Video-Erklärungen

Originale Erklärartikel aus der Videobibliothek von Cyber Crucible — Ransomware, Datendiebstahl, Identitätsdiebstahl, autonome Sicherheit und FortressAI — jeweils mit dem zugehörigen Video.

- Wer trägt das größte Risiko eines Ransomware-Angriffs, und warum werden diese Ziele ausgewählt?
- Wer führt Ransomware-Angriffe tatsächlich aus und wie gehen sie vor?
- Wer ist der ideale Kunde für den Ransomware-Schutz von Cyber Crucible?
- Warum werden Ransomware-Angriffe von Jahr zu Jahr häufiger?
- Warum setzt Cyber Crucible auf KI anstelle eines menschlichen SOC-Teams, um Ransomware zu stoppen?
- Warum erhalten Sicherheitsteams täglich Tausende von Warnmeldungen, und wie können sie damit umgehen?
- Warum ist Anmeldedaten- und Identitätsdiebstahl gefährlicher als Ransomware-Verschlüsselung?
- Warum ist Ransomware so schwer zu stoppen und wiederherzustellen?
- Warum kann herkömmliche Antivirensoftware Zero-Day- und dateilose Ransomware-Angriffe nicht stoppen?
- Werden Hacker 2025 mehr KI bei Ransomware-Angriffen einsetzen?
- Senkt der Einsatz von Cyber Crucible das gesamte Sicherheitsbudget eines Unternehmens?

Überreagieren Unternehmen beim Thema KI-Risiko, oder handelt es sich um ein Sichtbarkeitsproblem?

Kurze Antwort: Die meisten Organisationen überreagieren nicht auf KI-Risiken – ihnen fehlt schlicht die tatsächliche Sichtbarkeit darüber, wie KI-Tools in ihrer gesamten Umgebung tatsächlich genutzt werden. Ohne diese Sichtbarkeit ist die sicherste Annahme, dass das aktuelle Risiko unterschätzt wird, nicht übertrieben dargestellt.

Warum „KI-Risiko" oft auf blinde Flecken hinausläuft

Wenn Unternehmen ihre Exposition gegenüber KI-bezogenen Risiken bewerten, zeigt sich ein häufiges Muster: Manche Organisationen geben offen zu, kein klares Bild davon zu haben, wie KI-Tools intern genutzt werden. Andere glauben, über Sichtbarkeit zu verfügen, stellen jedoch etwas anderes fest, sobald tatsächlich ein Monitoring eingerichtet wird. In der Praxis ist der Umfang und die Vielfalt der zutage tretenden KI-Tool-Nutzung, sobald die Nachverfolgung aktiviert wird, oft überraschend – so sehr, dass Sichtbarkeitsfunktionen mitunter in einem kontrollierten oder simulierten Modus betrieben werden müssen, um mit der Menge an Aktivität Schritt zu halten, die fast unmittelbar sichtbar wird.

Diese Lücke deutet darauf hin, dass Bedenken hinsichtlich KI-Risiken selten übertrieben sind. Häufiger werden die Bedenken untertrieben dargestellt, weil Führungskräfte ohne die Daten arbeiten, die zur genauen Beurteilung der Lage erforderlich wären.

Warum unbekanntes Risiko als hohes Risiko behandelt werden sollte

Eine nützliche Denkweise hierzu ähnelt den persönlichen Finanzen: Wer nie seinen Kontostand prüft, sollte verantwortungsbewusst davon ausgehen, nicht über nennenswerte verfügbare Mittel

zu verfügen – nicht umgekehrt. Die gleiche Logik gilt für die KI-Nutzung innerhalb eines Unternehmens. Ohne konkrete Variablen – etwa welche Tools genutzt werden, wie oft und von wem – haben Organisationen keine verlässliche Grundlage für die Annahme, dass das Risiko gering ist. Der verantwortungsvolle Standardansatz besteht darin, vom ungünstigsten Fall auszugehen, bis tatsächliche Nutzungsdaten das Gegenteil belegen.

Das größere Muster hinter der KI-Einführung

Über Nutzer, Geschäftsbereiche und die KI-Tools selbst hinweg entstehen ständig neue und oft nicht genehmigte Anwendungsfälle – schneller, als die Governance Schritt halten kann. Dieses durchgängige Muster zeigt, dass die meisten Organisationen, unabhängig von Größe oder Branche, noch dabei sind, aufzuholen, wie KI in ihrer Umgebung tatsächlich genutzt wird. Die Herstellung klarer Sichtbarkeit ist der notwendige erste Schritt, bevor KI-Risiken präzise bewertet oder gesteuert werden können.

https://player.vimeo.com/video/1176539821

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Warum haben traditionelle SOC-Sicherheitsmodelle Schwierigkeiten mit Cyberangriffen in Maschinengeschwindigkeit?

Kurze Antwort: Traditionelle Security Operations Center wurden für eine langsamere, vorhersehbarere Ära des Hackings entwickelt und verlassen sich auf Signaturen und menschliche Analyse, um Bedrohungen nachträglich zu erkennen. Heutige Angreifer nutzen automatisierte Werkzeuge, die sich ständig verändern, sodass Verteidigungsmaßnahmen zu signaturlosen, präventiven Ansätzen übergehen müssen, die schneller agieren als der Angriff selbst.

Wie sich die Bedrohungslandschaft verändert hat

Vor Jahren verhielten sich bösartige Werkzeuge auf ziemlich konsistente, identifizierbare Weise. Sicherheitsteams konnten Erkennungsmethoden auf Basis bekannter Muster entwickeln, da Angreifer noch nicht stark auf Automatisierung setzten, um ihre Techniken kontinuierlich zu verändern. Dieser Ansatz funktionierte gut genug, um einige der raffiniertesten Bedrohungen jener Zeit zu erkennen, einschließlich hochgezielter Angriffe, die vor über einem Jahrzehnt entdeckt wurden.

Diese Landschaft existiert nicht mehr. Moderne Angreifer nutzen Automatisierung, um schnell Variationen ihrer Werkzeuge zu erzeugen, wodurch es für signaturbasierte Erkennung schwierig wird, Schritt zu halten. Bis eine neue Signatur identifiziert, katalogisiert und im gesamten Sicherheits-Stack ausgerollt wurde, ist der Angreifer oft bereits zu einer neuen Variante übergegangen.

Warum veraltete SOC-Modelle zurückbleiben

Traditionelle SOC-Arbeitsabläufe basieren darauf, bekannte Indikatoren zu identifizieren und anschließend über weitgehend manuelle oder halbmanuelle Prozesse zu untersuchen und zu reagieren. Dieses Modell setzt voraus, dass Angreifer in einem Tempo agieren, das Verteidigern Zeit zur Analyse und Reaktion lässt. Wenn Angriffe automatisiert sind und sich in Echtzeit verändern können, funktioniert diese Annahme nicht mehr, was zu einer anhaltenden Lücke zwischen dem Auftreten einer Bedrohung und ihrer Bewältigung führt.

Was moderne Verteidigungsmaßnahmen stattdessen leisten müssen

Sicherheitswerkzeuge müssen heute nicht mehr ausschließlich auf zuvor bekannte Signaturen angewiesen sein. Stattdessen müssen sie bösartiges Verhalten direkt erkennen und verhindern, indem sie in Maschinengeschwindigkeit agieren, statt auf von Menschen gesteuerte Analysezyklen zu warten. Die FortressAI-Technologie von Cyber Crucible basiert auf diesem Prinzip und konzentriert sich darauf, Ransomware, Datendiebstahl und Identitätsdiebstahlversuche durch automatisiertes, präventives Handeln zu stoppen, statt durch nachträglichen Signaturabgleich.

https://player.vimeo.com/video/1182235055

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Wie sieht wirklich autonome Cybersicherheit im Alltag tatsächlich aus?

Kurze Antwort: Echte autonome Sicherheit sollte sich routinemäßig und mühelos anfühlen – nicht wie eine ständige Quelle von Warnmeldungen oder Sorgen. Wenn ein Sicherheitstool ständige Aufmerksamkeit, Feinjustierung oder Sorgen erfordert, arbeitet es nicht autonom.

Warum „langweilig" das Ziel ist

Sicherheitsteams und IT-Mitarbeiter jonglieren bereits mit mehr Aufgaben, als sie realistisch bewältigen können. Ein Tool hinzuzufügen, das regelmäßige Kontrollen, die manuelle Überprüfung von Warnmeldungen oder nächtliche Fehlerbehebung erfordert, konterkariert den Sinn der Automatisierung. Effektiver autonomer Schutz sollte still im Hintergrund arbeiten, ähnlich wie ein an der Wand montierter Feuerlöscher. Die meisten Menschen denken nicht an ihren Feuerlöscher, bis einmal im Jahr ein Prüfer vorbeikommt, um zu bestätigen, dass er geladen und einsatzbereit ist. Die restliche Zeit steht er einfach da und erfüllt seine Aufgabe, ohne Aufmerksamkeit zu erfordern.

Das ist der Standard, den autonome Sicherheit erfüllen sollte. Sie sollte Bedrohungen eigenständig bewältigen, ohne Mitarbeiter von anderen Prioritäten abzulenken oder zu einem weiteren Punkt auf einer bereits langen To-do-Liste zu werden.

Was das in der Praxis bedeutet

Wenn ein Sicherheitsprodukt dazu führt, dass Sie ständig Dashboards überprüfen, sich fragen, ob es etwas erkannt hat, oder schlaflose Nächte darüber haben, ob es tatsächlich funktioniert, dann ist es nicht wirklich autonom – es ist nur eine weitere manuelle Aufgabe mit einem anderen Etikett. FortressAI von Cyber Crucible basiert auf diesem Gedanken: Ransomware, Datendiebstahl und Identitätsdiebstahl-Aktivitäten zu erkennen und zu stoppen, ohne dass ständige menschliche Aufsicht erforderlich ist, damit es korrekt funktioniert.

Der Maßstab für Erfolg ist nicht, wie viel Aktivität ein Sicherheitstool erzeugt oder wie oft es angepasst werden muss. Es ist, wie wenig man darüber nachdenken muss. Wenn autonome Sicherheit so funktioniert, wie sie soll, sollte sie unauffällig sein – präsent, zuverlässig und weitgehend unsichtbar, bis der Moment kommt, in dem sie gebraucht wird.

https://player.vimeo.com/video/1190816235

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Können KI-Tools wie ChatGPT ein menschliches Cybersicherheitsteam ersetzen?

Kurze Antwort: Nein. Universelle KI-Tools können Sicherheitsarbeit unterstützen, indem sie Informationen zusammenfassen oder grundlegende Fragen beantworten, aber sie sind nicht zuverlässig genug, um ein geschultes Sicherheitsteam zu ersetzen, wenn es um echte Risikoentscheidungen geht.

Warum die Sicherheit von KI-Antworten irreführend sein kann

Tools wie ChatGPT präsentieren Antworten oft mit einem Ton der Gewissheit, selbst wenn die zugrunde liegenden Informationen unvollständig oder falsch sind. Dies kann ein falsches Gefühl von Autorität erzeugen, ähnlich wie bei einer überzeugenden Person, die etwas so selbstbewusst äußert, dass andere es als Tatsache akzeptieren, ohne es weiter zu überprüfen. Im alltäglichen Gespräch ist diese Art von fehlgeleitetem Selbstvertrauen ein kleineres Problem. In der Cybersicherheit, wo Entscheidungen darüber getroffen werden, wie eine Organisation Bedrohungen erkennt und darauf reagiert, kann die unkritische Übernahme ungenauer Ergebnisse zu echtem Schaden führen. Sicherheitsanalyse hängt von Kontext, Verifizierung und Urteilsvermögen ab, die aktuelle allgemeine KI-Modelle nicht vollständig nachbilden können.

