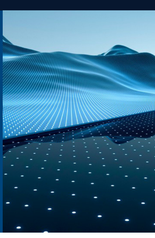
10 Empfehlungen für mehr Cybersicherheit

Die Technologie entwickelt sich rasant weiter. Mit der Einführung neuer Tools und Systeme, die unsere Möglichkeiten erweitern, schaffen wir gleichzeitig neue Angriffsflächen für Cyberbedrohungen, die Sicherheitslücken ausnutzen wollen. In einem solchen Umfeld ist es von entscheidender Bedeutung, robuste Cybersicherheitsmaßnahmen umzusetzen, die vor neuen Bedrohungen schützen und dafür sorgen, dass Innovationen in einer sicheren Umgebung gedeihen können. Für die Anpassung an die neuen Risiken in Unternehmen empfehlen Cybersicherheitsexpertinnen von Dell Technologies zehn grundlegende Maßnahmen, um Ihre Cybersicherheitsreife zu verbessern.

1 Bedrohungsrisikolandschaft analysieren



Erfahrene Partner für Cybersicherheit können wertvolles Fachwissen und Ressourcen bereitstellen, um die sich schnell entwickelnde Bedrohungslandschaft zu analysieren.

- Führen Sie gründliche Schwachstellenbewertungen und Penetrationstests durch, um potenzielle Schwachstellen zu identifizieren, die behoben werden müssen, und um mögliche Lücken in Ihrer Strategie zu identifizieren.
- Profitieren Sie von spezialisierten Fähigkeiten und Kenntnissen, die in Ihrem Unternehmen intern möglicherweise nicht verfügbar sind, z. B. Analysen neu auftretender Risiken und fortschrittlicher Angriffstechniken sowie die neuesten Sicherheitsstrategien und Best Practices.
- Definieren Sie Zugriffsberechtigungen und deren Begründungen, damit Sie ein geeignetes Sicherheits-Framework für die Implementierung Ihrer Unternehmenskontrollen und -governance einrichten können.

2 Legen Sie eine umfassende Cybersicherheitsstrategie fest.

Das Gewährleisten von Ausfallsicherheit bei Cyberangriffen erfordert eine koordinierte Anstrengung, an der IT-Teams, Expertinnen für Cybersicherheit, das Management und manchmal auch externe Expertinnen beteiligt sind.

- Unterstützen Sie die Bereitschaft im gesamten Unternehmen – Sicherheit liegt in der Verantwortung aller.
- Nutzen Sie Automatisierung, wo immer möglich.
- Achten Sie darauf, einen gut eingeübten IRR-Plan zu haben, der die richtigen Personen über einen Cybervorfall informiert.

3 Mit Lieferanten arbeiten, deren Lieferkette sicher ist

Sicherheit beginnt früher, als man denken würde. Sorgen Sie für eine vertrauenswürdige Grundlage, indem Sie mit Lieferanten zusammenarbeiten, für die Sicherheit bei Design, Herstellung und Bereitstellung von Geräten und Infrastruktur oberste Priorität hat. Mit Lieferanten, die eine sichere Lieferkette, einen sicheren Entwicklungslebenszyklus und eine rigorose Bedrohungsmodellierung bieten, sind Sie Angreifern eher einen Schritt voraus.

- Sorgen Sie für Vertraulichkeit, Integrität und Verfügbarkeit von Informationen über die IT-Lieferkette oder im Zusammenhang mit ihr sowie über alle Beteiligten.
- Achten Sie darauf, dass die IT-Produkte oder -Services in der Lieferkette echt und unverändert sind und den Spezifikationen der erwerbenden Partei entsprechen, ohne zusätzliche unerwünschte Funktionen.
- Reduzieren Sie Sicherheitslücken, die die beabsichtigte Funktion einer Komponente einschränken, zum Ausfall einer Komponente führen oder Möglichkeiten für Exploits bieten.

4 Zero-Trust-Prinzipien umsetzen

Zero Trust ist ein Sicherheitskonzept, das auf der Überzeugung basiert, dass Unternehmen nicht automatisch irgendetwas innerhalb oder außerhalb ihrer Grenzen vertrauen sollten. Stattdessen müssen sie alles überprüfen, was versucht, eine Verbindung zu ihren Systemen herzustellen, bevor sie Zugriff gewähren.

