DELL Technologies

5 Recomendações para um ambiente de inovação seguro

1	2	3	4	5
Comunique-se com antecedência e com frequência	**Racionalize e simplifique a pilha de segurança**	**Estabeleça barreiras de segurança cibernética**	**Seja flexível e criativo**	**Promova uma cultura de segurança sólida**
Envolva os executivos e as principais partes interessadas	Reduzir a complexidade	Defina políticas	Esteja aberto a novos métodos de segurança	Facilite o amplo envolvimento
Entenda os planos de inovação	Elimine a redundância	Implemente controles de acesso	Concentre-se em métodos de segurança que acomodam a inovação	Promova a transparência
Capacite a equipe de segurança para iniciar a conversa	Crie um único painel de controle	Integração entre sistemas lógicos e físicos	Lembre-se de que a inovação pode ocorrer no escritório de segurança	Promova a colaboração
	Desenvolva um sólido processo de avaliação de compras			

Crie um ambiente seguro para inovação.

Para maximizar a inovação em nosso mundo orientado por dados e tecnologia, a segurança cibernética deve ser desenvolvida para apoiar a inovação. Mas como uma organização cria um ambiente que capacita o crescimento, a criatividade e a inovação sem comprometer a segurança?

Para investigar um exemplo real desse ambiente, Sameer Shah, da área de marketing de segurança cibernética da Dell, reuniu-se com o Dr. Tony Bryson, Diretor de segurança da informação (CISO) da cidade de Gilbert, Arizona, para discutir a inovadora iniciativa Cidade do Futuro e o papel que a segurança desempenhou ao impulsioná-la.

Continue lendo para obter um resumo das recomendações do Dr. Bryson e para assistir a toda a conversa. Visite **dell.com/cybersecuritymonth**.

> "Certifique-se de saber para onde [as partes interessadas] querem ir e como elas provavelmente aproveitarão a tecnologia e a inovação para beneficiar a empresa e o cliente."
>
> ***Dr. Tony Bryson**, Diretor de segurança da informação (CISO) da cidade de Gilbert*

A cidade do futuro

A iniciativa Cidade do Futuro da cidade de Gilbert foi projetada para construir uma infraestrutura sustentável e resiliente que usa dados para melhorar a vida de seus cidadãos. A tecnologia está fortemente envolvida na prestação de serviços, desde os moradores que pagam suas contas, até as operações de tráfego, a disponibilidade e qualidade da água. Ela também envolve a coleta de dados para prever o uso e as necessidades futuras dos serviços. A iniciativa não tem um ponto final definido, mas é um processo iterativo que impulsiona o progresso contínuo.

Como seu primeiro CISO, o mandato do Dr. Bryson era adotar uma abordagem mais estratégica para a segurança cibernética. Fornecer serviços urbanos modernos e habilitados para tecnologia exigiria forte proteção de dados e funções de classificação e controle projetadas para apoiar os objetivos ambiciosos da cidade.

À medida que esse processo continuou e teve sucesso, o Dr. Bryson identificou algumas recomendações importantes que facilitaram o sucesso e criaram o ambiente certo para crescer e inovar com segurança.

Comunique-se com antecedência e com frequência

O Dr. Bryson enfatizou a necessidade de envolver executivos e outras partes interessadas importantes no início do processo de inovação. "Certifique-se de saber para onde eles querem ir e como eles provavelmente aproveitarão a tecnologia e a inovação para beneficiar o negócio e o cliente", disse ele.

Uma extensão natural da comunicação precoce é ter uma conversa sobre segurança cibernética no início do ciclo de inovação. E como um parceiro-chave, a equipe de segurança cibernética pode ser o catalisador dessas discussões.

O uso de IA pela cidade de Gilbert é um excelente exemplo. O Escritório de segurança iniciou essas conversas há dois anos e assumiu um papel de liderança ao fazer perguntas críticas: como confiar nos dados gerados pela IA, como armazená-los e como garantir que os residentes entendessem corretamente o uso da IA. Isso levou à criação de um comitê multifuncional, que levou à contratação do diretor de inteligência artificial em tempo integral de Gilbert, também uma novidade para o oeste dos EUA.

"Nada disso teria acontecido se estivéssemos desenhando uma cerca de segurança que impedisse essa inovação em particular de acontecer", diz Bryson. "Então, quando se trata de tentar inovar e fazer as coisas da maneira certa, a conversa é o ponto de partida".

Racionalize e simplifique a pilha de segurança

Uma das primeiras tarefas do Dr. Bryson foi inventariar a pilha de segurança para entender o uso de cada produto e serviço. Esse esforço revelou uma redundância significativa. Reduzir e racionalizar economizaria dinheiro, mas, mais importante, daria à pequena equipe de segurança um painel de controle único e uma única fonte de verdade para administrar os recursos de segurança cibernética e resolver problemas.

O Dr. Bryson ecoou o velho ditado de que a complexidade é inimiga da segurança cibernética quando disse: "Não quero ver as pessoas tendo que pular de sistema em sistema tentando descobrir o que está acontecendo".

Estabeleça as proteções de segurança cibernética certas

Os inovadores na organização precisam entender e respeitar os guias de segurança que mantêm os sistemas e dados seguros. Essas regras podem ser políticas, controles de acesso ou outros princípios que ajudam os inovadores a entender o campo de atuação. Ele representa o ambiente seguro para a inovação, criado por meio de uma parceria eficaz entre a segurança e os inovadores.

Seja flexível e criativo

O Dr. Bryson observou que, embora seja importante ter e aplicar padrões de segurança cibernética, a inovação exigirá fluidez e criatividade às vezes. Ele ressaltou: "A inovação não acontece apenas na unidade de negócios. A inovação muitas vezes acontece dentro da tecnologia da informação e até mesmo no escritório de Segurança da informação. Talvez você precise encontrar maneiras novas e criativas de proteger seus sistemas e dados à medida que sua empresa inova ao seu redor. Então esteja preparado para isso".

DELL Technologies

Promova uma forte cultura de segurança cibernética

Dr. Bryson enfatizou a importância de desenvolver uma forte cultura de segurança. "Cultura é praticamente tudo... quando se trata de segurança cibernética. Se você não tem uma cultura em que as pessoas estejam cientes da segurança cibernética, reconheça a superfície de ameaça".

A base de uma cultura de segurança cibernética robusta é construída sobre muitos dos elementos já discutidos: diálogo aberto e transparente, amplo envolvimento, padrões claramente articulados e um espírito de colaboração entre a equipe de segurança e seus clientes, internos e externos.

À medida que o crescimento acelera, a segurança cibernética deve evoluir de uma postura reativa focada na defesa para uma abordagem proativa que priorize a facilitação de resultados positivos.

As organizações devem adotar uma mentalidade de segurança moderna que não apenas proteja, mas também capacite a inovação. Isso pode ser alcançado por meio de comunicação e colaboração que integrem medidas de segurança no processo de desenvolvimento. O objetivo é um ambiente em que a criatividade prospere sem comprometer a segurança.

Saiba como lidar com alguns dos principais desafios de segurança cibernética atuais em **dell.com/cybersecuritymonth**

DELL Technologies