Wo KI dennoch helfen kann

Trotz dieser Einschränkungen sind KI-Tools im Sicherheitskontext nicht ohne Wert. Sie können als Ausgangspunkt für Recherchen dienen, dabei helfen, Konzepte zu erklären, oder beim Verfassen und Organisieren von Informationen unterstützen. So eingesetzt, fungiert KI als Unterstützungswerkzeug und nicht als Entscheidungsträger. Entscheidend ist, den Unterschied zwischen KI, die einen sachkundigen Analysten unterstützt, und KI, die versucht, Risiken eigenständig zu bewerten und zu mindern, zu erkennen – Letzteres erfordert tiefere Fachkenntnisse, als diese Tools derzeit bieten können.

Das Argument für ehrliche Erwartungen

KI-Anbieter und Praktiker, die realistische Erwartungen setzen, anstatt zu übertreiben, was diese Tools leisten können, bauen mit größerer Wahrscheinlichkeit dauerhaftes Vertrauen auf. Die Fähigkeiten von KI im Sicherheitsbereich zu überverkaufen, birgt das Risiko, Vertrauen zu untergraben, sobald die Grenzen sichtbar werden. Klare, maßvolle Kommunikation darüber, was KI kann und was nicht, hilft Organisationen, fundierte Entscheidungen darüber zu treffen, wie sie diese verantwortungsvoll einsetzen können. Der Ansatz von Cyber Crucible spiegelt genau dieses Prinzip wider: Anstatt KI als Ersatz für qualifizierte Verteidiger darzustellen, sind autonome Schutztechnologien wie FortressAI so konzipiert, dass sie mit menschlichem Fachwissen zusammenarbeiten und die Fähigkeit einer Organisation stärken, Ransomware, Datendiebstahl und Identitätsdiebstahl zu verhindern, ohne vorzugeben, die Notwendigkeit einer informierten Aufsicht zu beseitigen.

https://player.vimeo.com/video/1134578207

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Kann Ransomware weiterhin auf Daten zugreifen, die in Cloud-Diensten wie OneDrive oder Google Drive gespeichert sind?

Kurze Antwort: Ja. Während Cloud-Speicher früher für Ransomware unerreichbar war, haben Angreifer ihre Methoden angepasst und können nun cloudbasierte Daten durch Techniken wie Laufwerkszuordnung (Drive Mapping) und, heute noch häufiger, den Diebstahl von API-Schlüsseln und Sitzungstoken angreifen.

Wie sich Ransomwares Vorgehen bei Cloud-Daten verändert hat

Als die Remote-Arbeit einen raschen Wandel hin zu Cloud-Speichern auslöste, mussten sich sowohl Unternehmen als auch Cyberkriminelle gleichzeitig an die neue Umgebung anpassen. In den frühen Phasen dieses Wandels konnte Ransomware in der Regel keine Dateien auf Cloud-Plattformen erreichen – lagen die Daten in der Cloud statt auf einem lokalen Server, ließen Angreifer sie meist unangetastet, da ihnen ein direkter Zugriffsweg fehlte.

Das änderte sich, als Angreifer lernten, Cloud-Speicher wie ein Amazon-, OneDrive- oder Google-Drive-Konto manuell mit einem infizierten System zu verbinden. Sie taten dies, indem sie den Cloud-Speicher als lokalen Laufwerksbuchstaben einbanden – ähnlich wie ein USB-Gerät auf einem Computer als eigenes Laufwerk erscheint. Sobald der Cloud-Speicher auf diese Weise eingebunden war, waren die cloudbasierten Dateien der Verschlüsselung genauso ausgesetzt wie Dateien auf einer lokalen Festplatte.

Die größere Bedrohung heute: gestohlene Schlüssel und Token

Mit der Reifung der Cloud-Nutzung verlagerten sich auch die Taktiken der Angreifer erneut. Anstatt Laufwerke manuell einzubinden, gehen viele nun gezielt gegen API-Schlüssel und Sitzungstoken vor – Zugangsdaten, die direkten, programmgesteuerten Zugriff auf Cloud-Konten und -Daten

gewähren. Der Erwerb eines solchen Tokens ist vergleichbar mit dem Diebstahl eines Passworts, bietet jedoch oft einen breiteren und schnelleren Zugriff auf Cloud-Ressourcen als ein gestohlenes Passwort allein.

Diese Verlagerung ist bedeutsam, denn dieselbe Geschwindigkeit und Skalierbarkeit, die Cloud-Computing für legitime IT-Teams wertvoll machen, stehen nun auch Angreifern zur Verfügung. Unter den Kunden von Cyber Crucible erlebte im vergangenen Jahr mehr als die Hälfte einen versuchten Diebstahl eines Cloud-Sitzungstokens, mit dem Ziel, die aktive Sitzung eines Nutzers zu übernehmen, während weniger als 9 % einen tatsächlichen Datenkompromiss verzeichneten. Dies deutet darauf hin, dass Angreifer den Diebstahl von Zugangsdaten und Token als primären Einstiegspunkt priorisieren, wobei Datendiebstahl ein sekundäres Ziel darstellt.

Sind Cloud-Daten automatisch sicher?

Cloud-Speicher garantiert keinen Schutz vor Ransomware oder Datendiebstahl. Er verändert lediglich die Methode, die Angreifer anwenden müssen, um an diese Daten zu gelangen – wobei sich das primäre Risiko hin zur Kompromittierung von Zugangsdaten und Sitzungstoken verschiebt, statt zur direkten Dateiverschlüsselung.

https://player.vimeo.com/video/1047006345

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Bedeutet es, dass der Angriff vorbei ist, wenn sich Ransomware selbst löscht?

Kurze Antwort: Nein. Moderne Ransomware ist häufig so konzipiert, dass sie sich selbst löscht, sobald die Verschlüsselung der Dateien abgeschlossen ist – doch diese Selbstlöschung hat nichts damit zu tun, ob Ihre Systeme oder Daten tatsächlich sicher sind. Sie beseitigt lediglich die Spuren des Werkzeugs, das den Schaden verursacht hat.

Warum das „Verschwinden“ der Ransomware keine Wiederherstellung bedeutet

Heutige Angreifer verlassen sich bei einem gesamten Angriff nur selten auf ein einziges Stück Schadsoftware. Stattdessen verwenden sie in der Regel eine Abfolge separater Werkzeuge: eines, um Zugangsdaten abzugreifen, ein weiteres, um wertvolle Daten aufzuspüren und zu exfiltrieren, und ein letztes, um Dateien zur maximalen Druckausübung zu verschlüsseln. Sobald dieses letzte Verschlüsselungswerkzeug seine Aufgabe erledigt hat, löscht es sich häufig selbst vom System. Zurück bleiben Erpresserschreiben mit Kontaktanweisungen und, was noch wichtiger ist, Dateien, die weiterhin gesperrt sind. Das Fehlen der Schadsoftware selbst ist kein Zeichen dafür, dass das Problem gelöst ist – es bedeutet lediglich, dass die Aufgabe des Angreifers aus dessen Sicht erledigt ist.

Was tatsächlich mit Ihren Daten geschieht

Zum Zeitpunkt der Verschlüsselung hat ein etwaiger Datendiebstahl in der Regel bereits stattgefunden, und diese Informationen sind unabhängig vom weiteren Verlauf verloren. Die verbleibenden verschlüsselten Dateien können in manchen Fällen durch Verhandlungen mit dem Angreifer oder durch Entschlüsselungswerkzeuge wiederhergestellt werden, jedoch ohne Erfolgsgarantie. Techniken, die früher eine automatisierte Entschlüsselung ohne Zahlung an die Angreifer ermöglichten, sind mittlerweile weit weniger wirksam, da Ransomware-Betreiber ihre

Methoden angepasst haben. Es gibt keine einfache Wiederherstellungsmaßnahme, wie etwa einen Neustart des Geräts, die die Verschlüsselung rückgängig machen würde.

Die tatsächliche Wahl nach einem Angriff

Sobald die Ransomware ihren Lauf genommen und sich selbst gelöscht hat, bleiben Organisationen in der Regel zwei Wege: der Wiederaufbau betroffener Systeme und Daten aus sauberen Backups oder der Versuch einer Entschlüsselung durch Zahlung und Verhandlung mit dem Angreifer. Keine der beiden Optionen ist schnell oder garantiert erfolgreich – weshalb Prävention, also die Verhinderung von Verschlüsselung und Datendiebstahl, bevor sie geschehen, weiterhin deutlich wirksamer ist als der Versuch, im Nachhinein zu reagieren.

https://player.vimeo.com/video/1043482941

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Sollte sich Cybersicherheit auf Resilienz oder auf die Verhinderung von Angriffen von vornherein konzentrieren?

Kurze Antwort: Resilienz – die Wiederherstellung nach einem Angriff – ist wichtig, aber das wichtigere Ziel ist es, Ransomware, Datendiebstahl und Identitätsdiebstahl zu verhindern, bevor Schaden entsteht, da automatisierte Angriffe unaufhörlich sind und zunehmend gut darüber informiert sind, wann sie zuschlagen sollten.

Zwei Bedeutungen von "Resilienz"

Der Begriff "Resilienz" in der Cybersicherheit hat sich in Richtung zweier unterschiedlicher Konzepte entwickelt. Das eine ist die Frage, ob Ihre Sicherheitstools selbst unter Angriff weiter funktionsfähig bleiben können – im Wesentlichen, ob die Software, die Sie schützen soll, einen direkten Angriff oder eine Manipulation überstehen kann, ähnlich wie man fragen würde, ob eine Überwachungskamera weiter aufzeichnen kann, nachdem jemand versucht hat, sie auszuschalten. Die andere, eher traditionelle Bedeutung ist die Frage, ob sich Ihr Unternehmen erholen und wieder aufrichten kann, nachdem es bereits zu einem Sicherheitsvorfall gekommen ist.

Beides ist wichtig, aber keines sollte die primäre Strategie sein. Moderne Angriffe sind automatisiert und beständig. Der Hauptgrund, warum Organisationen nicht ununterbrochen angegriffen werden, liegt darin, dass Angreifer mittlerweile gut darin geworden sind, Signale darüber zu lesen, welche Ziele ihre Zeit wert sind – zum Beispiel, indem sie Unternehmen meiden, die eindeutig nicht über die finanziellen Ressourcen verfügen, um einen Angriff profitabel zu machen. Dieses Ausmaß an automatisierter Zielauswahl bedeutet, dass Resilienz allein eine reaktive Haltung gegenüber einem Gegner darstellt, der ständig sondiert.

Warum Prävention an erster Stelle stehen sollte

Nach einem Sicherheitsvorfall resilient zu sein, ist vergleichbar damit, nach einem Autounfall eine gute Werkstatt zur Hand zu haben. Das ist nützlich, aber es ist weitaus besser, den Unfall von

vornherein zu vermeiden. Niemand möchte testen, wie gut der Reparaturprozess funktioniert, wenn er stattdessen die Kollision von vornherein vermeiden kann.

Auf die Unternehmenssicherheit übertragen bedeutet dies, dass die Priorität darin bestehen sollte, Angriffe zu stoppen, bevor sie erfolgreich sind – das Äquivalent dazu, verlässliche Bremsen zu haben, anstatt nur einen guten Reparaturplan für die Zeit nach einem Unfall. Cyber Crucible arbeitet auf dieses Ergebnis hin, indem es sich auf autonome Prävention konzentriert, mit dem Ziel, Versuche von Ransomware, Datendiebstahl und Identitätsdiebstahl zu stoppen, bevor sie Schaden anrichten können, anstatt sich ausschließlich auf Wiederherstellung und Aufräumarbeiten im Nachhinein zu verlassen.

https://player.vimeo.com/video/1194994916

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Wie unterstützt Cyber Crucible mich bei der Verwaltung von Cybersecurity-Anbietern und -Ergebnissen?

Kurz gefasst: Cyber Crucible übernimmt die automatisierte Prävention am Endpunkt, sodass Sie frei sind, Ihren eigenen Monitoring- oder Response-Anbieter auszuwählen und zur Rechenschaft zu ziehen – anstatt an einen gebündelten, schwer zu bewertenden Service gebunden zu sein, der an einen einzelnen EDR- oder XDR-Anbieter geknüpft ist.

