Gerir o risco (que está sempre à espreita)

itsecurity.pt/news/analysis/gerir-o-risco-que-esta-sempre-a-espreita

O ambiente de negócio é cada vez mais dinâmico. As organizações têm de lidar com novas ferramentas, novas oportunidades e, também, novos riscos que vão aparecendo à medida que o negócio evolui.

Gerir o risco é, assim, imperativo para as organizações que pretendem avançar o seu negócio com as menores preocupações possíveis. Uma abordagem integrada da gestão de riscos traz vários benefícios para as organizações, mas, também, desafios que os líderes têm de enfrentar.

Benefícios

> ***"Estes utilizadores precisam de soluções que integrem o poder da Inteligência Artificial (IA) e soluções baseadas nas melhores práticas da gestão de risco integrada: flexíveis na adaptação às mudanças regulatórias, mas simples o suficiente para utilizadores funcionais sem grande esforço de formação"***
>
> ***Duarte Caldas, Data & AI Partner Technical Specialista da IBM Portugal***

Duarte Caldas, Data & AI Partner Technical Specialista da IBM Portugal, refere que, cada vez mais, "as empresas precisam de ter a capacidade de reconhecer e gerir quer riscos, quer desafios de conformidade". Com o "aumento dramático de utilizadores ativos" que as empresas estão a testemunhar, as organizações estão a utilizar "ferramentas com recursos inconsistentes". Diz Duarte Caldas que "estes utilizadores precisam de soluções que integrem o poder da Inteligência Artificial (IA) e soluções baseadas nas melhores práticas da gestão de risco integrada: flexíveis na adaptação às mudanças regulatórias, mas simples o suficiente para utilizadores funcionais sem grande esforço de formação".

Uma abordagem integrada à gestão de riscos ajuda, assim, as organizações "a simplificar processos, melhorar a tomada de decisão e fornecer uma visão abrangente dos potenciais riscos, levando a uma mitigação de riscos mais eficaz".

Bruno Castro, Fundador & CEO da VisionWare, relembra que uma abordagem integrada à gestão de riscos se concentra "na avaliação de riscos no contexto mais amplo da estratégia empresarial" o que, "por si só", já "é vantajoso na medida em que atua como

uma estrutura que garante que os principais riscos são compreendidos e considerados em conjunto com outros riscos, e não de forma isolada". Esta visão holística, explica, facilita o processo de tomada de decisão – já que permite ter uma maior compreensão dos riscos –, assim como da conformidade com as diferentes regulamentações.

Outro benefício, refere, é, "sem dúvida, o aumento da resiliência e eficiência operacional, já que permite às organizações, identificar e mitigar proativamente os riscos, evitar interrupções nos processos de negócios e assim minimizar potenciais perdas financeiras".

Fábio Ribeiro, Sales Engineer da WatchGuard Portugal, defende que "a adoção de uma abordagem integrada à gestão de riscos é vital para fortalecer a postura de cibersegurança de uma organização", uma vez que permite ter uma visão holística e abrangente dos riscos de segurança. Esta estratégia "facilita a identificação e avaliação proativa de riscos, desde ameaças externas até vulnerabilidades internas, e promove uma resposta coordenada e eficaz a incidentes de segurança".

Ao mesmo, permite uma "alocação mais eficiente de recursos de segurança e assegura a conformidade com regulamentações, resultando numa melhor proteção contra ataques informáticos e numa postura de segurança mais robusta em todos os níveis da organização".

Desafios para os líderes

"Sem dúvida, o aumento da resiliência e eficiência operacional, já que permite às organizações, identificar e mitigar proativamente os riscos, evitar interrupções nos processos de negócios e assim minimizar potenciais perdas financeiras"

Bruno Castro, Fundador & CEO da VisionWare

Bruno Castro indica que um dos grandes desafios que os líderes têm de enfrentar é o equilíbrio entre "as múltiplas necessidades inerentes à segurança da informação numa organização, perante o cenário atual de riscos". O fundador e CEO da VisionWare diz que "existe todo um conjunto de ameaças a ter em conta, externas e internas, e o CISO e o CSO têm o desafio de acompanhar a evolução e a inovação dessas mesmas ameaças para garantir que as defesas estão atualizadas, são eficazes, abordando os riscos de forma proativa".