- Verabschieden Sie sich von einem perimeterbasierten Sicherheitsmodell und führen Sie Zero-Trust-Prinzipien ein.
- Implementieren Sie das Prinzip der geringsten Berechtigung, das Nutzer- und Systemkonten so einschränkt, dass sie nur die mindestens erforderlichen Zugriffsrechte für ihre Aufgaben haben. Dieser Ansatz reduziert die Angriffsfläche und die potenziellen Auswirkungen eines unbefugten Zugriffs durch Angreifer.
- Integrieren Sie Lösungen wie Mikrosegmentierung, Identitäts- und Zugriffsmanagement (IAM), Multi-Faktor-Authentifizierung (MFA) und Sicherheitsanalysen, um nur einige zu nennen.

5 Angriffsfläche reduzieren

Die Angriffsfläche stellt potenzielle Sicherheitslücken und Einstiegspunkte dar, die von böswilligen Akteuren ausgenutzt werden können. Ihren Sicherheitsstatus verbessern Unternehmen, wenn sie diese Angriffsfläche minimieren, Risiken mindern und die allgemeine Cyberabwehr gegen neue und aufkommende Bedrohungen verbessern.

- Schulen Sie MitarbeiterInnen und NutzerInnen darin, potenzielle Sicherheitsbedrohungen, Phishing-Versuche und Social-Engineering-Taktiken zu erkennen und zu melden, um das Risiko erfolgreicher Angriffe zu minimieren, bei denen die Sicherheitslücke „Mensch" ausgenutzt wird.
- Implementieren Sie vorbeugende Maßnahmen wie eine umfassende Netzwerksegmentierung, die Isolierung kritischer Daten, die Durchsetzung strenger Zugriffskontrollen und die regelmäßige Aktualisierung und das Patchen von Systemen und Anwendungen.
- Achten Sie darauf, dass Systeme, Netzwerke und Geräte ordnungsgemäß mit Best Practices für die Sicherheit konfiguriert sind, z. B. durch das Deaktivieren unnötiger Services, die Verwendung sicherer Kennwörter und das Erzwingen von Zugriffskontrollen.

6 Cyberbedrohungen erkennen und auf sie reagieren

Angesichts ausgeklügelter Bedrohungen reichen herkömmliche Sicherheitsmaßnahmen nicht mehr aus. Unternehmen sollten fortschrittliche Technologien und Methoden zur Bedrohungserkennung nutzen, um bekannte und unbekannte Bedrohungen effektiv zu identifizieren und darauf zu reagieren.

- Überwachen und analysieren Sie den Netzwerkverkehr, Systemprotokolle und andere Bereiche sowie Sicherheitsdaten, um proaktiv Anzeichen für unbefugten Zugriff, Eindringen, Malware-Infektionen, Datenschutzverletzungen oder andere Cyberbedrohungen zu identifizieren.
- Setzen Sie einen Reaktionsplan um, mit dem bestätigte Sicherheits-Incidents untersucht und behoben werden. 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.
- Nutzen Sie KI/ML, um Cyberbedrohungen durch Echtzeitanalysen ungewöhnlicher Datenmuster oder Verhaltensweisen schnell zu erkennen. Diese Technologien erleichtern auch die schnelle Reaktion, indem sie den Schweregrad von Bedrohungen bewerten, Auswirkungen vorhersagen, bestimmte Abwehrmaßnahmen automatisieren und Sicherheitsmaßnahmen skalieren, um so potenzielle Schäden zu minimieren.

7 Systeme nach einem Cyberangriff wiederherstellen

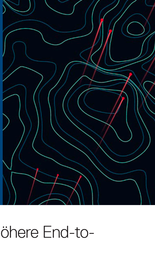
Selbst wenn kritische, proaktive Maßnahmen ergriffen wurden, sollten Unternehmen immer davon ausgehen, dass eine Sicherheitsverletzung vorliegt. Außerdem müssen robuste Funktionen vorhanden sein, die häufig getestet werden, um eine effektive Wiederherstellung nach einem erfolgreichen Cyberangriff sicherzustellen.

- Ergreifen Sie sofortige Maßnahmen, um den durch einen Cyberangriff verursachten Schaden zu minimieren, indem Sie die Auswirkungen isolieren und eindämmen.
- Trennen Sie betroffene Systeme vom Netzwerk, deaktivieren Sie kompromittierte Konten und ergreifen Sie Maßnahmen, um eine weitere Ausbreitung oder weiteren Schaden zu verhindern.
- Der Einsatz von KI/ML kann die Wiederherstellung beschleunigen, indem betroffene Systeme und Daten schnell identifiziert werden und der Ablauf der Wiederherstellung aus Backups automatisiert wird.