Das verborgene Problem gebündelter Sicherheitsdienstleistungen

Viele Organisationen zahlen erhebliche Summen für ein gehostetes Security Operations Center, das an ein bestimmtes Produkt zur Endpunkterkennung oder Extended Detection and Response gekoppelt ist. Das Problem dabei ist, dass diese Konstellation dem Kunden oft nur wenig Einblick lässt, wie aufmerksam oder wirksam dieser Überwachungsdienst tatsächlich ist. Möglicherweise wissen Sie nicht, wie genau Ihre Umgebung überwacht wird, wie schnell Vorfälle eskaliert werden oder ob Sie für diesen Anbieter ein priorisiertes Konto sind. Da die Überwachung an die zugrunde liegende Technologie gebunden ist, bleibt kaum Spielraum, um den Service zu verhandeln, zu messen oder auszutauschen, falls er nicht überzeugt.

Die Trennung von Prävention und Überwachung stellt die Kontrolle wieder her

Cyber Crucible konzentriert sich auf die Präventionsebene des Endpunktschutzes und stoppt Ransomware, Datendiebstahl und Identitätsdiebstahlversuche automatisch. Da die Prävention unabhängig gehandhabt wird, sind Organisationen nicht länger gezwungen, ein einziges Gesamtpaket für Erkennung und Reaktion zu wählen. Stattdessen erhalten Sie die Freiheit, den

Managed-Detection-and-Response-(MDR)- oder Managed-Security-Services-(MSSP)-Partner zu wählen, der zu Ihren Anforderungen passt – sei es Ihr eigenes internes Team, ein spezialisierter MSSP oder ein anderer MDR-Anbieter.

Warum Wahlfreiheit wichtig ist

Diese Trennung gibt Ihnen die Möglichkeit, eigene Service-Level-Agreements festzulegen, die Qualität und Reaktionsfähigkeit des Teams zu messen, das Ihre Umgebung überwacht, und diesen Anbieter über eine echte vertragliche Beziehung zur Rechenschaft zu ziehen. Anstatt zu hoffen, dass ein gebündelter Anbieter Ihnen ausreichend Aufmerksamkeit schenkt, können Sie Leistungsstandards nach Ihren eigenen Bedingungen bewerten und durchsetzen. Letztlich geht es beim Ansatz von Cyber Crucible darum, Organisationen echte Kontrolle zu geben – Kontrolle gegenüber Angreifern und ebenso wichtig, Kontrolle über die Anbieterbeziehungen und Verträge, die Ihr Sicherheitsprogramm stützen.

https://player.vimeo.com/video/1046829518

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Wie hilft Cyber Crucible mir dabei, Cybersicherheitsausgaben und Anbieterverträge zu kontrollieren?

Kurze Antwort: Cyber Crucible senkt nicht zwangsläufig Ihr gesamtes Sicherheitsbudget, gibt Ihnen jedoch mehr Kontrolle darüber, wie dieses Budget eingesetzt wird, indem es Ihnen ermöglicht, die Prävention von Ransomware und Datendiebstahl von Überwachungs- und Reaktionsdiensten zu trennen – sodass Sie den Anbieter, der Letzteres übernimmt, selbst auswählen und zur Rechenschaft ziehen können.

Die versteckten Kosten gebündelter SOC-Dienste

Viele Organisationen zahlen erhebliche Summen an ein gehostetes Security Operations Center (SOC), das mit einer EDR- oder XDR-Plattform gebündelt ist. Die Herausforderung bei dieser Anordnung besteht darin, dass der Kunde in der Regel kaum Einblick hat, wie aufmerksam oder effektiv das Überwachungsteam tatsächlich arbeitet. Es gibt keine einfache Möglichkeit, die Qualität der Reaktion, das Engagement des Personals oder die Priorität, die Ihrem Konto eingeräumt wird, zu messen. Im Grunde vertrauen Sie darauf, dass der Dienst im Hintergrund gut funktioniert, ohne eine praktikable Möglichkeit zur Überprüfung zu haben.

Trennung von Prävention und Überwachung

Cyber Crucible konzentriert sich speziell auf die Präventionsseite des Endpunktschutzes – das Verhindern von Ransomware, Datendiebstahl und Identitätsdiebstahl, bevor Schaden entsteht. Da die Prävention unabhängig gehandhabt wird, sind Organisationen nicht mehr an einen einzigen

gebündelten Anbieter für Prävention und Überwachung gebunden. Das bedeutet, dass Sie Ihren eigenen Anbieter für Managed Detection and Response (MDR), MSSP oder sogar Ihr internes Team für die laufende Überwachung und Reaktion auswählen können.

Kontrolle über die Verantwortlichkeit der Anbieter zurückgewinnen

Diese Trennung ist wichtig, weil sie Ihre Fähigkeit wiederherstellt, klare Service-Level-Agreements mit den von Ihnen ausgewählten Anbietern auszuhandeln und durchzusetzen. Sie können die Reaktionsfähigkeit bewerten, die Leistung messen und Lieferanten in einer Weise zur Rechenschaft ziehen, die nicht möglich ist, wenn Prävention und Überwachung in einem einzigen Vertrag miteinander verknüpft sind. Kurz gesagt: Der Wert liegt nicht nur in der technischen Verteidigung gegen Angreifer – sondern darin, die Aufsicht und Kontrolle über Ihre eigenen Anbieterbeziehungen, Verträge und die Qualität der Dienstleistung, für die Sie bezahlen, zurückzugewinnen.

https://player.vimeo.com/video/1046667196

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Funktioniert Cyber Crucible zusammen mit anderen Cybersicherheits- und EDR-Tools?

Kurze Antwort: Ja. Cyber Crucible basiert auf eigenen, proprietären Sensoren und einer eigenen Verhaltensüberwachungstechnologie und läuft daher parallel zu praktisch jedem anderen Sicherheitsprodukt, ohne bestehende Tools zu beeinträchtigen.

Warum Kompatibilität kein Problem darstellt

Cyber Crucible ist nicht auf gemeinsam genutzte EDR-Hooks oder systemweite Integrationen angewiesen, auf die auch andere Sicherheitsanbieter zurückgreifen. Da der Erkennungs- und Überwachungsansatz, einschließlich der Methoden zur Verhaltenserfassung hinter FortressAI, von Grund auf individuell entwickelt wurde, konkurriert Cyber Crucible nicht um dieselben Systemressourcen und stört nicht die Hooks, die andere Endpoint-Protection-Tools verwenden. Durch dieses Design kann Cyber Crucible als zusätzliche Schutzebene fungieren, statt als Ersatz oder als störende Überlagerung. Die Lösung wurde bereits gemeinsam mit Produkten einer Vielzahl etablierter Sicherheitsanbieter eingesetzt, und in der Praxis zeigen sich in den meisten Umgebungen überhaupt keine Kompatibilitätsprobleme.

Wann Anpassungen erforderlich sind

Die seltene Situation, die zusätzliche Konfiguration erfordert, betrifft individuell entwickelte, intern erstellte Software eines Unternehmens. Gelegentlich zeigen diese selbst entwickelten Tools Verhaltensmuster, die den Aktivitäten ähneln, die Cyber Crucible erkennen soll, etwa schnelle Dateiänderungen oder ungewöhnliche Systeminteraktionen. In solchen Fällen ist die Lösung einfach: Eine Ausschlussregel kann hinzugefügt werden, damit Cyber Crucible das interne Tool als legitim erkennt. Dieser Ausschluss bleibt zuverlässig, solange die interne Software ordnungsgemäß signiert und unverändert bleibt, das heißt, solange sie weiterhin ihrem erwarteten, verifizierten Zustand entspricht. Sind diese Bedingungen erfüllt, funktioniert das Tool ohne fortlaufende Reibung

normal neben Cyber Crucible.

Was das für Sicherheitsteams bedeutet

Organisationen müssen ihren aktuellen Sicherheits-Stack nicht entfernen oder neu konfigurieren, um Cyber Crucible einzuführen. Die Lösung wurde entwickelt, um bestehende Schutzmaßnahmen zu ergänzen, indem sie eine dedizierte Ebene hinzufügt, die sich auf die Prävention von Ransomware, Datendiebstahl und Identitätsdiebstahl konzentriert, ohne die bereits vorhandenen Schutz-Tools in der Umgebung zu stören.

https://player.vimeo.com/video/1043463490

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Warum ist KI für Unternehmensführungen ein Geschäftsrisiko und nicht nur ein Produktivitätswerkzeug?

Kurze Antwort: Führungsteams betrachten KI oft ausschließlich als Produktivitätsbooster, doch unkontrollierte KI-Nutzung kann zentrale Geschäftsgeheimnisse – Produktpläne, Umsatzdaten und Vertriebsstrategien – direkt gegenüber Außenstehenden offenlegen. Dies ist ein strategisches und finanzielles Risiko, das auf den Schreibtisch des CEO, CFO, COO und der Vertriebsleitung gehört – nicht nur in die IT-Abteilung.

Eine andere Art der Gefährdung

Klassische Cybersicherheitsvorfälle, etwa ein Datenleck, bei dem Kundendaten im Darknet landen, folgen einem bekannten Muster: Die Unternehmensführung reagiert, Aufsichtsbehörden werden gegebenenfalls eingeschaltet, mitunter werden Bußgelder gezahlt, und der Vorstand wird informiert. Unternehmen kennen dieses Szenario, und es existieren Prozesse zu dessen Bewältigung.

KI führt eine neue und weniger gut verstandene Kategorie der Gefährdung ein. Wenn Mitarbeiter KI-Tools ohne angemessene Schutzmaßnahmen nutzen, geben sie unter Umständen vertrauliche Geschäftsinformationen – zukünftige Produktpläne, Gewinnprognosen, Vertriebspipelines – an Systeme weiter, die niemals dafür ausgelegt waren, diese Informationen sicher zu verwahren. Anders als bei einem Hacking-Vorfall handelt es sich hierbei nicht zwangsläufig um einen Angriff. Es kann schlicht durch die normale, gutgemeinte Nutzung von KI durch das Personal geschehen.

Das Problem interner Abfragen

Ein oft übersehenes Risiko betrifft das, was intern in einem Unternehmen geschieht, sobald ein KI-Tool umfassenden Zugriff auf interne Dokumente und Daten hat. Wenn Zugriffskontrollen nicht sorgfältig gestaltet sind, könnte ein Mitarbeiter einem KI-Assistenten eine einfache Frage stellen und eine detaillierte Antwort mit sensiblen Plänen erhalten, die niemals frei zirkulieren sollten – nicht einmal intern. Das ist ein Governance-Versagen, kein technischer Fehler, und kann ebenso schädlich sein wie ein externes Datenleck.

Warum dies auf Führungsebene gehört

Die Entscheidung, nicht in eine ordnungsgemäß kontrollierte, interne KI-Umgebung zu investieren, beseitigt diese Risikokategorie nicht – sie verlagert sie lediglich außerhalb der direkten Aufsicht des Unternehmens. Unternehmensleiter würden niemals in Erwägung ziehen, Gewinn- und Verlustrechnungen oder Vertriebspipelines auf einer öffentlichen Website zu veröffentlichen. Unkontrollierte KI-Nutzung kann ein ähnliches Ergebnis herbeiführen, ohne dass dies jemand beabsichtigt. Dies als grundlegendes Geschäftsrisiko und nicht als rein technisches Problem zu behandeln, ist entscheidend, um die Wettbewerbsvorteile zu schützen, die die Unternehmensführung sich erarbeitet hat.

https://player.vimeo.com/video/1211538534

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Nutzen Mitarbeiter bereits KI-Tools, bevor unser Unternehmen über eine offizielle KI-Richtlinie verfügt?

Kurze Antwort: Ja. Die meisten Organisationen stellen fest, dass Mitarbeiter, Auftragnehmer, Berater und Anbieter bereits auf kreative und unerwartete Weise KI-Tools nutzen – lange bevor eine formelle KI-Richtlinie oder ein Governance-Projekt abgeschlossen ist. Wer darauf wartet, eine „perfekte“ Richtlinie zu erstellen, bevor die KI-Nutzung angegangen wird, bleibt gegenüber dem, was bereits geschieht, blind.

