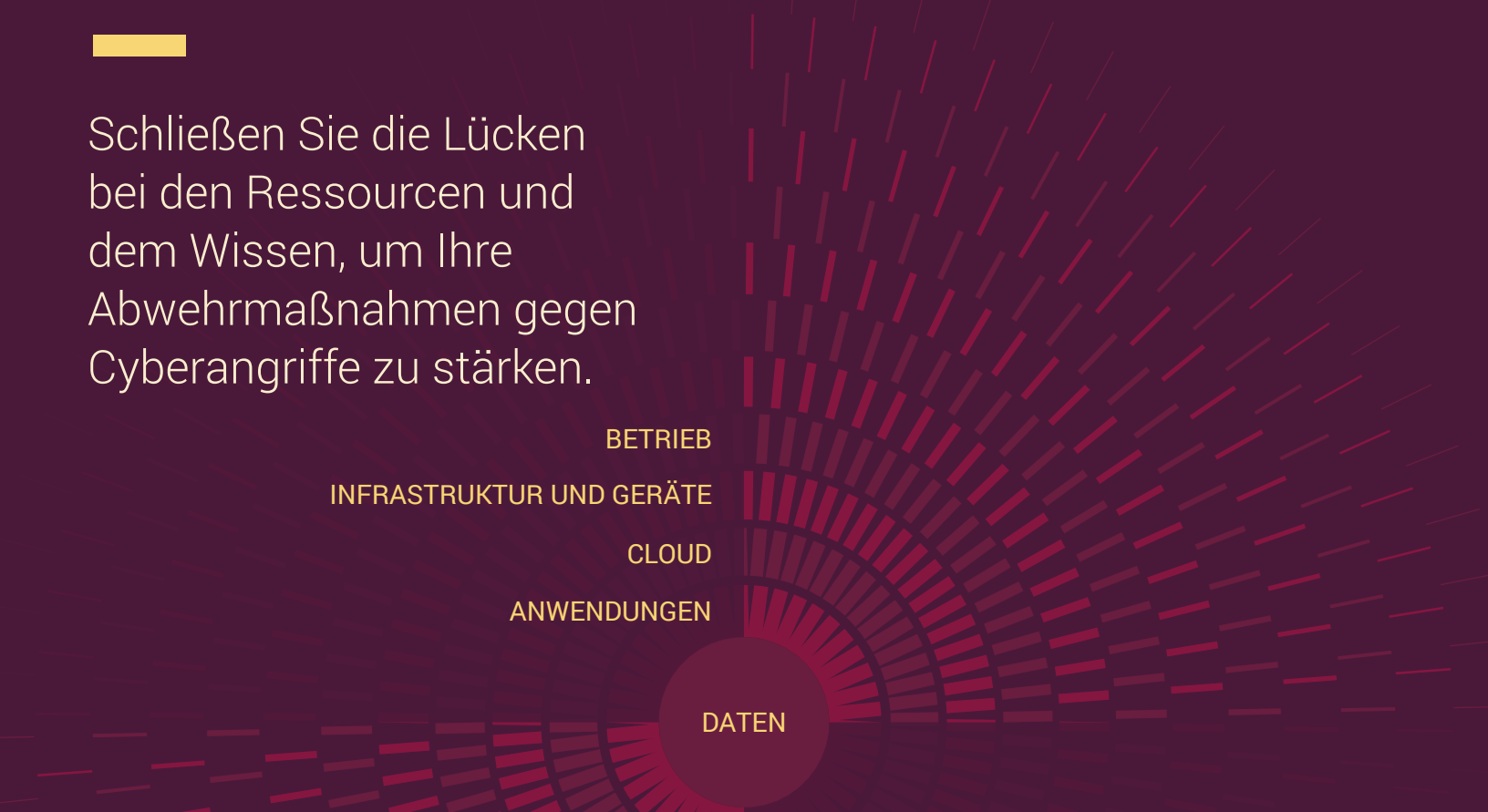
DELL Technologies

Verbesserung Ihrer Cybersicherheit und des Zero-Trust-Reifegrads

Schließen Sie die Lücken bei den Ressourcen und dem Wissen, um Ihre Abwehrmaßnahmen gegen Cyberangriffe zu stärken.



