Gestão de Vulnerabilidades para CIOs:

o que você não pode deixar de saber!

ECOTRUST

A adaptabilidade e a promoção de mudanças constantes são características esperadas em um CIO. Por isso, esse gestor deve caminhar por diversos terrenos, sendo um profissional que foca não apenas na expansão dos negócios e na manutenção dos custos baixos, mas também na **análise de dados e ativos, além das redes e aplicativos que os hospedam.**

Com tudo isso em jogo, é possível perceber que a proteção da sua infraestrutura corporativa contra ameaças cibernéticas é uma questão multifacetada, já que a superfície de atuação dos cibercriminosos cresce à medida que a própria organização é expandida.

Ou seja, para a consolidação e o crescimento do negócio, é preciso contar com uma **gestão de vulnerabilidades cada vez mais dedicada e assertiva.**

Dessa forma, é preciso tratar esse gerenciamento de forma integrada, perpassando todos os setores do negócio. A gestão de vulnerabilidades não pode ser tomada como apenas mais um elemento da sua operação.

Por isso, as **áreas de segurança e desenvolvimento em TI não devem ser separadas da área de operações.** Em outras palavras, se você ainda não implementou o conceito de DevSecOps, que integra essas três áreas da TI, é hora de implementá-lo.

É frequente entre CIOs a ideia de espaços de atuação bem delimitados: a segurança gerencia, e as operações implementam. Nesse contexto, a gestão de vulnerabilidades acaba sendo mais uma questão técnica ou tarefa rotineira, sem receber a devida atenção.

Mas esta é uma tarefa que não deve se restringir às equipes de segurança, mas à área de tecnologia como um todo. E para que ela seja cumprida devidamente e não como mais uma burocracia, as equipes envolvidas precisam **contar com habilidades multifuncionais e atuar de maneira colaborativa.**

Vale lembrar que as vulnerabilidades, quando negligenciadas pelo CIO (e, consequentemente, por toda a equipe que não se dedica diretamente à segurança de TI), podem comprometer ativos estratégicos e até mesmo o funcionamento da própria empresa, já que a exposição às ameaças cibernéticas evolui a cada dia.

Enfim, a operação de gerenciamento de vulnerabilidades não é apenas benéfica para os CIOs e empresas de várias maneiras. Ela é essencial e deve ser tratada como prioridade, até mesmo para ajudar o gestor a se tornar um profissional mais estratégico.

Por isso, ela é o assunto deste e-book e nos próximos tópicos vamos abordar os fatos que todo CIO deve saber sobre a gestão de vulnerabilidades.

Sumário

7

Coisas que todo **CIO** deve saber sobre **gestão de vulnerabilidades**

Se você pretende avançar em seu gerenciamento de vulnerabilidades de modo a torná-lo mais efetivo e dinâmico, confira em seguida os pontos que você não pode ignorar para alcançar essa meta.

1

Você não precisa resolver todas as **vulnerabilidades cibernéticas** do seu negócio

Você não precisa resolver todas as vulnerabilidades cibernéticas do seu negócio.

Uma empresa tem milhões de vulnerabilidades. Não é um exagero. Uma boa análise vai confirmar isso dentro do seu próprio negócio.

É claro que é plenamente possível resolver cada uma delas, mas isso demandaria muito tempo, dedicação e recursos direcionados.

A boa notícia é que **nenhuma organização realmente precisa resolver todas as vulnerabilidades de segurança** presentes em suas rotinas.

Isso porque **nem toda vulnerabilidade que você encontra em seu ambiente representa um risco** para seus ativos específicos ou negócios.

Na verdade, apenas 4% de todas as vulnerabilidades comuns e exposições atendem aos critérios críticos de serem ambas observadas dentro das organizações e conhecidas por serem exploradas na natureza.

Na maioria das empresas, uma porcentagem muito pequena das vulnerabilidades e fraquezas representam riscos legítimos.

Então, não basta mover todos os esforços possíveis para mitigar toda e qualquer vulnerabilidade encontrada.

Para seguir o caminho certo, você deve se perguntar se **os esforços da sua equipe estão sendo dedicados ao conserto das vulnerabilidades que mais importam.**

Essa correspondência é a chave do sucesso na gestão de vulnerabilidades.

Os scanners de vulnerabilidade típicos e as ferramentas de avaliação de aplicativos são úteis para encontrar potenciais exposições, mas eles geram uma lista interminável com centenas de páginas, que pode confundir uma equipe que já está sobrecarregada.

