Sicher durch die Cyberlandschaft – ein Leitfaden:

Wie Sie auf moderne Cyberbedrohungen reagieren

Die digitale Welt ist zu einer tückischen Wildnis geworden, in der jeder Klick, jeder Download oder jede Anmeldung eine versteckte Cyberfalle auslösen kann.

Die Cyberlandschaft von heute ist gefährlicher denn je. Bedrohungen wie Ransomware, DDoS-Angriffe, Phishing-Betrug und Backup-Infiltrationen werden immer weiter entwickelt. HackerInnen nutzen nun KI, um traditionelle Verteidigungsmethoden zu überlisten, und verwandeln das, was einst opportunistische Angriffe waren, in kalkulierte und anhaltende Bedrohungen, die in der Lage sind, weitreichenden Schaden anzurichten.

Dell Kunden berichten von alarmierenden KI-gesteuerten Angriffen, bei denen HackerInnen soziale Medien durchforsten, um überzeugende Nachrichten zu verfassen, die selbst die cyberbewusstesten MitarbeiterInnen täuschen können.

Diese Berichte erinnern daran, wie AngreiferInnen fortschrittliche Technologien nutzen, um Unternehmen mit beispielloser Genauigkeit zu manipulieren, zu täuschen und zu infiltrieren.

Um in dieser feindlichen Umgebung zu bestehen, benötigen Unternehmen eine umfassende Cybersicherheitsstrategie – ein Überlebenspaket, das fortschrittliche Tools, proaktive Strategien und eine Kultur der Wachsamkeit kombiniert. In diesem Leitfaden werden die Bestandteile einer solchen Strategie analysiert. Das hilft Unternehmen dabei, sich gegen die dringendsten Cyberbedrohungen von heute abzusichern.

Der Weg zum Schutz Ihres Unternehmens: ein Zero-Trust-Framework

In der heutigen KI-gesteuerten Bedrohungslandschaft ist die Einführung eines Zero-Trust-Frameworks nicht mehr optional. AngreiferInnen nutzen KI, um die Aufklärung zu automatisieren, Zugangsdaten zu stehlen und ihre Techniken schnell anzupassen. Herkömmliche Abwehrmaßnahmen greifen daher nicht mehr ausreichend. Zero Trust basiert auf dem Grundsatz der „Annahme einer Sicherheitsverletzung“, wobei jede Zugriffsanfrage kontinuierlich überprüft und strenge Authentifizierungsprozesse implementiert werden, um Risiken zu minimieren.

Durch das proaktive Monitoring von NutzerInnen, Geräten und Anwendungen reduziert Zero Trust die Wahrscheinlichkeit, dass unbefugter Zugriff und Datenschutzverletzungen stattfinden. Es handelt sich um einen modernen, einheitlichen Ansatz für das Identitätsmanagement.

Alles gut gesichert: Angriffsfläche reduzieren

Die Reduzierung der Angriffsfläche ist für die Abwehr KI-gesteuerter Bedrohungen von entscheidender Bedeutung, da Endpunkte, APIs und Sicherheitslücken in der Lieferkette häufig von AngreiferInnen ausgenutzt werden. Endpunkte und APIs dienen als Einstiegspunkte in Netzwerke und werden häufig zum Einschleusen von Malware oder zum Diebstahl sensibler Daten genutzt.

Die Sicherung dieser Bereiche erfordert eine mehrschichtige Verteidigungsstrategie. Achten Sie auf starke Authentifizierung und Datenverschlüsselung während der Übertragung, führen Sie regelmäßig Sicherheitslückentests durch, nutzen Sie Endpoint Detection and Response-Tools (EDR) sowie Patch-Management und sichern Sie Ihre Geräte ab. Lösungen für das Endpunktmonitoring und die kontinuierliche Bedrohungserkennung helfen dabei, bösartige Aktivitäten in Echtzeit zu erkennen und zu blockieren.

Unternehmen müssen proaktive Strategien einführen, um ihre Softwarelieferketten und ihren Entwicklungslebenszyklus zu sichern. Durch die Vergabe von Zugriffsrechten nach dem Least-Privilege-Prinzip wird sichergestellt, dass nur autorisierte BenutzerInnen und Anwendungen mit kritischen Systemen interagieren können, während die automatisierte Bedrohungserkennung und -abwehr Schwachstellen schnell beheben kann, sobald sie auftreten.