Die sich schnell weiterentwickelnden Bedrohungen von heute, insbesondere mit dem Aufkommen von GenAI, stellen selbst die erfahrensten ExpertInnen für Cybersicherheit vor neue und unerwartete Herausforderungen. Erfahren Sie, wie Sie durch die Zusammenarbeit mit erfahrenen SicherheitsexpertInnen Cyberangriffe vermeiden und robuste Sicherheitspraktiken aufrechterhalten können.

Cyberbedrohungen sind wie Ameisen bei einem Picknick

Man kümmert sich um die eine. Dann kommt schon die nächste.

In einer zunehmend vernetzten Welt, in der Unternehmen in hohem Maße auf digitale Infrastrukturen angewiesen sind und Daten zu einer weitreichenden Ware geworden sind, sollten Sie davon ausgehen, dass raffinierte AngreiferInnen bereits in Ihre IT-Umgebung eingedrungen sind.

Die gute Nachricht ist, dass es erfahrene Partner gibt, die sich auf die Schnittstelle von Technologie und Cybersicherheit spezialisiert haben.

Dell Technologies bietet innovative Lösungen und wertvolles Fachwissen, das im eigenen Unternehmen möglicherweise nicht zur Verfügung steht, um Sie bei der Navigation in der sich ständig weiterentwickelnden Bedrohungslandschaft zu unterstützen.

- Hardware- und Softwaresicherheit
- Einblicke in neue Risiken
- Verständnis fortschrittlicher Angriffstechniken
- AIOps zur Bewältigung sich schnell entwickelnder Bedrohungen
- Neue Sicherheitsstrategien und Best Practices

Bauen Sie Abwehrebenen auf, die die Sicherheitspraktiken kontinuierlich verbessern, und setzen Sie auf einen Zero-Trust-Ansatz.

Dell Technologies ist ein Partner für Cybersicherheit, der umfassende Dienstleistungen, Hardware- und Softwarelösungen sowie ein robustes Partnernetzwerk bereitstellt, das die Angriffsmöglichkeiten einschränkt, Sicherheitslücken identifiziert und minimiert und Ihnen hilft, den Geschäftsbetrieb schnell wiederherzustellen.

Verringerung der Angriffsfläche →

Erkennung von und Reaktion auf Cyberbedrohungen →

Schnelle Recovery nach einem Angriff →

Edge **Core** **Multi-Cloud**

Dienstleistungen

Business-/Technologiepartnernetzwerk **Sichere Lieferkette**

DELL Technologies

Verringerung der Angriffsfläche

Verstärken Sie Ihre Abwehrmaßnahmen und machen Sie sich selbst zu einem kleineren Ziel, indem Sie die Möglichkeiten reduzieren, die Cyberkriminelle gerne ausnutzen.

Um Ihren Sicherheitsstatus zu verbessern, müssen Sie Sicherheitslücken und Eintrittspunkte identifizieren und minimieren, die Anwendungen, Systeme oder Netzwerke in verschiedenen Bereichen, einschließlich Edge, Core und Cloud, gefährden können.

IDENTIFIZIEREN von Sicherheitslücken

- Softwaresicherheitslücken
- Fehlkonfigurationen
- Schwache Authentifizierungsmechanismen
- Ungepatchte Systeme
- Übermäßige Nutzerberechtigungen
- Offene Netzwerkanschlüsse
- Mangelhafte physische Sicherheit

IMPLEMENTIEREN präventiver Maßnahmen

- Zusammenarbeit mit sicheren Lieferanten
- Anwendung umfassender Netzwerksegmentierung
- Isolieren kritischer Daten
- Durchsetzung strenger Zugriffskontrollen
- Aktualisieren und Patchen von Systemen und Anwendungen
- Identifizieren und Beheben von Sicherheitslücken mithilfe von KI, regelmäßigen Bewertungen und Tests

