Uma escolha para o futuro: conheça as duas opções em orçamento para a cibersegurança do seu negócio

Calcular qual será o seu orçamento para cibersegurança não é algo fácil. Conheça duas abordagens diferentes para o setor e o que você pode aprender sobre cada uma delas.

AUTOR
Alexander Moiseev

Ao redor do mundo, os gastos com produtos e serviços de cibersegurança vêm crescendo nos últimos anos. De acordo com a Gartner, o valor total passou de US$ 114 bilhões em 2018, um valor já 12,4% maior que o de 2017, para mais de US$ 124 bilhões em 2019. Ou seja, o momento para se juntar à corrente é agora.

Além disso, os próprios líderes de segurança de TI dentro das empresas também têm expectativas altas para o setor, já que 72% deles afirmam que seus orçamentos para 2020 aumentaram. Porém, com mais dinheiro investido na segurança de dados, uma pergunta paira no ar: como está sendo investido esse dinheiro?

A questão é: existem duas formas de decidir o futuro da cibersegurança dentro da sua empresa:

Apostar na sua intuição e experiência prévia em situações similares ou seguir as decisões de terceiros. Essa é a abordagem convencional.

Analisar o seu caso especificamente, separá-lo em pequenas partes e tentar calcular a probabilidade de que cada uma dessas partes mude num futuro próximo. Isso é o que chamamos de uma abordagem baseada em risco.

Agora vamos analisar essas duas estratégias em detalhes, o que cada uma delas significa em termos práticos e qual delas têm mais chance de se encaixar ao seu negócio.

Orçando sua segurança digital – Abordagem 1: Convencional

A estratégia mais comum na hora de planejar o orçamento de cibersegurança de uma empresa está comumente baseada nas necessidade atuais e imediatas ou em experiências prévias, especialmente nos casos de companhias em crescimento que precisam ter medidas mínimas de cibersegurança e as ferramentas para seguir crescendo.

Para esse tipo de organização, o planejamento de orçamentos é baseado no patrimônio, com o nível de orçamento sendo mantido por vários ciclos, somente com os mínimos ajustes. Não existe a prática de definir objetivos estratégicos de segurança de TI ou de avaliar riscos específicos, e o dinheiro geralmente é gasto em necessidades emergentes e suporte, numa abordagem despreocupada. Quem chegar primeiro pega.

Essa estratégia tem tudo para funcionar, a menos que haja mudanças repentinas na empresa. Por exemplo, você pode decidir de uma hora pra outra que quer dar um gás na transformação digital da empresa ou trazer um serviço de CRM ou contabilidade baseado na nuvem. Só que ações como essas exigem, no cenário ideal, aumentar rapidamente os gastos com segurança de TI e mão de obra qualificada na área para poder se proteger das ameaças que a tecnologia traz consigo. Com isso, outras mudanças e implantações são adiadas e acumuladas para o futuro.

Infelizmente, isso significa que mais dinheiro será gasto. Por quê? Os gastos em segurança podem aumentar consideravelmente cada vez que algo inesperado acontecer, porque ainda será necessário resolver o problema o mais rápido possível, não importa o valor, mas sem uma defesa preventiva. Ao mesmo tempo, organizações de grande porte, que já têm uma abordagem mais experiente e madura para o gerenciamento de riscos, podem terminar gastando menos em segurança de TI com essa abordagem. De qualquer forma, essa é a primeira opção.

Orçando sua segurança digital – Abordagem 2: Calculando os riscos

Não é algo surpreendente que em 2019, a expertise em gerenciamento de riscos tenha sido citada dentro das três habilidades mais importante para os gestores de segurança de dados. Ao redor do mundo, empresas maduras atuam com o gerenciamento de riscos como parte fundamental de suas operações. E TI e cibersegurança não são alheios a isso.

A questão não é sobre tentar tapar todos os buracos ao mesmo tempo, é sobre estratégia. Primeiro, vale dar uma olhada nos riscos associados a casos críticos de ataques virtuais, sejam eles a diminuição na oferta e na qualidade do serviço oferecidos aos clientes, danos à reputação da empresa, a perda de oportunidades de negócio ou até mesmo prejuízos diretamente financeiros. Logo, você calcula os riscos: multiplique a probabilidade de que um desses incidentes ocorra pelo custo que ele teria e decida se existe a necessidade de implementar medidas de segurança para evitá-lo. Para negócios com este tipo de pensamento, a segurança digital não é um hábito ou um investimento tido como um "mal necessário" causado por manchetes sensacionalistas. É uma ação apropriada e derivada de cálculos e planejamento.

Cada negócio é único, o que significa que eles enfrentam diferentes tipos de riscos. Por exemplo, para um e-commerce, existe uma boa chance de que um ataque DDoS (Negação de serviço distribuído, em tradução livre), que tiram servidores do ar ao sobrecarregá-los e aumentar o volume do tráfego de internet, possam causar danos massivos, tanto no âmbito financeiro quanto na reputação da empresa. Enquanto isso, organizações financeiras e governamentais estão sujeitas a penalidade e multas no caso de que seus sistemas sejam invadidos ou atacados, o que exige que grande parte do seu orçamento seja gasto para conter esses ataques.

Além disso, os desenvolvedores de softwares e fornecedores de serviços também podem ser alvos de ataques, assim como uma invasão à sua cadeia de suprimentos pode terminar em um problema para seus consumidores. Em outras palavras: existem quase tantos modelos de ataques quanto de negócio, cada um com riscos bem específicos e em constante evolução.

