DELL Technologies

Verbesserung Ihrer Cybersicherheit und des Zero-Trust-Reifegrads

Lassen Sie nicht zu, dass Sicherheitsrisiken Innovationen ausbremsen

Erkennen, wie es um Ihre Cybersicherheit steht –

und erfahren, wie sie aussehen sollte

In der heutigen komplexen und sich schnell entwickelnden Bedrohungslandschaft stoßen Unternehmen oft an die Grenzen ihrer Ressourcen und ihres Wissens, wenn es darum geht, robuste Cybersicherheitsverfahren aufrechtzuerhalten. Die Förderung des Reifegrads der Cybersicherheit und des Zero-Trust-Ansatzes ist für die Bekämpfung der sich entwickelnden Cyberbedrohungen unerlässlich. Sie schützt Ihre Umgebung und verhindert gleichzeitig, dass Innovationen ausgebremst werden.

Verwenden Sie die folgenden Prüflisten, um den aktuellen Status Ihrer Cybersicherheitsreife zu bewerten. Wenn Sie die Stärken und Schwachstellen Ihres Unternehmens kennen, können Sie die richtigen nächsten Schritte unternehmen, um Ihre Cybersicherheit zu verbessern.

Inhalt

Checklist: Reduzierung der Angriffsfläche 3

Checklist: Bedrohungen erkennen und auf sie reagieren 4

Checklist: Systeme nach einem Cyberangriff wiederherstellen 5

Mehr erfahren

Weitere Informationen dazu, wie Sie den Reifegrad Ihrer Cybersicherheit und des Zero-Trust-Ansatzes verbessern können

Checklist:

Reduzierung der Angriffsfläche

Mit „Angriffsfläche“ ist die Summe aller möglichen Punkte oder Bereiche in einer Umgebung gemeint, die von einem Cyberangreifer angegriffen oder ausgenutzt werden können. Zu diesen Punkten können Softwareschwachstellen, Fehlkonfigurationen, schwache Authentifizierungsmechanismen, ungepatchte Systeme, übermäßige Nutzerrechte, offene Netzwerkports, schlechte Vor-Ort-Sicherheit und mehr gehören. Anhand dieser Fragen können Sie herausfinden, wie Sie Sicherheitslücken und Einstiegspunkte minimieren, die von böswilligen Akteuren kompromittiert werden können.

Ja	Nein	
☐	☐	Führt Ihr Unternehmen regelmäßige Bewertungen, Penetrationstests oder Angriffssimulationen durch, um Sicherheitslücken und Schwachstellen in Systemen und Netzwerken zu identifizieren, damit zeitnah Korrekturen und Verbesserungen möglich sind?
☐	☐	Führt Ihr Unternehmen regelmäßige Sicherheitsschulungen für MitarbeiterInnen durch?
☐	☐	Verwendet Ihr Unternehmen Multifaktor-Authentifizierung (MFA) und rollenbasierte Zugriffskontrollen (RBAC)?
☐	☐	Hat Ihr Unternehmen eine Netzwerksegmentierung implementiert, um kritische Ressourcen zu isolieren und den Zugriff zwischen verschiedenen Teilen Ihres Netzwerks zu beschränken?
☐	☐	Implementiert Ihr Unternehmen sichere Codierungspraktiken, führt regelmäßige Sicherheitstests und Codeüberprüfungen durch und verwendet Web Application Firewalls (WAFs), um sich gegen gängige Angriffe auf Anwendungsebene zu schützen und die Angriffsfläche von Webanwendungen zu verringern?
☐	☐	Entscheidet sich Ihr Unternehmen für IT-Anbieter, die ihre Prozesse und Verfahren zur Sicherung der Lieferkette nachweisen können?
☐	☐	Implementiert Ihr Unternehmen Zero-Trust-Prinzipien statt herkömmlicher perimeterbasierter Sicherheitskonzepte?
☐	☐	Nutzt Ihr Unternehmen das Prinzip der geringsten Berechtigungen, um Nutzer- und Systemkonten so zu beschränken, dass sie nur die mindestens erforderlichen Zugriffsrechte zur Ausführung ihrer Aufgaben haben?
☐	☐	Patcht Ihr Unternehmen regelmäßig Systeme und Software?
☐	☐	Nutzen die Sicherheitstools Ihres Unternehmens KI-/ML-Funktionen, um Sicherheitslücken proaktiv zu identifizieren?