Verfolgen eines Zero-Trust-Ansatzes

Eine Zero-Trust-Architektur bedeutet, dass Ihr Unternehmen nicht automatisch allem vertraut, was sich innerhalb oder außerhalb seiner Grenzen befindet. Stattdessen werden alle Instanzen, die versuchen, eine Verbindung zu Ihren Systemen herzustellen, überprüft, bevor der Zugriff gewährt wird. Es handelt sich dabei um ein vom US-Verteidigungsministerium entwickeltes und vorgeschriebenes Modell, das **7 miteinander verknüpfte Säulen** umfasst, die systematisch einen Reifegrad aufbauen.

1. Vertrauensstellung bei NutzerInnen
2. Vertrauensstellung bei Geräten
3. Vertrauensstellung bei Daten
4. Anwendung und Workload
5. Netzwerk und Umgebung
6. Transparenz und Analysen
7. Automatisierung und Orchestrierung

DELL Technologies

Verringerung der Angriffsfläche

Identifizieren Sie die Schwachstellen, die Ihre Systeme gefährden, bevor Probleme auftreten.

Cybersicherheit ist keine einmalige Aufgabe, sondern ein fortlaufender Prozess. Regelmäßige Audits, Penetrationstests und Sicherheitslückenbewertungen können mit Hilfe eines erfahrenen Partners für Sicherheitsservices dazu beitragen, Lücken zu erkennen und zu schließen, um Risiken zu verringern.

Sichere Lieferketten-praktiken

Sicherheit beginnt früher als Sie denken. Schaffen Sie eine vertrauenswürdige Grundlage mit Geräten und Infrastrukturen, die unter Verwendung einer sicheren Lieferkette, eines sicheren Entwicklungslebenszyklus und einer strengen Bedrohungsmodellierung entwickelt, hergestellt und bereitgestellt werden.

Integrierte Sicherheit

Arbeiten Sie mit Geräten und Infrastrukturen, die über integrierte, hardwarebasierte Sicherheitsfunktionen verfügen, um Angriffe zu erkennen und abzuwehren, bevor sie Schaden anrichten.

Regelmäßige Patchings und Updates

Beheben Sie bekannte Sicherheitslücken und minimieren Sie das Risiko einer Ausnutzung, indem Sie Anwendungen, Firmware und Betriebssysteme mit den aktuellen Sicherheitspatches auf dem neuesten Stand halten.

Geringste Berechtigungen

Beschränken Sie Nutzer- und Systemkonten auf die minimalen Zugriffsrechte, die für die Ausführung ihrer Aufgaben erforderlich sind. Dieser Ansatz begrenzt die potenziellen Auswirkungen von AngreiferInnen, die sich unbefugten Zugriff verschafft.

Netzwerk-segmentierung

Isolieren Sie kritische Ressourcen, um den Netzwerkzugriff zu begrenzen, indem Sie eine moderne Netzwerksegmentierung für kritische Daten, Geschäftsgruppen und Anwendungen verwenden. Dadurch wird ein Angriff eingedämmt, indem Seitwärtsbewegungen verhindert werden.

Anwendungs-sicherheit

Implementieren Sie sichere Codierungspraktiken, führen Sie regelmäßige Sicherheitstests und Codeüberprüfungen durch und verwenden Sie Web Application Firewalls (WAFs), um sich gegen gängige Angriffe auf Anwendungsebene zu schützen und die Angriffsfläche von Webanwendungen zu verringern.

Dienstleistungen und Partnerschaften

Arbeiten Sie mit Serviceanbietern für Cybersicherheit zusammen und bilden Sie Partnerschaften mit Business- und Technologiepartnern, um Fachwissen und Lösungen einzubringen, die intern möglicherweise nicht verfügbar sind.

Nutzerschulung und -sensibilisierung

Schulen Sie MitarbeiterInnen und NutzerInnen darin, potenzielle Sicherheitsbedrohungen, Phishing-Versuche und Social-Engineering-Taktiken zu erkennen und zu melden, um die Risiken zu minimieren, die menschliche Sicherheitslücken ausnutzen.