Die verbreitete Annahme

Viele Führungskräfte gehen davon aus, dass die KI-Einführung in ihrer Organisation ruht, bis eine offizielle Richtlinie geschrieben, genehmigt und eingeführt wurde. Der Gedanke dahinter ist, dass Mitarbeiter geduldig auf klare Regeln warten, bevor sie mit neuen Tools experimentieren. In der Praxis hält diese Annahme selten stand. Menschen suchen tendenziell nach Wegen, effizienter zu arbeiten – unabhängig davon, ob bereits formale Vorgaben existieren.

Was Organisationen tatsächlich feststellen

Wenn Unternehmen Überwachungs- oder Durchsetzungstools einführen, wie zum Beispiel FortressAI von Cyber Crucible, entdecken sie oft, dass die KI-Nutzung weitaus verbreiteter und vielfältiger ist als erwartet. Mitarbeiter sind von Natur aus einfallsreich; genau diese Kreativität und Problemlösungsfähigkeit, die sie zu wertvollen Mitarbeitern macht, führt auch dazu, dass sie neue, nicht genehmigte Wege finden, um KI-Tools zu nutzen und Zeit zu sparen oder ihre Ergebnisse zu verbessern. Dies ist weniger ein Zeichen böser Absicht als vielmehr menschlicher Natur: Menschen nutzen verfügbare Werkzeuge, um ihre Arbeit zu erleichtern – unabhängig davon, ob eine Richtlinie dies offiziell erlaubt.

Warum Transparenz wichtiger ist als eine perfekte Richtlinie

Das eigentliche Risiko besteht nicht darin, dass eine Richtlinie noch nicht fertiggestellt wurde. Es besteht vielmehr darin, dass Organisationen oft keinen Einblick haben, wie KI bereits in ihrer Umgebung eingesetzt wird. Ohne diese Transparenz können Sicherheits- und Compliance-Teams das Risiko von Datenlecks, unautorisierter Tool-Nutzung oder anderen mit der KI-Einführung verbundenen Gefahren nicht bewerten. Anstatt auf die Fertigstellung eines umfassenden KI-Governance-Frameworks zu warten, profitieren Organisationen davon, zunächst Einblick in die aktuellen Nutzungsmuster zu gewinnen. Das Verständnis dessen, was tatsächlich vor Ort geschieht, ermöglicht es, Richtlinien auf der Realität und nicht auf Annahmen über das Verhalten der Mitarbeiter aufzubauen.

https://player.vimeo.com/video/1176537677

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Welche Warnzeichen deuten darauf hin, dass ein Ransomware-Angriff im Gange ist?

Kurze Antwort: Sobald Ransomware ausgelöst wird, kann sie ein Unternehmen innerhalb von nur 60 bis 90 Sekunden lahmlegen. Sichtbare Warnzeichen treten daher in der Regel erst auf, wenn der Angriff bereits im Gange ist – nicht rechtzeitig genug, um manuell einzugreifen. Die eigentliche Verteidigung besteht darin, die Vorbereitungsarbeiten der Angreifer im Vorfeld zu erkennen, bevor sie den finalen Auslöser betätigen.

Warum Ransomware plötzlich wirkt

Ransomware-Angriffe werden oft als augenblicklich beschrieben, doch das ist irreführend. Angreifer verbringen typischerweise Zeit unbemerkt im Netzwerk, kartieren Systeme, verschaffen sich Zugang und positionieren sich, um maximalen Schaden anzurichten. Diese Vorarbeit ähnelt der eines Militärteams, das ein Schlachtfeld vorbereitet, bevor eine Operation beginnt. Sobald alles vorbereitet ist, kann sich das eigentliche Verschlüsselungs- oder Aussperrungsereignis in unter zwei Minuten vollziehen. Bis Mitarbeiter bemerken, dass etwas nicht stimmt, ist der Schaden meist bereits im Gange.

Wie der Moment des Angriffs aussieht

Wenn ein Angriff ausgeführt wird, bemerken Unternehmen häufig einen plötzlichen und unheimlichen Wandel: Bestimmte Anwendungen oder Dienste reagieren nicht mehr, Netzwerkverbindungen werden instabil, Telefonsysteme können ausfallen, und der normale Betrieb wird nahezu gleichzeitig gestört. Ebenso beunruhigend ist, dass manche Systeme in diesem Zeitfenster weiterhin normal laufen. Diese scheinbare Normalität ist kein gutes Zeichen. Sie bedeutet oft, dass Angreifer diese nicht betroffenen Systeme als Tarnung nutzen, während der Rest der Umgebung kompromittiert wird.

Warum frühe Erkennung wichtiger ist als Reaktion

Da die sichtbaren Anzeichen von Ransomware erst in den letzten, rasant ablaufenden Sekunden eines Angriffs auftreten, ist es keine zuverlässige Strategie, auf diese Anzeichen zu warten und dann zu reagieren. Wirksamer Schutz hängt davon ab, bösartige Aktivitäten bereits in der Vorbereitungsphase zu erkennen und zu stoppen, bevor Angreifer bereit sind zu handeln. Auf dieser Ebene setzen autonome Erkennungstools wie FortressAI von Cyber Crucible an, mit dem Ziel, das Verhalten der Angreifer zu unterbrechen, bevor es den Punkt ohne Wiederkehr erreicht, anstatt auf die äußeren Symptome zu warten, die erst auftreten, wenn der Angriff bereits im Gange ist.

https://player.vimeo.com/video/1043488930

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Was passiert tatsächlich in den Momenten während eines Ransomware-Angriffs?

Kurze Antwort: Die eigentliche Verschlüsselungsphase eines Ransomware-Angriffs ist bemerkenswert schnell und dauert nach Auslösung oft nur etwa 60 bis 90 Sekunden, obwohl Angreifer zuvor erhebliche, unbemerkte Zeit damit verbringen, sich innerhalb eines Netzwerks zu positionieren. Wenn sichtbare Symptome auftreten, entfaltet sich der Schaden bereits in Echtzeit – weshalb die Erkennung vor dem endgültigen Auslöser erfolgen muss, nicht danach.

Die Ruhe vor dem Angriff

Bevor Ransomware jemals aktiviert wird, verbringen Angreifer typischerweise Zeit damit, sich unbemerkt durch die Systeme eines Unternehmens zu bewegen, wertvolle Daten zu identifizieren, Backups zu deaktivieren und die Bedingungen für einen erfolgreichen Angriff zu schaffen. Diese Vorbereitungsarbeit kann unbemerkt bleiben, da der normale Geschäftsbetrieb wie gewohnt weiterläuft. Das Netzwerk kann bis zu dem Moment, in dem der Angreifer beschließt, die finale Phase einzuleiten, stabil und unauffällig erscheinen. Ähnlich wie eine unheimliche Stille kurz vor einem katastrophalen Ereignis kann diese ruhige Phase trügerisch sein, da sie nicht die bevorstehende Störung widerspiegelt.

Der rasante Beginn des Schadens

Einmal ausgelöst, kann sich ein Ransomware-Ereignis in weniger als zwei Minuten vollständig entfalten. In diesem kurzen Zeitfenster bemerken Mitarbeitende möglicherweise plötzliche Ausfälle: E-Mail funktioniert nicht mehr, Telefonsysteme verstummen, Anwendungen verhalten sich fehlerhaft oder Netzwerkverbindungen werden instabil. Dies sind Symptome einer Verschlüsselung und Systemkompromittierung, die gleichzeitig in der gesamten Umgebung stattfinden. Da der Prozess so schnell abläuft, bleibt in der Regel nicht genug Zeit, um manuell einzugreifen, sobald er begonnen hat.

Warum manche Systeme weiterlaufen

Ein beunruhigendes Detail vieler Ransomware-Vorfälle ist, dass nicht alles gleichzeitig ausfällt. Manche Dienste laufen möglicherweise normal weiter, während andere zusammenbrechen. Dies liegt oft daran, dass genau diese nicht betroffenen Systeme der Ort sind, an dem der Angreifer noch aktiv ist, und sie als Stützpunkt oder Ausgangsbasis nutzt. Dieses Muster zu erkennen ist wichtig, da die Annahme, ein Problem sei „nur teilweise“ vorhanden, ein falsches Sicherheitsgefühl erzeugen kann, während die Kompromittierung aktiv fortschreitet. Eine wirksame Prävention hängt davon ab, bösartige Aktivitäten zu erkennen und zu stoppen, bevor die finale, zerstörerische Phase beginnt, da nach der Auslösung nur ein extrem kurzes Zeitfenster zum Handeln bleibt.

https://player.vimeo.com/video/1046658956

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Was passiert tatsächlich, wenn Ransomware einen Unternehmensserver trifft?

Kurze Antwort: Wenn Ransomware einen Server trifft, deaktivieren Angreifer in der Regel zunächst dessen Dienste und verschlüsseln anschließend die Daten – dabei schneiden sie IT- und Sicherheitsteams vom Eingreifen ab und nutzen mitunter Dutzende oder sogar Hunderte kompromittierter Arbeitsstationen, um die Verschlüsselung remote durchzuführen.

Die ersten Anzeichen eines Angriffs

Eines der frühesten Anzeichen dafür, dass ein Server kompromittiert wurde, ist ein plötzlicher Dienstausfall. Da Angreifer wissen, dass Ransomware Dateien während der Verschlüsselung versehentlich beschädigen kann, deaktivieren viele bewusst die auf einem Server laufenden Anwendungen, bevor der Verschlüsselungsprozess beginnt. Das bedeutet, dass Mitarbeiter oder Kunden, die auf dieses System angewiesen sind – sei es eine Gehaltsabrechnungsplattform, eine Webanwendung oder ein anderer geschäftskritischer Dienst – möglicherweise einen Ausfall bemerken, bevor jemand erkennt, dass ein Sicherheitsvorfall im Gange ist.

Verteidiger aussperren, während sich die Verschlüsselung ausbreitet

Sobald der Angriff im Gange ist, beginnt die Ransomware, die auf dem Server gespeicherten Daten zu verschlüsseln. Um zu verhindern, dass Sicherheitsteams oder Administratoren eingreifen, blockieren Angreifer häufig den Netzwerkzugriff auf den Server und isolieren ihn von den Personen, die normalerweise auf die Bedrohung reagieren würden. Diese Taktik verschafft dem Angreifer Zeit, die Verschlüsselung der Dateien abzuschließen, bevor Verteidiger handeln können.

Arbeitsstationen können die eigentliche Schwachstelle sein

Interessanterweise liegt die Gefahr nicht immer beim Server selbst. In vielen Fällen kompromittieren Angreifer eine große Anzahl von Mitarbeiter-Arbeitsstationen – manchmal 50, 70 oder mehr –, die bereits legitimen Zugriff auf den Server haben. Diese Arbeitsstationen werden dann gleichzeitig genutzt, um die Daten des Servers remote zu verschlüsseln. Da der Angriff von mehreren Endpunkten gleichzeitig ausgeht, stellen die mit dem Server verbundenen Arbeitsstationen oft eine größere Schwachstelle dar als die Serverinfrastruktur selbst.

Dieses Muster verdeutlicht, warum sich die Ransomware-Abwehr nicht ausschließlich auf Server konzentrieren darf. Endpunktsicherheit auf jedem Gerät mit Serverzugriff spielt eine entscheidende Rolle dabei, Angriffe zu stoppen, bevor sich die Verschlüsselung ausbreitet. Cyber Crucibles' FortressAI wurde entwickelt, um diese Verhaltensweisen bereits im frühesten Stadium zu erkennen und zu unterbrechen – unabhängig davon, ob die Bedrohung von einem Server ausgeht oder sich von verbundenen Arbeitsstationen ausbreitet.

https://player.vimeo.com/video/1041172405

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Warum greift Ransomware freigegebene Dateien an, bevor sie meinen Desktop trifft?

