everbridge™ + PRIANTO

Leitfaden: In zehn Schritten neuen Sicherheitsbedrohungen immer voraus sein

Übersicht

Sicherheitsbedrohungen immer einen Schritt voraus zu sein ist für Führungskräfte von zentraler Bedeutung. Und diese Bedrohungen werden jedes Jahr komplexer.

Neuartige Bedrohungen können wirtschaftlicher, ökologischer, geopolitischer, gesellschaftlicher oder technologischer Art sein. Das Narrativ der neuen Bedrohungen darf nicht zu stark vereinfacht werden. Die Sicherheitsrisiken entwickeln sich schneller als sich Organisationen darauf einstellen können.

Dieser Leitfaden bündelt hilfreiche Erkenntnisse von führenden Unternehmen, die einige der umfangreichsten und komplexesten Sicherheitssysteme der Welt implementiert haben.

Dieser Leitfaden bündelt hilfreiche Erkenntnisse und Erfahrungen aus der Implementierung einiger der umfangreichsten und komplexesten Sicherheitssysteme der Welt.

01 Geschäftsfall

Den Stakeholdern den Wert des Projekts aufzuzeigen ist für jeden Sicherheitsmanager unabdingbar.

Nur wenige CEOs haben Erfahrungen im Risikomanagement oder Sicherheitsbereich. Deshalb fühlen sie sich vielleicht unwohl dabei, Investitionen eine hohe Priorität einzuräumen, die dazu dienen, neuartigen Bedrohungen immer einen Schritt voraus zu sein und ganzheitlich mit alltäglichen betrieblichen Risiken umzugehen.

Erstellen Sie einen Business Case, der den CEO die Themen Sicherheit und Schutz als kommerzielle Investition erkennen lässt – und nicht als Ausgabe für Technologie oder Einrichtungen.

Eine Erneuerung der kompletten Technologie wird nur sehr unwahrscheinlich eine Genehmigung erhalten. Messen Sie stattdessen Ihre betrieblichen Risiken und kombinieren Sie diese Informationen mit einem vollständig durchkalkulierten strategischen Sicherheitsplan und einer Roadmap für die Umsetzung.

02 Sicherheitsstrategie und Roadmap

Als Sicherheitsmanager müssen Sie immer vielfältigere Strategien und Roadmaps entwickeln, um bestehende und neuartige Risiken zu kontrollieren.

Ihre Strategie sollte zunächst die Parameter der Sicherheits-anforderungen für Ihre Organisation eindeutig definieren oder erklären.

Im nächsten Schritt legen Sie den Ansatz für den Umgang mit diesen Anforderungen unmissverständlich fest. Zum Abschluss sollte Ihre Roadmap einen zeitlichen Ablauf kohärenter Maßnahmen determinieren, mit denen die Herausforderung gemeistert werden kann.

Starke Führungskompetenzen sind ebenso notwendig, um eine Sicherheitskultur in der Organisation zu fördern.

Wir leben in einer unsicheren globalisierten Welt mit wachsenden Risiken. Viele Mitarbeiter lassen sich von einem Sicherheits-verantwortlichen inspirieren, der vorlebt, wie wichtig es ist, Kollegen und ihr Arbeits- und Lebensumfeld proaktiv zu schützen.

03 Sicherheitsarchitektur

Wahrscheinlich haben viele Sicherheitsmanager nicht die Möglichkeit, ihre Technologiearchitektur von Grund auf zu errichten. Das wäre schlichtweg unerschwinglich.

Entwickeln Sie Ihren Security Stack strategisch und konzeptionell so, dass er sich kontrolliert weiterentwickeln kann; das macht es einfacher, ihn auszustatten, zu implementieren und zu betreiben.

Durch die Evaluierung der Sicherheitsarchitektur sollten folgende Eigenschaften des Systems sichergestellt werden:

- so widerstandsfähig wie möglich,
- interoperabel,
- offen für die Integration vorhandener und zukünftiger Systeme und Geräte,
- angetrieben durch Daten und Erkenntnisse,
- benutzerfreundlicher,
- effizienter im Betrieb,
- schneller bei der Reaktion auf Ereignisse,
- kosteneffizienter werden,
- effektiver beim Schutz von Mitarbeitern, Einrichtungen und Vermögenswerten,
- und effektiver bei der Gewährleistung eines unterbrechungsfreien Geschäftsbetriebs.