Nesse caso, a gestão de vulnerabilidades é operada sem nenhuma estratégia e acaba não colhendo os bons resultados esperados e necessários.

As áreas de segurança e desenvolvimento em TI não podem (ou pelo menos não precisam e não contam com a viabilidade necessária para) consertar tudo. Então, quais vulnerabilidades devem ser priorizadas? Quais pontos abordar primeiro? É preciso **saber quais falhas representam os maiores riscos** para a sua organização, considerando seu segmento de atuação e suas especificidades.

E para fazer a associação efetiva entre as falhas e os maiores riscos, você precisa adotar uma **abordagem de segurança cibernética baseada em riscos ao negócio** para que o gerenciamento de vulnerabilidades possa ser colocado em prática de maneira realmente eficiente.

2

O programa de **gestão de vulnerabilidades** certo pode ser muito eficiente

Você já pode ter passado pela compreensão, expressa no tópico anterior, de que não é necessário corrigir todas as vulnerabilidades de segurança existentes nas operações do seu negócio.

Mas essa descoberta pode não ter ajudado muito se você ainda não encontrou uma forma eficaz de definir, então, quais vulnerabilidades serão mitigadas.

Se você já passou por reuniões intermináveis em que se discute quais vulnerabilidades serão corrigidas e tem lidado **com conflitos persistentes sobre prioridades,** certamente sua gestão de vulnerabilidades já não é tão assertiva quanto poderia ser.

E isso, é claro, não é desejável para as rotinas da sua área de TI como um todo nem para os processos de DevOps.

Esse tipo de situação é comum quando as equipes trabalham com **ferramentas e processos desatualizados**, que não preveem ameaças ou indicam a priorização de correções.

A adoção de uma **gestão de vulnerabilidades baseada em riscos resolve essa questão**, pois prioriza soluções que pesam diversos fatores, incluindo a análise das vulnerabilidades e considerando os ativos e aplicativos nos quais você confia para que a sua equipe conte com o contexto necessário para focar onde realmente a empresa está mais vulnerável no momento.

Ou seja, essa abordagem baseada em risco ajuda suas equipes a trabalharem mais eficientemente.

Assim, elas podem deixar de discutir sobre o que deve ser feito e quem o fará, e adotar uma estratégia de segurança que não se restrinja à carga diária de envio de listas de vulnerabilidades de TI, dedicando **mais tempo a tarefas mais estratégicas.**

3

A adoção de uma **abordagem baseada em risco** reduzirá os riscos de segurança e TI

A ideia de risco pode significar coisas diferentes dependendo das áreas e abordagem, e essa diferença pode gerar atritos.

Para equipes de segurança, reduzir o risco muitas vezes significa corrigir todas as vulnerabilidades que podem ser transformadas em ataques, não importando o impacto em operações de infraestrutura ou DevOps.

Para a TI, risco geralmente significa qualquer coisa que ameace sua capacidade de continuidade e entrega para o negócio.

Ou seja, **as duas áreas estão frequentemente em desacordo.** Correções indiscriminadas, por instância, podem interromper processos ou aplicativos, restringir disponibilidade e ameaçar os acordos de nível de serviço (SLAs).

Mas ignorar as vulnerabilidades que são (ou correm o risco de ser) alvo de exploits, pode viabilizar ataques que vão acabar prejudicando seus negócios, suas operações e sua marca.

Assim, a melhor maneira de reduzir o risco para as áreas de segurança e de tecnologia conjuntamente é **ter uma linguagem compartilhada sobre o que é considerado risco** e, claro, uma abordagem baseada em risco que mede a probabilidade real de uma exploração ter como alvo as vulnerabilidades que são de alto risco em seu ambiente específico.

Dessa forma, sua equipe de segurança pode produzir relatórios que o gerenciamento de TI entenderá. E como você não está perdido em meio a centenas de vulnerabilidades “críticas”, é mais fácil avaliar propostas de correções contra o risco de que um patch ou código reescrito do aplicativo cause tempo de inatividade ou outros problemas.

Quando isso acontece, significa que a sua gestão de vulnerabilidades baseada em riscos não está se tornando apenas mais eficiente, mas também está atendendo melhor a todos: enquanto a área da segurança protege seus dados, ativos e aplicativos, a área de TI protege sua capacidade de atender às necessidades do negócio.

O melhor dos dois mundos, certo?

4

Uma **abordagem baseada em dados** te ajuda a tomar as rédeas da gestão de vulnerabilidades

A desconexão entre segurança da informação e TI traz prejuízos para ambas as áreas.

