Como Melhorar a Segurança Cibernética com Arquitetura Corporativa

Marc Lankhorst

Introdução

Não é segredo que as ameaças de segurança cibernética estão aumentando cada vez mais. É comum se dizer que existem somente dois tipos de organizações: aquelas que sabem que foram atacadas, e aquelas que não sabem disso ainda. Para mitigar o risco e o dano associado com a segurança cibernética, é importante saber como avaliar estes riscos e melhorar suas defesas através da segurança-por-desenho. É importante, também, planejar o que fazer se (e quando) as coisas saem dos trilhos. Então, vamos dar uma olhada em alguns passos importantes que você pode dar para gerenciar efetivamente o risco e se manter tão seguro quanto possível neste mundo perigoso.

5 Passos para Estar Seguro em um Mundo Perigoso

Garantir a conscientização por toda a organização

Na maioria das organizações, a conscientização das gerências de nível superior em relação às ameaças cibernéticas tem crescido em função dos numerosos incidentes com grande impacto ocorridos nos últimos tempos. O custo associado com ransomware, vazamento de informações e outros problemas pode facilmente chegar à casa das centenas de milhões.

No entanto, muitos ainda veem a segurança cibernética apenas como um problema técnico, que deve ser tratado pelo Diretor de TI e sua equipe. Uma forma garantida de acordar toda a Diretoria para a conscientização sobre a segurança cibernética é a conformidade regulatória. Nestes casos, a Direção pode ser pessoalmente responsabilizada pela não-conformidade, de forma que existe uma forte motivação para agir.

Novas regulações sobre privacidade de dados, como a Lei Geral de Proteção de Dados (LGPD), são apenas um exemplo onde preocupações de segurança e privacidade chegaram até a sala da Diretoria. Regulações regionais e específicas de um setor, como a Lei de Privacidade HIPAA, dos Estados Unidos, para o setor de cuidados de saúde, ou a regulação NYDFS para Segurança Cibernética, para o setor financeiro em Nova York, são outros exemplos.

Na maioria das vezes, a gerência se sente como um animal sob a luz dos faróis quando o assunto é ameaça cibernética. Eles vêm o perigo, mas não sabem o que fazer frente a estas ameaças. A extensão e a profundidade destes problemas podem, realmente, parecer incompreensíveis e não solucionáveis. Para ajudar a gerência a superar esta paralisia, você deve apresentar soluções, não apenas problemas. Arquitetos corporativos estão posicionados de forma única para contribuir para fornecer isso. Voltaremos a este tema um pouco mais à frente.

Alinhar o gerenciamento de risco e segurança com a estratégia do negócio

Para gastar seu dinheiro de forma inteligente, você precisa investir na segurança onde ela realmente conta - ou seja, onde ela é estrategicamente importante. Você deveria, desta forma, classificar seus ativos a partir da perspectiva da sua estratégia, levando em consideração a conformidade regulatória e outras orientações. Qual o valor destes ativos, não somente em termos financeiros, mas em um sentido mais amplo?

Por exemplo, proteger o valor da propriedade intelectual ou dados sensíveis à privacidade pode ser crucial para a continuidade do seu negócio ou essencial a partir de uma perspectiva de conformidade regulatória. Tal classificação ajuda você a decidir suas prioridades de investimento e evitar gastar demais em medidas relativamente pouco importantes ou ineficazes.

Infelizmente, muitas organizações não têm uma conexão clara entre a sua estratégia e seus ativos. Uma sólida arquitetura corporativa relacionada com a motivação e direção estratégicas, bem como com a implementação dentro da organização, fornece o "tecido conjuntivo" que você precisa. O BiZZdesign Enterprise Studio oferece o suporte integrado para descrever a estratégia, a arquitetura, os processos, os sistemas e os dados que você precisa para criar esta linha de visão.

Analisar suas vulnerabilidades e riscos

Ataques cibernéticos estão se tornando cada vez mais sofisticados, usando uma combinação de técnicas digitais, físicas e de engenharia social. Um exemplo comum é o assim chamado "ataque da maçã na beira da estrada". Um possível invasor "acidentalmente" deixa um pen-drive USB em um lugar público, tal como o estacionamento da empresa. Algum empregado pega o pen-drive, e grandes são as possibilidades de que ele não resistirá à curiosidade e o conectará ao seu PC. Surpresa: o pen-drive está infectado com algum malware que infecta o PC e envia informações sensíveis para o invasor.