Checklist:

Bedrohungen erkennen und auf sie reagieren

Cyberbedrohungen zu erkennen und auf sie zu reagieren, ist ein wesentlicher Bestandteil jeder Sicherheitsstrategie. Dazu gehört die Überwachung und Analyse des Netzwerkverkehrs, von Systemprotokollen und anderen Bereichen sowie von Sicherheitsdaten, um Anzeichen für unbefugten Zugriff, Eindringen, Malware-Infektionen, Datenschutzverletzungen oder andere Cyberbedrohungen zu identifizieren. Anhand dieser Fragen lässt sich feststellen, wie Ihr Unternehmen potenzielle Sicherheitsvorfälle und bösartige Aktivitäten innerhalb eines Computernetzwerks, -systems oder einer Organisation proaktiv identifiziert und bekämpft.

Ja	Nein	
☐	☐	Überwacht Ihr Unternehmen kontinuierlich Netzwerk- und Systemaktivitäten mithilfe von Sicherheitstools und -technologien wie Extended Detection and Response (XDR), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), SIEM und Protokollanalyse?
☐	☐	Analysiert Ihr Unternehmen erfasste Daten, um Muster, Anomalien und Indikatoren für eine Gefährdung (Indicators of Compromise, IoCs) und/oder Angriffsindikatoren (IOA) zu identifizieren, die auf eine potenzielle Cyberbedrohung hinweisen können?
☐	☐	Verfügt Ihr Unternehmen über die neuesten Transparenz- und Monitoringtools, um potenzielle Gefährdungen schnell zu erkennen und zu melden?
☐	☐	Überwacht Ihr Unternehmen den Netzwerkverkehr auf ungewöhnliche Muster oder verdächtige Aktivitäten, die auf einen laufenden Cyberangriff hinweisen können?
☐	☐	Hat Ihr Unternehmen KI-/ML-Tools implementiert, um Cyberbedrohungen durch Echtzeitanalysen ungewöhnlicher Datenmuster oder Verhaltensweisen zu erkennen?
☐	☐	Hat Ihr Unternehmen die Implementierung einer SIEM-Lösung der nächsten Generation in Betracht gezogen, um Sicherheitswarnmeldungen besser zu managen und Sicherheitsereignisdaten aus der gesamten IT-Umgebung in Korrelation zu einander zu setzen?
☐	☐	Nutzt Ihr Unternehmen Sicherheitslückentests und -management, um vorhandene Sicherheitslücken zu priorisieren und zu beheben und effizient auf neue Sicherheitslücken zu reagieren?
☐	☐	Verfügt Ihr Unternehmen über einen Incident-Response-Plan zur Untersuchung und Abwehr bestätigter Sicherheitsvorfälle?
☐	☐	Setzt Ihr Unternehmen SOAR-Tools (Security Orchestration, Automation and Response) ein, um Incident-Response-Maßnahmen zu beschleunigen und so die Ausbreitung eines Cyberangriffs potenziell schneller einzudämmen?
☐	☐	Umfasst der Incident-Response-Plan Ihres Unternehmens Eindämmungsrichtlinien, Kommunikationspläne, Complianceanforderungen, forensische Analysen und Recovery-Prozesse?

Checklist:

Recovery nach einem Cyberangriff

Bei der Wiederherstellung nach einem Cyberangriff geht es darum, die betroffenen Systeme, Netzwerke und Daten nach einem Sicherheitsvorfall wieder in einen sicheren und betriebsbereiten Zustand zu versetzen. Dazu gehören das Ergreifen von Maßnahmen zur Behebung des durch den Angriff verursachten Schadens, die Wiederherstellung kompromittierter oder unterbrochener Dienste und Geräte, die Analyse des Incidents, um zukünftige Angriffe zu verhindern, und die Rückkehr zum normalen Betrieb des Unternehmens. Mit diesen Fragen können Sie feststellen, ob sich Ihr Unternehmen effektiv von Cyberangriffen erholen kann.