8 Binden Sie vertrauenswürdige Partner ein.

Kein einzelner Anbieter verfügt über alle notwendigen Funktionen, um durchgängige Sicherheit in allen Bereichen, einschließlich Personal, Prozessen oder Technologie zu gewährleisten. Alle haben ihre Spezialisierung. Daher ist es unerlässlich, mit einem Netzwerk von erfahrenen Partnern zusammenzuarbeiten.

- Arbeiten Sie mit erfahrenen Cybersicherheitspartnern zusammen, die wertvolles Fachwissen und Ressourcen zur Verfügung stellen, um Sie im Umgang mit der sich schnell entwickelnden Bedrohungslandschaft zu unterstützen.
- Profitieren Sie von spezialisierten Fähigkeiten und Kenntnissen, die in Ihrem Unternehmen intern möglicherweise nicht verfügbar sind, z. B. Analysen neu auftretender Risiken und fortschrittlicher Angriffstechniken sowie die neuesten Sicherheitsstrategien und Best Practices.
- Nutzen Sie das Fachwissen erfahrener Dienstleister und bauen Sie Kooperationsbeziehungen mit vertrauenswürdigen Businesspartnern auf, um einen umfassend geschützten Sicherheitsstatus zu schaffen, der effektiv vor sich entwickelnden Cyberbedrohungen schützt.



9 Cybersicherheit auf Edge- und Cloud-Umgebungen ausdehnen

Mit der Ausbreitung von Netzwerken vom Core über den Edge bis zur Cloud sind all diese Bereiche zu wichtigen gefährdeten Stellen geworden. Unabhängig davon, wie Anwendungen bereitgestellt werden, benötigen sie das gleiche Maß an Sicherheit und die gleiche Ausrichtung an Unternehmensrichtlinien, um Konsistenz für Anwendungsnutzerinnen und das Management zu gewährleisten.

- Stellen Sie sicher, dass Zero-Trust-Prinzipien auf Edge- und Cloud-Umgebungen ausgeweitet werden, um robuste Zugriffskontrollen, kontinuierliche Authentifizierung und umfassende Transparenz und Kontrolle über den Netzwerkverkehr zu ermöglichen.
- Implementieren Sie Sicherheitsmaßnahmen wie Netzwerksegmentierung, Verschlüsselung und kontinuierliches Monitoring sowohl im Kernnetzwerk als auch in Cloud-Umgebungen, um sich vor potenziellen Bedrohungen zu schützen.
- Arbeiten Sie mit erfahrenen professionellen Dienstleistern zusammen, die sich auf Edge-, Core- und Cloud-Sicherheit spezialisiert haben, um deren Fachwissen bei der Implementierung effektiver Maßnahmen zu nutzen und Ihr Unternehmen in alle Richtungen abzusichern.

10 Proaktives Management und höhere End-to-End-Ausfallsicherheit

Das Management von Threat Intelligence, Incident und Response sowie Sicherheitsabläufen kann die Fähigkeiten eines Unternehmens bei der Erkennung von und Reaktion auf Cyberbedrohungen verbessern.

- Richten Sie proaktive Incident-Response- und Recovery-Protokolle ein, in denen Rollen und Verantwortlichkeiten klar umrissen sind und eine nahtlose Kommunikation und Koordination zwischen den Teammitgliedern sichergestellt sind.
- Verbessern Sie die Übersicht über Ihre Umgebung, damit Abteilungen Bedrohungen in ihren Netzwerken proaktiv überwachen und darauf reagieren können. Gleichzeitig werden bei Bedarf Warnmeldungen für die Recovery bereitgestellt.
- Verbessern Sie Ihre Fähigkeit, Cyberbedrohungen proaktiv zu erkennen und darauf zu reagieren, indem Sie erweiterte Threat Intelligence, Sicherheitsinformations- und Ereignismanagement (SIEM), Lösungen für den Endpunktschutz und Verhaltensanalysen nutzen.

Lassen Sie nicht zu, dass Sicherheit Ihre Innovationen ausbremst. Erfahren Sie, wie Sie Ihren Cybersicherheits- und Zero-Trust-Reifegrad verbessern können unter dell.com/SecuritySolutions

DELL Technologies