Erfahrung nutzen: proaktive Bedrohungserkennung und -abwehr

KI-gestützte Angriffe nutzen Sicherheitslücken aus, ahmen legitimes Verhalten nach und passen sich dynamisch an, um Sicherheitsmaßnahmen zu umgehen. Damit sind sie schwer zu erkennen. Um diese ausgeklügelten Bedrohungen zu bekämpfen, dürfen Unternehmen nicht mehr in der reaktiven Position verharren – fortschrittliche Bedrohungserkennungssysteme und hohe Reaktionskapazität sind gefragt. Durch die Nutzung von KI und maschinellem Lernen können Sicherheitsteams Verhaltensmuster analysieren, Anomalien erkennen und in Echtzeit auf Bedrohungen reagieren, um Probleme zu beheben, bevor erhebliche Schäden auftreten.

Effektive Erkennungs- und Reaktionssysteme müssen riesige Mengen an Betriebsdaten aufnehmen, damit sie Risiken erkennen und automatisierte Reaktionen auslösen können. Diese Threat Intelligence baut auch auf sich selbst auf. Dadurch wird das System intelligenter und in die Lage versetzt, neue Taktiken von AngreiferInnen proaktiv zu identifizieren und zu bekämpfen.

Übung macht den Meister: Incident Response and Recovery

Zwar ist das Verhindern von Angriffen ein erster Schritt, doch kann stets ein Angriff gelingen und Unternehmen müssen darauf gefasst sein. Ziel ist es, den Angriff mit minimalem Schaden zu überstehen. Eine effektive Strategie umfasst zwei Teile:

- einen soliden Plan für die Incident Response and Recovery (IRR).
- Technologiemaßnahmen, die auf das Sichern kritischer Daten und Anwendungen ausgerichtet sind.

Ein Incident-Recovery-Plan sollte umfassend sein. Da ein umfassender Angriff wahrscheinlich den Betrieb des Unternehmens stark oder gar vollkommen beeinträchtigen wird, sollten im Plan entsprechende Maßnahmen für den Fall eines Cyber-Incidents für sämtliche Abteilungen des Unternehmens enthalten sein. Der Plan sollte darlegen, wie das Unternehmen dann intern und extern kommuniziert. Vorgefertigte Kommunikationsvorlagen sollten abrufbar sein. Der Plan muss regelmäßig aktualisiert und gepflegt werden. Und schließlich kann der Plan nur gut wirken, wenn seine Anwendung geübt wird. Wenn der Angriff stattfindet, müssen alle instinktiv bereit sein, zu handeln.

Aus technologischer Sicht sollten Unternehmen zunächst festlegen, wie ein **Minimum Viable Company**-Betrieb (MVC) aussieht: Welche Systeme MÜSSEN betriebsbereit bleiben, auch wenn dies bedeutet, dass Papier und Bleistift zum Einsatz kommen müssen? Ist es wichtig, dass der Vertrieb weiterhin arbeiten kann? Wie sieht es mit dem Kundendienst aus?

Sobald diese Fragen beantwortet sind, sollten die Backup- und Recovery-Mechanismen um die Antworten herum aufgebaut werden. Die Möglichkeit, auf schadfreie Daten zurückzugreifen, ermöglicht es dem Unternehmen nicht nur, den Betrieb schnell wieder aufzunehmen, sondern nimmt auch böswilligen Akteuren, die versuchen, Ihre Daten als Geiseln zu nehmen, den Hebel aus der Hand. Außerdem müssen moderne IR-Strategien über traditionelle Ansätze hinausgehen und KI-/LLM-Systeme wie Chatbots und virtuelle Agenten als Tier-1-Assets mit derselben Recovery-Priorität wie Zahlungssysteme oder Kundendaten behandeln.