Você precisa adotar uma abordagem integral para se defender contra tais ataques, incorporando todos os aspectos da sua empresa.

Com o Enterprise Studio, você pode capturar e visualizar vários aspectos de risco e segurança da sua organização. Isto ajuda você a visualizar os perigos, riscos e medidas mitigatórias em relação à sua arquitetura, estratégia de negócio e ativos, como um todo, de forma que você possa realizar uma avaliação de conformidade e riscos verdadeiramente baseada na estratégia e no valor de negócio. Você pode medir e visualizar o impacto potencial destes riscos e usar estas percepções para priorizar os investimentos em medidas de mitigação como parte do seu próximo passo.

Adotar uma abordagem de segurança por desenho

As vulnerabilidades não deveriam ser tratadas após o fato, especialmente não apenas aplicando alguma medida de segurança imediata não planejada, como colocar um novo firewall. Ao invés de definir uma arquitetura de segurança separada, você deveria desenvolver uma arquitetura segura e endereçar os riscos proativamente na arquitetura e no desenho através de todos os níveis da sua organização, desde as pessoas e responsabilidades até os processos e tecnologia.

Você também precisa considerar a posição da sua organização em um ecossistema mais amplo. Manter a sua casa em ordem pode não ser suficiente. Por exemplo, se você confia extensivamente em algum parceiro externo, a segurança deles pode ser crucial para as operações do seu próprio negócio. Algumas organizações tentam confiar em contratos e acordos para lidar com isso, mas isto pode ser insuficiente.

Legalmente, você pode ser considerado responsável por um vazamento que aconteça, digamos, em um parceiro de terceirização. Regulações como a LGPD explicitamente declaram que a sua organização continua responsabilizável pelo processamento de informações sensíveis e sigilosas, mesmo se você contratar alguém para fazê-lo para você. Em alguns casos, você pode, inclusive, precisar auditar seus parceiros para garantir a conformidade.

Em uma abordagem de segurança por desenho, você prioriza os investimentos em segurança com base no valor dos seus ativos e nas vulnerabilidades que você tiver identificado nas etapas anteriores. Você calcula o valor de negócio e o impacto dos projetos de segurança e usa isso para fazer a priorização das medidas de TI. Nossa plataforma pode ajudar você a identificar onde gastar o seu orçamento de forma mais efetiva, graças às suas capacidades de gerenciamento de portfólio corporativo.

Assumir que você está comprometido

Nenhuma quantidade de medidas de segurança irá torná-lo 100% seguro, de forma que é melhor você estar preparado para agir quando as coisas saírem dos trilhos. Muitas organizações se desesperam para saber o que fazer quando eles são atacados, porque eles não sabem que partes da organização ou dos sistemas podem ter sido afetados.

Criar planos de contingência baseados em percepções claras em relação à estrutura e às operações da sua organização é essencial. Modelos atualizados da sua arquitetura, processos, sistemas e dados pode ser uma enorme ajuda para a avaliação de quanto um problema pode se espalhar, e em que pontos você deveria agir rapidamente para limitar o impacto de uma falha de segurança.

Mas lembre-se de um dito de Eisenhower: "Planos não são nada; planejamento é tudo". Nada vai sair sempre completamente de acordo com os planos, mas o desenvolvimento em si de tais planos tornará claro o que você precisa saber, o que é desconhecido, e onde você deve atualizar seu conhecimento sobre o funcionamento e estrutura da sua organização. Conectar o Enterprise Studio com ferramentas como CMDBs (Sistemas de Gerenciamento de Infraestrutura), que gerenciam e monitoram a realidade operacional, ajuda a garantir que você está usando os melhores e mais atualizados dados disponíveis.

Finalmente, toda esta informação precisa estar rapidamente acessível para a "linha de frente" da sua organização. O portal BiZZdesign HoriZZon oferece uma ótima solução para isso, fornecendo visões e painéis de controle fáceis de usar para os vários tipos de usuários, desde os executivos tomadores de decisões até os gerentes operacionais e pessoas no chão-de-fábrica.

Analisar sua Segurança com Modelos de Arquitetura

Até aqui nós falamos sobre os passos principais para manter sua organização segura em um ambiente digital cada vez mais perigoso. Na continuação, vamos olhar mais detalhadamente os instrumentos que podem ser usados para que você possa alcançar a segurança cibernética - em particular, nos passos 3 e 4. Não vamos surpreendê-lo ao defender uma abordagem baseada em modelos para analisar e mitigar os riscos cibernéticos. Claramente, descrições formais da sua organização ajudarão você a obter o entendimento necessário para fornecer soluções de segurança cibernética ótimas.