“É ainda importante alinhar as estratégias de cibersegurança e de gestão de riscos com os objetivos de negócios, isto é, garantir que as medidas de segurança além de protegerem a organização contra ameaças, também estão alinhadas com as metas e a continuidade dos negócios”, explica Bruno Castro. “Outro desafio reside na avaliação e comunicação de riscos. Avaliar e comunicar efetivamente os riscos para as partes interessadas é crucial”. Por fim, “um desafio a ter em conta e, simultaneamente, uma meta é criar uma cultura de segurança, crucial para gerir riscos externos e internos”.

Fábio Ribeiro relembra que os Chief Information Security Officers e os Chief Security Officers enfrentam “desafios notáveis no contexto da gestão integrada de riscos, marcado pela complexidade e pela evolução constante das ameaças”. Assim, a principal dificuldade reside “em manter a segurança num cenário que está em constante modificação, exigindo uma resposta ágil e adaptável. A integração de informações de segurança provenientes de diversas fontes para uma análise de risco coesa e abrangente também representa um desafio considerável, requerendo habilidades técnicas avançadas e uma gestão eficaz de recursos”.

Para Duarte Caldas, os líderes de segurança das organizações enfrentam desafios na necessidade de colaboração entre departamentos, acompanhando a evolução das ameaças e garantindo uma “comunicação perfeita” entre vários domínios de segurança. Os CISO e CSO precisam de “ter insights sobre questões sistémicas em controlos, processos e conformidade para áreas dinâmicas, como o risco cibernético. Isto exige que os sistemas tenham uma biblioteca ligada de itens de conformidade de potenciais riscos que possam ser visualizados em diferentes dimensões de negócio”.

Gerir o risco em tempo real

> ***Os Chief Information Security Officers e os Chief Security Officers enfrentam “desafios notáveis no contexto da gestão integrada de riscos, marcado pela complexidade e pela evolução constante das ameaças”***
>
> ***Fábio Ribeiro, Sales Engineer da WatchGuard Portugal***

No atual ambiente de cibersegurança – que é cada vez mais complexo –, as organizações estão a adaptar- se a gerir o risco em tempo real. Fábio Ribeiro refere que as empresas estão a implementar tecnologias avançadas, como inteligência artificial e sistema de monitorização contínua, para detetar e dar uma resposta rápida a ameaças emergentes. Ao mesmo tempo, é preciso uma análise profunda e específica da segurança dos endpoints, um “aspeto essencial na gestão de riscos eficaz”.

Duarte Caldas, da IBM Portugal, diz que as organizações estão a adotar uma gestão de riscos em tempo real através da adoção de soluções de “monitorização contínua, integração de inteligência de ameaças e mecanismos de resposta automatizados para identificar e lidar rapidamente com ameaças emergentes”.

Já Bruno Castro diz que “um indício positivo é que cada vez mais organizações reconhecem” a necessidade de gerir em tempo real o risco das organizações e muitas acabam por contratar um serviço de SOC. “Implementar ou adquirir um serviço de SOC é atualmente uma solução essencial para as empresas lidarem com a gestão de risco em tempo real. Um SOC compreende monitorização contínua 24/7, o que permite a deteção precoce de ameaças e, por consequência, uma resposta imediata a incidentes para mitigar ameaças, reduzir o tempo de resposta e o impacto dos ataques. Disponibiliza ainda a proteção dos dados e ativos, ao garantir que uma organização fica menos vulnerável a ciberataques e é uma garantia da continuidade dos serviços através de estabilidade operacional e recuperação rápida cujo foco é minimizar as consequências de um ciberataque a longo prazo”, explica.

Outra necessidade que as organizações devem apostar, refere o representante da VisionWare, é o investimento em treino e formação contínua dos colaboradores e, também, em testes de intrusão e simulação de ataques, que pretendem “reduzir os riscos associados a atividades humanas e fortalecer a primeira linha de defesa contra ameaças”.