IT2TA de março: Cyber Security Management: “as equipas de segurança não podem funcionar como bombeiros”

No dia 21 de março fizemos mais um It’s Time To Talk About. Nesta sessão, o itSMF Portugal reforçou as preocupações para com a partilha dass questões de gestão da cibersegurança com o Fractional CISO em várias organizações e CISO da miioelectric.com, José Casinha.

A apresentação sobre “Cyber Security Management” focou-se na vertente do Outcome Based Security Program e ainda em Priorities and Capacity. O tema da gestão da cibersegurança pode ser endereçado pelas organizações de diferentes maneiras; as maiores contratam consultoras que instalam processos detalhados e implicam a compra de materiais e **partilha de responsabilidades entre a organização e os fornecedores.** Esses programas podem, por vezes, não potenciar as mudanças internas que as organizações atravessam e podem ser vistos como um paliativo aos olhos de uma lógica de projeto temporário.

Um programa de cibersegurança baseado no resultado e no valor que vai acrescentar à organização é o que tem melhores hipóteses de ser bem-sucedido. A *framework* é uma abordagem que está adaptada para proteger os ativos de uma organização das suas maiores ameaças. As iniciativas a desenvolver por uma equipa de cibersegurança devem ter em conta os objetivos da organização no momento em que são aplicadas e é

preciso ter-se a consciência que estes não serão os que se verificam no final porque são muitas áreas e muitas as ISO que dizem respeito a um programa de segurança. Colaboradores e fornecedores têm de trabalhar, também, nessa ciber-resiliência, seja de serviços seja de produtos.

Quais os critérios que são a prioridade?

Em primeiro lugar, o gestor de cibersegurança deve olhar para a atividade que está em causa com a perspetiva de mapear o trabalho e alinhar o seu esforço com a atividade e objetivos da empresa (que vão mudando). **Esse trabalho a desenvolver tem de estar alinhado com todas as áreas de negócio da empresa**. Com o Outcome Based Security Program, e percebendo bem os objetivos da organização, consegue-se uma otimização de recursos, aumento do foco e uma lógica de gestão de risco mais assertiva.

A mensagem que vai para o exterior da organização tem de estar alinhada com a mensagem interna e têm de se encontrar métricas – uma definição de "done" para a segurança não ser um constrangimento. Complementarmente aos objetivos de longo prazo, a getão da cibersegurança também os deve ter, enquanto os diferentes departamentos da organização devem estar informados sobre o progresso alcançado nesta matéria. Os riscos têm de ser acautelados muito cedo em todo o processo: por exemplo, se o *outcome* é que não vai haver sistemas na *cloud* com vulnerabilidade, então tem de se mudar essa ambição para se ter *security access* com zero vulnerabilidades no ponto de partida. "As equipas de segurança não são bombeiros das organizações, tem de haver trabalho prévio de acompanhamento com todos os departamentos", salienta José Casinha.

Para o trabalho ser automatizado, tem de se repensar a forma como se trabalha.

A proposta de José Casinha para o Outcome Based Security Program passa por se fazer uma aproximação que faz parte da Scaled Agile Framework ® (SAFe ®) - um conjunto de padrões organizacionais e de fluxo de trabalho para implementar práticas ágeis em escala empresarial.

A SAFe promove alinhamento, colaboração e entrega entre um grande número de equipas devidamente alinhadas com o objetivo global da organização. À medida que as empresas crescem, o SAFe fornece uma abordagem estruturada para escalar a agilidade.

Já o PR Planning olha para o trabalho a fazer no prazo compreendido entre 8 a 12 semanas e junta equipas sob o mesmo desígnio com um planeamento conjunto (logo desde o início): área do legal, engenharia, IT, *sales support*, recursos humanos e produto - todas têm de estar alinhadas e são acompanhadas em termos de segurança.

A capacidade é planeada em função da velocidade (o número de pessoas disponíveis e do esforço que cada uma tem de fazer para determinada análise de capacidade), nível de complexidade (será um assunto novo) e conhecimento sobre o mesmo.

O próximo It's Time To Talk About realiza-se a 17 de abril sob o tema "ISO 42001 - AI Management System".