DELL Technologies

5

Aanbevelingen voor een veilige omgeving voor innovatie

1	2	3	4	5
Communiceer tijdig en vaak	**Rationaliseer en vereenvoudig de beveiligingsstack**	**Stel richtlijnen voor cyberbeveiliging vast**	**Blijf flexibel, wees creatief**	**Stimuleer een sterke veiligheidscultuur**
Betrek leidinggevenden en belanghebbenden	Reduceer complexiteit	Definieer beleidsregels	Sta open voor nieuwe beveiligingsmethoden	Faciliteer brede betrokkenheid
Begrijp de plannen voor innovatie	Elimineer redundantie	Implementeer toegangscontroles	Richt u op beveiligingsmethoden die innovatie mogelijk maken	Bevorder transparantie
Geef het beveiligingsteam meer mogelijkheden om het gesprek aan te gaan	Creëer een centraal overzicht	Integreer in logische en fysieke systemen	Houd er rekening mee dat innovatie kan plaatsvinden binnen de beveiligingsafdeling	Stimuleer samenwerking
	Ontwikkel een sterk inkoopevaluatieproces			

Creëer een veilige omgeving voor innovatie.

Om innovatie te maximaliseren in onze technologie- en datagedreven wereld, moet cyberbeveiliging worden opgebouwd om innovatie te ondersteunen. Maar hoe creëert een organisatie een omgeving die groei, creativiteit en innovatie mogelijk maakt zonder dat dit ten koste gaat van de beveiliging?

Om een praktijkvoorbeeld van een dergelijke omgeving te onderzoeken, heeft Sameer Shah van Dell Cybersecurity Marketing een ontmoeting gehad met Dr. Tony Bryson, de Chief Information Security Officer (CISO) van de stad Gilbert, Arizona, om het innovatieve initiatief City of the Future en de rol die beveiliging heeft gespeeld bij het aansturen ervan te bespreken.

Lees verder voor een samenvatting van de aanbevelingen van Dr. Bryson en om het volledige gesprek te bekijken, bezoek **dell.com/cybersecuritymonth**.

> Zorg ervoor dat u weet waar [belanghebbenden] naartoe willen en hoe ze technologie en innovatie waarschijnlijk zullen inzetten om het bedrijf en de klant te bevoordelen."
>
> ***Dr. Tony Bryson**, de Chief Information Security Officer (CISO) voor de stad Gilbert*

De City of the Future

Het City of the Future-initiatief van de stad Gilbert is ontworpen om een duurzame, veerkrachtige infrastructuur te bouwen die data gebruikt om het leven van haar burgers te verrijken. Technologie speelt een grote rol bij het leveren van diensten, van het betalen van rekeningen door bewoners tot verkeersbeheer en de beschikbaarheid en kwaliteit van water. Het omvat ook het verzamelen van data om toekomstig gebruik van diensten en behoeften te voorspellen. Het initiatief heeft geen duidelijk eindpunt, maar is een iteratief proces dat voortdurende vooruitgang stimuleert.

Als de eerste CISO kreeg Dr. Bryson de opdracht om een meer strategische benadering van cyberbeveiliging te hanteren. Het leveren van moderne, op technologie gebaseerde stadsdiensten vereiste sterke databescherming, classificatie en controlefuncties die waren ontworpen om de ambitieuze doelstellingen van de stad te ondersteunen.

Naarmate dat proces werd voortgezet en succesvol was, heeft Dr. Bryson een paar belangrijke aanbevelingen geïdentificeerd die het succes mogelijk maakten en de juiste omgeving creëerden om veilig te groeien en te innoveren.

Communiceer tijdig en vaak

Dr. Bryson benadrukte de noodzaak om leidinggevenden en andere belangrijke belanghebbenden vroeg in het innovatieproces te betrekken. "Zorg ervoor dat u weet waar ze naartoe willen en hoe ze technologie en innovatie waarschijnlijk zullen inzetten om het bedrijf en de klant te bevoordelen", zei hij.

Een natuurlijke uitbreiding van vroege communicatie is om het gesprek over cyberbeveiliging al bij de start van de innovatiecyclus te voeren, en als belangrijke partner kan het cyberbeveiligingsteam de katalysator zijn voor deze gesprekken.