Um Advanced Threats entgegenzuwirken, sollten IR-Pläne ein Gleichgewicht zwischen Automatisierung und manueller Überprüfung herstellen. Es ist wichtig zu wissen, wie Ihr Unternehmen im Falle eines Totalausfalls den Betrieb aufrecht erhalten kann. Was ist, wenn Sie zu Stift und Papier greifen müssen?

Jeder muss mithelfen: Sensibilisierung der MitarbeiterInnen

Ihre MitarbeiterInnen sind Ihre erste Verteidigungslinie gegen Cyberbedrohungen, ähnlich wie ein Team, das beim Überlebenskampf in der Wildnis Gefahren bewältigt. Jedes Mitglied spielt eine wichtige Rolle bei der Identifizierung von Risiken und beim Schutz von Ressourcen. Um diese Verteidigung zu stärken, benötigen Unternehmen robuste Sensibilisierungsprogramme, beispielsweise Angriffssimulationen, die KI-spezifische Bedrohungen wie fortgeschrittenes Phishing und Deepfakes vorspielen.

Die besten Programme kombinieren fortlaufende Schulungen, offene Kommunikation, reale Simulationen und eine Kultur der gemeinsamen Verantwortlichkeit. Wenn alle, vom Frontpersonal bis zur Führungsetage, sowohl mit traditionellen als auch KI-gesteuerten Bedrohungen vertraut sind, wird das Unternehmen zu einer wachsamen, gut informierten Einheit. Durch die Förderung von Teamarbeit und Vorbereitung kann Ihr Unternehmen den sich entwickelnden Cyberrisiken einen Schritt voraus sein und eine resiliente Verteidigung gegen potenzielle Angriffe aufbauen.

Best Practices für Resilienz gegenüber KI-gesteuerten Angriffen

Um gegen KI-gesteuerte Angriffe resilient zu bleiben, müssen Unternehmen einen proaktiven und strategischen Ansatz verfolgen. Hier sind 10 Best Practices:

Zero-Trust-Architektur

Sorgen Sie für kontinuierliche Verifizierung, strenge Zugriffskontrollen und Netzwerksegmentierung, um sicherzustellen, dass alle NutzerInnen und Geräte authentifiziert werden, bevor sie Zugriff erhalten. Das hilft, schnelle, KI-gesteuerte Angriffe zu blockieren und einzudämmen.

Stärkung des Identitäts- und Zugriffsmanagements:

Nutzen Sie robuste Authentifizierungsverfahren (MFA, RBAC) und setzen Sie strenge Richtlinien für Anmeldedaten durch, um Phishing und Credential Stuffing zu reduzieren.

Automatisierte Erkennung und Bestandsaufnahme für Assets:

Erfassen und überwachen Sie kontinuierlich alle Assets, einschließlich Cloud, IoT und Schatten-IT, um versteckte Risiken zu vermeiden.

Mikrosegmentierung und Netzwerkzugriffskontrollen:

Segmentieren und isolieren Sie Netzwerke und Workloads, um laterale Angriffsbewegungen zu verhindern und Bedrohungen einzudämmen.

Endpunkt- und API-Absicherung:

Verwenden Sie erweiterten Endpunktschutz (EDR/XDR) und sichere API-Gateways, starke Authentifizierung, Ratenbegrenzung, Eingabevalidierung und Verschlüsselung.

Rigoroses Schwachstellen- und Patch-Management:

Automatisieren Sie das Scannen und schnelle Patchen von Betriebssystemen, Firmware, Anwendungen, APIs und Software von Drittanbietern.

KI-gesteuerte Erkennung und Überwachung von Bedrohungen:

Nutzen Sie die KI/ML-gestützte Verhaltens- und Anomalieerkennung, um subtile oder automatisierte Bedrohungen in Echtzeit zu entlarven.

Automatisierte Incident Response:

Verwenden Sie automatisierte Playbooks, um Bedrohungen schnell zu isolieren, einzudämmen und zu beheben und so die Verweildauer der AngreiferInnen zu minimieren.

Regelmäßige realistische Simulationen und kontinuierliche Verbesserung:

Führen Sie theoretische Übungen, Red-Teaming-Aktivitäten und Phishing-Simulationen durch; stützen Sie sich bei der Aktualisierung von IR-Plänen und Erkennungsmodellen auf die entsprechenden Ergebnisse.

