DELL Technologies

5

Consigli per un ambiente sicuro per l'innovazione

1	2	3	4	5
Comunica in anticipo e a cadenze regolari	**Razionalizza e semplifica lo stack di sicurezza**	**Stabilisci le barriere di sicurezza informatica**	**Sii flessibile, sii creativo**	**Promuovi una solida cultura della sicurezza**
Coinvolgi dirigenti ed entità interessate principali	Riduzione della complessità	Definisci le policy	Sii aperto a nuovi metodi di sicurezza	Favorisci un coinvolgimento ampio
Comprendi i piani per l'innovazione	Elimina la ridondanza	Implementa controlli degli accessi	Concentrati sui metodi di sicurezza che si adattano all'innovazione	Promuovi la trasparenza
Consenti al team addetto alla sicurezza di avviare la conversazione	Crea un unico pannello di gestione	Integrazione tra sistemi logici e fisici	Tieni presente che l'innovazione può avvenire nell'ufficio della sicurezza	Punta sulla collaborazione
	Sviluppa un solido processo di valutazione dell'approvvigionamento			

Crea un ambiente sicuro per l'innovazione.

Per massimizzare l'innovazione nel nostro mondo tecnologico e basato sui dati, la sicurezza informatica deve essere costruita per supportare l'innovazione. Ma in che modo un'organizzazione crea un ambiente che favorisce la crescita, la creatività e l'innovazione senza compromettere la sicurezza?

Per esaminare un esempio reale di tale ambiente, Sameer Shah di Dell Cybersecurity Marketing ha incontrato il Dott. Tony Bryson, Chief Information Security Officer (CISO) per la città di Gilbert, AZ, per discutere dell'innovativa iniziativa City of the Future e del ruolo che la sicurezza ha svolto.

Continua a leggere per un riepilogo delle raccomandazioni del Dott. Bryson e per guardare l'intera conversazione visita il sito **dell.com/cybersecuritymonth**.

> Assicurati di sapere quali sono gli obiettivi [delle entità interessate] e in che modo possono sfruttare la tecnologia e l'innovazione a vantaggio dell'azienda e del cliente".
>
> ***Dott. Tony Bryson**, Chief Information Security Officer (CISO) della città di Gilbert*

The City of the Future

L'iniziativa City of the Future della città di Gilbert è stata concepita per creare un'infrastruttura sostenibile e resiliente che utilizza i dati per arricchire la vita dei suoi cittadini. La tecnologia è fortemente coinvolta nella fornitura di servizi dal pagamento delle bollette per i residenti, alle operazioni sul traffico, alla disponibilità e alla qualità dell'acqua. Comporta anche la raccolta dei dati per prevedere l'utilizzo futuro dei servizi e le esigenze future. L'iniziativa non ha una data di conclusione predefinita, ma si tratta di un processo iterativo e dinamico che mira a garantire il progresso costante dell'iniziativa.

In qualità di primo CISO, il compito del Dott. Bryson era quello di adottare un approccio più strategico alla sicurezza informatica. La fornitura di servizi urbani moderni e tecnologici richiede solide funzioni di protezione dei dati, classificazione e controllo progettate per sostenere gli ambiziosi obiettivi della città.

Man mano che questo processo è proseguito e ha ottenuto risultati positivi, il Dott. Bryson ha identificato alcune raccomandazioni chiave che hanno facilitato il successo e creato il giusto ambiente in cui crescere e innovare in modo sicuro.

Comunica in anticipo e a cadenze regolari

Il dott. Bryson ha sottolineato la necessità di coinvolgere dirigenti e altre entità interessate principali nelle prime fasi del processo di innovazione. "Assicurati di sapere qual è il loro obiettivo e in che modo possono sfruttare la tecnologia e l'innovazione a vantaggio dell'azienda e del cliente", ha affermato.

Un'estensione naturale della comunicazione precoce è quella di avere la conversazione sulla sicurezza informatica all'inizio del ciclo di innovazione e, in qualità di partner chiave, il team di sicurezza informatica può essere il catalizzatore di queste discussioni.