Kurze Antwort: Wenn Ransomware einen einzelnen Arbeitsplatzrechner infiziert, ist dieser Rechner selten das eigentliche Ziel. Angreifer nutzen die Erstinfektion als Ausgangspunkt, um freigegebene Netzwerkressourcen zu erreichen, und verschlüsseln oder beschädigen den lokalen Desktop erst, nachdem sie bereits wertvollere Daten an anderer Stelle angegriffen haben.

Warum der Desktop die letzte Station ist, nicht die erste

Ein weitverbreiteter Irrglaube ist, dass es sich bei den Dateien eines bestimmten Mitarbeiters um das Ziel der Angreifer handelt, sobald Ransomware auf dessen Computer gelangt. In Wirklichkeit ist die Schadsoftware so programmiert, dass sie fast sofort über den lokalen Rechner hinausblickt. Sobald sie Fuß gefasst hat, beginnt sie, das Netzwerk nach erreichbaren Ressourcen mit größerem Wert zu durchsuchen, etwa Dateiservern, internen Wikis oder Datenbanken mit Kundendaten. Die Verschlüsselung oder Exfiltration dieser zentralen Daten ist das eigentliche Ziel, da sie einen weitaus größeren Teil der Organisation betrifft als der Ordner eines einzelnen Nutzers.

Die Lösegeldforderung erscheint zuletzt, nicht zuerst

Da Angreifer netzwerkweiten Daten Priorität einräumen, bevor sie das ursprünglich infizierte Gerät angreifen, ist der betroffene Mitarbeiter in der Regel die letzte Person, die etwas Ungewöhnliches bemerkt. Bis eine Lösegeldforderung auf dem Bildschirm dieser Person erscheint, haben die Angreifer typischerweise bereits die Verschlüsselung oder den Diebstahl von Daten in großen Teilen der Unternehmensinfrastruktur abgeschlossen. Diese Reihenfolge ist beabsichtigt. Sie ermöglicht es den Angreifern, maximalen operativen Schaden anzurichten, bevor jemand in der Organisation die Chance hat, den Einbruch zu erkennen oder darauf zu reagieren. Die sichtbare Lösegeldforderung ist im Grunde ein Signal dafür, dass der schwerwiegendere Schaden bereits im Verborgenen entstanden ist.

Was das für die Verteidigung bedeutet

Persönliche Fotos oder Dokumente, die lokal auf einem Desktop gespeichert sind, sind bei einem Ransomware-Angriff in der Regel das unwichtigste Ziel, auch wenn sie das sichtbarste Anzeichen dafür sein können. Eine wirksame Verteidigung muss dieses Muster berücksichtigen, indem sie sich darauf konzentriert, bösartige Aktivitäten so früh wie möglich zu erkennen und zu stoppen, bevor sie freigegebene Systeme erreichen können. FortressAI von Cyber Crucible wurde mit dieser Angriffssequenz im Hinterkopf entwickelt und zielt darauf ab, bereits in den frühen Phasen eines Einbruchs einzugreifen, anstatt erst zu reagieren, wenn die Verschlüsselung auf einzelnen Rechnern sichtbar wird.

https://player.vimeo.com/video/1043466243

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Was hat den Gründer dazu inspiriert, Cyber Crucible zu gründen?

Kurze Antwort: Cyber Crucible entstand aus einer Karriere, die der Entwicklung maßgeschneiderter Lösungen für geheime Regierungsmissionen gewidmet war, sowie dem Wunsch, denselben Erfindergeist einzusetzen, um weitaus mehr Menschen weltweit im Kampf gegen Ransomware und Cyberkriminalität zu unterstützen.

Von geheimen Missionen zu einem globalen Problem

Lange bevor Cyber Crucible als Unternehmen existierte, löste der Gründer bereits schwierige Sicherheitsprobleme – darunter auch, wie man die Kontrolle über ein Botnetz übernehmen kann, um Menschen davor zu schützen. Dieses Muster, komplexe technische Herausforderungen zu zerlegen und praktische Lösungen zu entwickeln, zog sich durch eine Karriere bei der National Security Agency und anderen Regierungsorganisationen. Immer wieder wurde ein neues Werkzeug oder Verfahren entwickelt, um einen bestimmten Missionsbedarf zu erfüllen – nur um dann einmal genutzt, an ein verbündetes Team weitergegeben oder nach Erfüllung seines engen Zwecks beiseitegelegt zu werden. Jede Erfindung war wichtig, aber ihre Wirkung endete an der Grenze einer einzelnen geheimen Mission.

Aus Einzellösungen etwas machen, das jeder nutzen kann

Dieser Kreislauf – ein Problem zu lösen und dann zu sehen, wie sein Nutzen auf ein einzelnes Team oder eine einzelne Operation beschränkt blieb – wurde mit der Zeit frustrierend, auch wenn die Arbeit selbst bedeutsam war. Als Ransomware sich zu einer weitverbreiteten Bedrohung entwickelte, ergab sich eine andere Art von Gelegenheit: die Chance, denselben erfinderischen Ansatz anzuwenden, diesmal jedoch gerichtet auf ein Problem, das Organisationen und Einzelpersonen überall betrifft – nicht nur eine einzelne spezialisierte Einheit. Die Erkenntnis war, dass es mehr brauchte als ein weiteres maßgeschneidertes Werkzeug für einen engen Anwendungsfall, um einer breiteren Bevölkerung zu helfen. Es erforderte ein kommerzielles

Produkt, das sich einfach und zuverlässig im großen Maßstab einsetzen lässt.

Warum dies Cyber Crucible heute prägt

Dieser Denkwandel bildet das Fundament des Ansatzes von Cyber Crucible. Anstatt eine Lösung für ein einzelnes Team oder eine einzelne Mission zu entwickeln, besteht das Ziel darin, eine Technologie zu schaffen, angetrieben von FortressAI, die automatisch und zuverlässig für Organisationen überall funktioniert, damit weniger Menschen die Schäden und Störungen durch Ransomware, Datendiebstahl und Identitätsdiebstahl erleben müssen. Die missionsorientierte Arbeit der Vergangenheit bleibt weiterhin bedeutsam, doch der treibende Zweck hinter Cyber Crucible ist es, so viele Menschen wie möglich zu erreichen und zu schützen.

https://player.vimeo.com/video/1046673820

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Woher kommen Ransomware-Angriffe eigentlich?

Kurze Antwort: Ransomware-Akteure sind nicht auf eine Handvoll bekannter Länder beschränkt; Automatisierung und günstige kriminelle Tools ermöglichen es Angreifern heute, nahezu von überall auf der Welt aus zu operieren.

Die vereinfachte Medien-Erzählung stimmt nicht mit der Realität überein

Nachrichtenberichte verweisen häufig auf ein einzelnes Land oder eine Region als Ursprung von Ransomware-Angriffen, weil sich damit eine schnelle, leicht verständliche Schlagzeile erzeugen lässt. In der Praxis zeigt die direkte Erfahrung bei der Reaktion auf akute Vorfälle ein weitaus komplizierteres Bild. Als Cyber Crucible begann, aktive Ransomware-Fälle zu bearbeiten, erhielt unser Team eine Vielzahl von Anrufen im Zusammenhang mit den Angriffen – viele davon von Prepaid- oder Wegwerf-„Burner“-Telefonen ohne nachverfolgbare Besitzhistorie. Diese Anrufe kamen aus vielen verschiedenen Regionen, darunter Südasien, dem Nahen Osten, Teilen Europas, Südamerika und sogar Nordamerika. Einige Anrufer waren Akteure auf niedrigerer Ebene, während andere offenbar die eigentlichen Entwickler der Schadsoftware waren und gelegentlich überraschend professionelle Peer-to-Peer-Gespräche über die technischen Details ihrer Angriffe führten.

Automatisierung hat die Einstiegshürde gesenkt

Zwar bringen bestimmte Regionen der Welt möglicherweise weiterhin einen unverhältnismäßig hohen Anteil qualifizierter Ransomware-Entwickler hervor, doch das Aufkommen von Ransomware-as-a-Service-Kits, Automatisierungstools und einfacher KI-gestützter Kontaktaufnahme hat es weniger versierten Akteuren erheblich erleichtert, sich zu beteiligen. Wer über begrenzte technische Fähigkeiten verfügt, kann heute Angriffsinfrastruktur mieten, gestohlenen Netzwerkzugang von sogenannten Initial-Access-Brokern kaufen und mit minimalem Vorabaufwand eine Erpressungskampagne durchführen. Dies hat effektiv die Tür für opportunistische Kriminelle geöffnet, die sich unabhängig von ihrem Standort beteiligen können, anstatt Ransomware-Aktivitäten auf eine kleine Gruppe staatlich verbundener Akteure zu beschränken.

Warum das für die Verteidigung wichtig ist

Regionaler Slang, Sprachmuster und das bei diesen Vorfällen beobachtete Anrufverhalten bestätigen, dass Angreifer geografisch vielfältig sind und nicht auf ein einzelnes „Schurkenstaat“-Land beschränkt sind. Ransomware als global verteiltes, automatisierungsgetriebenes kriminelles Unternehmen zu verstehen – statt als vereinfachte geopolitische Erzählung – führt zu besser fundierten Verteidigungsstrategien und einem klareren Bild des tatsächlichen Risikos, dem Organisationen ausgesetzt sind.

https://player.vimeo.com/video/1047715735

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Wen greifen Ransomware-Angreifer heute tatsächlich an?

Kurze Antwort: Ransomware-Betreiber konzentrieren sich nicht mehr nur auf große, prominente Organisationen. Automatisierung und KI-gestützte Tools haben es rentabel gemacht, Unternehmen nahezu jeder Größe anzugreifen. Das bedeutet, dass die meisten Organisationen davon ausgehen sollten, ein potenzielles Ziel zu sein.

Wie sich die Zielauswahl seit 2020 verändert hat

In den Anfängen moderner Ransomware erforderte die Durchführung eines Angriffs vom initialen Zugriff bis zur Erpressung erfahrene, versierte Hacker, die größtenteils manuell arbeiteten. Das begrenzte den Kreis der fähigen Angreifer und lenkte den Fokus auf große, hochwertige Ziele, bei denen der Ertrag den Aufwand rechtfertigte.

Mit wachsender Nachfrage begannen etablierte Hackergruppen, zunehmend wie skalierende Unternehmen zu agieren. Statt sich ausschließlich auf eine kleine Zahl von Elite-Operatoren zu verlassen, entwickelten sie Ransomware-as-a-Service-Programme, die bewährte Angriffsmethoden in wiederholbare, automatisierte Playbooks verpacken. Dies ermöglichte es weniger erfahrenen Akteuren, effektive Kampagnen durchzuführen – vergleichbar damit, wie ein Junior-Vertriebsmitarbeiter mithilfe eines aus den Methoden eines Top-Performers erstellten Skripts erfolgreich sein kann.

Warum kleinere Organisationen nun gefährdet sind

Automatisierung, maschinelles Lernen und robotergestützte Prozessautomatisierung ermöglichen es diesen Akteuren, viele Angriffe gleichzeitig durchzuführen, Lösegeldverhandlungen zu führen und Zahlungs- oder Wiederherstellungsunterstützung in großem Maßstab zu verwalten. Sobald diese Funktionen weitgehend automatisiert waren, wurde auch das Vorgehen gegen kleinere Unternehmen rentabel, da Maschinen – nicht Menschen – den Großteil der Kontaktaufnahme und Nachverfolgung übernehmen.

Dieser Wandel bedeutet, dass Angreifer weniger selektiv vorgehen. Große „Big Game“-Ziele ziehen aufgrund der Höhe des potenziellen Gewinns weiterhin Aufmerksamkeit auf sich, doch der alltägliche Betrieb dieser kriminellen Operationen ähnelt zunehmend routinemäßiger Vertriebsakquise: Automatisierte Systeme suchen kontinuierlich nach jeder Organisation, die zahlen könnte. Die Systeme, die die Zielauswahl durchführen, haben in der Regel kein Bewusstsein dafür, wer oder was das Ziel tatsächlich ist – ob es sich um ein großes Unternehmen oder eine kleine gemeinnützige Organisation handelt.