04 Sicherheitsoperationen

Security Operations müssen zuallererst einen ausfallsicheren Umgang mit neuen Bedrohungen und kritischen Ereignissen ermöglichen.

Wenn etwas passiert, benötigen Sicherheitsverantwortliche folgende Möglichkeiten: umfassende Situationserkennung in Echtzeit, anwendbare Einblicke, schnelle Entscheidungsfindung und die Fähigkeit, Bedrohung durch eine schnelle Reaktion abzuwehren. Sie benötigen vollständige Transparenz und Kontrolle über alle Mitarbeiter, Einrichtungen und Vermögenswerte oder die Gewissheit, dass die lokalen Verantwortlichen damit ausgestattet sind.

Eine standardisierte Benutzeroberfläche und ein allgemeines operatives Framework ermöglichen es Sicherheitsmanagern, ihre Tätigkeiten effektiver auszuführen.

Standardarbeitsverfahren (SOPs) und Workflows sollten vordefiniert und konfiguriert werden. So lässt sich das für neuartige Bedrohungen und kritische Ereignisse erforderliche Sicherheitsniveau etablieren.

Das Ziel aller Sicherheitsmaßnahmen ist, Mitarbeiter, Einrichtungen und Vermögenswerte zu schützen und für einen unterbrechungsfreien Geschäftsbetrieb zu sorgen.

05 Skalierbarkeit und Flexibilität

Jede Organisation entwickelt sich weiter, sei es durch Fusionen und Übernahmen, organisches Wachstum oder personelle Veränderungen. Zudem verändern sich auch die Prozesse, um neue Geschäfts- und Compliance-Anforderungen zu erfüllen.

Sicherheit ist immer eine langfristige Investition. Eine heute getroffene Entscheidung muss auch für zukünftige Anforderungen tragfähig sein - unabhängig davon, welche neuen Bedrohungen entstehen.

Sie sollten den Sicherheitsanspruch über die komplette Organisation hinweg prüfen. Danach verfügen Sie über eine vollständige Liste an Anforderungen, mit der Sie Technologien und Prozesse zukunftsfähig gestalten können.

Wählen Sie Lösungen, die sich unkompliziert und kosteneffizient nach oben und unten skalieren lassen. Dann können sie unproblematisch an veränderte Anforderungen angepasst werden. Das Risiko, teure Systeme in wenigen Jahren schon wieder austauschen zu müssen, sinkt dadurch.

06 Daten und Einsichten

Um die ständig zunehmenden Datenmengen von Organisationen verarbeiten zu können, müssen die richtigen Sicherheitsprozesse und -verfahren implementiert werden.

Siloprozesse und fehlende technologische Interoperabilität erschweren die Auswertung von Daten. Schlechtes Datenmanagement kann außerdem zu Datendiebstählen führen, die sowohl dem Geschäft als auch der Reputation einer Organisation erheblichen Schaden zufügen.

In die Sicherheitsprozesse fließen täglich Informationen aus vielen verschiedenen internen und externen Quellen ein; und die erforderlichen Aktionen wurden dynamischer und vielfältiger.

Security Operations erfordern eine vorausschauende Intelligenz, um neuartige Bedrohungen zu identifizieren und während kritischer Ereignisse anwendbare Einsichten zu gewinnen. Automatisierte Tools ermöglichen es den Verantwortlichen, auf neue Bedrohungen und kritische Ereignisse prompt zu reagieren.

Sinn und Zweck einer Sicherheitskultur ist es, die Sicherheitsagenda innerhalb der Organisation zu priorisieren.

07 Kennzahlen messen und berichten

Zu einem robusten Sicherheitskonzept gehört auch, dass Sicherheitsmanager relevante Kennzahlen messen und sie an das Senior Management berichten.

Beispiele für solche Kennzahlen sind:

- die Anzahl und Klassifizierung kritischer Ereignisse
- Die Zeitspanne bis zur Reaktion auf Vorfälle und kritische Ereignisse
- Messbare Auswirkungen auf Mitarbeiter, Einrichtungen, Vermögenswerte und/oder den Geschäftsbetrieb

Zusätzlich zu den reinen Zahlen sollten Sie ein Sicherheitsnarrativ anbieten, mit dem das oberste Management den Erfolg und den Wert der Sicherheitsinvestitionen leichter verstehen kann.