DELL Technologies

Erkennung von und Reaktion auf Cyberbedrohungen

Althergebrachte Sicherheitspraktiken sind wie ein Einwahl-Internetanschluss: zu langsam und ineffektiv in der anspruchsvollen Umgebung von heute.

Um ausgefeilte Cyberbedrohungen zu bekämpfen, benötigen Sie bessere Sicherheitstricks wie KI und ML, die in Anwendungen und Methodiken integriert sind, die Bekanntes und Unbekanntes erkennen und darauf reagieren.

Implementieren leistungsstarker Systeme für die Erkennung und Abwehr von Angriffen

Nutzung von KI und ML für die Erkennung von Anomalien

Einrichten des Echtzeitmonitorings von Netzwerkverkehr und Nutzerverhalten

Erhöhen Sie die Ausfallsicherheit, indem Sie mit erfahrenen Dienstleistungen zusammenarbeiten, um spezielles Fachwissen zu erwerben.

Als erfahrener Technologiepartner kann Dell Technologies Ihnen dabei helfen, proaktive Protokolle für die Incident Response und die Recovery zu erstellen, die die Rollen und Verantwortlichkeiten festlegen und eine nahtlose Kommunikation und Koordination zwischen den Beteiligten gewährleisten.

Verbessern Sie Ihre Fähigkeit, Cyberbedrohungen proaktiv zu erkennen und darauf zu reagieren, indem Sie folgende fortschrittliche Technologien einsetzen:

- Threat Intelligence
- Incident Response
- Verwaltung von Sicherheitsinformationen und -ereignissen (Security Information und Event Management)
- Endpunktschutz
- Verhaltensanalysen

Erleichtern Sie eine effiziente, rasche Recovery und minimieren Sie Datenverluste mit Folgendem:

- Klar definierter Plan für Incident Response und Zusammenarbeit
- Regelmäßige Backups kritischer Daten und Systeme
- Sichere externe Storage-Lösungen und Datenverschlüsselung

DELL Technologies

Erkennung von und Reaktion auf Cyberbedrohungen

Seien Sie wachsam und ergreifen Sie schnell Maßnahmen.

Sie müssen wachsam bleiben und für den schlimmsten Fall planen, um Cyberbedrohungen zu erkennen und auf sie zu reagieren. Erstellen Sie einen Reaktions- und Recovery-Plan, der kontinuierlich aktualisiert und routinemäßig geübt wird, damit Ihr gesamtes Unternehmen weiß, wie die Auswirkungen eines Angriffs verringert werden können. Es handelt sich um einen fortlaufenden und sich wiederholenden Prozess, der eine Kombination aus Technologie, qualifiziertem Personal, klar definierten Prozessen und Teamzusammenarbeit erfordert.

Kontinuierliches Monitoring

Sicherheitstools wie Systeme zur Erkennung von Angriffen (Intrusion Detection Systems, IDS), Systeme zur Verhinderung von Angriffen (Intrusion Prevention Systems, IPS), Protokollanalyse und Threat Intelligence helfen bei der Erkennung von Anzeichen für unbefugte Zugriffe, Angriffe, Malware-Infektionen und Datenschutzverletzungen.

Bedrohungserkennung

Nutzen Sie die Vorteile von KI und ML zur Analyse von Daten, um Muster, Anomalien und Kompromittierungsindikatoren (Indicators of Compromise, IoCs) zu erkennen, die auf eine Bedrohung hindeuten können. Dazu gehören die Erkennung bekannter Angriffssignaturen und die Identifizierung von abweichendem Verhalten.

Alarmierung und Benachrichtigung

Stellen Sie frühzeitige Warnungen für schnelle Ermittlungen und Reaktionen bereit. Sorgen Sie dafür, dass Warnmeldungen und Benachrichtigungen sofort sichtbar sind, um mit integrierter Sicherheit schnell handeln zu können. Übermitteln Sie Telemetriedaten auf Geräteebene oberhalb des Betriebssystems, um die Erkennung von Bedrohungen zu beschleunigen und Sicherheitspersonal oder ein Security Operations Center (SOC) einzuschalten, wenn potenzielle Bedrohungen oder Incidents erkannt werden.