Enquanto a segurança sente que tem que desenvolver suas estratégias sem o suporte da TI, a TI se sente pressionada pela segurança, que tem ganhado maior visibilidade nos últimos anos.

Nada disso é necessário e com certeza essa divisão não te ajuda a promover uma gestão voltada para os resultados.

A verdade é que, como CIO, você precisa se posicionar no banco do motorista.

Você quer garantir que suas equipes de TI estejam cumprindo os SLAs enquanto a segurança mantém os dados, ativos e aplicativos seguros.

Você também quer que seus recursos limitados se concentrem no trabalho mais importante e estratégico.

Isso só é possível com a implementação de uma **abordagem baseada em dados.**

Um moderno programa de gestão de vulnerabilidades baseado em dados elimina as suposições porque é baseado em **montanhas de dados contextuais e em inteligência externa em tempo real** combinada com dados exclusivos sobre seu ambiente de TI, que mostram não apenas quais exposições você tem, mas o que elas significam para sua organização.

Com esse programa baseado em evidências incontestáveis que são compartilhadas automaticamente entre as equipes, tanto de TI quanto de segurança, você entende imediatamente onde deve concentrar seus esforços.

Dessa forma, os papéis dentro da gestão de vulnerabilidades são esclarecidos e a segurança deixa de ser vista como aquela área que dita o que a TI deve fazer, já que esta última agora conta com um **sistema que elimina a desordem e mantém as prioridades alinhadas.**

É nesse contexto que a confiança compartilhada surge entre as duas equipes e o trabalho colaborativo passa a fluir de maneira mais harmoniosa. Longe dos conflitos e dúvidas, você consegue tomar as rédeas e não só compreender as vulnerabilidades prioritárias, como gerenciá-las com resultados de alto nível, ou seja, a abordagem baseada em dados te coloca no controle da gestão de vulnerabilidades.

5

Você pode explorar **alternativas de mitigação** para vulnerabilidades que não podem ser corrigidas

Nem sempre é possível corrigir todas as falhas de alto risco no momento em que você descobre a vulnerabilidade em questão.

Em alguns casos, a vulnerabilidade está no centro de uma missão crítica do aplicativo ou serviço da web voltado para o cliente, onde qualquer tempo de inatividade é inaceitável.

Outras vezes, ela pode estar localizada em dispositivos que são impossíveis de corrigir ou que exigem que a equipe de DevOps reescreva os códigos.

Mas, se você está no controle do seu processo de gestão de vulnerabilidades, certamente será capaz de **decidir o que é importante corrigir agora,** ao determinar um cronograma para a correção de outras vulnerabilidades ao longo do tempo.

Você também pode pensar em **estratégias alternativas de mitigação** para remediar essas vulnerabilidades mais difíceis de corrigir, pois quando as suas áreas de TI e segurança estão alinhadas em prioridades, há pouco o que discutir.

Com a TI no comando de uma abordagem de gerenciamento de vulnerabilidades baseada em riscos, você terá muito mais controle sobre a avaliação do risco em comparação com a recompensa dos esforços de remediação.

E, o mais importante de tudo, você vai ter todas as suas equipes trabalhando em conjunto para reduzir o perfil de risco geral.

6

Você pode dividir a sua **gestão de vulnerabilidades em ciclos**

Em seu recente Guia de Gerenciamento de Vulnerabilidades, a Secretaria de Governo Digital sugere a **implementação de ciclos gerenciáveis** para o preenchimento de lacunas relacionadas à segurança da informação.

O Guia tem como propósito a elucidação de diversas ações que devem ser avaliadas em cada fase de um ciclo de gerenciamento, proporcionando aos responsáveis pela segurança dos ativos de informação a possibilidade de aprimoramento contínuo.

Ele também tem o objetivo de facilitar a adequação à Lei Geral de Proteção de Dados e a elevação do grau de maturidade das instituições ligadas à administração pública federal em termos de proteção de dados e ações de segurança da informação.

É claro que os parâmetros sugeridos podem ser implementados também em organizações de natureza privada, já que a ideia dos ciclos de gerenciamento pode proporcionar uma **organização mais eficaz das ações relacionadas à gestão de vulnerabilidades.**

Os ciclos sugeridos são três:

- Detecção
- Relatórios
- Remediação

Cada ciclo conta com quatro tarefas principais e cada tarefa inclui uma lista de ações a serem executadas.

Existe uma ordem lógica para a execução dessas ações, mas adaptações podem ser promovidas em função dos objetivos de cada instituição.

