DELL Technologies

5

Zalecenia dotyczące bezpiecznego środowiska dla innowacji

1	2	3	4	5
Komunikuj się wcześnie i często	**Racjonalizuj i upraszczaj stos zabezpieczeń**	**Ustal bariery bezpieczeństwa cybernetycznego**	**Zachowaj elastyczność, wykaż się kreatywnością**	**Wspieraj silną kulturę bezpieczeństwa**
Zaangażuj kadrę kierowniczą i kluczowych interesariuszy	Redukuj złożoność	Definiuj zasady	Zachowaj otwartość na nowe metody zabezpieczeń	Zachęcaj do ogólnego zaangażowania
Poznaj plany dotyczące innowacji	Wyeliminuj nadmiarowość	Wdrażaj mechanizmy kontroli dostępu	Skoncentruj się na metodach zabezpieczeń uwzględniających innowacje	Promuj przejrzystość
Umożliw zespołowi ds. bezpieczeństwa rozpoczęcie rozmowy	Utwórz pojedynczy panel	Integruj systemy logiczne i fizyczne	Pamiętaj, że w biurze bezpieczeństwa można wprowadzać innowacje	Stymuluj współpracę
	Opracuj solidny proces oceny zamówień			

Wytwórz bezpieczne środowisko dla innowacji.

Aby zmaksymalizować innowacyjność w naszym świecie opartym na technologii i danych, cyberbezpieczeństwo musi być budowane z myślą o wspieraniu innowacji. Ale w jaki sposób organizacja może utworzyć środowisko umożliwiające rozwój, kreatywność i innowacyjność bez uszczerbku dla bezpieczeństwa?

Aby zbadać rzeczywisty przykład takiego środowiska, Sameer Shah z działu marketingu cyberbezpieczeństwa firmy Dell spotkał się z dr Tonym Brysonem, dyrektorem ds. bezpieczeństwa informacji (CISO) w mieście Gilbert w stanie Arizona w celu omówienia innowacyjnej inicjatywy „Miasto przyszłości” oraz roli, jaką odegrały zabezpieczenia w jej realizacji.

Czytaj dalej, aby zapoznać się z podsumowaniem zaleceń dr Brysona. Całą rozmowę możesz obejrzeć na stronie **dell.com/cybersecuritymonth**.

> Musisz wiedzieć, dokąd [interesariusze] chcą się udać i w jaki sposób mogą wykorzystać technologię i innowacje z korzyścią dla firmy i klienta.
>
> ***Dr Tony Bryson**, dyrektor ds. bezpieczeństwa informacji (CISO) dla miasta Gilbert*

Miasto przyszłości

Inicjatywa „Miasto przyszłości” miasta Gilbert ma na celu zbudowanie zrównoważonej, odpornej infrastruktury wykorzystującej dane do wzbogacenia życia mieszkańców. Technologia jest mocno zaangażowana w świadczenie usług — od mieszkańców płacących rachunki przez ruch drogowy po dostępność i jakość wody. Wiąże się również z gromadzeniem danych w celu przewidywania przyszłego korzystania z usług i potrzeb. Inicjatywa nie ma określonego punktu końcowego, jest raczej procesem iteracyjnym, który napędza ciągły postęp.

Zadaniem dr. Brysona jako pierwszego dyrektora ds. bezpieczeństwa informacji było przyjęcie bardziej strategicznego podejścia do cyberbezpieczeństwa. Zapewnienie nowoczesnych, opartych na technologii usług miejskich wymagałoby silnych funkcji ochrony danych, klasyfikacji i kontroli, zaprojektowanych z myślą o wspieraniu ambitnych celów miasta.

Ponieważ proces ten był kontynuowany i zakończył się sukcesem, dr Bryson zidentyfikował kilka kluczowych zaleceń, które umożliwiły sukces i wytworzyły odpowiednie środowisko, w którym można się bezpiecznie rozwijać i wprowadzać innowacje.

Komunikuj się wcześnie i często

Dr Bryson podkreślił potrzebę zaangażowania kadry kierowniczej i innych kluczowych interesariuszy na wczesnym etapie procesu innowacji. „Musisz wiedzieć, dokąd chcą się udać i w jaki sposób mogą wykorzystać technologię i innowacje z korzyścią dla firmy i klienta” — powiedział.

Naturalnym rozszerzeniem wczesnej komunikacji jest rozmowa na temat cyberbezpieczeństwa na początku cyklu innowacji, a zespół ds. cyberbezpieczeństwa, jako kluczowy partner, może być katalizatorem takich dyskusji.