Como calcular riscos envolve sempre um certo nível de probabilidade, a experiência em segurança de TI está se tornando uma parte crucial dos processos de análise de riscos. Nesse caso, os experts em cibersegurança, incluindo aqueles terceirizados, podem ajudar a avaliar as possibilidades e usar sua experiência para causar um impacto positivo.

Serviços de saúde: atenção especial para os dispositivos portáteis

Hospitais, centros cirúrgicos e centros de atendimento no mundo todo estão, em geral, sobrecarregados de pacientes doentes buscando por ajuda. O 5G tem a capacidade de mudar isso. Ele fornecerá às pessoas saudáveis e às que estão confinadas em casa acesso mais rápido a serviços, como portais on-line e dispositivos digitais diferentes, reduzindo a pressão sobre a infraestrutura de serviços de saúde.

Um dos maiores avanços que o 5G fornecerá para esse setor será a tecnologia portátil. Desde um dispensador automático de comprimidos da MedMinder até a capacidade do SpiroSmart de transformar celulares em medidores de fluxo respiratório, o 5G significará a proliferação de dispositivos de saúde revolucionários projetados para monitorar nossa saúde e, até mesmo, usar a inteligência artificial e consultas por telepresença para definir diagnósticos.

Ele também mudará totalmente a nossa visão sobre casas inteligentes. Weihua Sheng, professor associado da Oklahoma State University e diretor do Advanced Sensing, Computation and Control Lab, está trabalhando para levar sensores de saúde para dentro de nossas casas. A equipe de Sheng está desenvolvendo uma plataforma para casas inteligentes baseada em nuvem para monitorar a saúde que inclui sensores de ambiente, dispositivos portáteis e um assistente robô. Por exemplo, usando diferentes sensores, o sistema pode detectar se o usuário está desidratado. O assistente robô poderá, então, pedir que ele beba mais água. A plataforma também pode determinar se uma pessoa cair e pedir ajudar.

Finalmente, quando essa é a abordagem escolhida para decidir sobre a compra de uma solução ou serviço de cibersegurança, geralmente existe um processo mais transparente de aprovação com os diretores e gerentes do alto escalão. Isso significa que são evitadas decisões repentinas e centralizadas, onde um funcionário do TI toma uma decisão para escolher a forma mais barata e eficiente de lidar com um desses problemas, mas acaba escolhendo outra solução, por exemplo, por já estar familiarizado com a ferramenta ou por ter trabalhado com ela no passado, entre outros motivos.

É claro que os processos de análise de risco diferem de uma empresa para a outra, e estão em constante evolução. Ainda assim, três componentes permanecem fundamentais para ajudar a tornar o planejamento de orçamento mais eficiente: experts, avaliação de riscos e o estabelecimento de uma cadeia clara de tomadas de decisão. No fundo, essa ainda é a melhor forma de assegurar que os investimentos feitos em segurança de TI estejam alinhados com o que as necessidades e interesses da companhia.

Que lições as empresas podem aprender com isso?

Planejar um orçamento de segurança é parecido com cuidar da manutenção de um carro. Como dono, você deve fazer uma conta aproximada para estimar o valor médio gasto em despesas regulares, como pneus, revisões e outras coisas. Mas, aqueles que são entusiastas das corridas sabem que é necessário praticamente trocar as rodas em movimento, antes mesmo de estarem gastas, para estar sempre preparado para completar a corrida e assegurar que você tem orçamento suficiente para todos os componentes do carro que costumam ter vida curta, como pneus e freios. Essa segunda abordagem é mais madura e geralmente costuma ajudar a economizar dinheiro, mas também exige mais experiência, tempo e dedicação.

Em geral, existem algumas considerações na hora de calcular seu orçamento para TI:

Conhecimento é poder

Quando estiver avaliando riscos, fique atento às ameaças que mais costumam afetar empresas do seu ramo e porte, e planeje de acordo com isso. Para isso, é crucial se informar e acessar os relatórios mais atualizados sobre ameaças inteligentes.

Abrace a experiência

Independente de se você estiver usando talentos internos, externos ou ambos, é importante que eles possam avaliar os riscos e o valor potencial de soluções e serviços de cibersegurança. Inclusive, a maioria dos fornecedores oferece uma variedade de treinamentos para que as organizações possam melhorar seus níveis internos de experiência sobre o assunto

Chame os experts (se precisar)

A terceirização é uma opção muito válida para organizações que ainda não têm experiência suficiente entre seus funcionários, nem processos estabelecidos de avaliação de riscos. O importante é ter um acordo de serviço (SLA) para poder transferir os valores investidos da planilha de gastos de capital (CapEx) para a de gastos de operação (OpEx), e assim manter um nível seguro de gastos em segurança.

Experimente diferentes ferramentas

Estudar somente benchmarks e referências da indústria para tomar uma decisão sobre orçamento não é suficiente, mas ferramentas como a Kaspersky IT Security Calculator podem fornecer informações sobre ameaças, mensuração e números que ajudem a avaliar as opções para uma indústria em particular, seu tamanho e localização.

Quando você está lidando com algo tão sério como a segurança digital de uma corporação, ou se preparando para correr em alta velocidade, como comparamos, é melhor gastar um bom tempo para se preparar com antecipação, consultar os experts no assunto e planejar possíveis situações. Afinal, como diz o ditado, a pressa é inimiga da perfeição.