Gartner

IT-Roadmap für Cybersicherheit

Auszug

Wie entwickeln erfolgreiche Unternehmen risikobasierte Sicherheitsprogramme zur Unterstützung der geschäftlichen Agilität und Widerstandsfähigkeit?

Die digitale Geschäftstransformation und neu entstehende cyber-physische Systeme stellen ein noch nie dagewesenes Sicherheitsrisiko dar. Bis 2027 werden 75 % der Mitarbeiter Technologien erwerben, anpassen oder entwickeln, die nicht im Einflussbereich der IT-Abteilung liegen – ein deutlicher Anstieg gegenüber 41 % im Jahr 2022. Als Reaktion darauf verfolgen viele Unternehmen neue Ansätze im Bereich Cybersicherheit.

Unternehmen haben jedoch Schwierigkeiten damit, die Cybersicherheit mit den Prioritäten der Unternehmensführung in Einklang zu bringen. Chief Information Security Officers (CISOs) können bei der Entwicklung von Prozessen helfen, die risikobasierte Entscheidungen ermöglichen und gleichzeitig vor Sicherheitsrisiken schützen sowie Datenschutzverletzungen und andere Vorfälle im Bereich der Cybersicherheit verhindern.

Auf der Grundlage unserer fachkundigen Studie und Interaktionen mit Tausenden von Unternehmen in verschiedenen Branchen haben wir Best Practices für die Cybersicherheit in einer anpassbaren Roadmap zusammengestellt. Verwenden Sie diese Roadmap, um sich einen Überblick über die wichtigsten Phasen, Ressourcen und Mitarbeiter zu verschaffen, die für die Planung und Durchführung einer wirksamen Initiative im Bereich der Cybersicherheit erforderlich sind.

67 %

der CEOs und leitenden Angestellten wollen, dass mehr Technologiearbeit direkt in den betroffenen Geschäftsabteilungen anstatt von der IT geleistet wird.

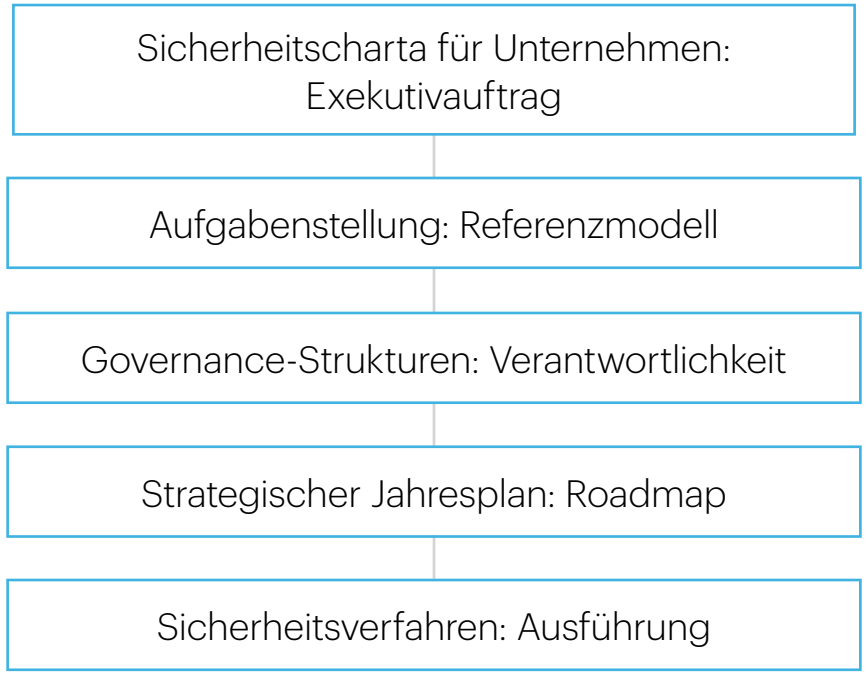
Quelle: Gartner CEO and Senior Business Executive Survey 2022

Durch die Entwicklung und Umsetzung eines robusten und verlässlichen Cybersicherheitsprogramms

Die einzige Möglichkeit, den sich entwickelnden Risiken der Digitalisierung und den zunehmenden Cyber-Bedrohungen wirksam zu begegnen, ist die Einführung eines kontinuierlichen Sicherheitsprogramms. Leider haken zu viele Unternehmen beim Aufbau von Sicherheitskapazitäten einfach nur die „Kästchen“ ab – das heißt, sie erstellen in der Regel eine Menge Dokumentation und investieren aggressiv in Technologie. Allerdings investieren sie kaum Zeit darin, eine effektive Unternehmensführung oder die Fähigkeit zur effektiven Risikobewertung und -interpretation aufzubauen.