Was das für Organisationen bedeutet

Da die Zielauswahl weitgehend automatisiert und unspezifisch erfolgt, ist für die meisten Organisationen nicht die Frage relevant, ob sie gezielt ausgewählt werden könnten, sondern wie gut sie auf einen eventuellen Angriffsversuch vorbereitet sind. Lösungen wie Cyber Crucible, die auf FortressAI basieren, sind darauf ausgelegt, Organisationen dabei zu unterstützen, Ransomware und verwandte Bedrohungen zu erkennen und zu stoppen – unabhängig von Größe oder Profil des Ziels.

https://player.vimeo.com/video/1047715793

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Wer trägt das größte Risiko eines Ransomware-Angriffs, und warum werden diese Ziele ausgewählt?

Kurze Antwort: Das Ransomware-Risiko hängt oft davon ab, wen kriminelle „Access Broker“ am leichtesten kompromittieren können oder gezielt dafür bezahlt werden, zu kompromittieren. Das bedeutet, dass Schulen, Krankenhäuser und Infrastrukturanbieter mit schwächeren Verteidigungsmaßnahmen oder wertvollen Daten häufig ganz oben auf der Liste stehen.

Wie Ziele überhaupt ausgewählt werden

Hinter den meisten Ransomware-Vorfällen steht ein Marktplatz, den die meisten Menschen nie zu Gesicht bekommen. Eine Gruppe, oft als Initial Access Broker bezeichnet, verbringt ihre Zeit damit, in Netzwerke einzudringen, ohne einen konkreten Plan dafür zu haben, was danach geschieht. Sobald sie sich Zugang verschafft haben, bieten sie diesen Zugang zum Verkauf an und beschreiben genau, was sie kontrollieren – etwa administrative Rechte für Sicherheitstools, die Fähigkeit, Virenschutzmaßnahmen zu deaktivieren, oder Zugriff auf einen großen Teil der Geräte einer Organisation. Sie könnten beispielsweise beschreiben, dass sie die Geräteflotte eines Schulbezirks oder die Remote-Access-Tools eines IT-Anbieters kompromittiert haben. Käufer – von Gruppen für Datendiebstahl über Ransomware-Betreiber bis hin zu staatlich unterstützten Akteuren – bieten dann auf diesen Zugang, je nachdem, wie wertvoll und vollständig er erscheint.

Wenn Angriffe in Auftrag gegeben werden, nicht nur opportunistisch erfolgen

Es gibt außerdem ein zweites, gezielteres Muster. Hierbei stellt ein Käufer, etwa eine Ransomware-Gruppe oder ein staatlich unterstützter Akteur, eine konkrete Anfrage: Man soll eine bestimmte

Anzahl von Organisationen finden und kompromittieren, die bestimmten Kriterien entsprechen – zum Beispiel Krankenhäuser einer bestimmten Größe in einer bestimmten Region oder Versorgungsunternehmen wie Wasseraufbereitungsanlagen. Access Broker behandeln dies dann wie einen Verkaufsauftrag und suchen aktiv nach Organisationen, die dem Profil entsprechen. Sobald sie erfolgreich sind, verkaufen sie diesen Zugang an den ursprünglichen Auftraggeber weiter, auch wenn beide Seiten in der Regel nie direkt miteinander in Kontakt treten oder die Identität der jeweils anderen kennen. Aus diesem Grund spiegeln plötzliche Häufungen von Angriffen auf ähnliche Organisationen, etwa mehrere Krankenhäuser in einer Region, oft eine koordinierte Kaufanfrage wider und keinen Zufall.

Warum das für die Verteidigung wichtig ist

Da die Zielauswahl sowohl opportunistisch als auch gezielt in Auftrag gegeben erfolgen kann, kann jede Organisation mit schwachen Sicherheitskontrollen, sensiblen Daten oder kritischen Diensten zum Ziel werden, unabhängig von Größe oder Branche. Das Verständnis dieser Dynamik zwischen Käufern und Verkäufern unterstreicht, warum proaktive, durchgehend aktive Verteidigungsmaßnahmen wichtiger sind als eine Reaktion, nachdem ein Zugang bereits an den Höchstbietenden verkauft wurde.

https://player.vimeo.com/video/1047715835

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Wer führt Ransomware-Angriffe tatsächlich aus und wie gehen sie vor?

Kurze Antwort: Ransomware-Angriffe werden von einem lose organisierten Netzwerk aus Entwicklern, Wiederverkäufern und Operatoren durchgeführt, das ähnlich wie eine Lieferkette in der Wirtschaft funktioniert. Die effektivsten unter ihnen betreiben Erpressung als professionelles Handwerk und nicht als persönliche Racheaktion.

Ransomware als organisierte Lieferkette

Ransomware ist selten das Werk eines einzelnen, allein handelnden Hackers. Stattdessen funktioniert sie eher wie eine verteilte Branche, bestehend aus Malware-Entwicklern, die die Werkzeuge entwickeln, Wiederverkäufern oder Affiliates, die Zugang zu dieser Malware verteilen, und Operatoren, die die eigentlichen Angriffe auf die Opfer durchführen. Jede Gruppe übernimmt eine eigene Rolle, ähnlich wie sich ein legitimer Softwareanbieter auf Hersteller, Vertriebspartner und Vertriebsteams verlässt. Diese mehrschichtige Struktur trägt maßgeblich zur Widerstandsfähigkeit von Ransomware bei: Die Störung eines einzelnen Glieds in der Kette stoppt nicht zwangsläufig die gesamte Operation.

Die Profis im Vergleich zu den emotionalen Angreifern

Nicht alle Angreifer verhalten sich gleich, sobald ihre Versuche vereitelt werden. Cyber Crucible hat diesen Kontrast unmittelbar erlebt. In einem Fall rief ein Angreifer mit Verbindungen nach Osteuropa an, nachdem er gestoppt worden war, und behandelte die Begegnung als technisches Rätsel, das es zu lösen galt, statt als persönliche Beleidigung. Diese Person verwies sogar auf interne Software-Details, um zu beweisen, dass sie das Produkt zurückentwickelt hatte, und meldete sich danach regelmäßig wieder, wobei sie ihre Operationen fast wie unter Kollegen besprach.

Im Gegensatz dazu reagierte ein anderer Angreifer mit Verbindungen nach Bangladesch nach der Vereitelung mit Wut und Feindseligkeit und griff eher zu Beleidigungen als zu Problemlösungsansätzen. Dieser Kontakt setzte die Kommunikation nicht fort.

Warum das für die Abwehr wichtig ist

Diese Erfahrungen deuten darauf hin, dass die „erfolgreicheren“ und hartnäckigeren Bedrohungsakteure tendenziell diejenigen sind, die Ransomware als geschäftliche Herausforderung angehen – methodisch, geduldig und darauf fokussiert, Umgehungsmöglichkeiten zu finden. Angreifer als geschäftsmäßig handelnde Gegner zu verstehen, statt als rein chaotische Kriminelle, hilft dabei, die Gestaltung von Verteidigungstechnologien wie FortressAI von Cyber Crucible zu informieren: darauf ausgelegt, kalkulierte Versuche zur Umgehung von Schutzmaßnahmen zu antizipieren, nicht nur isolierte oder emotional getriebene Angriffe.

https://player.vimeo.com/video/1047715866

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Wer ist der ideale Kunde für den Ransomware-Schutz von Cyber Crucible?

Kurze Antwort: Cyber Crucible eignet sich am besten für Menschen, die in geschäftlichen Auswirkungen denken, nicht nur in technischen Merkmalen. Dazu gehören IT-Verantwortliche mit knappen Ressourcen ebenso wie Führungskräfte, die verstehen, was selbst ein kurzer Ausfall das Unternehmen kosten könnte.

Warum unternehmerisches Denken wichtiger ist als der Jobtitel

Es gibt keinen einzelnen Jobtitel, der den idealen Cyber Crucible-Kunden definiert. Entscheidend ist, ob die Person die realen Konsequenzen eines Ransomware- oder Datendiebstahlvorfalls versteht: entgangene Umsätze, gestörte Abläufe und die Art von finanziellem Schaden, der sich über Monate oder Jahre hinziehen kann. Jemand mit dieser Denkweise muss nicht davon überzeugt werden, dass automatisierte Prävention sinnvoll ist – er versteht bereits, dass die Vermeidung von Ausfallzeiten direkt mit dem Schutz des Gewinns und der Aufrechterhaltung des Geschäftsbetriebs zusammenhängt.

Das unterscheidet sich von einem rein technischen Verkaufsgespräch, bei dem der Wert eines Produkts in Fachjargon untergeht, dem nur Spezialisten folgen können. Der Ansatz von Cyber Crucible, angetrieben von FortressAI, wurde zunächst um ein einfaches, praktisches Ergebnis für die Kunden herum gestaltet, wobei die zugrunde liegende Technologie entwickelt wurde, um dieses Ergebnis zu unterstützen. Aus diesem Grund entstehen die klarsten Gespräche in der Regel mit Menschen, denen wichtig ist, was ein Sicherheitsvorfall für das Unternehmen bedeutet – nicht nur, wie die Software im Detail funktioniert.

Beispiele für die richtigen Gesprächspartner

Ein IT-Leiter, der mit begrenztem Personal und Budget arbeitet und persönlich für Betriebszeit und Systemzuverlässigkeit verantwortlich ist, erkennt den Nutzen oft schnell, da Ausfallzeiten seinen

täglichen Arbeitsaufwand und seine Leistung beeinträchtigen. Auf der anderen Seite drängt ein CEO oder CFO möglicherweise auf automatisierten Schutz, selbst wenn ein Sicherheitsteam mit den bestehenden Maßnahmen zufrieden ist – einfach weil sie erkennen, dass eine kurze Unterbrechung, manchmal nur eine Stunde lang, einen finanziellen Schaden verursachen kann, von dem man sich erst nach weit über einem Jahr wieder erholt.

Der gemeinsame Nenner

Ob das Gespräch mit einem betriebsorientierten IT-Leiter oder einer finanziell denkenden Führungskraft beginnt – der stärkste Fit für Cyber Crucible ist jeder, der Cybersicherheit aus der Perspektive von Geschäftskontinuität und finanziellem Risiko bewertet, statt allein aus technischer Sicht.

https://player.vimeo.com/video/1046877762

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Warum werden Ransomware-Angriffe von Jahr zu Jahr häufiger?

Kurze Antwort: Ransomware-Angriffe nehmen zu, weil sich Cyberkriminelle Gruppen von unorganisierten, opportunistischen Akteuren zu disziplinierten Operationen entwickelt haben, die Automatisierung nutzen, um viele Opfer effizient anzugreifen und schnell Zahlungen zu erpressen.

Vom chaotischen Start-up zur organisierten Operation

Als Ransomware erstmals zu einer weitverbreiteten Bedrohung wurde, waren viele Angreifer unerfahren. Eine Welle neu arbeitsloser Personen versuchte sich während der Pandemie an Cyberkriminalität, oft mit uneinheitlichen Ergebnissen. Wie in jeder aufstrebenden Branche überlebten diese frühe Marktbereinigung nur die organisierteren und leistungsfähigeren Akteure. Im Laufe der Zeit begannen diese Gruppen weniger wie verstreute Gelegenheitsakteure und mehr wie strukturierte Unternehmen zu agieren, die auf konstante Einnahmen ausgerichtet sind.

Bis 2024 hat sich diese Reife in einer starken Abhängigkeit von Automatisierung niedergeschlagen. Etablierte Ransomware-Operationen setzen mittlerweile automatisierte Tools ein, um weniger erfahrene Teilnehmer in ihre Angriffe einzubinden und dabei effiziente, wiederholbare Prozesse beizubehalten. Dies hat es ihnen ermöglicht, ihre Aktivitäten weit über das hinaus zu skalieren, was ein kleines Team versierter Hacker manuell erreichen könnte.

