DELL Technologies

5 Empfehlungen für eine sichere Umgebung für Innovationen

1	2	3	4	5
Kommunizieren Sie frühzeitig und oft	**Rationalisieren und vereinfachen Sie den Sicherheitsstack**	**Richten Sie Cyber-sicherheitsschutz-maßnahmen ein**	**Bleiben Sie flexibel, werden Sie kreativ**	**Fördern Sie eine starke Sicherheitskultur**
Führungskräfte und wichtige StakeholderInnen einbeziehen	Komplexität reduzieren	Policies definieren	Für neue Sicherheitsmethoden offen sein	Umfassende Einbeziehung vereinfachen
Pläne für Innovationen verstehen	Redundanz beseitigen	Zugriffskontrollen implementieren	Auf Sicherheits-methoden fokussieren, die Innovationen ermöglichen	Transparenz fördern
Sicherheitsteam unterstützen, das Gespräch in Gang zu bringen	Eine zentrale Benutzeroberfläche erstellen	Integration über logische und physische Systeme hinweg ermöglichen	Bedenken, dass Innovationen auch in der Sicherheitsabteilung stattfinden können	Zusammenarbeit verstärken
	Einen soliden Beschaffungsbewer-tungsprozess entwickeln			

Copyright © 2024 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

Schaffen Sie eine sichere Umgebung für Innovationen

Für maximale Innovationen in unserer technologie- und datengesteuerten Welt muss Cybersicherheit darauf ausgelegt sein, Innovationen zu unterstützen. Aber wie kann ein Unternehmen eine Umgebung schaffen, die Wachstum, Kreativität und Innovationen fördert, ohne die Sicherheit zu beeinträchtigen?

Sameer Shah von Dell Cybersecurity Marketing hat sich mit Dr. Tony Bryson, dem Chief Information Security Officer (CISO) der Stadt Gilbert, Arizona, getroffen, um sich die innovative Initiative „City of the Future“ als reales Beispiel für eine solche Umgebung näher anzusehen und über die Rolle zu sprechen, die Sicherheit dabei spielt.

Lesen Sie weiter, um eine Zusammenfassung der Empfehlungen von Dr. Bryson zu erhalten. Das ganze Gespräch finden Sie unter **dell.com/cybersecuritymonth**.

> Stellen Sie sicher, dass Sie wissen, was das Ziel [Ihrer StakeholderInnen] ist und wie sie Technologie und Innovationen zum Vorteil des Unternehmens und der Kunden nutzen werden.“
>
> ***Dr. Tony Bryson**, Chief Information Security Officer (CISO) der Stadt Gilbert*

Die Stadt der Zukunft

Die Initiative „City of the Future“ der Stadt Gilbert wurde entwickelt, um eine nachhaltige und ausfallsichere Infrastruktur aufzubauen, die Daten nutzt, um das Leben der BürgerInnen zu bereichern. Technologie wird umfassend eingesetzt, um Services in verschiedenen Bereichen bereitzustellen – von Zahlungsmöglichkeiten für BürgerInnen über den Verkehrsbetrieb bis hin zur Verfügbarkeit und Qualität von Wasser. Dazu gehört auch das Sammeln von Daten, um die künftige Servicenutzung und -nachfrage zu prognostizieren. Die Initiative hat kein festgelegtes Ende, sondern ist ein iterativer Prozess, der den kontinuierlichen Fortschritt fördert.

Die Aufgabe von Dr. Bryson als erstem CISO der Stadt bestand darin, einen strategischeren Ansatz für die Cybersicherheit zu verfolgen. Die Bereitstellung moderner, technologiegestützter städtischer Services erforderte solide Data-Protection-, Klassifizierungs- und Kontrollfunktionen, die darauf ausgelegt sind, die ehrgeizigen Ziele der Stadt zu unterstützen.

Im Verlauf des erfolgreichen Prozesses hat Dr. Bryson einige wichtige Empfehlungen identifiziert, die den Erfolg vereinfachten und das richtige Umfeld für Sicherheit bei Wachstum und Innovationen schufen.

Kommunizieren Sie frühzeitig und oft

Dr. Bryson betont die Notwendigkeit, Führungskräfte und andere wichtige StakeholderInnen frühzeitig in den Innovationsprozess einzubeziehen. „Stellen Sie sicher, dass Sie wissen, was ihr Ziel ist und wie sie Technologie und Innovationen zum Vorteil des Unternehmens und der Kunden nutzen werden“, erklärt er.

Ein wesentlicher Aspekt der frühzeitigen Kommunikation ist, das Gespräch über Cybersicherheit am Anfang des Innovationszyklus zu führen. Als wichtiger Partner kann das Cybersicherheitsteam der Katalysator für diese Gespräche sein.