08 Partnerschaften mit wichtigen Stakeholdern aufbauen

Ein Bewusstsein und ein Eintreten für Sicherheit über eine gesamte Organisation hinweg zu erreichen, kann schwierig sein. Menschen scheuen sich oft vor Veränderungen.

Sinn und Zweck einer Sicherheitskultur ist es, die Sicherheitsagenda innerhalb der Organisation zu priorisieren und festzulegen, wie die Kollegen eingebunden werden können.

Den CEO in den Sicherheits-Business-Case einzubinden und seine Genehmigung dafür zu erhalten ist ganz entscheidend, wenn die Organisation breiter involviert werden soll. Wenn ein CEO davon überzeugt ist, dass Sicherheit und Schutz wichtig sind und das auch kommuniziert, motiviert das viele Mitarbeiter zur Beteiligung.

Es sollten außerdem abteilungsübergreifende Partnerschaften etabliert und alle Stakeholder hinter dem gemeinsamen Ziel versammelt werden. Nur so lässt sich die nötige Unterstützung für die Umsetzung eines organisationsweiten Sicherheitsansatzes erreichen.

Ihr Team und Ihre Agenda sollten den Kollegen aufzeigen, wie sie Sicherheit aktiv leben können, anstatt lediglich Verbote auszusprechen.

Durch einen regelmäßigen Austausch mit allen Stakeholdern lassen sich Probleme schnell erkennen und lösen.

09 Neue Bedrohungen

Um in einer vernetzten Welt sicher zu sein, müssen Organisationen alle neuartigen Bedrohungen verfolgen und ermitteln, welche finanziellen und betrieblichen Auswirkungen kritische Ereignisse haben könnten.

Das Bedrohungsumfeld wird immer komplexer und unberechenbarer. Deshalb war es nie wichtiger, schnell zu handeln. Durch komplettere Informationen können Sie die Entscheidungsfindung beschleunigen, Risiken schneller bewerten und verhindern, dass diese Risiken Ihren Mitarbeiter oder Ihrem Geschäftsbetrieb Schaden zufügen.

10 Everbridge Control Center

Marktführende Plattformen für physische Sicherheit sind darauf ausgelegt, zahlreiche losgelöste Sicherheitsanwendungen und Geräte zu integrieren; und sie über eine einzige umfassende Benutzeroberfläche zu kontrollieren.

Diese Plattformen erfassen und korrelieren Ereignisse aus verteilten vorhandenen Sicherheitsgeräten und Informationssystemen (Video, Zutrittskontrolle, Sensoren, Analysesysteme, Netzwerke, Gebäudesysteme usw.). Damit ermöglichen sie es Sicherheitsmanagern kritische Ereignisse zu identifizieren und proaktiv zu beheben.

Eine solche Plattform bietet Organisation zahlreiche Vorteile. Dazu zählen erhöhte Kontrolle, verbesserte Situationserkennung, anwendbare Einsichten und ein proaktives Management-Reporting.

Nicht zuletzt können Organisationen damit durch gesteigerte Effizienz Kosten senken und durch optimiertes Wissen die Sicherheit erhöhen.

Control Center von Everbridge ist eine Plattform für physische Sicherheit, der führende Organisationen weltweit vertrauen, wenn Sicherheit und Schutz von unternehmenskritischer Bedeutung sind.

© 2023 Everbridge

Über Everbridge

Everbridge, Inc. (NASDAQ: EVBG) ist ein weltweit tätiges Software-Unternehmen. Everbridge bietet Enterprise-Software-Anwendungen, mit denen Organisationen die Reaktion auf kritische Ereignisse automatisieren und beschleunigen und so die Sicherheit von Menschen gewährleisten und den Geschäftsbetrieb aufrechterhalten (Keep People Safe and Organizations Running™) können.

Erfahren Sie mehr über Everbridge, indem Sie uns auf LinkedIn und Twitter folgen.

Prianto GmbH
Value Added Distribution
everbridge@prianto.com
Tel.: +49 89 416 148 210

Axel Plage
Senior Account Executive, Everbridge
axel.plage@everbridge.com
Tel.: +49 30 383 05 669

Nehmen Sie Kontakt auf, um mehr über Everbridge zu erfahren - und die Resilienz zu stärken.