Ein verlässliches Sicherheitsprogramm untermauert die Antwort auf die wichtige Frage der Stakeholder: „Schützt das Unternehmenseine Informationsressourcen angemessen?“

Komponenten eines Cybersicherheitsprogramms



Quelle: Gartner

Einige der wichtigsten Fragen der Initiative im Bereich der Cybersicherheit sind:

1. Wie wird dies die Widerstandsfähigkeit und die Wachstumsziele des Unternehmens unterstützen und gleichzeitig das Risiko verringern?
2. Wie können wir einen ergebnisorientierten Ansatz verwenden, um Prioritäten und Investitionen im Bereich der Cybersicherheit festzulegen?
3. Welche Führungskräfte und Teams müssen einbezogen werden?

Was sind die wichtigsten Phasen?

Diese Einblicke in die Best Practices basieren auf der Zusammenarbeit mit Kunden, die erfolgreich Initiativen im Bereich der Cybersicherheit umgesetzt haben. Diese Darstellung zeigt die Abfolge der Ziele und gewünschten Ergebnisse und ist bei der Abstimmung mit allen Stakeholdern hilfreich.

Im Folgenden werden einige wichtige Meilensteine und eine Auswahl der entsprechenden Ressourcen von Gartner hervorgehoben, aber die vollständige Roadmap wird sämtliche Details zu allen Meilensteinen und Ressourcen für jede Phase enthalten.

Die Strategie ausrichten

Ziele setzen und ein Geschäftsszenario aufbauen

Bewusste Maßnahmen

- ☐ Verstehen der wichtigsten Geschäftsprioritäten; Definition des Programmauftrags und der Vision; Identifizierung von Unternehmens-, Technologie- und Bedrohungsfaktoren
- ☐ Identifizierung der Ziele, des Programmwertes und der Rollen und Verantwortlichkeiten der Key-Stakeholder
- ☐ Definition von Sicherheitskontrollen im Einklang mit den Unternehmensstrategien und deren Zuordnung zu einem standardisierten Sicherheits-Framework
- ☐ Einholen von Feedback der Stakeholder, Definition der wichtigsten Ziele und Fertigstellung einer ersten Zusammenfassung des Dokuments zur Sicherheitsstrategie

und mehr

Beispiel für zugehörige Gartner-Ressourcen

- **Analystenanfrage:** Zusammenarbeit mit einem Analysten, um die richtigen Metriken festzulegen, mit denen die Auswirkungen der Cybersicherheit gemessen werden können
- **Analystenanfrage:** Zusammenarbeit mit einem Analysten, um den richtigen Ansatz zu finden, der den Stakeholdern die Auswirkungen der Cybersicherheit auf das Unternehmen vermittelt
- **Forschung:** Wie man ein robustes, verlässliches Sicherheitsprogramm aufbaut, das Geschäftswachstum und Agilität ermöglicht

und mehr

Einen Action Plan entwickeln

Framework zur Risikopriorisierung erstellen

Bewusste Maßnahmen

- ☐ Durchführung von Schwachstellenbewertungen und Eindringtests
- ☐ Ermittlung der aktuellen Ausgereiftheit des Ausgangswerts, Definition des Zielzustands und Durchführung einer Lückenanalyse
- ☐ Unterstützung von Buy-in und Ressourcen durch die Führungskräfte oder den Vorstand
- ☐ Entwicklung einer Sicherheitsarchitektur, eines Richtlinien-Frameworks und einer Lösungsschicht

und mehr

Beispiel für zugehörige Gartner-Ressourcen

- **Forschung:** CISO Foundations, Toolkit: Strategieplan – Präsentation und Übersichtstabellen
- **Tool:** IT Score für Sicherheit und Risikomanagement
- **Forschung:** Ignition Guide zur Erstellung eines Jahresbudgets für Cybersicherheit