Die richtige Dosierung des Angriffs für maximale Auszahlung

Ein wesentlicher Teil dieser Entwicklung besteht darin, zu lernen, wie ein Angriff richtig dimensioniert wird. Ist ein Eindringen zu geringfügig, kann ein gut vorbereitetes IT-Team die Systeme einfach wiederherstellen und muss nichts zahlen. Ist ein Angriff zu umfangreich und löscht die gesamte Unternehmensinfrastruktur, bleibt möglicherweise kein tragfähiges Unternehmen mehr übrig, das überhaupt eine Lösegeldzahlung leisten könnte. Moderne Ransomware-Gruppen zielen auf einen Mittelweg ab: genug Störung, um ein Unternehmen zu einer schnellen Zahlung zu

drängen, ohne so viel Schaden anzurichten, dass eine Wiederherstellung oder Verhandlung irrelevant wird.

Warum Automatisierung den Anstieg antreibt

Sobald ein Angriffsprozess automatisiert werden kann, geben sich Cyberkriminelle nicht mehr damit zufrieden, jeweils nur ein Opfer zu verfolgen. Mithilfe von Tools, die künstlicher Intelligenz, maschinellem Lernen und robotergestützter Prozessautomatisierung ähneln, können sie Dutzende oder Hunderte von Organisationen parallel ins Visier nehmen. Viele Opfer entscheiden sich dafür, Vorfälle nicht öffentlich bekannt zu machen, sodass Angreifer einen Erpressungszyklus abschließen und zu neuen Zielen übergehen können. Dieses skalierte, wiederholbare Geschäftsmodell – und nicht eine einzelne neue Technologie – ist der Hauptgrund, warum Ransomware-Angriffe weiter zunehmen.

https://player.vimeo.com/video/1043463561

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Warum setzt Cyber Crucible auf KI anstelle eines menschlichen SOC-Teams, um Ransomware zu stoppen?

Kurze Antwort: Cyber Crucible wurde von Anfang an als vollständig automatisiertes System entwickelt, weil sich Ransomware-Angriffe weitaus schneller entfalten, als es ein menschliches Sicherheitsteam bewältigen könnte, und künstliche Intelligenz die einzige praktikable Möglichkeit ist, Angriffsverhalten in Echtzeit zu modellieren und darauf zu reagieren.

Das Problem mit der Verlässlichkeit auf menschliche Reaktionszeiten

Als Cyber Crucible erstmals entwickelt wurde, um das Jahr 2019, überholte Ransomware bereits die Fähigkeit von Security-Operations-Teams, angemessen zu reagieren. Selbst frühe Ransomware-Varianten konnten die gesamten Systeme einer Organisation innerhalb weniger Minuten lahmlegen. Das ließ keinen realistischen Zeitraum, in dem eine Person die Warnzeichen bemerken, die Situation einschätzen und eingreifen konnte, bevor ernsthafter Schaden entstand. Seitdem haben sich Angriffe nur noch beschleunigt – einigen Berichten zufolge kann das Netzwerk eines mittelständischen Unternehmens innerhalb von nur 90 Sekunden vollständig kompromittiert werden. Bei dieser Geschwindigkeit ist es schlicht nicht realistisch zu erwarten, dass ein menschlicher Analyst einen laufenden Angriff erkennt und stoppt – ganz gleich, wie qualifiziert oder gut besetzt das Team ist.

Warum Verhaltensmodellierung KI erfordert

Um einen derart schnellen Angriff zu stoppen, braucht es mehr als schnelle Alarmmeldungen – es braucht Software, die bösartige Verhaltensmuster erkennt und sofort eine Eindämmungsentscheidung trifft, ohne darauf zu warten, dass eine Person die Daten interpretiert. Eine solch detaillierte Verhaltensmodellierung manuell zu erstellen, die die vielen möglichen

Verlaufsformen eines Angriffs abdeckt, würde weitaus mehr Zeit in Anspruch nehmen, als einem Verteidiger zur Verfügung steht. Künstliche Intelligenz wurde zum notwendigen Werkzeug, um diese Verhaltensmodelle effizient genug zu konstruieren, dass sie direkt in Sicherheitssoftware integriert werden können – so lassen sich Entscheidungen in dem Moment treffen, in dem ein Angriff beginnt, statt erst im Nachhinein.

KI als praktische Notwendigkeit, nicht als Trend

Die Hinwendung zu KI-gestützter Verteidigung folgte keinem Branchentrend – sie war eine praktische Antwort auf ein Zeitproblem, das menschenbasierte Überwachung nicht lösen konnte. Cyber Crucibles' Ansatz spiegelt den Grundsatz wider, das richtige Werkzeug für die richtige Aufgabe einzusetzen: Wenn sich Angriffe auf Sekunden verdichten, muss die Verteidigung im selben Zeitmaßstab agieren – das bedeutet automatisierte, KI-basierte Entscheidungsfindung statt manueller Prüfung.

https://player.vimeo.com/video/1046871333

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Warum erhalten Sicherheitsteams täglich Tausende von Warnmeldungen, und wie können sie damit umgehen?

Kurze Antwort: Die Alarmüberflutung ist nicht über Nacht entstanden – sie hat sich allmählich aufgebaut, da Angreifer zunehmend automatisierter und ausweichender wurden und einst eindeutige Warnzeichen in schwache, mehrdeutige Hinweise verwandelten, die tiefgreifendes Fachwissen zur Interpretation erfordern. Cyber Crucible wurde entwickelt, um diesen Kreislauf zu durchbrechen, indem Erkennung und Reaktion automatisch erfolgen, anstatt menschliche Teams damit zu beauftragen, endlose Signale mit geringer Zuverlässigkeit zu durchforsten.

Wie Alarmmüdigkeit zur Norm wurde

Die Verschlechterung der Sicherheitsalarmierung geschah nicht, weil Anbieter beschlossen hätten, die Last auf die Kunden abzuwälzen. Sie entstand schleichend, da Angreifer ihre Techniken verfeinerten, um schneller zu mutieren und zu automatisieren, als Verteidigungstools ein Ereignis eindeutig als bösartig einstufen konnten. Was früher ein klarer Kompromittierungsindikator war, wurde zu einem schwachen Hinweis, verborgen unter unzähligen anderen schwachen Hinweisen. Diese ordnungsgemäß zu sichten, kostet erfahrene Analysten erhebliche Zeit, und oft stellt sich heraus, dass das Verdächtige nichts weiter als ein fehlerhafter Druckertreiber ist. Gleichzeitig kann eine einzige übersehene Warnmeldung mit geringer Zuverlässigkeit die einzige sichtbare Spur eines ernsthaften, aktiven Eindringens sein.

Warum mehr Warnmeldungen nicht zu besserer Sicherheit führten

Während Erkennungstools versuchten, mit sich weiterentwickelnden Bedrohungen Schritt zu halten, kompensierten sie dies, indem sie alles auch nur geringfügig Ungewöhnliche kennzeichneten. Dies führte zu einer Flut von Warnmeldungen, die formal zwar die Anforderung

erfüllten, Kunden zu warnen, Sicherheitsteams jedoch nicht realistisch in die Lage versetzten, jede einzelne zu untersuchen. Das natürliche Ergebnis ist eines von zwei Szenarien: Teams beginnen, Warnmeldungen mit geringer Zuverlässigkeit zu ignorieren – genau dort, wo sich raffinierte Angreifer bevorzugt verstecken – oder sie werden überwältigt, und wichtige Arbeit bleibt schlicht liegen, unabhängig von Bemühen oder Absicht.

Ein anderer Ausgangspunkt

In der Erkenntnis, dass punktuelle Verbesserungen ein Problem, das auf Jahren angehäufter Komplexität beruht, nicht lösen würden, näherte sich Cyber Crucible dem Thema aus einem völlig anderen Blickwinkel. Anstatt mehr Warnmeldungen zu erzeugen, die von Menschen priorisiert werden müssen, ist unsere FortressAI-Technologie darauf ausgelegt, Ransomware-, Datendiebstahl- und Identitätsdiebstahlbedrohungen in Echtzeit autonom zu erkennen und darauf zu reagieren. Mit modernen Ansätzen wie generativer KI verfolgt Cyber Crucible das Ziel, die Abhängigkeit von manueller Alarmprüfung zu verringern und das zugrunde liegende Ungleichgewicht zwischen der Automatisierung der Angreifer und den Kapazitäten der Verteidiger zu beheben.

https://player.vimeo.com/video/1186492629

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Warum ist Anmeldedaten- und Identitätsdiebstahl gefährlicher als Ransomware-Verschlüsselung?

Kurze Antwort: Ransomware-Verschlüsselung ist der sichtbare, letzte Schritt eines Angriffs, aber der eigentliche Schaden entsteht oft schon früher und bleibt unbemerkt, wenn Angreifer automatisiert Passwörter, Sitzungstoken, Schlüssel und Krypto-Wallets abgreifen. Cyber Crucible konzentriert sich darauf, diese frühe, verborgene Phase zu erkennen und zu stoppen, statt auf den Moment zu warten, in dem Daten gesperrt werden.

Warum Sicherheitstools die größere Bedrohung oft übersehen

Viele Sicherheitsprodukte sind darauf ausgelegt, auf die Verschlüsselung zu reagieren, da dies der Teil eines Angriffs ist, den ein Unternehmen tatsächlich bemerkt – Systeme fallen aus, Dateien werden unlesbar, der Betrieb steht still. Diese sichtbare Störung zieht naturgemäß die meiste Aufmerksamkeit und die meisten Investitionen auf sich. Die Verschlüsselung ist jedoch in der Regel die letzte Handlung eines Angreifers, nicht die erste. Wenn ein Unternehmen die Auswirkungen von Ransomware bemerkt, hat der Angreifer meist bereits den folgenreicheren Teil des Eindringens abgeschlossen: das unbemerkte Sammeln identitätsbezogener Daten wie Anmeldedaten, Authentifizierungstoken, Verschlüsselungsschlüssel und Zugriffe auf digitale Wallets. Diese frühe Phase verursacht keine sichtbare Störung und wird daher tendenziell unterschätzt, obwohl sie Angreifern langfristigen, wiederholbaren Zugriff auf ein Netzwerk verschafft.

Die stille erste Phase eines Angriffs

Moderne Angriffe sind größtenteils automatisiert, und die Phase des Identitätsdiebstahls kann innerhalb weniger Sekunden für eine gesamte Organisation abgeschlossen werden. Da es keine unmittelbare Betriebsunterbrechung gibt, fehlt dieser Phase die Dringlichkeit und Sichtbarkeit, die eine Ransomware-Verschlüsselung erzeugt, wodurch sie leicht übersehen wird. Dennoch ist es genau diese Phase, die Angreifern die Möglichkeit gibt, jederzeit zurückzukehren und weiteren

Schaden anzurichten, einschließlich der späteren Bereitstellung von Ransomware.

Wie Cyber Crucible diese Lücke schließt

Cyber Crucible ist darauf ausgelegt, unbefugten Zugriff auf Identitätsdaten in dem Moment zu erkennen, in dem er geschieht, statt auf den Beginn der Verschlüsselung zu warten. Da diese Aktivität so schnell und unauffällig erfolgt, wurde erheblicher technischer Aufwand betrieben, um die Erkennung sowohl schnell als auch präzise zu gestalten – um zu identifizieren, wer auf sensible Identitätsdaten zugreift, ohne den alltäglichen Geschäftsbetrieb oder die Benutzeraktivität zu verlangsamen.

https://player.vimeo.com/video/1141670023

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Warum ist Ransomware so schwer zu stoppen und wiederherzustellen?

Kurze Antwort: Ransomware hat sich von einem einfachen Hacking-Trick zu einer ausgereiften, geschäftsähnlich organisierten kriminellen Operation entwickelt, die mehrschichtige Verschlüsselung und verschwindende Schlüssel nutzt, um eine Wiederherstellung ohne Zahlung nahezu unmöglich zu machen. Wer versteht, wie die Verschlüsselung und die Schlüsselverwaltung tatsächlich funktionieren, erkennt, warum Backups, Beschlagnahmungen durch Strafverfolgungsbehörden und schnelle Lösungen oft nicht ausreichen.

