**A natureza evolutiva dos CISOs em 2023**

À medida que iniciamos 2023, percebemos que a função do Chief Information Security Officer(CISO) está a mudar mais do que nunca. Uma vez que a cibersegurança continua a ser uma discussão da responsabilidade da direção, e os riscos de cibersegurança continuam a aumentar, os CISOs têm acesso substancial dentro de uma organização, mas também enfrentam uma pressão significativa:

**1) Uma das maiores mudanças da sua função dentro de uma empresa nos últimos 3 anos?**

Nos últimos anos, a função do CISO alterou-se drasticamente. Com o aumento dos ciberataques, espera-se agora que os CISOs não só protejam os dados, mas também sejam proativos na identificação e prevenção de potenciais ameaças. Além disso, os CISOs são, atualmente, e frequentemente, encarregados de desenvolver e implementar estratégias de segurança para toda a organização, e não apenas para o departamento de TI. Algo que, há uma década, era impensável, na medida em que os CISOs não eram considerados tão importantes como são hoje.

O recém considerado CISO conta, agora, com um orçamento, uma equipa e o direito de recrutar diretamente. Por vezes, a voz do CISO prevalece sobre a de outros profissionais com mais anos de empresa e mesmo estabelecidos a um nível superior. De facto, ao longo dos últimos anos, a política de teletrabalho, a base de dados colaborativa, os relatórios legais, e mesmo os itinerários de desenvolvimento de aplicações core inovadoras têm sido colocados sob a sua liderança direta.

**2) A função mudou o foco operacional?**

Nos últimos anos, tem havido uma mudança na função do CISO, passando de um foco operacional para um foco estratégico. Isto deve-se ao aumento das exigências colocadas aos CISOs para proteger as organizações contra as ciber ameaças. Para ter sucesso, os CISOs devem agora ter uma compreensão complexa do negócio, dos seus riscos e dos seus objetivos, bem como serem capazes de construir e manter relações com as principais partes interessadas.

Um exemplo desta mudança é que, agora, a direção quer mais do que apenas um acordo a nível de serviço sobre a resposta a incidentes de segurança. Em vez disso, procuram um acordo a nível de proteção para assegurar que os bens digitais sejam continuamente corrigidos e protegidos para reagir proactivamente a ciberataques que possam impactar os negócios.

**3) Ao demonstrar o valor do negócio, qual é a estratégia mais importante que devem ter em conta?**

Os CISOs devem ter sempre em mente a importância da estratégia ao demonstrarem o valor do negócio. Isto significa considerar tanto os efeitos a curto, como a longo prazo, das decisões, fazendo escolhas que beneficiarão a empresa como um todo. A curto prazo, pode ser tentador cortar cantos ou escolher atalhos, mas fazê-lo pode colocar em risco a segurança da empresa a longo prazo. É crucial lembrar que o objetivo é proteger os dados e bens da organização, não apenas para poupar dinheiro. Desta forma, uma das estratégias mais eficazes de demonstrar o valor do negócio passa por compreender a sua "kill chain". A maioria dos CISOs estão muito familiarizados com o conceito técnico" kill chain" em cibersegurança, mas é importante compreender também o impacto que um ciberataque pode ter em operações críticas e respetiva perda de receitas ou reputação que dele pode resultar. Os CISOs devem, não só priorizar e salvaguardar os bens e dados, de acordo com a kill chain de valor de negócio, como adotar uma abordagem holística, considerando os benefícios das soluções.

Ao discutir o acesso seguro, por exemplo, a implementação de tecnologias de autenticação poderia parecer uma mudança de comportamento aos olhos dos utilizadores que só são expostos à VPN uma vez por dia. Contudo, o benefício global de toda uma infraestrutura dinamicamente protegida por uma estratégia ZTNA holística é muito superior à segurança da sessão, da aplicação ou do segmento. O CISO deve ser fluente na articulação destes benefícios e na sua expressão em termos de riscos, para que as partes interessadas compreendam que os prós compensam os contras.

**4) Quais são algumas das novas funções “esperadas” nas organizações de hoje?**

A função do CISO evoluiu e expandiu-se para satisfazer as necessidades em constante mudança das organizações. Atualmente, espera-se que os CISOs não sejam apenas tecnicamente conhecedores, mas também pensadores estratégicos que possam ajudar as organizações a explorar o complexo panorama da cibersegurança. Para além das responsabilidades tradicionais, tais como o desenvolvimento e implementação de políticas e procedimentos de segurança, espera-se que tenha, também, uma compreensão profunda das operações e objetivos empresariais, alinhando as suas estratégias de segurança com os objetivos da organização.

Com a evolução da cibersegurança, também a função do CISO terá de evoluir, juntamente com a mentalidade de todas as organizações. A dimensão do papel humano é um fator-chave de sucesso quando se considera que 60% dos projetos de transformação continuam a falhar por terem subestimado o aspeto da adoção pelo utilizador. As políticas que mudam a forma como os colaboradores trabalham, tais como o teletrabalho, ZTNA, ou DevOps, precisam de ser explicadas antes de serem aplicadas. Explicar que o “porquê” da cibersegurança é tão importante como implementar o "como".

**5) Que comentário adicional pode incluir sobre a mudança da função do CISO?**

Em resumo, o papel do CISO já não consiste apenas em proteger a organização das ciber ameaças. Os CISOs são agora desbloqueadores chave dos negócios, incumbidos de fornecer valor a estes mesmos negócios. Atuar como Controlador de Risco reduz o risco operacional e melhora a postura de segurança da organização, atuando como agente de mudança. Além disso, o CISO atual atua como um comunicador eficaz para o conselho de administração para ajudar a fechar as lacunas de cibersegurança da organização.

*Daniel Kwong e Alain Sanchez, Fortinet Field CISOs*