und mehr

Die Ausführung einleiten

Die Teamstruktur gestalten und anpassen

Bewusste Maßnahmen

- ☐ Den Wert des Programms vermitteln
- ☐ Festlegung der Rollen und Verantwortlichkeiten des Sicherheitsteams und Identifizierung der Stakeholder, die zur Verantwortung gezogen, beraten und informiert werden müssen
- ☐ Entwicklung kritischer Kompetenzen und Schulungen für erwartete aber noch fehlende Fähigkeiten
- ☐ Verwendung von Metriken und Anreizen, um die Verantwortlichkeit der Eigentümer zu fördern

und mehr

Beispiel für zugehörige Gartner-Ressourcen

- **Beratung per Telefon:** Zusammenarbeit mit einem Experten zum Thema „Der CARE-Standard für Cybersicherheit“
- **Forschung:** Informationen über die Bedrohung der Cybersicherheit und ihre Auswirkungen auf das Unternehmen
- **Forschung:** Verfolgung von Metriken und Einholung von Feedback zur Bewertung und Verbesserung der Effektivität des Programms

und mehr

Ein Programm aufbauen und weiterentwickeln

Aufrechterhaltung der Verantwortlichkeit und Sicherheit durch Governance

Bewusste Maßnahmen

- ☐ Entwicklung einer Reaktionsfähigkeit im Falle kritischer Vorfälle und eines Action Plans im Falle von Verstößen
- ☐ Entwicklung einer Programmstruktur zur Überwachung und Bekämpfung fortschrittlicher Bedrohungen
- ☐ Verankerung einer Kultur des sicheren Verhaltens der Mitarbeiter und Initiierung maßgeschneiderter Schulungs- und Sensibilisierungskampagnen
- ☐ Entwicklung eines fortschrittlichen Reporting- und Reaktionssystems und Erstellung eines Kommunikationsplans für Cyberverstöße

und mehr

Beispiel für zugehörige Gartner-Ressourcen

- **Analystenanfrage:** Zusammenarbeit mit einem Analysten, um die richtigen Metriken festzulegen, mit denen die Auswirkungen der Cybersicherheit gemessen werden können
- **Analystenanfrage:** Zusammenarbeit mit einem Analysten, um den richtigen Ansatz zu finden, der den Stakeholdern die Auswirkungen der Cybersicherheit auf das Unternehmen vermittelt
- **Forschung:** Wie man ein robustes, verlässliches Sicherheitsprogramm aufbaut, das Geschäftswachstum und Agilität ermöglicht

und mehr

Neu bewerten und optimieren

Den Wert des Programms vermitteln

Bewusste Maßnahmen

- ☐ Erstellung eines Plans zur Vermittlung des Wertes an das Unternehmen und den Vorstand
- ☐ Verfolgung von Metriken und Einholung von Feedback zur Bewertung und Verbesserung der Effektivität des Programms
- ☐ Überprüfung der Bewertung der Ausgereiftheit zur weiteren Optimierung

und mehr

Beispiel für zugehörige Gartner-Ressourcen

- **Beratung per Telefon:** Diskussion über die wichtigsten Punkte, die bei der weiteren Optimierung der Vorbereitung auf die Cybersicherheit im Unternehmen helfen können
- **Analystenanfrage:** Wiederholung der Gartner IT Score-Bewertung, um den Fortschritt zu messen und neue Prioritäten zu setzen
- **Forschung:** Tool für das Vorstandsbriefing: Wie Sie die Cyberrisiken in Ihrem Unternehmen kommunizieren

und mehr

Wer muss eingebunden werden?

Die erfolgreichsten Unternehmen bilden funktionsübergreifende Teams für ihre Initiativen im Bereich der Cybersicherheit. Wir haben die Funktionen und Rollen umrissen, deren Einbeziehung wir empfehlen, um beim Erreichen der Meilensteine den bestmöglichen Erfolg zu gewährleisten.

