

5

Rekommendationer för en säker miljö för innovation



1	2	3	4	5
Kommunicera tidigt och ofta Engagera chefer och viktiga intressenter Förstå planerna för innovation Ge säkerhetsteamet möjlighet att inleda samtalet	Rationalisera och förenkla säkerhetsstacken Minska komplexiteten Eliminera redundans Skapa en enda hanteringskonsol Utarbeta en robust process för utvärdering av upphandling	Upprätta cybersäkerhet- skydd Definiera policyer Implementera åtkomstkontroller Integrera över logiska och fysiska system	Var flexibel och kreativ Var öppen för nya säkerhetsmetoder Fokusera på säkerhetsmetoder som tillgodoser innovation Tänk på att innovation kan ske på säkerhetskontolet	Främja en stark säkerhetskultur Underlätta ett brett engagemang Främja transparens Uppmuntra till samarbete

Skapa en säker miljö för innovation.

För att maximera innovationen i vår teknik- och datadrivna värld måste cybersäkerhet byggas upp för att stödja innovation. Men hur skapar en organisation en miljö som främjar tillväxt, kreativitet och innovation utan att kompromissa med säkerheten?

För att undersöka ett verkligt exempel på en sådan miljö hade Sameer Shah från Dell Cybersecurity Marketing ett möte med dr Tony Bryson, Chief Information Security Officer (CISO) för staden Gilbert i Arizona, där de diskuterade det innovativa initiativet City of the Future och säkerhetens roll i det.

Läs vidare för en sammanfattning av dr Brysons rekommendationer, och för att se hela samtalet kan du gå till dell.com/cybersecuritymonth.

Kommunicera tidigt och ofta

Dr Bryson betonade behovet av att engagera chefer och andra viktiga intressenter tidigt i innovationsprocessen. "Se till att du vet vart de vill och hur de sannolikt utnyttjar teknik och innovation för att gynna verksamheten och kunden", säger han.

En naturlig förlängning av att kommunicera tidigt är att ha samtalet om cybersäkerhet i början av innovationscykeln, och som en viktig partner kan cybersäkerhetsteamet vara en katalysator för dessa diskussioner.

Staden Gilberts användning av AI är ett utmärkt exempel. Säkerhetskontoret inledde dessa samtal för två år sedan och hade en ledande roll när det gäller att ställa kritiska frågor: hur kan man lita på AI-genererade data, hur lagrar man dem och hur säkerställer man att invånarna förstår användningen av AI rätt. Detta ledde till skapandet av en tvärfunktionell kommitté, som sedan ledde till anställningen av staden Gilberts heltidsanställda Chief Artificial Intelligence Officer, vilket även är den första i västra USA.

"Inget av detta skulle ha hänt om vi hade satt upp ett säkerhetsstängsel som förhindrade att just den innovationen skulle ske", säger dr Bryson. "Så när det gäller att försöka förnya sig och försöka göra saker på rätt sätt är det i samtalet det börjar."

Rationalisera och förenkla säkerhetsstacken

En av dr Brysons första uppgifter var att inventera säkerhetsstacken för att förstå användningen av varje produkt och tjänst. Det arbetet avslöjade betydande redundans. Att reducera och rationalisera skulle spara pengar, men ännu viktigare var att det skulle ge det lilla säkerhetsteamet en enda hanteringskonsol och en enda kunskapskälla för att kunna administrera cybersäkerhetsfunktionerna och ta itu med olika problem.

Dr Bryson refererade till det gamla ordspråket att komplexitet är cybersäkerhetens fiende när han sa: "Jag vill inte att människor ska behöva hoppa från system till system för att försöka ta reda på vad som händer."

Upprätta rätt cybersäkerhetsskydd

Innovatörerna i organisationen måste förstå och följa de säkerhetsriktlinjer som håller system och data säkra. Dessa regler kan vara policyer, åtkomstkontroller eller andra principer som hjälper innovatörerna att förstå spelplanen. Denna spelplan representerar en säker miljö för innovation, som skapas genom ett effektivt partnerskap mellan säkerhet och innovatörer.

Var flexibel och kreativ

Dr Bryson noterade att även om det är viktigt att ha och upprätthålla cybersäkerhetsstandarder kräver innovation ibland smidighet och kreativitet. Han påpekade att "innovation inte bara sker i affärsenheten. Innovation sker många gånger inom informationsteknik och även på avdelningen för informationssäkerhet. Du kan behöva hitta nya och kreativa sätt att skydda dina system och data när ditt företag förnyas runt omkring dig. Så var bara beredd på det."

Se till att du vet vart [intressenterna] vill och hur de sannolikt utnyttjar teknik och innovation för att gynna verksamheten och kunden."

Dr Tony Bryson, Chief Information Security Officer (CISO) för staden Gilbert

City of the Future

Staden Gilberts initiativ City of the Future utformades för att skapa en hållbar, tålig infrastruktur som använder data för att berika invånarnas liv. Tekniken är starkt involverad i att tillhandahålla alla möjliga tjänster, från invånare som betalar sina räkningar, till trafikkontroll, till vattentillgänglighet och vattenkvalitet. Det handlar också om att samla in data för att förutsäga framtida användning och behov av tjänster. Initiativet har ingen avgränsad slutpunkt, utan är en iterativ process som driver på utvecklingen.

Som dess första CISO var dr Brysons mandat att ha ett mer strategiskt förhållningssätt till cybersäkerhet. Att tillhandahålla moderna teknikbaserade kommunala tjänster skulle kräva robusta funktioner för dataskydd, klassificering och kontroll som är utformade för att stödja stadens ambitiösa mål.

I takt med att den processen har fortsatt och varit framgångsrik har dr Bryson identifierat några viktiga aspekter som bidragit till framgången och skapat rätt miljö för tillväxt och förnyelse på ett säkert sätt.

Främja en stark cybersäkerhetskultur

Dr Bryson betonade vikten av att utveckla en stark säkerhetskultur. "Kultur är i stort sett allt ... när det gäller cybersäkerhet. Om du inte har en kultur där människor är medvetna om cybersäkerheten måste du känna igen hotytan."

Grunden för en robust cybersäkerhetskultur bygger på många av de element som redan diskuterats: öppen och transparent dialog, brett engagemang, tydligt formulerade standarder och en anda av samarbete mellan säkerhetsteamet och dess kunder, både interna och externa.

I takt med att tillväxten accelererar måste cybersäkerheten utvecklas från en reaktiv hållning med fokus på försvar till en proaktiv strategi som prioriterar främjande av positiva resultat.

Organisationer bör anta ett modernt säkerhetstänk som inte bara skyddar utan även möjliggör innovation.

Detta kan uppnås genom kommunikation och samarbete som integrerar säkerhetsåtgärder i utvecklingsprocessen. Målet är en miljö där kreativiteten frodas utan att kompromissa med säkerheten.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på dell.com/cybersecuritymonth