Incident Response

Initiieren Sie einen Reaktionsplan, um bestätigte Sicherheits-Incidents zu untersuchen und abzuschwächen. Dazu gehören die Eindämmung der Auswirkungen, die Ermittlung der Ursache und die Durchführung der erforderlichen Maßnahmen zur Wiederherstellung der Systeme und zur Vermeidung weiterer Schäden.

Forensische Analyse

Führen Sie eine detaillierte Analyse von Incidents durch, um die Angriffsmethodik zu verstehen, das Ausmaß der Sicherheitsverletzung zu bestimmen, betroffene Systeme oder Daten zu identifizieren und Beweise zu sammeln, um Sicherheitslücken aufzudecken und zu beheben.

Korrektur und Recovery

Ergreifen Sie Maßnahmen zur Behebung von Sicherheitslücken, zum Patchen von Systemen, zur Entfernung von Malware und zur Einführung verbesserter Sicherheitsmaßnahmen, um ähnliche Incidents zu verhindern. Stellen Sie die betroffenen Systeme und Daten wieder in den Normalzustand her, um den Wiederherstellungsprozess abzuschließen.

DELL Technologies

Recovery nach Cyberangriffen

Geben Sie Vollgas und bringen Sie Ihr Unternehmen wieder auf die Überholspur.

Ausfallsicherheit bei Cyberangriffen ist in der heutigen datengesteuerten Welt notwendig und wird von KundInnen und PartnerInnen gleichermaßen erwartet. Für den Erfolg sind mehrere Schutzebenen erforderlich, um sicherzustellen, dass kritische Daten geschützt und isoliert sind, damit sie nach einem Angriff schnell und sicher wiederhergestellt werden können. Bewertung Ihrer Ausfallsicherheit bei Cyberangriffen ›

- Ergreifen von Maßnahmen zur Minderung der Schäden, die durch einen Cyberangriff verursacht werden
- Wiederherstellung infizierter oder unterbrochener Services und Geräte
- Analyse des Incident zur Vermeidung zukünftiger Angriffe
- Erfüllung geschäftlicher SLAs und Rückkehr des Betriebs zum Normalzustand

Erstellen Sie eine umfassende Cybersicherheitsstrategie, damit Ihr Unternehmen effektiv und effizient die Recovery durchführen kann.

Die Recovery nach einem Cyberangriff erfordert eine koordinierte Anstrengung, an der IT-Teams, ExpertInnen für Cybersicherheit, das Management und manchmal auch externe ExpertInnen beteiligt sind. Der Schlüssel zur Recovery liegt darin, die Systeme und Abläufe schnell wieder zu normalisieren und gleichzeitig aus dem Incident zu lernen, um Unterbrechungen und Ausfallzeiten zu reduzieren, Services und die Datenintegrität wiederherzustellen, die finanziellen Auswirkungen und Rufschädigungen zu minimieren und die Cybersicherheit zu stärken, um ähnliche Angriffe in Zukunft zu verhindern.

- Bewertung der Auswirkungen eines Angriffs auf den Geschäftsbetrieb
- Priorisierung kritischer Services
- Bereitstellung von Data-Protection-Systemen
- Kommunikation über jeden Incident- und Recovery-Fortschritt
- Entwicklung eines Plans und umfassende Anwendung, um die Kontinuität sicherzustellen

DELL Technologies

Recovery nach Cyberangriffen

Bringen Sie Systeme, Netzwerke und Daten nach einem Incident wieder zum Laufen.

Eine Strategie zur Ausfallsicherheit bei Cyberangriffen umfasst Menschen, Prozesse und Technologien in einem ganzheitlichen Framework, das Ihr gesamtes Unternehmen schützt.