Wie sich Ransomware von einem Datenschutzverstoß unterscheidet

Bei einem Datenschutzverstoß geht es darum, Informationen unauffällig zu stehlen und später zu verkaufen, während Ransomware-Akteure ein anderes Ziel verfolgen: so lange unbemerkt im Netzwerk zu bleiben, bis maximaler Schaden angerichtet werden kann, und sich dann zu offenbaren. Sobald der Schaden angerichtet ist, spielt es für sie keine Rolle mehr, sich zu verstecken. Diese Operation wird zunehmend automatisiert und wie ein Unternehmen betrieben, komplett mit Zahlungsabwicklung und einem „Kundenservice" für Entschlüsselung, da Angreifer eine zuverlässige Methode benötigen, um im großen Maßstab Geld einzutreiben.

Der Verschlüsselungstrick hinter dem Angriff

Ransomware setzt in der Regel auf zwei zusammenwirkende Verschlüsselungsarten. Eine schnelle symmetrische Verschlüsselung (wie AES) sperrt die eigentlichen Dateien, während eine langsamere asymmetrische Verschlüsselung – dieselbe Methode, die auch zur Absicherung von Webverkehr verwendet wird – den symmetrischen Schlüssel selbst schützt. Dies ist eine etablierte kryptografische Technik, die aus legitimen Sicherheitssystemen entlehnt wurde. Bei Ransomware bedeutet dies jedoch, dass selbst wenn der Schlüssel einer einzelnen Datei irgendwie wiederhergestellt werden könnte, Angreifer zusätzliche Komplexität eingebaut haben, sodass die Entschlüsselung einer Datei oft von der Erzeugung eines neuen Schlüssels für die nächste abhängt

– wodurch Abkürzungen weitaus schwieriger sind, als es zunächst klingt.

Warum die Wiederherstellungsoptionen immer schwächer werden

Frühe Ransomware verwendete einen einzigen Schlüssel für viele Opfer, was es Verteidigern gelegentlich ermöglichte, ein Entschlüsselungstool zu extrahieren und zu verbreiten. Angreifer reagierten darauf, indem sie einzigartige, einmalig verwendete Schlüssel erzeugten, die niemals an einem wiederauffindbaren Ort gespeichert werden. Dies eliminiert die Option der qu

https://player.vimeo.com/video/1065143398

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Warum kann herkömmliche Antivirensoftware Zero-Day- und dateilose Ransomware-Angriffe nicht stoppen?

Kurze Antwort: Signaturbasierte Sicherheitstools verlassen sich auf das Erkennen bekannter Angriffsmuster, aber moderne Angreifer testen ihre Werkzeuge gezielt gegen genau diese Abwehrmechanismen, bevor sie sie einsetzen, und vermeiden zunehmend, überhaupt erkennbare Dateien abzulegen. Diese Kombination aus mutierten, nicht erkannten Bedrohungen und rein speicherbasierten Techniken hat traditionelle Erkennungsmethoden deutlich unzuverlässiger gemacht.

Das Problem beim Vertrauen auf bekannte Signaturen

Zero-Day-Angriffe sind per Definition so neu oder verändert, dass sie außerhalb dessen liegen, was bestehende Sicherheitstools bereits erkennen. Hersteller versprechen seit Langem Verbesserungen bei der Erkennung solcher Bedrohungen, doch Angreifer haben einen inhärenten Vorteil: Sie haben Zugang zu denselben kommerziellen Sicherheitsprodukten, die auch von Verteidigern eingesetzt werden. Vor dem Start einer Kampagne testen Angreifer ihre Malware routinemäßig gegen gängige Erkennungstools und verfeinern sie so lange, bis sie unbemerkt bleibt. Dadurch wird Erkennung zu einem sich ständig verändernden Ziel statt zu einer festen Verteidigungslinie.

Dateilose Techniken untergraben das Whitelisting

Angreifer verzichten zunehmend darauf, offensichtlich bösartige ausführbare Dateien auf einem System abzulegen. Stattdessen kapern sie legitime, vertrauenswürdige Anwendungen, die bereits von Whitelisting-Tools für Anwendungen genehmigt wurden, und führen bösartige Aktivitäten über Prozesse aus, die von der Sicherheitssoftware als sicher eingestuft werden. Wird dieser dateilose Ansatz mit sich schnell verändertem Code kombiniert, können Angriffe in einem sehr kurzen

Zeitfenster abgeschlossen sein – manchmal innerhalb von nur einer halben Stunde –, lange bevor ein menschliches Incident-Response-Team realistisch eine Untersuchung durchführen könnte.

Angreifer verwischen ihre eigenen Spuren

In vielen Fällen löschen Angreifer, da der Angriff im Arbeitsspeicher und nicht auf der Festplatte stattfindet, Protokolle, Beweise und sogar Sicherheitssensoren, bevor sie ihre Operation abschließen. Dies ähnelt einem Einbrecher, der Überwachungskameras und Alarmanlagen deaktiviert, bevor er eine Straftat begeht: Wenn jemand nach Beweisen sucht, ist die nützlichste Sichtbarkeit bereits zerstört. Diese Mischung aus unvorhersehbaren Angriffsmethoden und selbstlöschenden Beweisen ist der Grund, warum Cyber Crucible erhebliche Anstrengungen in die Entwicklung eines automatisierten, skalierbaren Ansatzes investiert hat – einen Ansatz, der darauf ausgelegt ist, die entscheidenden Daten zu erfassen, die für präzise Entscheidungen notwendig sind, bevor Angreifer die Spur verwischen können, statt sich auf die nachträgliche Erkennung von Bedrohungen zu verlassen.

https://player.vimeo.com/video/1164197533

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Werden Hacker 2025 mehr KI bei Ransomware-Angriffen einsetzen?

Kurze Antwort: Ja. Es wird erwartet, dass Angreifer ihren Einsatz von künstlicher Intelligenz, insbesondere von großen Sprachmodellen, weiter ausbauen, um vertrauenswürdige Personen zu imitieren und Opfer dazu zu bringen, Zugriff oder Vertrauen zu gewähren.

Warum KI bei Hackern so beliebt geworden ist

Suchergebnisse, Nachrichtenfeeds und alltägliche Gespräche sind mittlerweile von KI-Bezügen durchdrungen, und dieselbe Begeisterung hat auch bei Cyberkriminellen Einzug gehalten. Wenn die meisten Menschen von KI sprechen, meinen sie damit in der Regel große Sprachmodelle wie jene, die hinter ChatGPT und ähnlichen Tools stehen und die menschliche Kommunikation überzeugend nachahmen können. Angreifer haben erkannt, dass diese Fähigkeit für Social Engineering äußerst nützlich ist. Anstatt sich auf generische Phishing-E-Mails zu verlassen, können sie Nachrichten, Stimmen oder Gespräche erzeugen, die einem echten Kollegen, Lieferanten oder einer Autoritätsperson stark ähneln, wodurch es erheblich leichter wird, das Vertrauen eines Ziels zu gewinnen, bevor zugeschlagen wird.

Mit ausgefeilteren Imitationstaktiken ist zu rechnen

Der Trend für 2025 besteht nicht darin, dass KI-gestützte Angriffe grundlegend neu sind, sondern dass sie ausgefeilter und geschäftsmäßiger werden. So wie seriöse Unternehmen KI-gestützte Vertriebsagenten und automatisierte Outreach-Tools einführen, verfeinern auch Angreifer ihre eigenen KI-gestützten Imitationstechniken. Das bedeutet überzeugendere Nachrichten, die Vorgesetzte, Kollegen oder vertrauenswürdige Partner nachahmen, allesamt darauf ausgelegt, die Arbeitsbeziehungen auszunutzen, auf die sich Menschen tagtäglich verlassen. Die Gefahr besteht darin, dass ein Gespräch, das sich persönlich und legitim anfühlt, in Wirklichkeit von einem hochentwickelten KI-System stammen könnte, das darauf ausgelegt ist zu manipulieren, nicht zu helfen.

Was das für die Verteidigung bedeutet

Da diese Imitationstaktiken ausgereifter werden, sollten Organisationen davon ausgehen, dass vertrauensbasierte Angriffe allein durch Intuition schwerer zu erkennen sein werden. Die Überprüfung von Anfragen über unabhängige Kanäle, anstatt einer Nachricht oder einem Anruf blind zu vertrauen, wird immer wichtiger. Da diese Angriffe darauf ausgelegt sind, das menschliche Urteilsvermögen zu umgehen, bietet das Vorhandensein automatisierter Erkennungs- und Reaktionsfähigkeiten, wie sie in Cyber Crucible's FortressAI integriert sind, eine zusätzliche Schutzebene, wenn Social Engineering die Abwehrmechanismen einer Person erfolgreich überwindet.

https://player.vimeo.com/video/1046827321

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Senkt der Einsatz von Cyber Crucible das gesamte Sicherheitsbudget eines Unternehmens?

Kurze Antwort: Cyber Crucible ist nicht darauf ausgelegt, Ihr Sicherheitsbudget unmittelbar zu verringern; stattdessen setzt es Zeit- und Personalressourcen frei, die zuvor für manuelles Monitoring und das Nachverfolgen von Fehlalarmen aufgewendet wurden, sodass Sie diese Kapazitäten auf Sicherheitslücken umlenken können, die Sie sich zuvor nicht leisten konnten.

Warum Automatisierung nicht automatisch Einsparungen bedeutet

Es liegt nahe anzunehmen, dass das Ersetzen manueller Sicherheitsprozesse durch ein automatisiertes Tool wie Cyber Crucible sofort Kosten senken würde. In der Praxis läuft es meist anders. Viele Sicherheitsprogramme stützen sich auf einen Flickenteppich aus Tools, die ständige Anpassung, Überwachung und manuelle Überprüfung von Warnmeldungen erfordern. Wenn Sie Automatisierung einführen, die diesen manuellen Aufwand reduziert, liegt der Wert nicht primär in einer niedrigeren Rechnung – er liegt in der zurückgewonnenen Zeit und Aufmerksamkeit, die Ihr Team gewinnt. Diese zurückgewonnene Kapazität wird tendenziell in andere Sicherheitsprioritäten reinvestiert, anstatt als reine Einsparung verbucht zu werden.

Wo sich der eigentliche Wert zeigt

Die meisten IT- und Sicherheitsverantwortlichen wissen bereits, dass ihre Aufgabenliste die verfügbaren Mitarbeiter und Tools übersteigt. Begrenzte Personalausstattung und technische Einschränkungen führen dazu, dass viele bekannte Risiken schlicht unbearbeitet bleiben. Indem Cyber Crucible den manuellen Aufwand reduziert, der für das Sortieren von Fehlalarmen und die Betreuung von Erkennungssystemen aufgewendet wird, verschafft es Teams den nötigen Freiraum, um sich endlich diesen vernachlässigten Problemen zu widmen. In diesem Sinne geht es beim Nutzen um Budgetflexibilität und -kontrolle, nicht zwangsläufig um ein kleineres Budget. Verantwortliche können selbst entscheiden, ob sie Ausgaben senken, umverteilen oder die

Abdeckung auf Bereiche ausweiten möchten, die zuvor aufgrund begrenzter Ressourcen unerreichbar waren.

Was Cyber Crucible leisten kann – und was nicht

Cyber Crucible kann nicht jede Budgetbeschränkung lösen, mit der ein Unternehmen konfrontiert ist. Was es leisten kann, ist Sicherheitsverantwortlichen mehr Kontrolle darüber zu geben, wie sich ihre Ausgaben in tatsächlichen Schutz übersetzen. Indem manuelles, arbeitsintensives Monitoring durch automatisierte Abwehr ersetzt wird, erhalten Teams die Möglichkeit, ihr bestehendes Budget darauf auszurichten, die Gesamtwirksamkeit des Sicherheitsprogramms zu stärken, das sie aufgebaut haben – anstatt es für die Pflege von Tools auszugeben, die ständige Aufmerksamkeit erfordern.

https://player.vimeo.com/video/1043470826

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch