MANDIANT
NOW PART OF Google Cloud

Eine Momentaufnahme der Cybersicherheitslage – Ausgabe 4

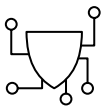
„Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage" bietet einen Einblick in zunehmend relevante Themen zur Cyberabwehr und liefert dazu passende Erkenntnisse aus Mandiant-Einsätzen und andere Praxisbeispiele. In dieser Ausgabe werden diverse Themen abgedeckt, unter anderem die Integration von Sicherheitsfunktionen in KI-Systeme, Best Practices für die effektive Krisenkommunikation bei einem Sicherheitsvorfall und die Abwehr der neuesten Bedrohungen für IoT- und Edge-Netzwerkinfrastrukturen.

Schutz von KI-Systemen

Da künstliche Intelligenz (KI) inzwischen in immer mehr Bereichen eingesetzt wird, müssen auch neue Strategien für ein effektives Risikomanagement entwickelt werden. Nach Ansicht von Mandiant sollten Sicherheitsfunktionen nativ in KI-Systeme integriert werden, um ein Flickwerk aus nachträglich hinzugefügten Sicherheitslösungen zu vermeiden, wie wir es bei Netzwerk- und DevOps-Strategien sehen. Um Unternehmen dabei zu unterstützen, hat Google vor Kurzem das Secure AI Framework (SAIF) vorgestellt, ein Konzept zum Schutz von KI-Systemen.

SAIF beinhaltet praktische Empfehlungen zu den größten Sicherheitsbedenken (z. B. Zugriffsmanagement, Netzwerk- und Endpunktsicherheit sowie Angriffe auf Lieferketten), Risikomanagement für KI/ML-Modelle (z. B. Transparenz und Zuständigkeit bei Modellen, Verunreinigung von Daten (Data Poisoning) und Datenherkunft), Datenschutz und Compliance (z. B. Schutz und Nutzung sensibler Daten) sowie Mitarbeiter und Unternehmen (z. B. Fachkräftemangel, Governance und Berichterstattung an Vorstände).

Die sechs Grundprinzipien von SAIF sollen Unternehmen helfen, KI-Systeme sicher und verantwortungsvoll zu erstellen und bereitzustellen.

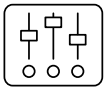


Implementierung effektiver Sicherheitsmaßnahmen für das gesamte KI-System

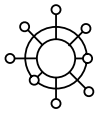
Einbindung von KI in die Bedrohungserkennung und Bedrohungsabwehr des Unternehmens

Automatisierung der Abwehrmaßnahmen zum Schutz vor aktuellen und neuen Bedrohungen

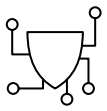
Vereinheitlichung der Kontrollfunktionen auf Plattformebene zur Durchsetzung konsistenter Sicherheitsmaßnahmen im gesamten Unternehmen



Anpassung der Sicherheitsfunktionen zur Optimierung der Abwehrmaßnahmen und Erstellung effektiverer Feedbackschleifen für KI-Implementierungen



Betrachtung der Risiken für KI-Systeme im Kontext der relevanten Unternehmensprozesse



Implementierung effektiver Sicherheitsmaßnahmen für das gesamte KI-System

- **Prüfen Sie, welche vorhandenen Sicherheitsmaßnahmen für KI-Systeme übernommen werden können.**

  Vorhandene Sicherheitsmaßnahmen können auf unterschiedliche Weise für KI-Systeme übernommen werden. Datensicherheitskontrollen können beispielsweise die Daten schützen, mit denen KI-Systeme trainiert und betrieben werden. Anwendungssicherheitskontrollen können wiederum die Software schützen, in die KI-Systeme implementiert wurden. Mit Infrastruktursicherheitskontrollen lassen sich die zugrunde liegenden Infrastrukturen absichern, auf denen KI-Systeme aufsetzen, und Prozesssicherheitskontrollen sorgen dafür, dass der Betrieb der KI-Systeme geschützt wird.

  Welche Sicherheitsmaßnahmen benötigt werden, hängt sowohl von der KI-Nutzung als auch von den spezifischen KI-Systemen und Umgebungen ab.

- **Ermitteln Sie mithilfe der verfügbaren Frameworks, welche herkömmlichen Sicherheitsmaßnahmen für KI-Bedrohungen und -Risiken relevant sind.**

  Herkömmliche Sicherheitsmaßnahmen können auch vor KI-Bedrohungen und -Risiken schützen, sie müssen unter Umständen nur angepasst oder ergänzt werden, um KI-spezifische Bereiche abzudecken. Mithilfe von Datenverschlüsselung können beispielsweise KI-Systeme vor nicht autorisiertem Zugriff geschützt werden, wenn die Schlüssel nur für bestimmte Rollen freigegeben werden. Außerdem lassen sich damit Datendiebstahl und Manipulationen an den KI-Modellen oder den zugrunde liegenden Daten verhindern.

- **Stellen Sie fest, welche Sicherheitsfunktionen hinzugefügt werden müssen, um beispielsweise KI-spezifische Bedrohungen oder Vorgaben abzudecken.**

  Besprechen Sie im gesamten Team, ob die aktuellen Funktionen die KI-Anwendungsfälle abdecken, prüfen Sie, ob diese Maßnahmen für die jeweiligen Anwendungszwecke geeignet sind, und planen Sie dann entsprechende Lösungen für die aufgedeckten Lücken. Ermitteln Sie anschließend die Effektivität dieser Maßnahmen: Werden die Risiken damit minimiert? Sind sie für die angestrebte KI-Nutzung hilfreich?

- **Treffen Sie entsprechende Vorbereitungen, um Lieferkettenressourcen, Code und Trainingsdaten zu speichern und nachzuverfolgen.**

  Unternehmen, die KI einsetzen möchten, müssen auch entsprechende Maßnahmen ergreifen, um Lieferkettenressourcen, Code und Trainingsdaten zu speichern und nachzuverfolgen. Dazu gehören unter anderem die Identifizierung, die Kategorisierung und der Schutz aller Ressourcen und die Überwachung auf nicht autorisierte Zugriffe und die nicht genehmigte Nutzung. Mit diesen Schritten können Unternehmen ihre KI-Systeme besser vor Angriffen schützen.

- **Sorgen Sie dafür, dass Ihre Prozesse für die Daten-Governance und das Lebenszyklusmanagement skalierbar und an die KI anpassbar sind.**

  Je nachdem, wie Sie Daten-Governance definieren, sind dabei bis zu sechs wichtige Punkte zu beachten:

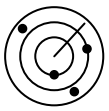
  - Datenqualität
  - Datensicherheit
  - Datenarchitektur
  - Metadaten
  - Datenlebenszyklus
  - Datenspeicherung

  Governance für KI-Daten wird immer wichtiger. So haben beispielsweise Trainingsdaten einen entscheidenden Einfluss auf die Effektivität von KI-Modellen. Richten Sie ein effektives Lebenszyklusmanagement für Datensätze ein und achten Sie dabei gezielt auf die Sicherheit – die gewählten Sicherheitsmaßnahmen sollten den gesamten Lebenszyklus von der Erstellung der Daten bis zur endgültigen Löschung abdecken. Auch die Datenherkunft spielt eine wichtige Rolle, insbesondere in Bezug auf Datenschutz und geistiges Eigentum. Wenn Sie wissen, wer die Daten erstellt hat, woher sie stammen und woraus sich die Datensätze zusammensetzen, können Sie Fragen zu den oben aufgeführten Punkten viel einfacher beantworten.

  Wenn immer mehr Unternehmen KI nutzen, wird eine schnelle Skalierung in diesen Bereichen zum entscheidenden Wettbewerbsvorteil. Daher sollten Sie im Vorfeld unbedingt Ihre Daten-Governance-Strategie mit einem Team besprechen, dessen Mitglieder aus unterschiedlichen Unternehmensbereichen stammen, und die Maßnahmen gegebenenfalls an die neuen KI-Entwicklungen anpassen.

- **Achten Sie auf die Bindung und das Training.**

  Dieser Punkt betrifft nicht die Daten, sondern Ihre Mitarbeiter. Viele Unternehmen benötigen mehrere Jahre, um Fachkräfte mit den notwendigen Kompetenzen in den Bereichen Sicherheit, Datenschutz und Compliance zu finden. Eine gute Mitarbeiterbindung trägt daher zum Unternehmenserfolg bei, da es einfacher und schneller ist, den vorhandenen Spezialisten die erforderlichen KI-Kenntnisse zu vermitteln, als neue Experten auf dem Arbeitsmarkt zu finden. Außerdem verfügen Ihre Mitarbeiter bereits über wichtige Unternehmenskenntnisse, die Außenstehenden fehlen.



Einbindung von KI in die Bedrohungserkennung und Bedrohungsabwehr des Unternehmens

- **Informieren Sie sich über die Bedrohungen für die KI-Anwendungsfälle, die verwendeten KI-Arten und Ähnliches.**

  Wenn Unternehmen KI-Systeme einsetzen, müssen sie auch die für ihre Anwendungsfälle relevanten Bedrohungen kennen. Sie müssen beispielsweise wissen, welche Arten von KI sie nutzen, mit welchen Daten die KI-Modelle trainiert werden und welche Gefahren bei einem Sicherheitsvorfall drohen. Mit diesen Schritten können Unternehmen ihre KI-Systeme besser vor Angriffen schützen.

- **Bereiten Sie Abwehrmaßnahmen für Angriffe auf KI-Systeme und Lösungen für Probleme in der KI-Ausgabe vor.**

  Unternehmen müssen eine Strategie zur Erkennung und Behebung von Sicherheitsvorfällen entwickeln und das Risiko minimieren, dass KI-Systeme schädliche oder verzerrte Ergebnisse ausgeben. Dadurch schützen sie sowohl ihre KI-Systeme als auch die Benutzer vor potenziellen Gefahren.

- **Konzentrieren Sie sich bei generativer KI besonders auf die Ausgabe und sorgen Sie dafür, dass Sie Richtlinien für den Inhaltsschutz durchsetzen können.**

  Mithilfe von generativer KI lassen sich zahlreiche unterschiedliche Inhalte erstellen – von Texten über Bilder bis zu Videos. Doch dadurch steigt auch die Gefahr des Missbrauchs. So könnten mit generativer KI beispielsweise schädliche Inhalte wie Hassreden oder Abbildungen von Gewalt erstellt werden. Um diese Risiken zu minimieren, müssen Unternehmen sicherstellen, dass sie Richtlinien für den Inhaltsschutz durchsetzen können.

- **Passen Sie die Missbrauchsrichtlinie und die Incident-Response-Prozesse an KI-spezifische Probleme an, zum Beispiel die Erstellung schädlicher Inhalte und Verstöße gegen den Datenschutz.**

  Mit der zunehmenden Verbreitung und steigenden Komplexität der KI-Systeme müssen Unternehmen auch ihre Richtlinien und Incident-Response-Prozesse anpassen, um den Missbrauch der Tools zu verhindern und KI-spezifische Probleme abzudecken. Dazu gehören unter anderem die Erstellung schädlicher Inhalte, Datenschutzverstöße und KI-Bias sowie der allgemeine Missbrauch der Systeme.

Automatisierung der Abwehrmaßnahmen zum Schutz vor aktuellen und neuen Bedrohungen

- **Erstellen Sie eine Liste der KI-Sicherheitsfunktionen für den Schutz von KI-Systemen, Pipelines für Trainingsdaten und andere KI-Bereiche.**

  KI-Sicherheitstechnologien können KI-Systeme vor diversen Bedrohungen schützen, wie beispielsweise Datenlecks, KI-Bias und der Erstellung schädlicher Inhalte. Dazu gehören auch herkömmliche Funktionen wie Datenverschlüsselung, Zugriffskontrollen und Auditprozesse, die durch KI und neuere Technologien ergänzt werden, um Trainingsdaten und -modelle zu schützen.

- **Nutzen Sie KI-Funktionen zur Abwehr von KI-Bedrohungen, aber binden Sie für wichtige Entscheidungen auch Ihre Mitarbeiter ein.**

  Mithilfe von KI-Funktionen lassen sich KI-Bedrohungen wie Datenlecks, Erstellung schädlicher Inhalte und KI-Bias aufdecken und beheben. Allerdings müssen Mitarbeiter in die Prozesse eingebunden werden, um gegebenenfalls wichtige Entscheidungen treffen zu können. Dazu gehören unter anderem die Feststellung, ob es sich tatsächlich um eine Bedrohung handelt, und die Wahl der Abwehrmaßnahmen. Das ist wichtig, da in KI-Systemen Bias oder Fehler auftreten können. Wenn aber Mitarbeiter die Kontrolle und Entscheidungsgewalt behalten, kann ein ethischer und verantwortungsbewusster Einsatz der KI-Systeme sichergestellt werden.

- **Nutzen Sie KI, um zeitaufwendige Aufgaben zu automatisieren, den Arbeitsaufwand zu reduzieren und die Bedrohungsabwehr zu beschleunigen.**

  Es mag zwar banal erscheinen, aber wenn mit KI zeitaufwendige Aufgaben beschleunigt werden, lassen sich auch schneller die angestrebten Ziele erreichen. Zum Beispiel ist das Reverse-Engineering von Malware-Binärcode in einigen Fällen äußerst zeitaufwendig. Ein KI-System kann jedoch den relevanten Code in kürzester Zeit überprüfen und einem Analysten die erforderlichen Informationen bereitstellen. Daraufhin fordert der Analyst das System auf, eine YARA-Regel zu erstellen, die nach diesen Informationen sucht. Wie dieses Beispiel zeigt, eignet sich KI, um den Arbeitsaufwand zu reduzieren und schnellere wichtige Informationen für den Schutz des Unternehmens bereitzustellen.

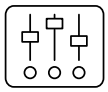
Vereinheitlichung der Kontrollfunktionen auf Plattformebene zur Durchsetzung konsistenter Sicherheitsmaßnahmen im gesamten Unternehmen

- **Prüfen Sie die Nutzung von KI und den Lebenszyklus KI-basierter Anwendungen.**

  Wie schon in Schritt 1 erwähnt, ist es wichtig, die Einsatzbereiche von KI zu kennen. Mit der zunehmenden KI-Nutzung in Ihrem Unternehmen sollten Sie Prozesse für die regelmäßige Überprüfung der Anwendungsfälle implementieren, um Sicherheitsrisiken zu erkennen und zu entschärfen. Dazu sollten Sie feststellen, welche Arten von KI-Modellen und -Anwendungen verwendet, welche Daten für das Training und den Betrieb der KI-Modelle genutzt, welche Sicherheitsmaßnahmen zum Schutz der KI-Modelle und -Anwendungen ergriffen und welche Prozesse für die Überwachung und Abwehr von KI-Sicherheitsvorfällen eingerichtet wurden. Prüfen Sie auch, ob allen Mitarbeitern Schulungen zur Sensibilisierung in Bezug auf KI-Sicherheitsrisiken angeboten werden.

- **Nutzen Sie einheitliche Tools und Frameworks, um fragmentierte Sicherheitsmaßnahmen zu vermeiden.**

  Wenn Sie die beschriebenen Prozesse implementiert haben, können Sie besser nachvollziehen, welche Tools, Sicherheitsmaßnahmen und Frameworks bereits vorhanden sind. Außerdem sollten Sie überprüfen, ob es mehrere Sicherheits- und Compliance-Frameworks gibt, die sich eventuell sogar überschneiden. Durch eine zu starke Fragmentierung steigt die Komplexität und es entstehen Überschneidungen, die wiederum höhere Kosten und ineffiziente Prozesse nach sich ziehen. Wenn Sie die Frameworks und Sicherheitsmaßnahmen vereinheitlichen und wissen, ob sie für Ihre KI-Anwendungsfälle notwendig sind, verringern Sie die Fragmentierung und können die jeweils besten Lösungen nutzen, um die Risiken zu minimieren. Dies bezieht sich vorrangig auf vorhandene Frameworks und Standards, aber dasselbe Prinzip (die Nutzung möglichst weniger Lösungen) gilt auch für neue KI-Frameworks und -Vorgaben.



Anpassung der Sicherheitsfunktionen zur Optimierung der Abwehrmaßnahmen und Erstellung effektiverer Feedbackschleifen für KI-Implementierungen

- **Führen Sie Red-Team-Übungen durch, um den Schutz KI-gestützter Produkte und Funktionen zu verbessern.**

  Bei Red-Team-Übungen wird die Effektivität der Sicherheitsmaßnahmen überprüft. Dazu versucht ein Team aus ethischen Hackern, Schwachstellen in den Systemen und Anwendungen eines Unternehmens auszunutzen. Mithilfe der gewonnenen Erkenntnisse kann das jeweilige Unternehmen dann Sicherheitsrisiken in den KI-Systemen identifizieren und beheben, bevor diese von Angreifern ausgenutzt werden.

- **Berücksichtigen Sie auch neuartige Angriffsmethoden, zum Beispiel die Einschleusung von Prompts, die Verunreinigung von Daten und Umgehungstaktiken.**

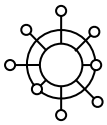
  Mit diesen Angriffsmethoden können Schwachstellen in KI-Systemen ausgenutzt werden, um beispielsweise sensible Daten zu stehlen, falsche Prognosen abzugeben oder den Betrieb zu stören. Wenn Unternehmen stets über die aktuellen Methoden informiert sind, können sie diese Risiken besser minimieren.

- **Nutzen Sie maschinelle Lernverfahren, um die Bedrohungserkennung zu präzisieren und zu beschleunigen.**

  Zwar spielt der Schutz der KI eine wichtige Rolle, aber KI kann auch die Sicherheitsbemühungen in Unternehmen unterstützen, beispielsweise durch KI-gestützte Funktionen für die Bedrohungserkennung und Bedrohungsabwehr. Gleichzeitig müssen aber auch die Mitarbeiter eingebunden werden, damit sie den Überblick über die relevanten KI-Systeme, -Prozesse und -Entscheidungen behalten. Im Laufe der Zeit können die gewonnenen Erkenntnisse in die Prozesse für das kontinuierliche Lernen einfließen, um die grundlegenden KI-Sicherheitsfunktionen zu verbessern, die Trainingsdaten zu aktualisieren, die Datensätze für die Basismodelle zu optimieren und die verwendeten ML-Modelle zu erweitern. Das hilft Unternehmen, auch auf neue Bedrohungen angemessen zu reagieren. Durch das kontinuierliche Lernen werden außerdem eine größere Genauigkeit erreicht, Latenzen reduziert und die Effizienz der Sicherheitsmaßnahmen verbessert.

- **Richten Sie eine Feedbackschleife ein.**

  Um die Vorteile der drei oben genannten Strategien optimal auszuschöpfen, benötigen Sie eine Feedbackschleife. Wenn das Red Team beispielsweise eine Lücke findet, über die das KI-System ausgenutzt werden könnte, sollten Sie sich nicht allein auf die Fehlerbehebung beschränken, sondern mithilfe dieser Informationen auch die Abwehrmaßnahmen verbessern. Gleiches gilt für den Fall, dass Ihre Mitarbeiter einen neuen Angriffsvektor identifizieren: Diese Informationen sollten dann im Rahmen des kontinuierlichen Lernens in die Trainingsdaten einfließen. Damit das Feedback optimal genutzt wird, empfiehlt es sich, verschiedene Einbindungsmethoden zu berücksichtigen und festzustellen, wie schnell die Informationen für die Sicherheitsfunktionen übernommen werden können.



Betrachtung der Risiken für KI-Systeme im Kontext der relevanten Unternehmensprozesse

- **Erstellen Sie ein Framework für das Risikomanagement der Modelle und ein Team aus Spezialisten, die sich mit KI-Risiken auskennen.**

  Unternehmen sollten einen Prozess für die Identifizierung, Einschätzung und Behebung von Risiken in Zusammenhang mit KI-Modellen einrichten. Das verantwortliche Team sollte aus Experten für KI, Sicherheit und Risikomanagement bestehen.

- **Erstellen Sie eine Liste der KI-Modelle und ihrer Risikoprofile basierend auf den unterschiedlichen Anwendungsfällen und dem Prinzip der gemeinsamen Verantwortung, wenn Sie Lösungen und Dienste von Dritten nutzen.**

  Unternehmen sollten eine Liste aller KI-Modelle erstellen und ihr Risikoprofil unter Berücksichtigung der jeweiligen Anwendungsfälle, der Vertraulichkeit der Daten und dem Prinzip der gemeinsamen Verantwortung bei der Nutzung von Drittanbieterlösungen und -diensten festlegen. Dazu müssen alle verwendeten KI-Modelle identifiziert, die jeweiligen Risiken ermittelt und Sicherheitsfunktionen implementiert werden, um diese Risiken zu minimieren und die Aufgaben und Zuständigkeiten eindeutig zuzuweisen.

- **Implementieren Sie Richtlinien, Protokolle und Sicherheitsfunktionen für Datenschutz, Cyberrisiken und Risiken von Drittanbieterlösungen für den gesamten Lebenszyklus der ML-Modelle, um die Entwicklung, Implementierung, Überwachung und Validierung der Modelle zu unterstützen.**

  Unternehmen sollten Richtlinien, Protokolle und Sicherheitsfunktionen für Datenschutz, Cyberrisiken und Risiken von Drittanbieterlösungen für den gesamten Lebenszyklus der ML-Modelle implementieren, um die Entwicklung, Implementierung, Überwachung und Validierung der Modelle zu unterstützen. Dazu müssen Richtlinien, Protokolle und Sicherheitsfunktionen entwickelt und implementiert werden, die die spezifischen Risiken in jeder Phase des Lebenszyklus eines ML-Modells abdecken. Berücksichtigen Sie dabei auch das vierte Prinzip des Frameworks, um eine Fragmentierung zu vermeiden.

- **Führen Sie eine Risikobewertung zur Nutzung von KI in Ihrem Unternehmen durch.**

  Unternehmen sollten die Risiken in Bezug auf die KI-Nutzung identifizieren und bewerten und dann entsprechende Sicherheitsmaßnahmen zur Risikominimierung implementieren. Außerdem sollten sie Prozesse einrichten, um die Effektivität der Sicherheitskontrollen zu überwachen und zu validieren. Dazu gehören auch die Nachvollziehbarkeit der Ausgabe der Modelle und die Überwachung auf Abweichungen. Wie bereits in den ersten beiden Punkten angesprochen, ist es wichtig, ein Team aus unterschiedlichen Experten zusammenzustellen, die sich mit den relevanten Anwendungsfällen auskennen. Unternehmen können durchaus vorhandene Frameworks für die Risikobewertung nutzen, müssen ihre Strategien aber vermutlich anpassen oder ergänzen, um neue Frameworks für das Management von KI-Risiken zu berücksichtigen.

- **Berücksichtigen Sie bei der KI-Sicherheit das Prinzip der gemeinsamen Verantwortung, also unterschiedliche Zuständigkeiten für die Entwicklung von KI-Systemen, die Bereitstellung von Modellen eines Anbieters, die Optimierung von Modellen und die Nutzung von Standardlösungen.**

  Die Sicherheit von KI-Systemen liegt in der gemeinsamen Verantwortung von Entwicklern, Betreibern und Benutzern. Der jeweilige Zuständigkeitsbereich der Beteiligten hängt von ihrer Rolle bei der Entwicklung und Bereitstellung der KI-Systeme ab. So müssen beispielsweise Entwickler dafür sorgen, dass die Sicherheit der KI-Systeme schon bei der Entwicklung berücksichtigt wird („Secure by Design"). Dazu gehören die sichere Programmierung, die Nutzung bereinigter Daten für das Training der Modelle und die Implementierung von Sicherheitsfunktionen zum Schutz der KI-Systeme vor Angriffen.

- **Legen Sie die Risikotoleranz für jeden KI-Anwendungsfall fest.**

  Dazu müssen Sie die Risiken für jeden einzelnen KI-Anwendungsfall kennen und angemessene Sicherheitsmaßnahmen implementieren. KI-Systeme, die Benutzern bei wichtigen Entscheidungen helfen, zum Beispiel in Gesundheits- oder Finanzfragen, müssen deutlich besser gesichert werden als KI-Systeme, die für allgemeinere Aufgaben wie Marketing oder Kundendienst eingesetzt werden.

Fazit

KI birgt ein enormes Potenzial und viele Unternehmen sehen in dieser neuen Technologie eine Möglichkeit, Kreativität zu fördern und die Produktivität zu steigern. SAIF soll Unternehmen, die KI-Systeme entwickeln und bereitstellen, helfen, die Sicherheit zu verbessern und die Risiken zu minimieren.

Die vier Phasen der Krisenkommunikation bei einem Cybersicherheitsvorfall

Die Kommunikation im Notfall fällt auch erfahrenen und gut vorbereiteten Unternehmen nicht leicht. Aufgrund des speziellen Ablaufs von Cyberangriffen und der Tatsache, dass Angreifer immer häufiger an die Öffentlichkeit gehen, kann die Art und Weise, wie ein betroffenes Unternehmen im Notfall mit Stakeholdern kommuniziert, entscheidenden Einfluss auf das Markenimage haben – und auch noch nachwirken, nachdem die technischen Probleme längst behoben wurden.

Erschwerend kommt hinzu, dass das Kommunikationsmanagement zu viel Zeit der Incident-Response-Teams und Führungskräfte in Anspruch nimmt, die versuchen, den Betrieb wiederherzustellen und die Folgen eines Cyberangriffs zu beheben. Häufig ist auch nicht klar, was die Krisenkommunikation umfasst. Der Kontakt zu Medien ist ein zentraler Bestandteil der Kommunikationsstrategie, doch Medienvertreter sind nicht die einzige Personengruppe, die informiert werden muss. Unternehmen sollten eine umfassende Kommunikationsstrategie entwickeln, mit der alle internen und externen Stakeholder informiert werden.

Um Fehler zu vermeiden – insbesondere in Krisensituationen, in denen jede Sekunde zählt –, lohnt es sich, die Unterstützung erfahrener Cybersicherheitexperten für die Krisenkommunikation in Anspruch zu nehmen, die Unternehmen und Vorständen helfen, angemessen zu reagieren. Da die Bedrohungslandschaft äußerst dynamisch ist und Cyberkriminelle stets neue Techniken entwickeln, bietet Mandiant jetzt nicht nur technische Hilfe von Incident-Response-Teams, sondern zusätzlich auch Unterstützung durch Spezialisten für die Krisenkommunikation an. Sie können Kunden helfen, die Krise zu bewältigen, den Kontakt zu Stakeholdern zu priorisieren und die übrige Kommunikation strategisch zu planen.

Was versteht man unter der Krisenkommunikation bei einem Cybersicherheitsvorfall?

Die cybersicherheitsspezifische Krisenkommunikation ist eine Kombination aus Incident-Response-Maßnahmen und Krisenmanagementprozessen. Dabei werden zu ganz bestimmten Zeitpunkten auf die jeweilige Zielgruppe zugeschnittene Nachrichten an die verschiedenen Stakeholder und Kanäle gesendet. Im Notfall sollten nicht nur die Folgen für den Geschäftsbetrieb, die Risikotoleranz und die potenziellen Schäden für den Ruf des Unternehmens und das Markenimage, sondern auch diverse andere Faktoren berücksichtigt werden. Bei Entscheidungen zu den Kommunikationsmitteln, den Inhalten und dem richtigen Zeitpunkt sind beispielsweise auch das Verhalten der Angreifer und die Bedrohungsdatentrends zu beachten. In einigen Fällen kann es sogar klug sein, gar nicht zu reagieren, da bestimmte Äußerungen die Angreifer dazu verleiten könnten, ihre Taktiken, Techniken und Prozesse zu ändern.

Während eines Cyberangriffs stehen Vertrauen und Markenresilienz auf dem Prüfstand – das ist eindeutig nicht der richtige Zeitpunkt für die Vertrauensbildung. Fehler bei der Krisenkommunikation, unzureichende Informationen und mangelnde Transparenz können sogar das Vertrauen in ein Unternehmen weiter schwächen. Das bedeutet, dass diese Fehler auch zum Gesamtverlust beitragen und den Geschäftsbetrieb beeinträchtigen. Daher müssen Unternehmen genau wissen, was die Krisenkommunikation umfasst, wie die Best Practices lauten und wie sie sich bestmöglich auf einen Notfall vorbereiten.

Wie gelingt die optimale Krisenkommunikation bei einem Cybersicherheitsvorfall?

Unsere Erfahrungen bei Mandiant-Einsätzen zeigen deutlich, dass sich erfolgreiche Unternehmen nicht erst in der akuten Notlage mit der Kommunikation befassen. Es ist vielmehr ein Zyklus, bei dem die Incident-Response- und Geschäftskontinuitätspläne eines Unternehmens kontinuierlich überprüft, analysiert und angepasst werden. Wir haben einige der wichtigsten Erkenntnisse zur Krisenkommunikation bei Cybersicherheitsvorfällen zusammengefasst, die unsere Experten bei Praxiseinsätzen gesammelt haben. Der Zyklus besteht aus vier Phasen: strategische Vorbereitung, Absicherung, Incident Response und Nachbereitung nach einem Sicherheitsvorfall.

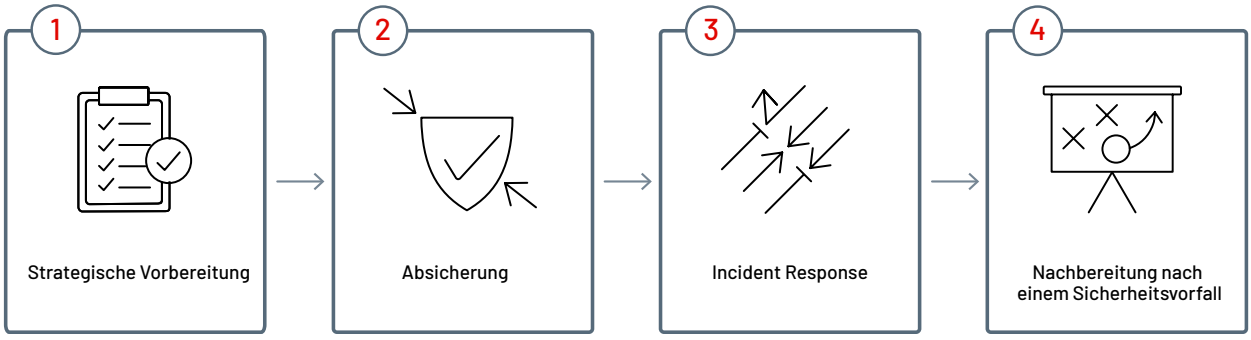
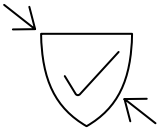


ABBILDUNG 1: Die Phasen der Krisenkommunikation bei einem Cybersicherheitsvorfall

Phase 1: Strategische Vorbereitung

Die erste Phase in diesem Zyklus ist die „strategische Vorbereitung" vor einem Angriff – oder einfach gesagt: die Planungsphase. Sie ist der Startpunkt und bildet die Grundlage für alle Unternehmen, unabhängig von deren Größe, Branche oder Standort. Die Strategie sollte individuell auf das Unternehmen abgestimmt und schriftlich festgehalten werden. Der Plan muss wiederholbar sein und eindeutig definierte Aufgaben und Zuständigkeitsbereiche, eine Governance-Struktur mit offiziellen Angaben zur Entscheidungskompetenz und ein Framework für die Reaktion im Notfall enthalten. Ähnlich wie ein Trainingsplan im Sport ist dies eine Vorlage für die Incident-Response-Teams und umfasst die potenziellen Aufgaben. Das Dokument sollte regelmäßig überprüft und aktualisiert und dann an alle Mitglieder des Incident-Response-Teams weitergegeben werden.

Wichtig ist ebenfalls, ein spezielles Team zusammenzustellen und konkrete Rollen und Zuständigkeitsbereiche zuzuweisen. Die Teammitglieder sollten aus verschiedenen Abteilungen stammen (unter anderem Personalmanagement, Beschaffung, Kommunikation, Recht, Logistik und Betrieb). Sie können nicht im Voraus wissen, was im Notfall benötigt wird – das kann von der Bereitstellung von Hardware über den Kommunikationsfluss von der Führungsetage zu den Mitarbeitern bis zu aussagekräftigen Folgeabschätzungen reichen. Das Team sollte ein Governance- und Managementmodell erstellen, bei dem verschiedene Gruppen für bestimmte Aufgaben verantwortlich sind. Ein Ziel der Planungsphase ist die Ergänzung des Incident-Response-Playbooks um einen Abschnitt zur Krisenkommunikation. Das Playbook sollte speziell auf die Anforderungen des Unternehmens abgestimmt sein und Abschnitte zu Incident-Response-Maßnahmen und zur Krisenkommunikation, wichtige Nachrichten basierend auf hypothetischen Szenarien, Angaben zu den Verantwortlichen und eine Festlegung der Kanäle enthalten. Außerdem empfiehlt es sich, eine alternative Kommunikationsmethode festzulegen, für die sogenannte „Out-of-Band-Kommunikation", falls der primäre Kanal durch einen Angriff beeinträchtigt wurde. Wenn sich Hacker bei einem Cybersicherheitsangriff oder Datendiebstahl im Netzwerk festsetzen, müssen Führungskräfte und Incident-Response-Teams auf andere Kommunikationsmittel ausweichen können.

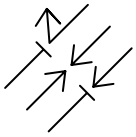


Phase 2: Absicherung

Die zweite Phase gehört ebenfalls zur proaktiven Vorbereitung. Es ist die „Absicherung" oder Übungsphase. Dabei sollten Unternehmen die Reaktion ihres Teams mit realen Angriffsmethoden und -szenarien testen. In einigen US-Bundesstaaten wird diese Phase inzwischen sogar im Cybersicherheitsplan für Vorstände vorgeschrieben.[1] Es lohnt sich, in dieser Phase mit erfahrenen Spezialisten zusammenzuarbeiten und Übungen basierend auf maßgeschneiderten, realistischen Szenarien durchzuführen. Auf diese Weise kann das Team die Ausführung des Plans üben, das Playbook testen und potenzielle Probleme aufdecken, die noch behoben werden müssen. Das gibt den Mitgliedern die Möglichkeit, die Abläufe in einer sicheren und stressfreien Umgebung zu üben, damit sie zur Routine werden und das Team im Notfall nahezu automatisch reagieren kann. In einer Krisensituation treten viel leichter Fehler auf und fallen dann auch schwerer ins Gewicht, aber wenn Sie die nächsten Schritte im Plan schon kennen, ist es wesentlich einfacher, Ruhe zu bewahren und besonnen zu reagieren.

Auch die Berücksichtigung und Umsetzung von Ratschlägen und Feedback sind wichtige Bestandteile dieser Phase. All diese Schritte sollten regelmäßig und sorgfältig durchgeführt und nicht nur „abgehakt" werden. Beteiligen Sie Mitarbeiter aus unterschiedlichen Positionen und Unternehmensbereichen an den Übungen – diese Tests sind nicht nur für die Unternehmensführung und den Vorstand gedacht. Außerdem empfiehlt es sich, ein Ablöseteam aus diversen Experten zu bilden. Der Notfallplan sollte mindestens 30 Tage abdecken und mehrere Incident-Response-Teams umfassen, die einander ablösen. In der ersten akuten Angriffsphase ist meist ein Einsatz rund um die Uhr notwendig, daher ist es hilfreich, weitere Mitarbeiter vorab einzuarbeiten, damit sie zur Ablösung bereitstehen. So lassen sich Burn-out und Übermüdung vermeiden. Stellen Sie außerdem sicher, dass die Geschäftskontinuitäts-, Disaster-Recovery- und Incident-Response-Pläne Ihres Unternehmens auch einen Abschnitt zur Kommunikation umfassen.

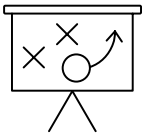
1. New York State Department of Financial Services, „DFS Superintendent Adrienne A. Harris announces updated cybersecurity regulation", November 2022



Phase 3: Incident Response

Die dritte Phase besteht aus den reaktiven Incident-Response-Maßnahmen. Je besser die Vorbereitungen und Übungen in den ersten beiden Phasen liefen, desto einfacher wird die Reaktion im tatsächlichen Notfall. Die 80/20-Regel (das heißt, 80% der Zeit auf die Planung und 20% auf die Durchführung aufzuwenden) hat durchaus einen wahren Kern. Im Notfall müssen Unternehmen schnell reagieren und ihre Teams optimal einsetzen können. Bei entsprechender Vorarbeit kennen diese bereits ihre Aufgaben und Zuständigkeitsbereiche und können sich an einer aktuellen Governance-Struktur orientieren. Sie können die notwendigen Kanäle für den Informationsaustausch einrichten und die anfallenden Schritte und Aufgaben nachverfolgen. Die Stakeholder und die Kommunikationskanäle sind dokumentiert und können schnell kontaktiert bzw. eingesetzt werden.

Reibungslose Einsätze und effektive Incident-Response-Teams sind in der Regel die Folge von umfassenden Schulungen und Übungen, einer guten Ausstattung und der Vorabeinrichtung der relevanten Tools. Sie handeln verantwortungsbewusst, respektieren das Team und überstürzen nichts – sie wissen, dass es sich eher um einen Marathon als einen Sprint handelt. Die Beteiligten arbeiten eng zusammen und tauschen Informationen aus, bevor Entscheidungen getroffen werden, verzögern den Einsatz aber auch nicht durch endlose Analysen. Wenn in Unternehmen Probleme auftreten, wurden meist Ratschläge oder Feedback nicht berücksichtigt, Leistungsprobleme nicht erkannt oder keine ausreichenden Vorbereitungen für koordinierte Maßnahmen und die Kommunikation getroffen.



Phase 4: Nachbereitung nach einem Sicherheitsvorfall

Das Krisenmanagement bei einem Sicherheitsvorfall ist nicht einfach und strapaziert alle Beteiligten sowohl in emotionaler als auch organisatorischer Hinsicht. Viele möchten anschließend nie mehr darüber sprechen. Doch auch wenn es schwerfällt – die letzte Phase, die Post-Mortem-Analyse, sollte keinesfalls ausgelassen werden. Diese Phase beginnt, wenn sich die größte Aufregung gelegt hat: Die Untersuchungen sind abgeschlossen, der Geschäftsbetrieb wurde durch die Maßnahmen zur Schadensbehebung wiederhergestellt und die Regulierungsbehörden und Betroffenen wurden informiert. Diese Phase wird manchmal auch „After Action Review" oder „Retrospektive" genannt. Nach der Planung ist dies eine der wichtigsten Phasen im Zyklus. Dabei können Spezialisten gemeinsam mit den Kunden Lücken aufdecken und Lösungen auswählen, um bei künftigen Vorfällen besser gewappnet zu sein.

Einige der aus Mandiant-Einsätzen abgeleiteten Best Practices stammen aus den Post-Mortem-Analysen. Jeder Vorfall und jede Abwehrmaßnahme läuft anders ab – bei einigen Einsätzen gibt es Fehlstarts, aber letztendlich werden die Probleme dennoch vollständig behoben, andere funktionieren von Anfang an reibungslos mit den branchenüblichen Best Practices. Wichtig ist jedoch, alle Erkenntnisse und Erfahrungen zu teilen, damit andere davon lernen können. Wie schon Winston Churchill sagte: „Wer nicht aus der Geschichte lernt, ist dazu verdammt, sie zu wiederholen."

Angriffe von Cyberspionagegruppen auf IoT-Geräte in Unternehmen

Schätzungen zufolge wird die Zahl der Geräte, die mit dem Internet der Dinge (Internet of Things, IoT) verbunden sind, 2023 auf fast 42 Milliarden steigen.[2] Sie fördern Innovations- und Automatisierungsbemühungen in diversen Branchen – von der intelligenten Fertigung über die Inventarverwaltung im Einzelhandel und digitale Zahlungen bis hin zu Sicherheit und Überwachung. Doch wie bei nahezu allen neuen Technologien müssen Unternehmen auch in diesem Fall die Cyberrisiken berücksichtigen.

Laut Beobachtungen von Mandiant haben Angreifer in der Vergangenheit IoT-Geräte, Smart-Geräte und Router ausgenutzt, um Botnets zu erstellen und groß angelegte finanziell motivierte Cyberangriffe auszuführen. Ein Botnet ist ein Netz aus Geräten, die die Angreifer infiltriert haben und für ihre Zwecke ausnutzen, zum Beispiel für DDoS-Angriffe (Distributed-Denial-of-Service) und die Verbreitung von Malware. Mandiant-Experten sind sich allerdings relativ sicher, dass staatlich geförderte Cyberspionagegruppen Botnets für diverse Zwecke genutzt haben.[3] Dieses Angriffsverhalten zeigt deutlich, welche Möglichkeiten die große Anzahl von IoT- und Smart-Geräten staatlich geförderten Hackergruppen bietet, die auf den Diebstahl strategischer Informationen und geistigen Eigentums spezialisiert sind.

Unternehmen, die ihre digitale Transformation vorantreiben, von der Automatisierung profitieren und Verluste aufgrund der wirtschaftlichen Lage während der COVID-19-Pandemie wettmachen möchten oder die Nutzung von 5G-Netzwerken in Betracht ziehen,[4] sollten sich mit ihrem Cybersicherheitsteam abstimmen und umfassende Cyberabwehrmaßnahmen zum Schutz des gesamten Unternehmens implementieren.

Ausnutzung von IoT-Geräten, Smart-Geräten und Routern zur Verschleierung von Angriffsaktivitäten

Mandiant hat festgestellt, dass staatlich geförderte Cyberspionagegruppen Botnets aus IoT- und Smart-Geräten sowie Routern ausnutzen, um ihre Aktivitäten zu verschleiern. Diese Taktik wurde sowohl von Mandiant-Experten bei mehreren Einsätzen als auch von anderen Sicherheitsunternehmen im privaten und öffentlichen Sektor beobachtet. In diesem Zusammenhang wurden unter anderem folgende Angriffe gemeldet:

- Im April 2022 berichtete Mandiant[5] von einer Kampagne von APT29, bei der ein Botnet aus IoT-Kameras mithilfe der QUIETEXIT-Malware für Command-and-Control-Aktivitäten (C2) ausgenutzt worden war (Abbildung 2). Die dabei verwendeten Domains wurden offenbar gezielt ausgewählt, damit sie im legitimen Datenverkehr der IoT-Geräte nicht auffielen und die Aktivitäten auch bei der Durchsicht der Logdateien nicht herausstechen würden.

2. Frost and Sullivan, „Internet of Things (IoT) Predictions Outlook", November 2022
3. Mandiant, „Espionage Actors Lurk in Compromised Device Botnets", April 2023
4. Frost and Sullivan, „The Top Growth Opportunities for IoT in 2023", März 2023
5. Mandiant, https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

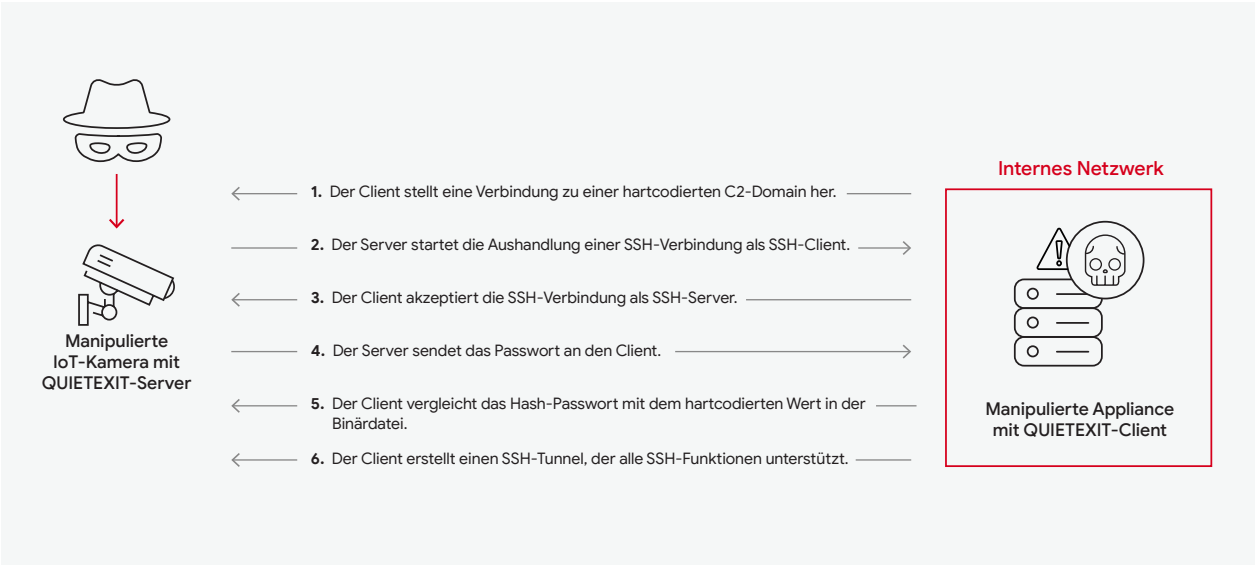


ABBILDUNG 2: Einsatz der QUIETEXIT-Malware auf IoT-Geräten

- In einem Bericht aus dem Jahr 2021[6] der französischen Sicherheitsbehörde Agence nationale de la sécurité des systèmes d'information (ANSSI) wird eine Kampagne beschrieben, die der chinesischen Hackergruppe APT31 zugeschrieben wird. Diese hatte ein Botnet aus Routern und eventuell auch anderen Geräten in kleinen Büros oder Homeoffices ausgenutzt, um ihre Aktivitäten in den Zielnetzwerken zu verbergen.
- PricewaterhouseCoopers berichtete 2022[7] von Malware, die Spezialisten bei einem Einsatz aufgedeckt und „BPFDoor" genannt hatten. Mandiant ordnet diese der Gruppe APT41 zu. Bei dieser Kampagne empfing die Malware offenbar Befehle von virtuellen privaten Servern (VPS), die über ein Netzwerk aus manipulierten Routern in Taiwan gesteuert wurden.
- Das chinesische Sicherheitsunternehmen Antiy beobachtete[8] 2022 ein großes Netzwerk aus manipulierten IoT- und Linux-Geräten, über das Datenverkehr zwischen C2-Servern und Torii-Malware übertragen wurde. Nach Angaben des Unternehmens ließen sich die Aktivitäten der Gruppe OceanLotus zuordnen, die Mandiant unter der Bezeichnung APT32 führt. Mandiant konnte diese Zuordnung allerdings bisher nicht bestätigen.
- 2018 berichteten Sicherheitsforscher öffentlich[9] über die Nutzung der VPNFILTER-Malware in Kampagnen, die auf Netzwerk- und NAS-Geräte (Network-Attached Storage) weltweit abzielten, insbesondere aber auf Geräte in der Ukraine. In einigen Fällen wurden Adversary-in-the-Middle (AitM) und Löschfunktionen eingesetzt, aber möglicherweise waren diese Module für andere Zwecke gedacht. Mandiant ist der Ansicht, dass diese Art der Nutzung von VPNFILTER mit den Aktivitäten von Russland gesponserter Cyberspionagegruppen übereinstimmt[10].

6. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-013/
7. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
8. https://mp.weixin.qq.com/s/2RluW4O56UWiNSQB2hQtGA
9. https://blog.talosintelligence.com/vpnfilter/
10. https://thehackernews.com/2018/06/vpnfilter-router-malware.html

Öffentlichen Berichten und Beobachtungen von Mandiant zufolge haben einige Angreifer auch vorhandene Botnets manipuliert oder übernommen, die von anderen Hackern erstellt worden waren. Mandiant-Experten vermuten allerdings, dass diese Taktik nur in sehr speziellen Fällen nützlich ist und daher von Cyberspionagegruppen in Zukunft nicht verstärkt eingesetzt werden wird.

- Im September 2022 identifizierte Mandiant[11] eine Kampagne der Gruppe UNC4210, die vermutlich zum Turla-Team gehört. Dabei kaperten die Hacker mindestens drei C2-Domains eines ANDROMEDA-Malware-Botnets. Die ANDROMEDA-Version, die von diesem Botnet genutzt wurde, war 2013 auf VirusTotal hochgeladen worden und wird über infizierte USB-Sticks verbreitet. Nachdem es die abgelaufenen C2-Domains erneut registriert hatte, konnte das Turla-Team offenbar die vorhandene Malware nutzen, um die Server aufzurufen und Opfer auszuwählen (Abbildung 3).

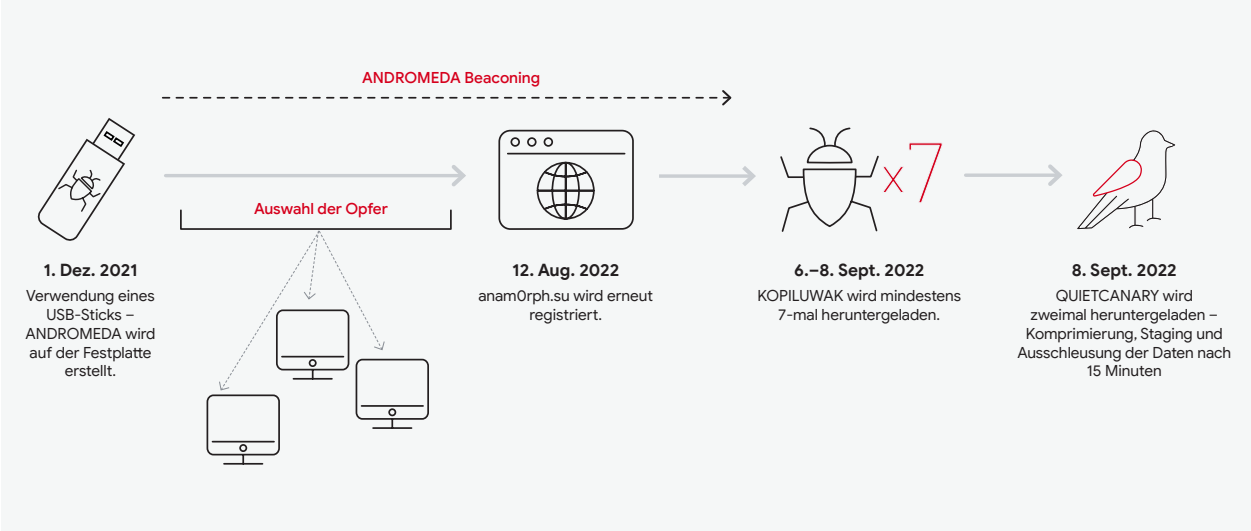


ABBILDUNG 3: Zeitleiste der ANDROMEDA-Angriffe des Turla-Teams

11. https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

Schutz von IoT-Geräten

Bei IoT- und Smart-Geräten hat Sicherheit meist nicht höchste Priorität. Sie verfügen häufig über hartcodierte Anmeldedaten und das Patching bei Softwareschwachstellen ist schwierig oder sogar unmöglich. Unternehmen, die diese Geräte bereits aktiv nutzen oder IoT-Geräte bei ihrer digitalen Transformation eingeplant haben, sollten für einen zuverlässigen Schutz sorgen und regelmäßig nach verdächtigen Aktivitäten suchen. In Abbildung 4 sind die Sicherheitsrisiken in Zusammenhang mit der Fertigung und dem Betrieb von IoT-Geräten aufgelistet, die Eigentümer vor der Bereitstellung berücksichtigen sollten.

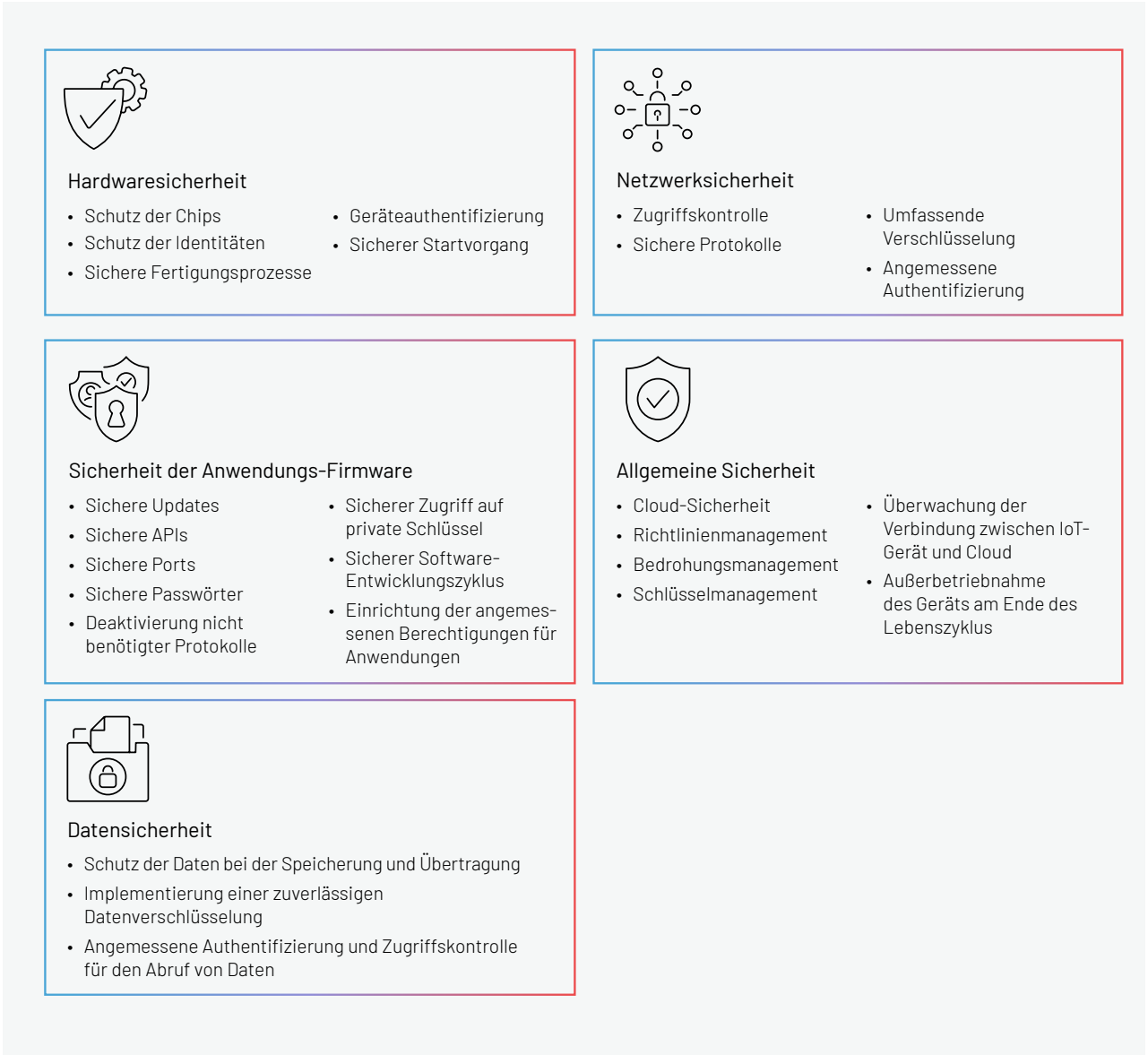


ABBILDUNG 4: Wichtige Punkte für den Schutz von IoT-Geräten

Was bedeutet das für die digitale Transformation von Unternehmen?

Mandiant geht davon aus, dass Cyberspionagegruppen diese Taktik auch weiterhin einsetzen werden. Da immer mehr IoT- und Smart-Geräte genutzt werden, die oft nur unzureichend geschützt sind, können die Hacker mit einem relativ geringen Aufwand ihre Ziele erreichen. Mit der zunehmenden Verbreitung von IoT- und Smart-Geräten werden auch mehr Tools in Untergrundforen und zum kostenlosen Download im Internet angeboten werden, die speziell auf diese Geräte ausgerichtet sind. Mandiant vermutet daher, dass Cyberspionagegruppen in Zukunft verstärkt Botnets ausnutzen werden, um ihre Aktivitäten zu verschleiern oder um opportunistische finanziell motivierte Angriffe durchzuführen.

Größere Resilienz bei Angriffen auf Edge-Geräte

In den letzten zehn Jahren haben Unternehmen die Transparenz ihrer digitalen Umgebungen deutlich verbessert. Dadurch können sie Angreifer schneller erkennen[12] und haben auch den proaktiven Schutz vor Bedrohungen wie der mehrfachen Verwendung von Passwörtern und Brute-Force-Angriffen verbessert. Das Ziel ist eine Defense-in-Depth-Architektur.

Dieser Trend geht zwar in die richtige Richtung, doch die meisten Unternehmen setzen dabei auf Lösungen für die Bedrohungserkennung und Bedrohungsabwehr auf Endpunkten (Endpoint Detection and Response, EDR). Diese werden allerdings, wie der Name schon sagt, auf Endpunkten implementiert. Das heißt, Firewalls, IoT-Geräte, VPNs, Hypervisors und viele andere Geräte werden von EDR meist nicht abgedeckt und daher im Allgemeinen unter der Kategorie „Edge-Geräte" zusammengefasst. Was passiert, wenn Angreifer diese Geräte ins Visier nehmen?

Da sich Edge-Geräte außerhalb des Radars der typischen Erkennungslösungen in Unternehmen befinden, stellen sie ein ideales Einfallstor für Angreifer dar. Edge-Geräte werden immer lohnenswerte Ziele für Angreifer sein, da sie von Unternehmen für wichtige Funktionen wie die Überwachung interner Sicherheitstools genutzt werden, aber bisher nicht von EDR-Lösungen abgedeckt wurden und nur selten auf Systemebene überwacht werden. Die Überwachung auf Systemebene ist notwendig, um festzustellen, ob Code geändert oder Malware installiert wurde.

Edge-Geräte werden für die Bedrohungssuche und den Schutz verwendet, sind aber selbst nicht sonderlich gut abgesichert. Erschwerend kommt hinzu, dass Anbieter Benutzern meist keinen direkten Zugriff auf das Betriebs- oder Dateisystem dieser Geräte geben. Da die Sicherheitsfunktionen die Edge-Geräte und -Systeme nicht abdecken, haben Sicherheitsteams kaum Möglichkeiten, das zugrunde liegende und potenziell anomale Verhalten zu analysieren.

12. Mandiant, „M-Trends 2023", April 2023

Aus den Beobachtungen der letzten fünf Jahren schließt Mandiant, dass staatlich gesponserte Hackergruppen zunehmend Edge-Geräte angreifen. Das bringt große Vorteile für die Angreifer und ebenso große Probleme für die Sicherheitsteams mit sich. Angreifer versuchen meist, sich über Edge-Geräte Zugriff auf Netzwerke zu verschaffen oder sich langfristig in den Zielumgebungen festzusetzen. Das ist jedoch nicht der einzige Vorteil. Diese Geräte bieten einen umfassenden Überblick über die Umgebung und verfügen über mehr Rechte, um die Netzwerküberwachung zu ermöglichen oder einen sicheren Zugriffspunkt bereitzustellen. Haben Angreifer Zugriff auf diese Geräte, können sie den Zeitpunkt des Angriffs so wählen, dass sie möglichst unerkannt bleiben. Da Edge-Geräte nicht von EDR-Lösungen abgedeckt werden, können die genannten Vorteile nicht nur für die Angriffe selbst, sondern auch zum Verbergen der Aktivitäten vor den Sicherheitsteams genutzt werden.

Staatlich gesponserte Hackergruppen investieren oft viel Zeit und Ressourcen in die Forschung und Entwicklung, um bisher nicht bekannte Schwachstellen zu identifizieren und entsprechende Exploits zu erstellen. Mandiant-Experten haben im Laufe der Jahre zahlreiche Angriffe untersucht, bei denen mutmaßlich von China unterstützte Hackergruppen Zero-Day-Sicherheitslücken ausgenutzt und speziell angepasste Malware installiert haben, um Anmeldedaten von Benutzern zu stehlen und den langfristigen Zugriff auf die Zielumgebungen sicherzustellen. UNC3886 griff beispielsweise 2022 gezielt Edge-Geräte wie Firewalls und in einer späteren Phase des Angriffszyklus auch Hypervisor-Technologien an.

Fallstudie: UNC3886

Die Hackergruppe UNC3886 griff diverse Fortinet-Komponenten an[13] und breitete sich anschließend in VMware-Infrastrukturen aus. Dabei wurden folgende Komponenten und Versionen ausgenutzt:

- **FortiGate 6.2.7**: FortiGate-Appliances sind Netzwerk-Firewalls, mit denen sich der Datenverkehr auf den Geräten kontrollieren und überwachen lässt.
- **FortiManager 6.4.7**: FortiManager dient als zentrale Managementplattform für Fortinet-Geräte.
- **FortiAnalyzer 6.4.7**: FortiAnalyzer ist eine Lösung für das zentrale Management von Logdateien von Fortinet-Geräten und die Berichterstellung.

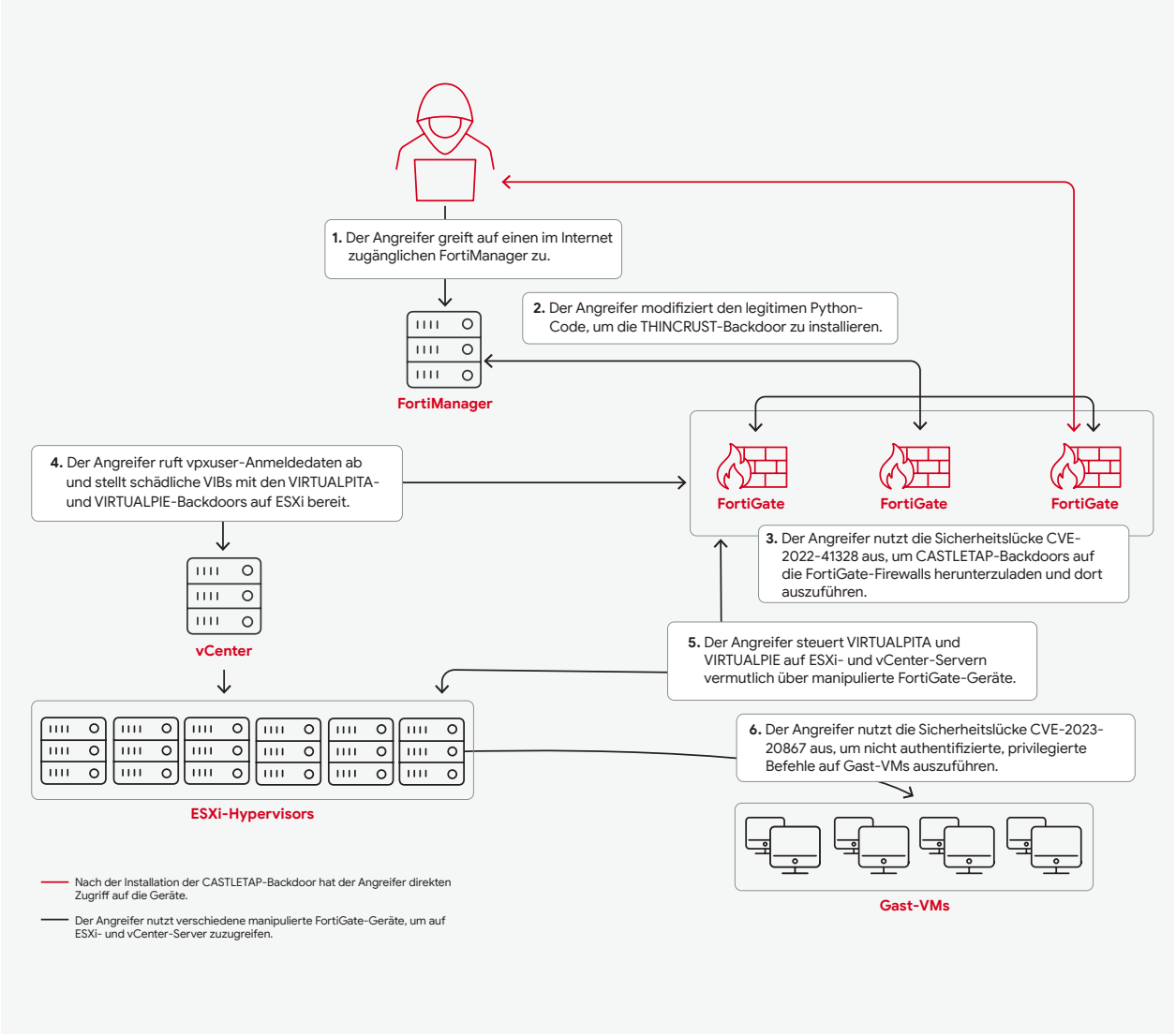


ABBILDUNG 5: Aktivitäten nach der Beschränkung des Internetzugriffs auf FortiManager

13. https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

Mandiant begann im Jahr 2022, die Gruppe UNC3886 zu verfolgen, die vermutlich von China gesponsert wird. Die Hacker griffen gezielt Fortinet-Systeme an und breiteten sich anschließend in der VMware-Infrastruktur der Zielumgebungen aus. Die UNC3886-Mitglieder verfügten über ausreichende Kenntnisse zu diversen Fortinet-Lösungen, um sich Zugriff zu verschaffen. Dazu gehörten FortiGate (Firewall), FortiManager (zentrale Managementlösung) und FortiAnalyzer (Plattform für das Management von Logdateien, Analysen und Berichten). Um sich langfristigen Zugriff zu sichern, implementierte UNC3886 auf den FortiManager- und FortiAnalyzer-Geräten eine Backdoor, die Mandiant unter der Bezeichnung **THINCRUST** verfolgt. Anschließend griff UNC3886 auf native FortiManager-Skripte zu, um die Sicherheitslücke CVE-2022-41328 auszunutzen und eine weitere Backdoor, **CASTLETAP**, auf FortiGate-Geräte herunterzuladen. Dadurch wurde der Zugriff auf die Umgebung sichergestellt.

Mandiant-Experten stellten fest, dass SSH-Verbindungen von den Fortinet-Geräten zu den ESXi-Servern in der Zielumgebung hergestellt und dann die vSphere Installation Bundles[14] installiert wurden, die die Backdoors **VIRTUALPITA** und **VIRTUALPIE** enthielten.

In einem anderen Fall, bei dem FortiManager nicht über das Internet zugänglich war, nutzte UNC3886 eine bestehende Zugriffsmöglichkeit aus, um auf FortiManager ein Programm für die Umleitung des Netzwerkverkehrs, das Mandiant unter der Bezeichnung **TABLEFLIP** verfolgt, sowie eine Reverse-Shell-Backdoor-Variante von **REPTILE** zu installieren. Mit dieser Malwarekombination konnte UNC3886 die Netzwerkzugriffslisten (Access Control Lists, ACLs) umgehen, mit denen der externe Zugriff eingeschränkt worden war.

In beiden Fällen wurden die schädlichen Aktivitäten nach einem umfassenden Angriff auf die Fortinet-Komponenten und VMware-Hypervisors aufgedeckt, als UNC3886 begann, Befehle zum Ausspähen der Umgebung auszuführen und legitime Systemprozesse für die Datenausschleusung auszunutzen.

Weitere Details zu dieser Fallstudie finden Sie im Blogbeitrag „Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation".

CASTLETAP ist ein Linux-Binärcode, der passiv nach Paketen sucht und die Backdoor-Funktion aktiviert, wenn er ein ICMP Echo-Paket empfängt. Diese Pakete durchsucht die Malware nach Informationen zu C2-Servern, um eine Verbindung über SSL herzustellen. Zu den Funktionen gehören das Hoch- und Herunterladen von Dateien, um normale und BusyBox-basierte Shells bereitzustellen.

THINCRUST ist eine Python-Backdoor, die in Code einer Drittanbieterbibliothek eingebettet ist und die Remoteausführung von Befehlen sowie das Lesen und Bearbeiten von Dateien über HTTP-Anfragen ermöglicht. Die verschlüsselten Befehle werden in HTTP-Cookies gespeichert.

VIRTUALPITA ist eine passive 64-Bit-Backdoor für Linux und VMware ESXi, die einen Listener für hartcodierte TCP- oder VMCI-Portnummern erstellt. Sie unterstützt die Ausführung beliebiger Befehle, das Hoch- und Herunterladen von Dateien und das Starten und Stoppen des vmsyslogd-Dienstes.

VIRTUALPIE ist eine Python-Backdoor, die einen schädlichen IPv6-Listener auf einem hartcodierten TCP-Port implementiert. Sie unterstützt die Übertragung von Dateien, die Ausführung beliebiger Befehle und Reverse-Shell-Funktionen. Die Kommunikation erfolgt über ein spezielles Protokoll und die Daten werden mit RC4 verschlüsselt.

TABLEFLIP ist ein Linux-Programm, mit dem Datenverkehr umgeleitet werden kann. Es kontrolliert passiv alle aktiven Schnittstellen auf spezielle Befehlspakete. Diese Pakete enthalten mit XOR verschlüsselte IP-Adressen und Portnummern, an die mithilfe von iptable-Befehlen Datenverkehr umgeleitet werden soll.

REPTILE ist ein öffentlich verfügbares Linux-Rootkit in C. Es unterstützt Backdoor-Funktionen, die durch Port Knocking über ICMP-, UDP- oder TCP-Pakete aktiviert werden können. Zu den weiteren Funktionen gehören Reverse Shell und die Dateiübertragung.

14. https://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

Fallstudie: APT29

Mandiant hat festgestellt, dass auch staatlich gesponserte Hackergruppen wie APT29 ähnliche Edge-Gerätetypen mit einem neuen Tunneling-Programm angreifen.

Anfang 2022 verschaffte sich APT29 Zugriff auf eine Zielumgebung und installierte **QUIETEXIT** auf den Endpunkten. In einem Fall griff APT29 auf legitime, anwendungsspezifische Startskripte zu, um die Ausführung von **QUIETEXIT** beim Start zu erzwingen, da ein nativer Persistenzmechanismus fehlte. **QUIETEXIT** unterstützt alle SSH-Funktionen und APT29 nutzte einen SOCKS-Tunnel in die Zielumgebung aus. Dadurch hinterließ APT29 beim Diebstahl der Daten nahezu keine Spuren auf dem Zielcomputer. APT29 griff auch NAS-Geräte (Network Attached Storage) an und veränderte den Namen der Binärdatei, damit sie unter den legitimen Dateien im Dateisystem nicht auffiel. Als zusätzliche Zugriffsmethode installierten die Hacker eine zweite Backdoor, eine **REGEORG**-Webshell, auf einem DMZ-Webserver. Diese Vorsichtsmaßnahme und die Tatsache, dass keine unterstützte Antiviren- oder EDR-Lösung vorhanden war, verschaffte den Hackern eine lange Verweildauer.

QUIETEXIT ist ein Reverse-SSH-Tunneling-Programm, das eine Verbindung zu einem externen C2-Server herstellt, aber ein Passwort für die Authentifizierung erfordert. QUIETEXIT kann Befehle ausführen oder Datenverkehr über SOCKS leiten. Die Malware wurde aus der Open-Source-SSH-Client-Server-Software DROPBEAR abgeleitet.

REGEORG ist ein Open-Source-Programm, mit dem Webshell-Datenverkehr über Tunnel geleitet wird.

QUIETEXIT: Laut Beobachtungen von Mandiant wurden als C2-Systeme vorrangig ältere Kamerasysteme in Konferenzräumen ausgenutzt und dazu vermutlich mit der Serverkomponente von QUIETEXIT infiziert. Durch die Ausnutzung dieser vertrauenswürdigen Systeme blieben die Aktivitäten von APT29 in den Zielumgebungen mindestens 18 Monate lang unentdeckt.

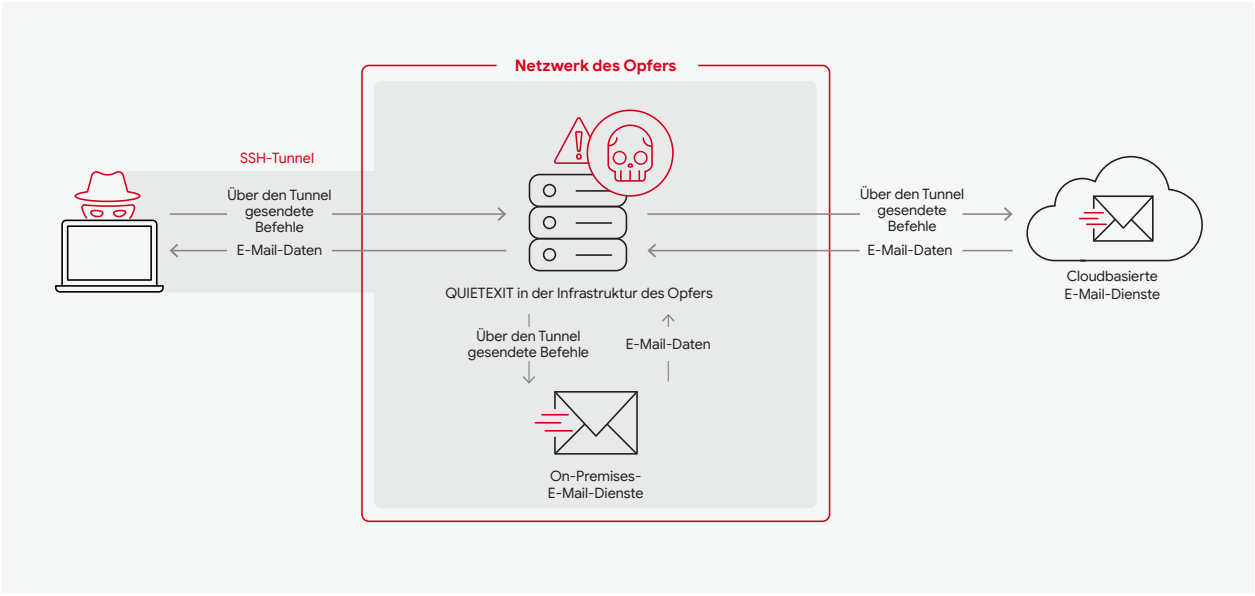


ABBILDUNG 6: Tunneling über QUIETEXIT

APT29 verschaffte sich privilegierte Anmeldedaten zur E-Mail-Umgebung des angegriffenen Unternehmens und wählte gezielt Führungskräfte und Mitarbeiter aus, die für die Unternehmenswicklung, Fusionen und Übernahmen, große Geschäftstransaktionen und die IT-Sicherheit verantwortlich waren. In einigen Fällen nutzte APT29 dieselben eDiscovery- und Graph-API-Tools für programmatische Suchvorgänge und den Zugriff auf E-Mail-Daten, mit denen auch Incident-Response-Teams arbeiten. Mithilfe dieser Tools konnten die Hacker eine große Anzahl an E-Mails ausschleusen.

Weitere Details zu dieser Fallstudie finden Sie im Blogbeitrag „Eye Spy on Your Email".

Fallstudie: APT28

2022 stellte Mandiant fest, dass die Hacker der Gruppe APT28 von ihren üblichen Aktivitäten abwichen. Die Hacker infiltrierten bevorzugt Edge-Infrastrukturen und führten anschließend verschiedene andere Aktivitäten aus. Diese Vorgehensweise wird als „Living on the Edge" bezeichnet. Seit Beginn des Krieges in der Ukraine versucht der russische militärische Nachrichtendienst durch nahezu ununterbrochene Cyberspionagekampagnen und disruptive Angriffe wichtige Dienstleister und Unternehmen in der Ukraine zu stören. Für den wiederholten Zugriff und Angriff auf die Opfer werden infizierte Edge-Infrastrukturen wie Router und andere Geräte mit Internetzugang missbraucht.

Weitere Details zu dieser Fallstudie finden Sie in unserem Bericht M-Trends 2023 im Kapitel „Invasion der Ukraine: Cyberaktivitäten vor dem Hintergrund militärischer Auseinandersetzungen".

Die wichtigsten Erkenntnisse

Bei den Vorfällen aus diesen Fallstudien wurden die Angriffe erst nach der Infiltration der Umgebung erkannt, da die Hacker ganz gezielt Edge-Netzwerke ausnutzten, um ihre Aktivitäten zu verbergen. Mandiant-Experten führten detaillierte Untersuchungen der betroffenen Systeme durch, um den ersten Angriffsvektor zu ermitteln. In diesen Fällen führten Spuren zu den IP-Adressen von Edge-Geräten. Daraufhin arbeiteten die Experten mit den Anbietern zusammen, um forensische Images der Geräte zu erhalten und weitere Analysen durchzuführen. Durch die Kommunikation mit externen Partnern und eine enge Zusammenarbeit können Hersteller frühzeitig über neue Angriffsmethoden informiert werden, bevor diese öffentlich bekanntgegeben werden, und Untersuchungsteams mit mehr Details versorgt werden, um diese neuen Taktiken zu identifizieren.