CISO

Führt die Entwicklung der Cybersicherheitsstrategie und des Cybersicherheitsprogramms an; stellt sicher, dass die Cybersicherheitsstrategie mit der Unternehmensstrategie und den Unternehmenszielen übereinstimmt; leitet die Bewertung, den Action Plan und die Ausführung; hilft bei der Vermittlung der Cybersicherheitsstrategie und des Fortschritts im gesamten Unternehmen; arbeitet bei der Programmimplementierung mit wichtigen Führungskräften und Stakeholdern zusammen

CIO

Zusammenarbeit mit Führungskräften in den Unternehmen und Führung des Aufbaus des Cybersicherheitsprogramms; Vermittlung von Strategien und Zielen im gesamten Unternehmen

Technisches Profi-Team

Entwurf, Implementierung oder Verbesserung und Pflege von Sicherheitsarchitekturen, -richtlinien und -verfahren; Überwachung und Bewertung der Cybersicherheitsleistung und deren Verbesserung auf der Grundlage neuer Bedrohungen; Verbesserung der Fähigkeiten nach Bedarf

Führender Anbieter von Unternehmenslösungen und Software-Engineering

Wichtiger Partner des CISO; Unterstützung bei der Implementierung und dem Betrieb von Schlüsselelementen des Sicherheitsprogramms und der Abläufe

Führungskräfte und Teams im Bereich Enterprise Architecture

Zusammenarbeit mit dem CISO und anderen IT-Führungskräften, um sicherzustellen, dass die Sicherheitsstrategie und -architektur aufeinander abgestimmt und in die gesamte Enterprise Architecture integriert sind

Führungskräfte und Teams im Bereich Infrastruktur und Abläufe

Wichtiger Partner des CISO; Unterstützung bei der Implementierung und dem Betrieb von Schlüsselelementen des Sicherheitsprogramms und der Abläufe

Führungskräfte im Bereich Data und Analytics

Wichtiger Partner des CISO; Unterstützung bei der Implementierung und dem Betrieb von Schlüsselelementen des Sicherheitsprogramms und der Abläufe

Erfolgsgeschichte eines Kunden: Ermöglichung der IT-Compliance mit der Roadmap für Cybersicherheit

Erfolgskritische Prioritäten

Mit dem Ziel, Geschäftsprozesse zu rationalisieren und eine für das Digital Business vorbereitete Umgebung zu entwickeln, wollte Pacific Textiles ein Framework entwickeln, das die IT-Compliance einhält und gleichzeitig das Cybersicherheitsrisiko minimiert.

Wie Gartner geholfen hat

Dank des Zugangs zu Experten, Forschungsergebnissen und Tools von Gartner konnte Pacific Textiles Informationen über ein ERP-System digitalisieren, Prozesse in der Herstellung mit neuen Technologien automatisieren und eine sofort umsetzbare Roadmap für die Cybersicherheit erstellen.

Mission erfüllt

Mit Hilfe von Gartner war Pacific Textiles in der Lage:

- Einen ganzheitlichen Ansatz für Governance- und Risikomanagementverfahren zu verfolgen
- Eine solide Grundlage für ihr Digital Business aufzubauen
- Geschäftsprozesse zu optimieren, Zeit und Energie für das Top-Management zu sparen

Gartner für Chief Information Security Officers

Sorgen Sie für Wertsteigerung im gesamten Unternehmen durch Experten-Beratung, Tools, Networking mit Kollegen und gezielte Veranstaltungen.

Demonstrieren Sie den Geschäftswert

Zeigen Sie erfolgreiche Führung im Bereich Cybersecurity bei bestimmten Themen:

- Rolle, Beziehungen, Talent und Kultur
- Vertretbare Budgets erhalten
- Strategie und Vision des Cybersicherheitsprogramms

Risikovermeidung durch starke tägliche Cybersicherheitsprogramme:

- Unternehmensrisikomanagement
- Future of Work, Risikoreaktionsstrategien, Change Management

Optimierung von Technologieinvestitionen und -ausführung:

- Trends zu neuen technischen Fortschritten
- Pragmatische Tools zur Messung und Entscheidungsfindung
- Ausführliche technische Implementierungsleitfäden
- Kontextualisierte Branchen-Insights

Mehr erfahren

Beschleunigung wichtiger Initiativen

Setzen Sie die Strategie mit Tools, die die Umsetzung beschleunigen und Geschäftsergebnisse liefern, in die Tat um:

- CISO-Wirksamkeitsdiagnostik
- Bewertung der Cybersicherheitskontrollen
- IT Score
- Vorlagen für Vorstandsbesprechungen