Naturalmente, não é possível alcançar a segurança absoluta; ao invés disso, você deveria focar onde você precisa investir a partir da perspectiva 1) do valor dos ativos que você quer proteger e 2) das vulnerabilidades associadas a estes ativos. Nossa abordagem para o gerenciamento de segurança e risco corporativo é baseada em vários padrões abertos, mais notadamente o padrão ArchiMate para a modelagem da arquitetura corporativa, bem como o padrão Open FAIR para o gerenciamento de risco da informação. Mais detalhes estão descritos neste artigo[1] do The Open Group sobre modelagem de segurança e gerenciamento de risco corporativo.

[1] https://publications.opengroup.org/w172

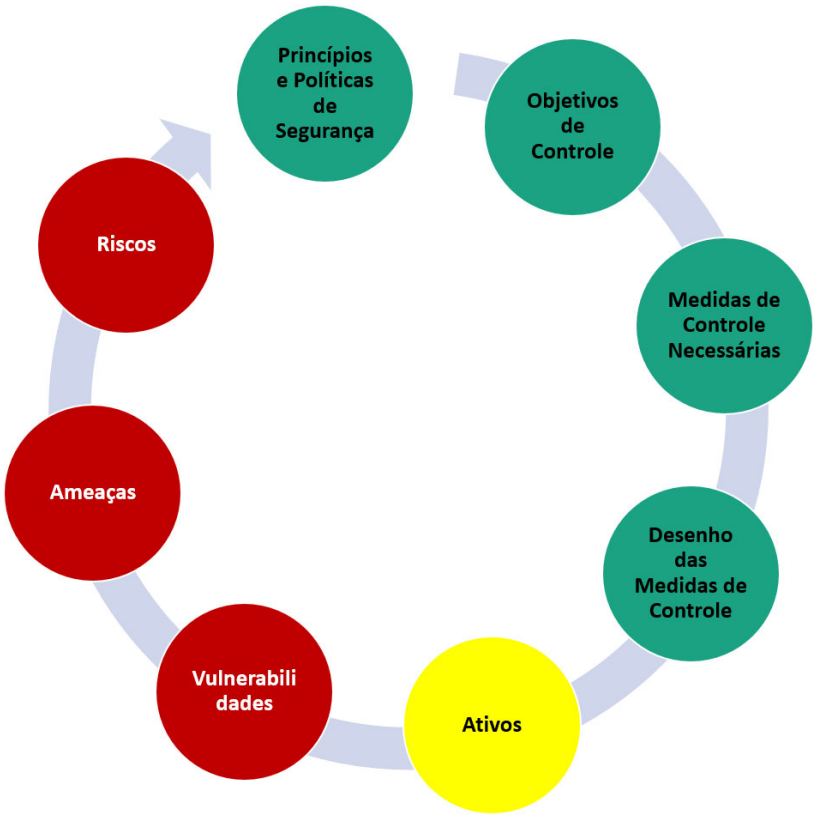

Figura 1: Os passos da nossa abordagem para o gerenciamento de segurança e risco

A figura acima mostra os passos principais da nossa abordagem, os quais estão embutidos na funcionalidade de Gerenciamento de Conformidade, Risco e Segurança do BiZZdesign Enterprise Studio. Na parte inferior da figura, você vê os ativos que você quer proteger de riscos cibernéticos, enquanto na parte superior você vê as políticas, princípios e objetivos que orientam a organização.

Entre estes extremos estão os passos que os conectam; no lado esquerdo (em vermelho), você vê a análise dos riscos cibernéticos na sua organização, e no lado direito (em verde) você vê a implementação dos controles para melhorar a sua segurança. Estas são as etapas para o gerenciamento de segurança e risco:

1. **Revisar os ativos**: Quais são os ativos mais importantes que são críticos para a sua organização? O que as regulações aplicáveis falam sobre estes ativos? Por exemplo, os dados pessoais dos seus clientes podem ser um destes ativos. Sua reputação como uma organização confiável pode ser outro. Você pode atribuir algum valor a estes elementos? Isso ajudará você posteriormente quando decidindo o que é mais importante proteger.