Tipps zum Schutz vor derartigen Angriffen

Cyberspionagegruppen investieren zunehmend in die Forschung und Entwicklung von Tools und Exploits für Systeme, die im Allgemeinen nicht von EDR-Lösungen abgedeckt werden. Dazu sind umfassende Kenntnisse der anvisierten Betriebssysteme notwendig. Unternehmen bauen zwar weiterhin ihre Security Operations Centers (SOCs) aus, sollten aber auch darauf achten, sich nicht allein auf die Bedrohungserkennung auf Endpunkten zu beschränken. Bei unzureichender Transparenz können Angreifer relativ einfach unerkannt agieren. Die blinden Flecken müssen also identifiziert werden, damit ein SOC das Unternehmen effektiv schützen kann. Unternehmen sollten eine Bestandsaufnahme aller Geräte im Netzwerk machen und prüfen, ob geeignete Überwachungstools vorhanden sind. Für Geräte, die keine Überwachungstools unterstützen, gibt es in der Regel anbieterspezifische Härtungsprozesse, um eine angemessene Protokollierung zu ermöglichen. Außerdem sollte sichergestellt werden, dass diese anbieterspezifischen Logdateien an ein zentrales Repository übermittelt werden. Unternehmen sollten zudem prüfen, ob es möglich ist, den ausgehenden Datenverkehr von diesen Geräten mit Netzwerkzugriffskontrollen zu beschränken oder sogar zu verhindern. Durch die Implementierung zusätzlicher Lösungen für die Netzwerküberwachung und Suche nach Anomalien im ein- und ausgehenden Datenverkehr auf Edge-Geräten und anderen Technologien, die von EDR nicht abgedeckt werden, lassen sich weitere Sicherheitsfunktionen nutzen, falls diese Netzwerkkontrollen nicht umsetzbar sind.

Weitere Informationen finden Sie in den folgenden Ressourcen:

Mandiant-Leitfaden zur Härtung von Microsoft 365

Mandiant-Blogartikel zur Bedrohungserkennung und Härtung auf ESXi-Hypervisors („Detection and Hardening within ESXi Hypervisors")

6 Tipps für die Implementierung von PAM-Lösungen

Durch die zunehmende Nutzung von Cloud-Diensten und SaaS-Anwendungen steigt auch die Zahl der Konten, die Unternehmen erstellen und verwalten müssen, exponentiell. Mitarbeiter können heutzutage im Durchschnitt auf 30 Unternehmenskonten und -anwendungen zugreifen. Außerdem gibt es inzwischen 45-mal mehr maschinelle Identitäten, digitale Zertifikate und Schlüssel als menschliche Benutzer.[15]

Für Unternehmen, die Schwierigkeiten haben, unnötige Konten zu entfernen und Zugriffsrechte für Mitarbeiter und Systeme zu widerrufen, die diese nicht benötigen, lohnt sich die Implementierung einer PAM-Strategie (Privileged Access Management).

Mit PAM wird der Zugriff auf Unternehmensressourcen mit den folgenden Maßnahmen kontrolliert und geschützt:

Einrichtung von Workflows für die Autorisierung

Sichere Speicherung und Verschlüsselung von Secrets

Überprüfung, Überwachung und Protokollierung von privilegierten Zugriffen

Festlegung von Richtlinien für das Secrets-Management (z. B. Passwortänderungen)

Absicherung und Isolierung des Zugriffs auf Zielsysteme mithilfe eines Sitzungsmanagers

Bisher haben sich Unternehmen bei ihrer PAM-Strategie meist auf Lösungen für die Multi-Faktor-Authentifizierung (MFA) verlassen. Doch wenn diese nicht korrekt implementiert und fortlaufend gepflegt werden, können unerwünschte Risiken für das Unternehmen auftreten.

15. CyberArk, „5 Reasons to Prioritize Privileged Access Management“, 2022

2017	2019	2021	2022
Equifax Angreifer verschafften sich Zugriff auf personenbezogene Daten von etwa 147 Millionen Kunden.	**Australian National University** Angreifer rieen personenbezogene Daten von Beschäftigten und Studierenden aus 19 Jahren ab.	**Verkada** Bei diesem Lieferkettenangriff verschafften sich die Angreifer Zugriff auf das Verkada-Überwachungskamerasystem, das in Krankenhäusern, Schulen und Gefängnissen im Einsatz ist.	**U.S. Dept. of Veterans Affairs** Sensible Anmeldedaten für Systeme, in denen Gesundheitsakten gespeichert waren, wurden bei GitHub offengelegt.

ABBILDUNG 7: Zeitleiste von Angriffen, bei denen Angreifer PAM-Lösungen ausnutzten

Angreifer waren bei der Ausnutzung von Schwachstellen in Lösungen für das Zugriffsmanagement bisher recht erfolgreich. Schon 2017 gab es erste schwerwiegende Angriffe, bei denen PAM-Schwachstellen für den Datendiebstahl ausgenutzt wurden. Ein Beispiel ist der Angriff auf Equifax, bei dem die Hacker personenbezogene Daten von 147 Millionen Kunden abrufen konnten.[16] Ein Jahr später wurden bei einem Angriff auf die Australian National University personenbezogene Daten von Beschäftigten und Studierenden aus 19 Jahren gestohlen.[17] 2021 verschafften sich Hacker bei einem Lieferkettenangriff auf das Sicherheitsunternehmen Verkada Zugriff auf das Überwachungskamerasystem, das in Krankenhäusern, Schulen und Gefängnissen im Einsatz ist.[18] Und 2022 wurde das U.S. Department of Veterans Affairs Opfer einer Datenpanne, bei der ein Auftragnehmer die Anmeldedaten eines privilegierten Kontos offenlegte.[19]

Laut Beobachtungen von Mandiant konnten Cyberkriminelle in mehreren Fällen MFA-Funktionen umgehen. So führten APT-Gruppen (Advanced Persistent Threat) aus Russland sogenannte „MFA-Fatigue-Angriffe"[20] durch. Dabei sendeten sie wiederholt Authentifizierungsanforderungen für den zweiten Faktor an die E-Mail-Adresse, das Mobiltelefon oder ein registriertes Gerät des Opfers, um sich Zugriff auf die E-Mail-Konten zu verschaffen, die einen Onlinebetrug ermöglichen würden.

In einem anderen Fall beobachteten Mandiant-Experten, wie APT29[21] den Selbstregistrierungsprozess für die MFA in einem Unternehmen ausnutzte, bei dem nur ein Benutzername und ein Passwort benötigt wurde, um ein Gerät zu registrieren. APT29 führte Brute-Force-Angriffe (Password Guessing) durch, um Konten zu finden, für die noch keine Geräte registriert waren, und dann eigene Geräte hinzuzufügen.

Sicherheitsteams aller Unternehmen, unabhängig von deren Größe oder dem Reifegrad des PAM-Programms, sollten für den bestmöglichen Schutz die folgenden sechs Tipps für die PAM-Implementierung berücksichtigen.

16. Wallix Cybersecurity, „Equifax Breach: Preventing Data Breaches with Privileged Access Management"
17. Australian National University, „Incident Report on the Breach of the Australian national Universities Administrative Systems", 2019
18. Verkada, „Summary: March 9, 2021 Security Incident Report", 2021
19. FedScoop, „VA investigates breach after federal contractor publishes source code", September 2022
20. Mandiant, „Suspected Russian Activity Targeting Government and Business Entities Around the Globe", Dezember 2021
21. Mandiant, „You Can't Audit Me: APT29 Continues Targeting Microsoft 365", August 2022

01

Korrekter Umgang mit privilegierten Konten

Sicherheits- und IT-Teams werden häufig gefragt: „Was ist ein privilegiertes Konto?" Alle Konten verfügen über bestimmte Berechtigungen, aber die Konten der folgenden Kategorien verfügen über mehr Rechte (und sind daher „privilegiert"):

- **Domainadministratoren:** Diese Benutzer haben die vollständige Kontrolle über eine Domain.
- **Persönliche privilegierte Konten:** Diese Benutzerkonten verfügen über mehr Berechtigungen als reguläre Benutzer und werden nach Bedarf eingesetzt.
- **Standardkonten:** Diese Konten werden automatisch von einem System oder einer Anwendung erstellt (z. B. SA, Root, mysql oder ec2-user).
- **Dienstkonten:** Diese Konten werden Geräten zugewiesen und bieten Zugriff auf Unternehmenssysteme, -dienste und -anwendungen.
- **„Root", „Super Administrator" oder „Globaler Administrator" (Cloud):** Dies sind zusätzliche Administratorkonten für ein System, die den Benutzern vollständige Kontrolle über das lokale Gerät geben.
- **Konten für den Notfallzugriff:** Mit diesen Konten kann bei einem Sicherheitsvorfall auf die Systeme zugegriffen werden.
- **Sicherheitskonten:** Mit diesen Konten greifen Sicherheitsteams auf Systeme zu, um Sicherheitsprüfungen und Untersuchungen durchzuführen.

Unternehmen müssen sich unbedingt einen Überblick über die Risiken des Missbrauchs von Konten mit privilegierten Zugriffsrechten verschaffen und diese einschätzen. Gewähren Sie zuerst nur minimale Zugriffsrechte (Least-Privilege-Prinzip), sodass Benutzer nur die für ihre Arbeit erforderlichen Aktivitäten ausführen können.

Achten Sie dabei insbesondere auf Positionen, die Zugriff auf personenbezogene Daten oder geistiges Eigentum haben.

Empfohlene Maßnahmen

- Analysieren Sie die Risiken des privilegierten Zugriffs in Ihrem Unternehmen. Identifizieren Sie Konten für Mitarbeiter und Systeme, die ein Risiko für kritische Ressourcen und Informationen darstellen. Berücksichtigen Sie die unterschiedlichen Arten von Berechtigungen, zum Beispiel Identifizierungsmethoden wie interaktive Anmeldungen. Priorisieren Sie sensible PAM-Konten.
- Sichern Sie sich die Unterstützung von Führungskräften und der Unternehmensleitung, um schneller Tools zu implementieren, mit denen sich das Gesamtrisiko im Unternehmen reduzieren lässt.
- Stellen Sie sicher, dass Sicherheits- und IT-Teams dabei zusammenarbeiten, um die Anforderungen der verschiedenen Benutzergruppen zu erfüllen sowie die Kommunikation und das Änderungsmanagement bei der PAM-Implementierung zu optimieren.
- Prüfen Sie regelmäßig die Zertifikate und die den Konten zugewiesenen Berechtigungen. Für aktive Konten sollten keine Änderungen anfallen – bei einem neuen Anwendungsfall sollte vielmehr ein neues Konto erstellt werden. Eine weitere Möglichkeit ist die Einrichtung einer zeitlich begrenzten Zugriffsrichtlinie, sofern dies genehmigt wird.

02

Festlegung eines fortlaufenden Prozesses für die Erstellung, Ermittlung und Einrichtung von Konten

Bei der Implementierung von PAM-Lösungen in einer Umgebung sollten die PAM-Teams proaktiv nach Sicherheitslücken im Unternehmen suchen und diese beheben. Ein wichtiger Schritt ist die Erfassung und Einrichtung der Konten, die von den Anwendungsteams identifiziert wurden, und die Berücksichtigung der Verwaltung dieser Konten über die PAM-Lösung.

Wird dieser Schritt ausgelassen, gibt es unter Umständen zahlreiche nicht geschützte Konten, die ein Risiko für das Unternehmen darstellen. Angreifer könnten diese Konten ausnutzen, um sich Zugriff auf Systeme zu verschaffen, Zugriffsrechte auszuweiten, sich im Netzwerk auszubreiten und dort festzusetzen.

Nicht geschützte privilegierte Konten werden besonders problematisch, wenn der Umgebung neue Konten und Dienste hinzugefügt werden. Dadurch vergrößern sich die Angriffsfläche und der Abfragebereich für privilegierte Konten, sodass das Risiko eines Sicherheitsvorfalls steigt.

Wenn Unternehmen eine umfassende Inventarliste aller alten und neuen Konten in einer Umgebung erstellen und regelmäßig aktualisieren, können sie bei einem Sicherheitsvorfall schnell feststellen, welche Konten betroffen oder gefährdet sind. Dadurch lassen sich die Konten besser schützen, die Systeme, auf die diese Konten Zugriff haben, identifizieren und vertrauenswürdige Pfade für den Zugriff auf wichtige Ressourcen einrichten. Das vereinfacht die Arbeit des internen Sicherheitsteams und der Incident-Response-Experten und -Manager in einer Krisensituation.