Doskonałym przykładem jest wykorzystanie sztucznej inteligencji przez miasto Gilbert. Biuro bezpieczeństwa rozpoczęło rozmowy dwa lata temu i przejęło wiodącą rolę w zadawaniu krytycznych pytań: jak ufać danym generowanym przez sztuczną inteligencję, jak je przechowywać i jak sprawić, aby mieszkańcy właściwie rozumieli wykorzystanie sztucznej inteligencji? Doprowadziło to do utworzenia wielofunkcyjnego komitetu, który następnie doprowadził do zatrudnienia pełnoetatowego dyrektora ds. sztucznej inteligencji w mieście Gilbert, również po raz pierwszy w zachodnich Stanach Zjednoczonych.

„Nic z tego nie miałoby miejsca, gdybyśmy wyznaczyli ogrodzenie ochronne, które uniemożliwiłoby realizację tej konkretnej innowacji” — mówi dr Bryson. „Więc jeśli chodzi o próby wprowadzania innowacji i próby właściwego postępowania, wszystko zaczyna się od rozmowy”.

Racjonalizuj i upraszczaj stos zabezpieczeń

Jednym z pierwszych zadań dr Brysona była inwentaryzacja stosu zabezpieczeń w celu zrozumienia zastosowania każdego produktu i usługi. Wysiłek ten ujawnił znaczną nadmiarowość. Ograniczenie i racjonalizacja pozwoliłyby zaoszczędzić pieniądze, ale co ważniejsze, dałyby małemu zespołowi ds. bezpieczeństwa pojedynczy panel i jedno źródło informacji do zarządzania możliwościami cyberbezpieczeństwa i rozwiązywania problemów.

Dr Bryson przywołał starą maksymę, według której złożoność jest wrogiem cyberbezpieczeństwa, mówiąc: „Nie chcę, aby ludzie musieli przeskakiwać z systemu na system, próbując dowiedzieć się, co się dzieje”.

Ustal odpowiednie bariery dla bezpieczeństwa cybernetycznego

Innowatorzy w organizacji muszą znać i przestrzegać wytycznych, które zapewniają bezpieczeństwo systemów i danych. Reguły te mogą być politykami, mechanizmami kontroli dostępu lub innymi zasadami, które pomagają innowatorom poznać pole gry. To pole gry stanowi bezpieczne środowisko dla innowacji, stworzone dzięki skutecznemu partnerstwu między zabezpieczeniami a innowatorami.

DELL Technologies

Zachowaj elastyczność, wykaż się kreatywnością

Dr Bryson zauważył, że chociaż ważne jest, aby mieć i egzekwować standardy cyberbezpieczeństwa, innowacje będą czasami wymagały płynności i kreatywności. Zwrócił uwagę, że: „Innowacje nie pojawiają się tylko w jednostce biznesowej. Innowacje często zdarzają się w technologii informacyjnej, a nawet w biurze bezpieczeństwa informacji. Być może będzie trzeba znaleźć nowe, kreatywne sposoby zabezpieczenia systemów i danych, ponieważ twoja firma wprowadza innowacje wokół ciebie. Po prostu się na to przygotuj”.

Wspieraj silną kulturę cyberbezpieczeństwa

Dr Bryson podkreślił znaczenie rozwijania silnej kultury bezpieczeństwa. „Kultura to właściwie wszystko... W przypadku cyberbezpieczeństwa, jeśli nie masz kultury, w której ludzie są świadomi cyberbezpieczeństwa, rozpoznaj powierzchnię zagrożeń”.

Fundament solidnej kultury bezpieczeństwa cybernetycznego opiera się na wielu z omówionych już elementów: otwartym i przejrzystym dialogu, szerokim zaangażowaniu, jasno sformułowanych standardach oraz duchu współpracy między zespołem ds. bezpieczeństwa a jego klientami, zarówno wewnętrznymi, jak i zewnętrznymi.

W miarę przyspieszania rozwoju cyberbezpieczeństwo musi ewoluować od postawy reaktywnej skoncentrowanej na obronie do podejścia proaktywnego, w którym priorytetem jest umożliwienie uzyskania pozytywnych wyników.

Organizacje powinny przyjąć nowoczesne podejście do bezpieczeństwa, które nie tylko chroni innowacje, ale także je umożliwia.

Można to osiągnąć poprzez komunikację i współpracę, która integruje środki bezpieczeństwa z procesem rozwoju. Celem jest środowisko, w którym kreatywność rozwija się bez uszczerbku dla bezpieczeństwa.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **dell.com/cybersecuritymonth**

DELL Technologies