Eindämmung des Incidents

Der erste Schritt besteht darin, die Auswirkungen des Cyberangriffs zu isolieren und einzudämmen. Dazu gehört, die betroffenen Systeme vom Netzwerk zu trennen, die kompromittierten Konten zu deaktivieren und Maßnahmen zu ergreifen, um eine weitere Ausbreitung oder weiteren Schaden zu verhindern.

Wiederherstellung von Systemen oder Geräten

Sobald ein Incident eingedämmt ist, werden die betroffenen Systeme und Netzwerke in einen sauberen und sicheren Zustand wiederhergestellt. Dazu kann es erforderlich sein, kompromittierte Systeme erneut aufzubauen, Software neu zu installieren und Sicherheitspatches und -updates anzuwenden. Automatisierung und automatische Fehlerkorrektur können eine wichtige Rolle bei der Wiederherstellung der Betriebsbereitschaft spielen.

Daten-Recovery

Daten, die während des Angriffs möglicherweise kompromittiert, verschlüsselt oder gelöscht wurden, müssen wiederhergestellt werden. Dies kann die Wiederherstellung von Daten aus Backups oder die Anwendung spezieller Daten-Recovery-Techniken umfassen, um verlorene oder verschlüsselte Dateien wiederherzustellen.

Forensische Analyse

Nach einem Angriff ist es wichtig zu verstehen, wie es zu der Sicherheitsverletzung gekommen ist, welche Sicherheitslücken ausgenutzt wurden und welche Schritte unternommen werden können, um ähnliche Angriffe zu verhindern. Systeme wie Security Information and Event Management (SIEM) und Funktionen wie BIOS-Vergleiche unabhängig vom Host liefern nützliche Erkenntnisse.

Auswertung der Reaktion auf den Incident

Nach der Recovery ist es wichtig, den Reaktionsprozess auf einen Incident zu bewerten und Bereiche mit Verbesserungspotenzial zu ermitteln. Die aus dem Angriff gezogenen Lehren können genutzt werden, um die Sicherheitspraktiken zu verbessern, die Reaktionspläne auf Incidents zu aktualisieren und einen besseren Schutz vor künftigen Incidents sicherzustellen.

Dienstleistungen und Partnerschaften

Serviceanbieter für Cybersicherheit und Technologiepartner verfügen über wertvolle Fachkenntnisse und Ressourcen, um Ihr Unternehmen bei der Recovery zu unterstützen. Sie können bei Aufgaben wie der forensischen Analyse, der Identifizierung des Auftretens der Sicherheitsverletzung und der Empfehlung von Maßnahmen zur Vermeidung künftiger Incidents helfen.

DELL Technologies

Ausdehnung der Cybersicherheit auf Edge- und Cloud-Umgebungen

Mit der Ausbreitung von Netzwerken vom Core über den Edge bis zur Cloud sind die Umgebungen zu einer entscheidenden Sicherheitslücke geworden.

Im Zuge der Weiterentwicklung Ihrer Cybersicherheitsstrategie muss Ihr Unternehmen die Zero-Trust-Prinzipien auf Edge- und Cloud-Umgebungen ausdehnen, um strenge Zugriffskontrollen, kontinuierliche Authentifizierung sowie umfassende Transparenz und Kontrolle des Netzwerkverkehrs sicherzustellen. Da sich die Bedrohungslandschaft weiterentwickelt, ist es ratsam, KI-Funktionen als erste Verteidigungslinie einzusetzen. Darüber hinaus ist eine Strategie nur dann vollständig, wenn Ihr Kernnetzwerk und Ihre Cloud-Umgebungen über Sicherheitsmaßnahmen wie Netzwerksegmentierung, Verschlüsselung und kontinuierliches Monitoring verfügen.

Dienstleistungen für Cybersicherheit können Ihnen dabei helfen, einen ganzheitlichen Ansatz zu verfolgen.

Die Verknüpfung verschiedener Sicherheitslösungen kann eine Herausforderung darstellen. Durch die Zusammenarbeit mit Dienstleistungen, die auf Edge-, Core- und Cloud-Sicherheit spezialisiert sind, erhalten Sie das Fachwissen, um wirksame Maßnahmen zu ergreifen, die Ihr Unternehmen umfassend schützen.

Edge

Richten Sie mehrere Sicherheitsebenen am Edge, im Netzwerk und in der Hardware und Software ein.

Core

Richten Sie Ihre Infrastruktur mithilfe von KI, ML und Automatisierung auf einen Zero-Trust-Ansatz aus.

Multi-Cloud

Schützen Sie alle Workloads in jeder Umgebung, einschließlich Public Cloud, Containern und cloudnativen Workloads.

DELL Technologies

GenAI: Ein zweischneidiges Schwert für die Cybersicherheit

Die nächste Generation der KI bringt neue Risiken mit sich, sorgt aber auch für mehr Sicherheit.

Als nächste Phase der KI umfasst GenAI Systeme, die in der Lage sind, eine Vielzahl von Aufgaben zu verstehen, zu erlernen, sich anzupassen und Wissen umzusetzen.

Einerseits verspricht GenAI eine verbesserte Erkennung von und Reaktion auf Bedrohungen sowie Vorhersagefähigkeiten und Betriebseffizienz. Andererseits bringt sie neue Herausforderungen mit sich, die eine Weiterentwicklung der Cybersicherheitsstrategien erfordern, um Risiken durch robuste Sicherheitsmaßnahmen, kontinuierliches Monitoring, regelmäßige Updates und Patches sowie einen sich ständig weiterentwickelnden Ansatz für Datenschutz und Ethik zu begegnen.

Schutz von Unternehmen mit GenAI

GenAI hat sich zu einem wichtigen Verbündeten in der Cybersicherheit entwickelt und eröffnet neue Wege zum Schutz von Unternehmen.

- Verbesserung der Effizienz der Bedrohungserkennung und -abwehr
- Vorhersage zukünftiger Bedrohungen oder Identifizierung potenzieller Sicherheitslücken
- Automatisierung der Erkennung von Bedrohungen und mehr Effizienz
- Forensische Analyse zur schnellen Identifizierung von Mustern, Anomalien und Anzeichen für eine Gefährdung
- Personalisierte Schulung zur Sicherheitssensibilisierung
- Skalierung der Sicherheitsabläufe mit schnellerem Zugriff auf umfassendere Erkenntnisse

Schutz von GenAI-Systemen

Auch wenn GenAI erhebliche Sicherheitsvorteile bietet, kann ihre Funktionalität in böswilliger Absicht genutzt werden, wenn sie nicht angemessen gesichert wird.

- Sicherstellen des Datenschutzes und der Datenintegrität
- Minderung gegnerischer Angriffe, die darauf abzielen, KI-Systeme zu täuschen und Fehlfunktionen zu verursachen
- Erkennung von und Reaktion auf Systemmissbrauch durch bösartige KI
- Prüfung und Minderung ethischer Fragen und Vorurteile
- Implementierung von strengen Zugriffskontrollen für KI-Systeme
- Sicherer Schutz und Wiederherstellung großer Sprachmodelle (Large Language Model, LLM)

Moderne Cybersicherheit muss intelligent, skalierbar und automatisiert sein

Dell Technologies kann Sie dabei unterstützen, eine umfassende Sicherheit zu schaffen, die vor den sich weiterentwickelnden Cyberbedrohungen schützt. Mit dem technologischen Fortschritt ist unser Ansatz für die Cybersicherheit immer einen Schritt voraus. Wir nutzen die Leistungsfähigkeit von KI und ML, um Ihre digitalen Infrastrukturen zu schützen und das Vertrauen in die digitale Welt zu erhalten. Unabhängig davon, wo Sie sich auf Ihrem Weg zur Cybersicherheit befinden, arbeiten wir mit Ihnen zusammen, um Ihr Unternehmen nicht nur zu schützen, sondern auch agil und widerstandsfähig zu machen.

DELL Technologies

Dell.com/SecuritySolutions

Rückruf anfordern

Mit unseren SicherheitsberaterInnen chatten

Telefon: 1-800-433-2393