L'uso dell'AI da parte della città di Gilbert è un ottimo esempio. L'ufficio per la sicurezza ha iniziato a discuterne due anni fa e ha assunto un ruolo di leadership nel porre domande critiche: come fidarsi dei dati generati dall'AI, come archiviarli e come garantire che i residenti abbiano compreso correttamente l'uso dell'AI. Ciò ha portato alla creazione di un comitato interfunzionale, che ha poi portato all'assunzione dello Chief Artificial Intelligence Officer a tempo pieno della città di Gilbert, una novità anche per gli Stati Uniti occidentali.

"Niente di tutto questo sarebbe successo se avessimo progettato una recinzione di sicurezza che impediva l'avvio di una particolare innovazione", afferma il Dott. Bryson. "Quindi, quando si tratta di cercare di innovare e cercare di fare le cose nel modo giusto, la conversazione è il punto iniziale".

Razionalizza e semplifica lo stack di sicurezza

Uno dei primi compiti del Dott. Bryson era fare l'inventario dello stack di sicurezza per comprendere l'uso di ciascun prodotto e servizio. Questo lavoro ha scoperto una ridondanza significativa. La riduzione e la razionalizzazione consentirebbero di risparmiare denaro, ma soprattutto offrirebbero al piccolo team di sicurezza un unico pannello di gestione e un'unica fonte di dati certi attraverso cui amministrare le funzionalità di sicurezza informatica e risolvere i problemi.

Il Dott. Bryson ha fatto eco al vecchio detto che la complessità è il nemico della sicurezza informatica quando ha detto: "Non voglio vedere persone costrette a rimbalzare da un sistema all'altro per cercare di capire cosa sta succedendo".

Stabilisci le barriere di sicurezza informatica giuste

Gli innovatori dell'organizzazione devono comprendere e rispettare le barriere per la sicurezza che garantiscono la sicurezza di sistemi e dati. Queste regole possono essere policy, controlli degli accessi o altri principi che aiutano gli innovatori a comprendere il terreno di gioco. Questo terreno rappresenta l'ambiente sicuro per l'innovazione, creato attraverso una partnership efficace tra sicurezza e innovatori.

DELL Technologies

Sii flessibile, sii creativo

Il Dott. Bryson ha evidenziato come, pur essendo fondamentale avere e far rispettare degli standard di sicurezza informatica, l'innovazione necessiterà talvolta di una certa fluidità e creatività. Ha sottolineato: "L'innovazione non si verifica solo nella business unit. Molte volte, l'innovazione nasce all'interno dell'ufficio informatico e persino nell'Information Security Office. Potrebbe essere necessario trovare modi nuovi e creativi per proteggere i sistemi e i dati man mano che l'azienda si innova. Quindi, bisogna essere sempre pronti".

Promuovi una solida cultura della sicurezza informatica

Bryson ha sottolineato l'importanza di sviluppare una solida cultura della sicurezza. "La cultura è praticamente tutto… quando si tratta di sicurezza informatica. Senza una cultura in cui le persone sono consapevoli della sicurezza informatica, si identifica solo la superficie delle minacce".

Le fondamenta di una solida cultura della sicurezza informatica si basano su molti degli elementi già discussi: dialogo aperto e trasparente, ampio coinvolgimento, standard chiaramente articolati e uno spirito di collaborazione tra il team di sicurezza e i suoi clienti, interni ed esterni.

Man mano che la crescita accelera, la sicurezza informatica deve evolversi da una posizione reattiva incentrata sulla difesa a un approccio proattivo che dà priorità a favorire risultati positivi.

Le organizzazioni devono adottare una moderna mentalità di sicurezza che non solo protegge ma favorisce anche l'innovazione.

Tutto questo può essere ottenuto attraverso la comunicazione e la collaborazione che integra le misure di sicurezza nel processo di sviluppo. L'obiettivo è un ambiente in cui la creatività prospera senza compromettere la sicurezza.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**

DELL Technologies