Netzwerke für Kollegen

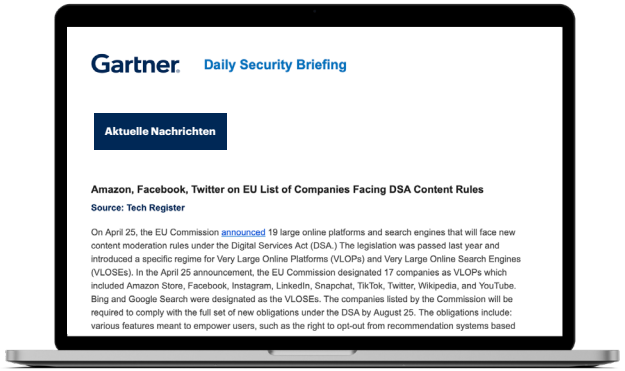
Treten Sie mit anderen Führungskräften der Sicherheitsbranche in persönlichen Chats, von Kollegen geführten Diskussionen und Umfragen in Kontakt und greifen Sie auf Technologiebewertungen und -rezensionen zu.

Fesselnde Events

Genießen Sie VIP-Zugang zum Gartner Security & Risk Management Summit mit zahlreichen pädagogischen Breakout-Sitzungen und vielen weiteren Möglichkeiten, mit Kollegen und Gartner-Experten in Kontakt zu treten. Bewerben Sie sich außerdem als Teil des CISO Circle für exklusive Sitzungen und Networking-Möglichkeiten

Tägliches Sicherheitsbriefing

Bleiben Sie über die dringendsten Nachrichten auf dem Laufenden mit einer Zusammenfassung von Artikeln aus seriösen Nachrichtenquellen, einschließlich einer branchenübergreifenden, globalen Zusammenfassung der neuesten Bedrohungen und Sicherheitsnachrichten des Tages.



„Die Nachrichten sind das Erste, was ich jeden Morgen lese. Ich nutze sie, um Bedenken von Führungskräften auszuräumen und alle neuen Schwachstellen an mein Team weiterzuleiten, damit sie sicherstellen, dass wir Maßnahmen zur Risikoentschärfung ergreifen."

CISO, Global Wireless Technology Provider

Umsetzbare, objektive Insights

Entdecken Sie diese zusätzlichen, ergänzenden Ressourcen und Tools für Führungskräfte im Bereich Cybersicherheit:

Studie

Der CISO-Leitfaden für Ihre ersten 100 Tage

Finden Sie heraus, welche Maßnahmen Sie in Ihren ersten 100 Tagen als CISO ergreifen sollten.

Webinar

Betrachten Sie Cybersicherheit als Geschäftsinvestition, um bessere Ergebnisse zu erzielen

Lernen Sie, wie Sie Ihrem Vorstand ergebnisorientierte Metriken vermitteln können

E-Book

Leadership Vision für Führungskräfte im Bereich Sicherheit und Risikomanagement

Erfahren Sie mehr zu den drei wichtigsten strategischen Prioritäten für Führungskräfte im Bereich Sicherheit und Risikomanagement

Konferenz

Mehr zur Gartner-Konferenz für Cybersicherheit

Bringen Sie Ihre Strategie für Cybersicherheit und Risiko-management voran, indem Sie an einer Gartner-Konferenz teilnehmen.

Bereits Kunde?
Erhalten Sie über Ihr Kundenportal Zugang zu weiteren Ressourcen. Anmelden

Entdecken Sie weitere Roadmaps aus dieser Serie

Schützen Sie Ihre Unternehmensressourcen mit einer Roadmap für ausgereifte Informationssicherheit

Roadmap: Erfolgreiches digitales Wachstum mit Data und Analytics vorantreiben

Migrieren Sie Daten- und Analyse-Architekturen in die Cloud: Roadmap

Verbessern Sie Ihre Roadmap für eine wirksame Daten-Governance

Roadmap: Entwicklung einer effektiven Cloud-Strategie

Ihr Kontakt zu uns

Erhalten Sie umsetzbare, objektive Insights, um Ihre unternehmenskritischen Ziele zu erreichen. Unsere Experten-Beratung und Tools ermöglichen schnellere, smartere Entscheidungen und bessere Leistung. Ihr Kontakt zu uns, um Kunde zu werden:

USA: +1 855 811 7593

International: +44 (0) 3330 607 044

Kunde werden

Erfahren Sie mehr über Gartner für Führungskräfte im Bereich Cybersicherheit
gartner.com/en/cybersicherheit

Bleiben Sie mit den neuesten Insights auf dem Laufenden

Gartner