Unveränderliche Air-Gap-Backups und Recovery:

Erstellen Sie manipulationssichere Backups – idealerweise mit Air Gap und regelmäßiger Überprüfung –, um eine saubere, schnelle Wiederherstellung zu ermöglichen.

DELL Technologies

Dell Technologies: Ihr Wegweiser durch unbekanntes Terrain

Um Ihr Unternehmen vor hochentwickelten Cyberbedrohungen zu schützen, benötigen Sie die richtigen Tools und Fachkenntnisse, mit denen Sie den sich ständig weiterentwickelnden Risiken immer einen Schritt voraus bleiben. In der komplexen Cybersicherheitslandschaft von heute ist eine robuste Strategie unerlässlich, um Ihre Daten, Systeme und Ihren Ruf zu schützen. Hier kommt Dell Technologies ins Spiel und bietet eine umfassende Suite an Lösungen, die auf die Anforderungen von Unternehmen jeder Größe zugeschnitten sind.

Von einer Sicherung der Lieferkette über erweiterte Bedrohungserkennung und Endpunktschutz bis hin zu sicherem Datenmanagement – Dell stattet Ihr Unternehmen mit der Technologie aus, die für den Schutz vor modernen Cyberangriffen erforderlich ist. Unterstützt durch branchenführendes Fachwissen arbeitet das Team von Dell eng mit Ihnen zusammen, um eine Sicherheitsstrategie zu entwickeln, die genau auf Sie zugeschnitten ist. Mit Funktionen wie Echtzeitmonitoring, automatisierter Reaktion auf Bedrohungen und Zero-Trust-Architektur trägt Dell dazu bei, dass Ihr Unternehmen proaktiv und resilient bleibt.

Ganz gleich, ob Sie sich mit Ransomware, Phishing-Angriffen oder der Einhaltung gesetzlicher Vorschriften befassen – Dell Technologies unterstützt Sie dabei, sich sicher in der heutigen Bedrohungslandschaft zu bewegen. Arbeiten Sie mit Dell zusammen, um Ihr Unternehmen zu schützen und im digitalen Zeitalter erfolgreich zu sein, um sicherzustellen, dass Ihr Betrieb sicher, effizient und für alles gerüstet ist, was als Nächstes kommt.

> „Ihr Incident-Response-Plan muss auf Papier gedruckt werden, da Ihre Systeme während eines Angriffs möglicherweise nicht zugänglich sind.“
>
> ***Rachel Tyler***
> *Cybersecurity Advisory Consultant, Dell Services*

Dell Produkte und Lösungen, die helfen können

Dell Lösung	Beschreibung
Dell Trusted Infrastructure	Eine Kombination aus Dell Servern, Netzwerken, Storage-Lösungen und Lösungen für die Ausfallsicherheit bei Cyberangriffen, die zusammen eine moderne, sichere und widerstandsfähige Grundlage für Innovationen schaffen.
Ausfallsicherheit bei Cyberangriffen	Ein umfassendes Lösungsportfolio, das darauf abzielt, Ihre Daten zu schützen und eine sichere Wiederherstellung zu gewährleisten. Umfasst Hardware, Software und As-a-Service-Angebote.
Cybersicherheitsservices	Eine Reihe von Services, die Sie bei der Entwicklung und Implementierung einer umfassenden Sicherheitsstrategie für alle Workloads unterstützen können. Das Angebot umfasst Beratungsdienste, vCISO, Managed Detection and Response, Penetrations- und Sicherheitslückentests sowie Incident Response and Recovery.
Dell Trusted Workspace (Endpunktsicherheit)	Eine Kombination aus integrierten und optionalen Zusatzfunktionen zum Schutz von PCs. Die integrierten Funktionen basieren auf sicheren Lieferkettenpraktiken und umfassen SafeBIOS und SafeID mit TPM. Zu den optionalen Zusatzfunktionen gehören SecureD Component Verification, SafeID mit ControlVault sowie die Partnersoftware CrowdStrike und Absolute, um die Sicherheit am Arbeitsplatz zu maximieren.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth.**