Der Einsatz von KI in der Stadt Gilbert ist ein Paradebeispiel dafür. Das Security Office nahm solche Gespräche vor zwei Jahren auf und spielte eine führende Rolle bei der Erwägung kritischer Fragen: Wie können wir den von KI erzeugten Daten vertrauen? Wie können wir sie speichern? Wie können wir sicherstellen, dass die BürgerInnen die Nutzung von KI richtig verstehen? Dies führte zur Gründung eines funktionsübergreifenden Komitees, das dann einen hauptamtlichen Chief Artificial Intelligence Officer für die Stadt Gilbert einstellte, ebenfalls ein Novum für den Westen der USA.

„Nichts davon wäre passiert, wenn wir eine Art Sicherheitszaun errichtet hätten, mit dem diese speziellen Innovationen nicht möglich gewesen wären“, so Dr. Bryson. „Wenn es darum geht, innovativ zu sein und alles richtig auf den Weg zu bringen, ist dieses Gespräch der Ausgangspunkt.“

Rationalisieren und vereinfachen Sie den Sicherheitsstack

Eine der ersten Aufgaben von Dr. Bryson bestand darin, den Sicherheitsstack zu inventarisieren, um die Nutzung der einzelnen Produkte und Services zu verstehen. Diese Aufgabe deckte erhebliche Redundanzen auf. Eine Reduzierung und Rationalisierung würde Geld sparen, aber noch wichtiger war, dass das kleine Sicherheitsteam eine zentrale Benutzeroberfläche und eine einzige Quelle der Wahrheit erhalten musste, über die es die Cybersicherheitsfunktionen verwalten und Probleme beheben kann.

Dr. Bryson zitiert den alten Spruch, dass Komplexität der Feind der Cybersicherheit ist, und ergänzt: „Ich möchte nicht, dass Menschen von System zu System springen müssen, um herauszufinden, was vor sich geht.“

Richten Sie die richtigen Cybersicherheitsschutzmaßnahmen ein

Die InnovatorInnen im Unternehmen müssen die Schutzmaßnahmen, die für sichere Systeme und Daten sorgen, verstehen und einhalten. Bei diesen Regeln kann es sich um Policies, Zugriffskontrollen oder andere Grundsätze handeln, die den InnovatorInnen helfen, die Rahmenbedingungen zu verstehen. Diese Rahmenbedingungen sorgen für eine sichere Umgebung für Innovationen, die durch eine effektive Partnerschaft zwischen Sicherheitsfachkräften und InnovatorInnen geschaffen wird.

Copyright © 2024 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

DELL Technologies

Bleiben Sie flexibel, werden Sie kreativ

Dr. Bryson weist darauf hin, dass es zwar wichtig sei, Cybersicherheitsstandards zu verfolgen und durchzusetzen, Innovationen jedoch manchmal Flexibilität und Kreativität benötigen. Er betont: „Innovationen finden nicht nur in der Geschäftseinheit, sondern oft in der Informationstechnologie- und sogar der Informationssicherheitsabteilung statt. Möglicherweise müssen Sie neue und kreative Wege finden, um Ihre Systeme und Daten zu sichern, während Ihr Unternehmen um Sie herum Innovationen entwickelt. Darauf sollten Sie vorbereitet sein."

Fördern Sie eine starke Cybersicherheitskultur

Dr. Bryson betont, wie wichtig es sei, eine solide Sicherheitskultur zu entwickeln. „Die Unternehmenskultur ist entscheidend, … wenn es um Cybersicherheit geht. Wenn Sie keine Unternehmenskultur haben, in der die MitarbeiterInnen auf Cybersicherheit achten, muss Ihnen die Angriffsfläche der Bedrohungen bewusst sein."

Die Grundlage einer soliden Cybersicherheitskultur basiert auf vielen der bereits besprochenen Elemente: einem offenen und transparenten Dialog, einer umfassenden Einbeziehung, klar formulierten Standards und einem Geist der Zusammenarbeit zwischen dem Sicherheitsteam und seinen Kunden, und zwar sowohl internen als auch externen.

Angesichts des beschleunigten Wachstums muss sich die Cybersicherheit von einer reaktiven Grundhaltung mit Schwerpunkt auf der Verteidigung zu einem proaktiven Ansatz entwickeln, der die Förderung positiver Ergebnisse priorisiert.

Unternehmen sollten eine moderne Sicherheitsmentalität einführen, die nicht nur Schutz bietet, sondern auch Innovationen fördert.

Dies kann durch Kommunikation und Zusammenarbeit in Bezug auf die Integration der Sicherheitsmaßnahmen in den Entwicklungsprozess erreicht werden. Das Ziel ist eine Umgebung, in der Kreativität gefördert wird, ohne die Sicherheit zu beeinträchtigen.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth**.

Copyright © 2024 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

DELL Technologies