel für Angreifer sein. Dies gilt insbesondere für politischen Hacktivismus, ist aber nicht auf diesen Bereich beschränkt.
- Entdeckung und Schutz vor digitalen Risiken (Digital Risk Discovery & Protection): Die Überwachung aktueller Diskussionen von Hackergruppen und die Analyse ihrer potenziellen Auswirkungen auf Unternehmen, aber auch die Identifizierung von Informationen, die im Dark Web geteilt werden, wie Quellcode, Passwörter, Exploits usw., helfen dabei, die aktuelle Bedrohung zu verstehen. Die Dark-Web-Analysefähigkeiten von CYFIRMA zählen zu den Alleinstellungsmerkmalen im Wettbewerb.
- Bewusstsein für die Risikosituation (Situational Awareness): Die Vielfalt der Erkenntnisse von der Angriffsfläche und den Schwachstellen bis hin zu konkreten Bedrohungen für eine Organisation müssen korreliert werden und führen zu einer Bewertung der aktuellen Cyber-Risikosituation.
- Cyber-Intelligenz (Cyber Intelligence): Auf dieser Grundlage lassen sich Bedrohungen und Angriffe besser vorhersagen und besser abwehren. Das Wissen darüber, wer am ehesten mit welchen Vektoren gegen welche Schwachstellen angreift, ist für die Verbesserung der

Cybersicherheitssituation von Unternehmen unerlässlich.

CYFIRMA hat eine Lösung entwickelt, die alle sechs Säulen abdeckt und eine Plattform für ein einheitliches Management der externen Bedrohungslandschaft bietet. Dies erweitert den Fokus über die üblichen, nur intern ausgerichteten Lösungen wie ASM (Attack Surface Management) und die verschiedenen Werkzeuge für Cybersicherheit hinaus.

Figure 3: Das Modell von CYFIRMA für Unified External Threat Landscape Management (Quelle: CYFIRMA).

Die Lösung von CYFIRMA basiert im Kern auf zwei SaaS-Lösungen:

- DeCYFIR: Diese Lösung ist die Plattform für External Threat Landscape Management (ETLM) und liefert die Einblicke in die Bedrohungen, denen ein Unternehmen ausgesetzt ist..
- DeTCT: Dabei handelt es sich um die Plattform für Digital Risk Discovery & Protection (DRDP), die weitere Informationen über konkrete Risiken und die digitalen Assets liefert, die für Angriffe auf das Unternehmen genutzt werden können.

DeCYFIR ist das Kernprodukt. Es bietet Einblicke in die Bedrohungen und Risiken, denen ein Unternehmen ausgesetzt ist. Es entdeckt und analysiert die aktuelle Angriffsfläche und liefert Echtzeitinformationen zu Schwachstellen, die von Angreifern ausgenutzt werden könnten. Es analysiert die marken- und

branchenbezogene Gefährdung durch Cyberangriffe, einschließlich der Analyse von Trends für Branchen, Technologie-Stacks und Standorte. Es gibt Aufschluss darüber, wie die Motive, Kampagnen und Methoden der Hacker zusammenhängen, so dass Unternehmen ihre Gefährdung verstehen und gezielte Gegenmaßnahmen ergreifen können.

CYFIRMA bietet eine umfassende Plattform für Unified External Threat Landscape Management, die Einblicke in die Absichten und Handlungen von Angreifern liefert

---

Die Informationen werden über Dashboards zur Verfügung gestellt, die es den Nutzern ermöglichen, Einblick in Details zu erhalten. DeCYFIR bietet eine strategische, eine Management- und eine operative Sicht. Die strategische Ansicht konzentriert sich auf das aktuelle Risiko und die Veränderung des Risikos. Die Management-Ansicht bietet einen geführten, systematischen Ansatz zur Adressierung der wichtigsten Bedrohungen. Die taktische Sicht liefert Informationen für die Umsetzung konkreter Sicherheitsmaßnahmen.

DeTCT, die zweite Komponente der CYFIRMA SaaS-Lösungen, bietet detaillierte Einblicke in das Bedrohungsumfeld, insbesondere das Dark Web. DeTCT bietet auch Dashboards, angefangen bei Risiko- und "Hackability"-Scores. Es liefert Metriken zu Angriffsflächen und der aktuellen Angriffssituation weltweit sowie für den jeweiligen Standort und die Branche. Es liefert auch Einblicke in Daten, die aus dem Unternehmen ins Dark Web gelangt sind und viele weitere Informationen.

CYFIRMA ist einzigartig mit seinem Ansatz, die Angriffsflächen umfassend zu analysieren und die externe Bedrohungslandschaft zu verstehen. Der Ansatz geht über die üblichen ASM-Ansätze hinaus, indem er die externe Bedrohungssituation mit einbezieht und eine breite Palette von Informationen sammelt, die zu einem besseren Verständnis der aktuellen Bedrohung für eine Organisation beitragen. Auf dieser Grundlage können gezielte Gegenmaßnahmen ergriffen werden, die sich auf die Bereiche konzentrieren, die das größte konkrete Risiko für ein Unternehmen darstellen.

7 Empfehlungen

Die Verbesserung der Cybersicherheitslage von Unternehmen ist nicht nur eine Frage von zusätzlichen Tools. Sie erfordert die richtigen Mitarbeiter und Prozesse sowie ein gründliches Verständnis der Risikoreduktion, die die verschiedenen Tools erzielen können.

Um diese Auswirkungen zu verstehen, darf man sich nicht nur auf die Analyse der Angriffsfläche beschränken, sondern muss eine breitere Perspektive einnehmen. Ob dies nun unter dem Motto "Kenne deinen Feind" steht oder ob eine andere Terminologie verwendet wird: Ein einheitlicher, umfassender Überblick über die externe Bedrohungslandschaft und die Anfälligkeit der internen IT ist die Grundlage für gezielte Gegenmaßnahmen.

Schlüsselelemente einer solchen Initiative sind

1. Verstehen der gesamten Angriffsfläche, einschließlich der Schatten-IT. Der nicht verwaltete Teil der IT ist für Angreifer der einfachste Zugang.
2. Verstehen des externen Risikos aus der Sicht des Unternehmens: Bedrohungen für die Marke, für die Branche, für den Standort.
3. Verstehen der aktuellen Angriffe: Welche Schwachstellen sind im Visier der Angreifer, welche Angriffsvektoren werden genutzt, worauf muss der Schutz ausgerichtet sein?
4. Verstehen der konkreten Exposition der Organisation: Welche Informationen, die von Angreifern genutzt werden können, befinden sich im Dark Web?
5. Korrelation: Welche konkreten Bedrohungen gibt es und welche Risiken ergeben sich aus den Schwachstellen und den Aktivitäten der Angreifer?
6. Schadensbegrenzung: Kontinuierliches Handeln bei der Ermittlung und Durchsetzung der richtigen, gezielten Gegenmaßnahmen.

Es ist wichtig, die Dynamik von Cyber-Risiken und die Tatsache zu verstehen, dass Bedrohungen, Schwachstellen und Risiken einem ständigen Wandel unterworfen sind. Die kontinuierliche Überwachung und Anpassung von Gegenmaßnahmen sowie die Fähigkeit, schnell zu reagieren, sind für eine erfolgreiche Eindämmung von Cyberrisiken unerlässlich.

8 Weiterer Research

Leadership Brief: Top Cyber Threats
Advisory Note: Business Continuity in the age of Cyber Attacks
Leadership Brief Cybersecurity Trends & Challenges

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.