Het gebruik van AI door de stad Gilbert is daar een goed voorbeeld van. Het Security Office begon deze gesprekken twee jaar geleden en nam een leidende rol op zich bij het stellen van kritische vragen: Hoe kan door AI gegenereerde data worden vertrouwd? Hoe kan deze worden opgeslagen? en Hoe kan ervoor worden gezorgd dat bewoners het gebruik van AI goed begrijpen? Dit leidde tot de oprichting van een cross-functionele commissie, wat vervolgens leidde tot de aanwerving van de fulltime Chief Artificial Intelligence Officer van de stad Gilbert, ook een primeur voor het westen van de VS.

"Niets van dit alles zou zijn gebeurd als we een veiligheidsbarrière hadden opgeworpen die die specifieke innovatie zou hebben tegengehouden", zegt Dr. Bryson. "Dus als het gaat om proberen te innoveren en dingen op de juiste manier doen, begint het met een gesprek."

Rationaliseer en vereenvoudig de beveiligingsstack

Een van de eerste taken van Dr. Bryson was het inventariseren van de beveiligingsstack om inzicht te krijgen in het gebruik van elk product en elke dienst. Die inspanning bracht aanzienlijke redundantie aan het licht. Verminderen en rationaliseren zou geld besparen, maar wat nog belangrijker is, het zou het kleine beveiligingsteam een enkel overzicht en een enkele bron van waarheid geven om de cyberbeveiligingscapaciteiten te beheren en problemen aan te pakken.

Dr. Bryson herhaalde het oude gezegde dat complexiteit de vijand van cyberbeveiliging is toen hij zei: "Ik wil niet dat mensen van systeem naar systeem moeten springen om erachter te komen wat er aan de hand is."

Stel de juiste richtlijnen voor cyberbeveiliging vast

De innovators binnen de organisatie moeten de veiligheidsrichtlijnen begrijpen en naleven die systemen en data beschermen. Die regels kunnen bestaan uit beleidslijnen, toegangscontroles of andere principes die de innovators helpen het speelveld te begrijpen. Dit speelveld vertegenwoordigt de veilige omgeving voor innovatie, gecreëerd door een effectief partnerschap tussen de beveiliging en de innovators.

DELL Technologies

Blijf flexibel, wees creatief

Dr. Bryson merkte op dat, hoewel het belangrijk is om cyberbeveiligingsnormen te hebben en te handhaven, innovatie soms flexibiliteit en creativiteit vereist. Hij wees erop: "Innovatie vindt niet alleen plaats binnen de business unit. Innovatie gebeurt vaak binnen de informatietechnologie en zelfs op de afdeling Informatiebeveiliging. Misschien moet u nieuwe en creatieve manieren vinden om uw systemen en data te beveiligen terwijl uw bedrijf om u heen innoveert. Dus wees daar op voorbereid."

Bevorder een sterke cyberbeveiligingscultuur

Dr. Bryson benadrukte het belang van het ontwikkelen van een sterke veiligheidscultuur. "Cultuur is zo'n beetje alles... als het gaat om cyberbeveiliging. Als u geen cultuur hebt waarin mensen zich bewust zijn van cyberbeveiliging, herken dan het dreigingsoppervlak."

De basis van een robuuste cyberbeveiligingscultuur is gebouwd op veel van de reeds besproken elementen: open en transparante dialoog, brede betrokkenheid, duidelijk geformuleerde normen en een geest van samenwerking tussen het beveiligingsteam en zijn klanten, zowel intern als extern.

Naarmate de groei versnelt, moet cyberbeveiliging zich ontwikkelen van een reactieve, op verdediging gerichte houding naar een proactieve aanpak die prioriteit geeft aan het bevorderen van positieve resultaten.

Organisaties moeten een moderne beveiligingsmentaliteit aannemen die niet alleen beschermt, maar ook innovatie mogelijk maakt.

Dit kan worden bereikt door middel van communicatie en samenwerking die beveiligingsmaatregelen integreert in het ontwikkelingsproces. Het doel is een omgeving waarin creativiteit gedijt zonder de beveiliging in gevaar te brengen.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van vandaag kunt aanpakken op **dell.com/cybersecuritymonth**

DELL Technologies