Empfohlene Maßnahmen

- Richten Sie Konten gleich nach der Erstellung ein, um die aufwendige Kontoermittlung zu vermeiden.
- Suchen Sie mithilfe von Tools nach Konten, die übersehen wurden, richten Sie sie ein und implementieren Sie effektive Kontrollmechanismen, um die Konten während des gesamten Lebenszyklus zu verwalten.
- Prüfen Sie die Berechtigungen privilegierter Konten. Stellen Sie fest, wo geistiges Eigentum, personenbezogene Daten oder geschützte Gesundheitsdaten gespeichert werden und mit welchen Methoden der Zugriff erfolgt.
- Richten Sie einen fortlaufenden Prozess zur Kontoermittlung ein. Arbeiten Sie mit den Teams zusammen, um die Erstellung, Ermittlung und Einrichtung zu automatisieren.
- Prüfen Sie im MITRE ATT&CK® Framework, welche Techniken häufig für Angriffe zur Ausweitung der Zugriffsrechte missbraucht werden.

03

Implementierung zuverlässiger Zugriffskontrollen für die PAM-Lösung

PAM dient dem Schutz des Zugriffs auf eine Umgebung. Daher sollte der Zugriff auf PAM-Lösungen verwaltet werden, da diese Benutzerkonten und Systeme unter Umständen für Angreifer interessant sind.

Die Rechte der PAM-Administratorkonten sollten nicht für die Verzeichnisse übernommen werden, die die Lösung schützt. Verwenden Sie dazu die in das Verzeichnis integrierten PAM-Tools.

Es empfiehlt sich auch, einen Workflow für die Autorisierung einzurichten. Damit kann sich ein Unternehmen besser vor Insiderbedrohungen schützen und PAM-Teams können besser nachvollziehen, wie sie das System konfigurieren müssen.

Empfohlene Maßnahmen

- **Richten Sie die folgenden Kontotypen ein:**
  - **PAM-Tool-Administratoren**
  - **Anwendungskonten**
  - **Serverkonten**
  - **Automatisierung und Skripting**
- **Überprüfen Sie das Zugriffsmodell für die PAM-Lösung und identifizieren Sie gefährliche Berechtigungskombinationen.**
- **Stellen Sie sicher, dass die Administratorkonten für die PAM-Lösung über die korrekten Berechtigungen verfügen, sodass der Zugriff auf die Anmeldedaten beschränkt wird, die die Anwendung schützt.**
- **Richten Sie Workflows für die Autorisierung und den Zugriff ein, um kritische Konten zu schützen.**
- **Bieten Sie Ihren Teams Schulungen und Unterstützung von Experten an, damit sie sich die notwendigen Sicherheitskenntnisse aneignen können, um das Sicherheitsniveau des Unternehmens kontinuierlich zu verbessern.**

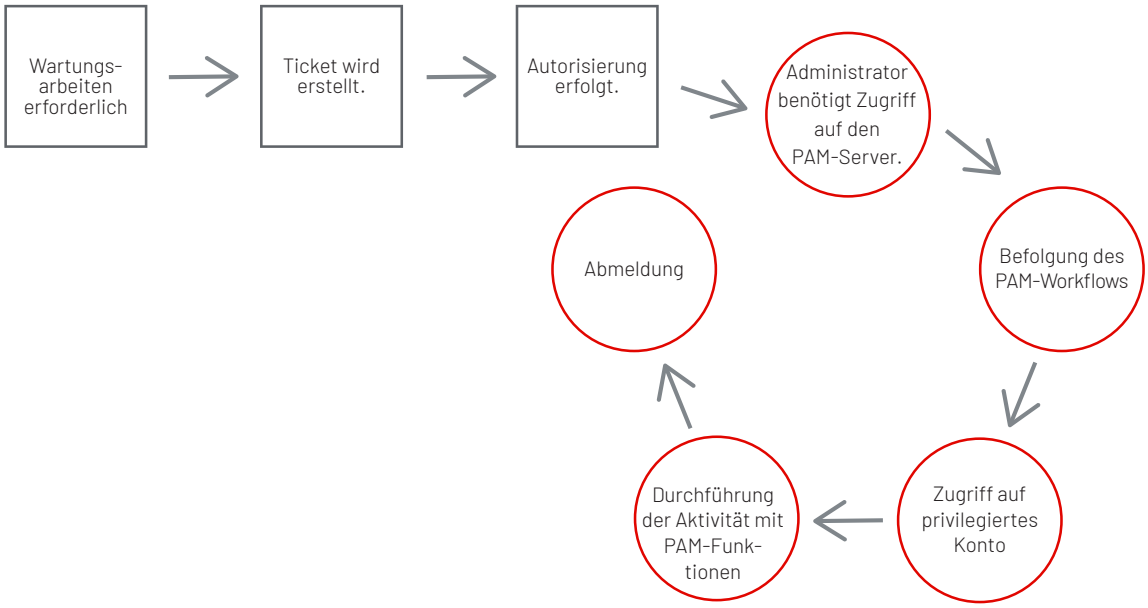


ABBILDUNG 8: Workflow für die PAM-Autorisierung

04

Ermittlung und Schutz von Zugriffspfaden

Es sollten bestimmte grundlegende Punkte zum Schutz des privilegierten Zugriffs auf Unternehmensressourcen beachtet werden. So ist beispielsweise darauf zu achten, dass Passwörter nicht auf Endpunkten offengelegt werden. Auch die Aktivitäten und Prozesse zwischen Benutzern und Zielsystemen sollten überprüft werden.

Wird der Datenverkehr über einen vertrauenswürdigen Pfad übertragen? Wie lässt sich dies erzwingen?

Weitere wichtige Fragen lauten:

- Läuft die Verbindung über eine Internetressource?
- Wird eine direkte Verbindung von einer Workstation zu der Internetressource hergestellt?
- Wird für die Verbindungen HTTPS verwendet?

Wenn Sie die Datenströme und die Pfade zu den Zielen kennen, können Sie das Bedrohungsrisiko besser einschätzen. Überprüfen Sie auch, wie Anwendungen Secrets abrufen und wie diese Secrets zwischen den Anwendungen und Servern übermittelt werden.

Empfohlene Maßnahmen

Ermitteln Sie alle Zugriffspfade in der Umgebung und prüfen Sie, ob diese Architektur den Vorgaben in den PAM-Tools entspricht.

- **Legen Sie fest, welche sicheren Protokolle verwendet werden sollen und über welche Pfade auf Sitzungsmanager und Ziele zugegriffen werden darf.**
  - **Nutzen Sie für Verbindungen HTTPS statt RDP.**
  - **Nutzen Sie gegebenenfalls einen Reverse-Listener, damit die Netzwerkzugriffslisten übersichtlich bleiben und nur ausgehender Datenverkehr zugelassen wird.**
  - **Erstellen Sie ein Modell für Anmeldedaten und Zugriffsebenen.**
- **Stellen Sie sicher, dass Drittanbieter mit zuverlässigen Authentifizierungsmechanismen geschützt werden und die Autorisierungsfunktionen korrekt implementiert wurden.**
- **Vergewissern Sie sich, dass Drittanbieter eine sichere Verbindungsmethode nutzen.**
- **Identifizieren Sie Zugriffspfade:**
  - **Ermitteln von Pfaden über interne und öffentliche Netzwerke**
  - **Bereinigen der Quellsysteme**
  - **Einrichten zuverlässiger Zugriffsebenen**
  - **Einrichten von Schutzfunktionen für Anmeldedaten**
  - **Testen der Zugriffspfade**

05

Implementierung von Protokollierungsprozessen mit einer angemessenen Aufbewahrung

Mithilfe von Protokollierungs- und Überwachungsprozessen lassen sich wichtige Informationen erfassen, die insbesondere nach einem Cyberangriff relevant sind. Damit können beispielsweise das Ausmaß und die Folgen eines Cybersicherheitsvorfalls besser bestimmt werden. Für Forensiker sind Logdateien besonders nützlich. Sie analysieren beispielsweise Firewall- oder NetFlow-Logdateien, um festzustellen, ob Daten ausgeschleust wurden. Anhand der Informationen in den Dateien lassen sich dann viele Fragen zur Ausschleusung beantworten und feststellen, wie viele Daten gestohlen wurden. Ein weiteres Beispiel ist die Nachverfolgung von Benutzeraktivitäten. Wenn ein privilegiertes Konto manipuliert wurde, lassen sich die Aktivitäten dieses Benutzers anhand der Logdateien ermitteln.

Empfohlene Maßnahmen

- Implementieren Sie eine Lösung für die Protokollierung und Überwachung der Aktivitäten privilegierter Konten im Unternehmen.
- Sorgen Sie für eine angemessene Aufbewahrung der Logdateien: Legen Sie eine Protokollierungs- und Überwachungsrichtlinie fest, in der die zu erfassenden Aktivitäten und die Aufbewahrungsvorgaben für die Logdateien angegeben sind.
- Vergewissern Sie sich, dass die Logdateien an die korrekten Systeme gesendet werden und dass sie zur Verbesserung der Abwehrfunktionen im Unternehmen verwendet werden. Sicherheitsteams können Bedrohungsanalysen nutzen, um die vorhandenen Sicherheitsmaßnahmen zu verbessern und um zu erkennen, ob Angreifer in die Umgebung eingedrungen sind.
- Suchen Sie nach Anomalien bei den Benutzeraktivitäten, einschließlich des Systemzugriffs.
- Legen Sie fest, welche Maßnahmen bei einem Sicherheitsvorfall ergriffen werden. Erstellen Sie einen Plan für die Überprüfung der Audit-Logdateien und -Daten, wenn diese nicht in einem SIEM-Tool aufbewahrt werden.

06

Implementierung der Multi-Faktor-Authentifizierung (MFA)

Mit der Multi-Faktor-Authentifizierung (MFA) lassen sich digitale Identitäten prüfen und der sichere Zugriff eines Benutzers oder einer Entität auf ein System sicherstellen.

MFA erfordert mehrere Authentifizierungsfaktoren von Benutzern, um den Zugriff auf eine Anwendung zu gewähren. Zwei der häufigsten MFA-Methoden sind Einmalpasswörter (One-Time Passcodes, OTP) und Push-Benachrichtigungen. Einmalpasswörter sind Codes, die Benutzer von MFA-Anwendungen (z. B. Google Authenticator) auf ihren Mobilgeräten empfangen und dann zur Authentifizierung eingeben. Push-Benachrichtigungen sind Benachrichtigungen, die an das Mobilgerät eines Benutzers gesendet werden, damit er den Anmeldeversuch bestätigen oder ablehnen kann.

Beide Methoden sind anfällig für Phishing-Versuche und Man-in-the-Middle-Angriffe. Wie Angriffe in der letzten Zeit gezeigt haben, bieten MFA-Push-Benachrichtigungen oder per SMS übermittelte Codes keinen ausreichenden Zugriffsschutz. Bei einem MFA-Fatigue-Angriff[22] senden Angreifer beispielsweise einem Benutzer zahlreiche Push-Benachrichtigungen und hoffen, dass er irgendwann genervt die Anfrage bestätigt.

Empfohlene Maßnahmen

- Implementieren Sie eine starke MFA-Methode, die nicht durch Phishing-Versuche ausgenutzt werden kann.
  - FIDO2-Authentifizierung mit biometrischen Daten oder Hardwareschlüsseln (z. B. YubiKey)
  - Challenge-Response-Verfahren, sodass eine reine Bestätigung nicht ausreicht (Nummernabgleich)
- Bieten Sie allen Mitarbeitern Schulungen an, damit sie wissen, wie die MFA korrekt genutzt wird.
- Richten Sie Warnmeldungen und risikobasierte Tags für Konten ein, die potenziell angegriffen werden:
  - Geografischer Standort
  - Ungewöhnliche Zugriffszeiten
  - Übermäßig viele Challenge-Response-Anfragen für die MFA
- Prüfen Sie das Sicherheitsniveau der verwendeten Authentifizierungsanwendung.
- Führen Sie eine Bedrohungssuche für diese Identitäten durch.

22. Mandiant, „Suspected Russian Activity Targeting Government and Business Entities Around the Globe", Dezember 2021

Fazit

Da immer mehr Unternehmen zur Verbesserung ihres Sicherheitsniveaus auf PAM-Lösungen setzen, muss sichergestellt werden, dass diese auch korrekt konfiguriert und implementiert werden. Fehlkonfigurationen, unzureichendes Zugriffsmanagement und die Missachtung integrierter Sicherheitsfunktionen zählen zu den größten Problemen, die Unternehmen ein falsches Sicherheitsgefühl vermitteln und in einigen Fällen sogar das Risiko steigern.

Weitere Informationen finden Sie unter www.mandiant.de

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
Virginia 20190, USA
+1 703 935 8012
+1 833 3MANDIANT (362 6342)
info@mandiant.com

Über Mandiant

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

MANDIANT
NOW PART OF Google Cloud