O grande destaque colocado no documento é que a concepção de uma **natureza cíclica da gestão de vulnerabilidades** possibilita a melhoria contínua do processo a partir da compreensão de que todas as tarefas estão interconectadas em três domínios e de que ele se alimenta de outros processos.

7

Você deve recorrer aos **frameworks de segurança da informação** para reduzir as vulnerabilidades

A expressão “framework”, em tradução livre, pode ser compreendida como “estrutura” e, como você já deve saber, corresponde a **modelos ou esqueletos utilizados na construção de um programa de cibersegurança.**

Nesse sentido, eles são poderosos aliados dos CIOs, pois sugerem uma série de procedimentos, análises e boas práticas a serem adotados de acordo com os objetivos, o modelo e o segmento de negócios da empresa.

Alguns dos frameworks mais recomendados neste contexto de promoção da segurança cibernética são o ISO/IEC 27.000, o NIST Cyber Security e os CIS Controls.

Na verdade, as normas ISO/IEC da família 27.000 se subdividem em outros documentos e tratam de diversos temas, que incluem a avaliação de riscos, tão importante na gestão de vulnerabilidades.

O objetivo geral é a proteção da integridade, confidencialidade e disponibilidade dos dados das organizações.

A ISO 27.001, por exemplo, conta com um catálogo de 114 salvaguardas distribuídas em 14 sessões, que representam excelentes apontamentos capazes de reduzir e mitigar as vulnerabilidades mais críticas.

O **NIST Cybersecurity framework** também é um conjunto de diretrizes e boas práticas traduzidos em controles e ações que visam à mitigação dos riscos de segurança da informação nas empresas.

O documento é publicado e atualizado pelo Instituto Nacional de Padrões e Tecnologias dos Estados Unidos e atualmente é dividido em cinco capítulos, dedicados às missões de **identificar, proteger, detectar, responder e recuperar.**

Os capítulos são subdivididos em categorias e subcategorias que resultam em um total de 108 controles.

Outra opção de framework que vem ganhando destaque são os **CIS Controls**, desenvolvidos pela Center for Internet Security, uma renomada entidade norte-americana sem fins lucrativos.

Já foram publicadas algumas versões dos CIS Controls e a mais recente delas é o CIS Controls V8, que traz 153 salvaguardas subdivididas em 18 controles de cibersegurança, com grupos de implementação muito bem definidos.

Esses **grupos de implementação são seu principal diferencial** por facilitarem e guiarem todo o processo. O primeiro grupo, por exemplo, é voltado para organizações com recursos limitados em cibersegurança. Os níveis mais altos de maturidade no assunto podem ser alcançados conforme a empresa vai avançando entre os diferentes grupos definidos pelos CIS Controls.

Agora que você já conferiu as principais informações sobre as quais é importante estar ciente para promover uma gestão de vulnerabilidades efetiva em sua empresa, é hora de **promover as mudanças necessárias em termos mais práticos**, utilizando a abordagem baseada em riscos, organizando as diferentes ações, promovendo o trabalho integrado da segurança da informação com a parte operacional da TI e utilizando os frameworks como fatores norteadores.
Acompanhe nosso blog para obter sempre novas informações e dicas úteis tanto para a sua gestão de vulnerabilidades quanto para a segurança da informação como um todo.

Eco Trust

Adotar métodos corretos e eficientes e aplicá-los com regularidade pode resultar na **economia de custos e aumento da competitividade** de negócios que dependem de tecnologia. As vantagens da segurança da informação e da proteção de dados para o presente e o futuro são diversas e podem evitar prejuízos muito severos.

É importante entender que processos relacionados a gestão de vulnerabilidades são os verdadeiros **investimentos em prevenção** e cuidados mais do que necessários. É hora de começar a agir de forma eficiente o mais rápido possível em favor da continuidade do negócio. Veja como a Eco IT pode te ajudar.

A **EcoTrust**, nossa **plataforma de *Inteligência em Riscos Cibernéticos***, possibilita que os líderes de Segurança e TI possam tomar decisões importantes de forma mais assertiva quando o assunto for segurança cibernética. Através da descoberta e gerenciamento de vulnerabilidades e riscos cibernéticos, de forma orquestrada, simplificada e com abordagem orientada aos riscos de negócio, a plataforma traz uma visão estratégica (negócio) com embasamento em indicadores técnicos (táticos e operacionais).

E para comprovar todas essas vantagens, você pode experimentar a plataforma gratuitamente. Basta clicar no botão abaixo.

Conhecer a solução

Entre em contato

site

www.ecotrust.io

ECOTRUST