Ja	Nein	
☐	☐	Hat Ihr Unternehmen Maßnahmen zur Eindämmung von Incidents ergriffen, um einen Cyberangriff zu isolieren und einzuschränken?
☐	☐	Verfügt Ihr Unternehmen über Prozesse für die System- und/oder Gerätewiederherstellung nach Eindämmung eines Incidents?
☐	☐	Nutzt Ihr Unternehmen beim Schutz Ihrer Daten Datenisolierung, Unveränderlichkeit oder einen Cyber-Vault?
☐	☐	Hat Ihr Unternehmen Verfahren zur sauberen Wiederherstellung von Daten im Falle von kompromittierten, verschlüsselten oder gelöschten Daten eingerichtet?
☐	☐	Nutzt Ihr Unternehmen KI-/ML-Technologien, um die Wiederherstellung nach einem Cyberangriff zu automatisieren oder zu beschleunigen?
☐	☐	Bewertet Ihr Unternehmen den Incident kontinuierlich und ermittelt Bereiche mit Verbesserungsbedarf nach einem Angriff und einer Wiederherstellung?
☐	☐	Hat Ihr Unternehmen eine forensische Analyse durchgeführt, um die Angriffsmethodik zu verstehen, das Ausmaß der Sicherheitsverletzung zu bestimmen, betroffene Systeme und Daten zu identifizieren und Beweise zu sammeln, die Ihnen helfen, Ihre Sicherheit zu erhöhen und rechtliche oder disziplinarische Maßnahmen einzuleiten?
☐	☐	Weiß Ihr Unternehmen, wie es betroffene Parteien, wie KundInnen, Partner und Anbieter, über einen Cyberangriff und mögliche Auswirkungen auf ihre Daten oder ihren Betrieb zu informieren hat?
☐	☐	Übt Ihr Unternehmen seine Recovery-Strategien mehrmals pro Jahr, um Vertrauen in die Wiederherstellungsfähigkeit des Unternehmens zu gewinnen und Ihre SLAs zu erfüllen?
☐	☐	Arbeitet Ihr Unternehmen mit Serviceanbietern zusammen, um Wiederherstellungsmaßnahmen Ihres Unternehmens zu unterstützen?

Erhöhen Sie den Reifegrad der Cybersicherheit und des Zero-Trust-Ansatzes.

IT-Abteilungen müssen dringend für Worst-Case-Situationen planen, wenn es um Cybersicherheit geht, und mehrere Abwehrebenen einrichten. Im sich stetig weiterentwickelnden Bedrohungsumfeld und der Cybersicherheit ist es von entscheidender Bedeutung, Sicherheitsmaßnahmen kontinuierlich zu verbessern und Zero-Trust-Prinzipien zu implementieren. Dies umfasst:

Reduzierung der Angriffsfläche

Minimieren Sie die Sicherheitslücken und Einstiegspunkte, die ausgenutzt werden können, um die Umgebung zu gefährden.

Erkennung von und Reaktion auf Cyberbedrohungen

Identifizieren und beheben Sie aktiv potenzielle Sicherheits-Incidents und bösartige Aktivitäten.

Systeme nach einem Cyberangriff wiederherstellen

Bringen Sie Ihr Unternehmen nach einem Sicherheits-Incident wieder in einen vorherigen, bekannten sicheren und betriebsfähigen Zustand zurück.

Durch die Nutzung des Fachwissens von Dienstleistern und die Zusammenarbeit mit vertrauenswürdigen Businesspartnern kann Dell Unternehmen dabei unterstützen, einen umfassend geschützten Sicherheitsstatus zu schaffen, der vor sich entwickelnden Cyberbedrohungen schützt. Mit dem technologischen Fortschritt muss auch unser Ansatz für die Cybersicherheit weiterentwickelt werden, um digitale Infrastrukturen zu schützen und das Vertrauen in die digitale Welt aufrechtzuerhalten.

DELL Technologies

Über Dell Technologies

Dell Technologies unterstützt Unternehmen und Privatpersonen, ihre digitale Zukunft zu gestalten und Arbeitsplätze sowie private Lebensbereiche zu transformieren. Das Unternehmen bietet das branchenweit umfangreichste und innovativste Technologie- und Serviceportfolio für das Datenzeitalter.

Weitere Informationen unter
www.dell.com/securitysolutions