2. **Analisar as vulnerabilidades**: De que forma os ativos da sua organização estão vulneráveis? Em segurança cibernética, "vulnerabilidades do dia zero", que não são conhecidas por ninguém exceto pelo atacante, são naturalmente as mais perigosas, e não aparecerão nesta lista. Mas outras vulnerabilidades que você possa reconhecer deveriam ser investigadas e ligadas com os ativos que elas expõem. Você pode reusar os modelos da sua arquitetura de negócios e de TI, possivelmente estendendo-os com os aspectos relevantes de segurança.
3. **Avaliar as ameaças**: Depois que você avalia as vulnerabilidades específicas dos seus ativos, você precisa avaliar se estas vulnerabilidades podem ser exploradas efetivamente pelos chamados "eventos de ameaça" e "agentes de ameaça". Isto pode ir desde hackers maliciosos até governos hostis e concorrentes desonestos, bem como seu próprio pessoal, mal funcionamento técnico, desastres naturais, e outros acidentes. Nós coletamos um extenso modelo contendo centenas de vulnerabilidades, agentes de ameaça e eventos de ameaça, que pode servir como um ponto de partida para as suas análises neste passo e no anterior.
4. **Calcular riscos**: Com base nas ameaças potenciais e no valor dos seus ativos, você pode avaliar os riscos que a sua organização enfrenta na realidade. Em uma fórmula simples, risco = valor x probabilidade, quanto maior o risco, mais você quererá investir para mitigá-lo. A Figura 2 mostra um exemplo de uma análise como esta, construída gradualmente através destes quatro primeiros passos.

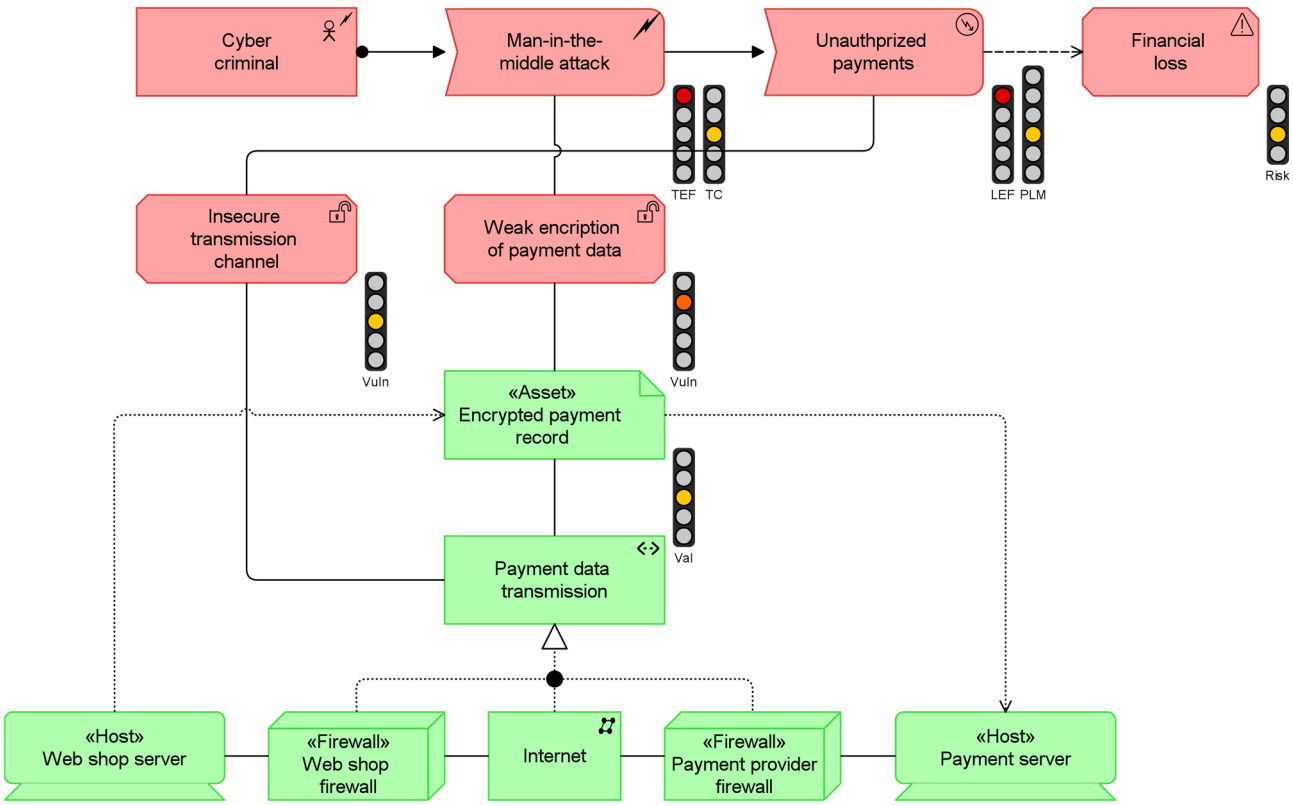

Figura 2: Exemplo de análise de risco

A parte inferior do modelo mostra a infraestrutura e os ativos que você quer proteger (“Registro de Pagamento Encriptado”). A parte superior mostra:

- Duas vulnerabilidades (‘Insecure transmission channel’ e ‘Weak encryption of payment data’)
- Um agente de ameaça (‘Cyber criminal’)
- Um evento de ameaça (‘Man-in-the-middle attack’)
- Um evento de perda potencial decorrente desta ameaça (‘Unauthorized payments’)
- O risco resultante (‘Financial loss’)

Os sinais de tráfego mostram os vários parâmetros, tais como o valor do ativo, o nível de vulnerabilidade e o nível de risco resultante. Todos eles são interconectados, e o nosso algoritmo de análise de risco calcula os resultados, ou seja, se você aumenta o valor do ativo ou a capacidade da ameaça o nível de risco aumenta.

5. Criar políticas: Para lidar proativamente com riscos cibernéticos potenciais, você deveria definir princípios e políticas de segurança apropriadas que estejam em linha com a sua estratégia de negócio e que também siga as regulações aplicáveis. Isto pode incluir, por exemplo, princípios tais como segurança por desenho, separação de responsabilidades, acesso restrito a dados pessoais, e outras políticas comuns. Frameworks regulatórios, como a LGPD, requerem políticas de proteção de dados sólidas, com altas multas em caso de não-conformidade. Isto, por sua vez, influencia o valor dos ativos que você quer proteger. Não é apenas o seu valor intrínseco que está em jogo; multas, danos à reputação e outros efeitos colaterais também deveriam ser levados em consideração.
6. Definir objetivos de controle: Com base nas políticas que você criou no passo anterior, você deveria agora definir objetivos de controle apropriados. Uma abordagem padrão é classificar a confidencialidade, integridade, disponibilidade, sensitividade à privacidade, e outros atributos dos seus dados, de acordo com casos de uso comuns que você tenha. Por exemplo, os dados no seu website precisarão de baixa confidencialidade, mas alta disponibilidade, enquanto os dados do cliente terão requisitos de confidencialidade e privacidade muito mais altos, enquanto a disponibilidade poderia ser uma preocupação menor.
7. Criar medidas de controle: Estes objetivos de controle são traduzidos em medidas de controle aplicáveis, que dizem o que deve ser feito para atingir estes objetivos. Padrões relevantes, como a ISO/IEC 27001, NIST 800-53, CSA e outros, podem ajudar fornecendo um conjunto predefinido e organizado de medidas de controle. Na Figura 3, vemos um pequeno extrato de um modelo do padrão ISO/IEC 27001, mostrando um objetivo de controle específico e várias medidas de controle relacionadas, expressas através da sobreposição de risco e segurança do ArchiMate que está definida no artigo do The Open Group mencionado acima. A Figura 4 mostra um conjunto de controles do padrão CSA, aplicável para encriptação.

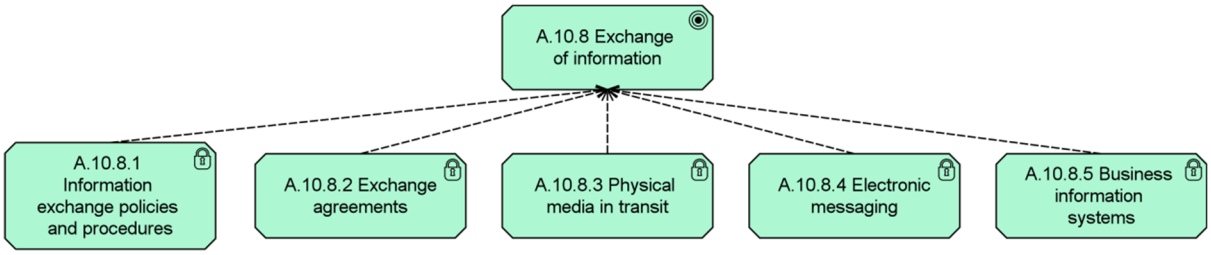

Figura 3: Exemplo de objetivos e medidas de controle ISO/IEC 27001

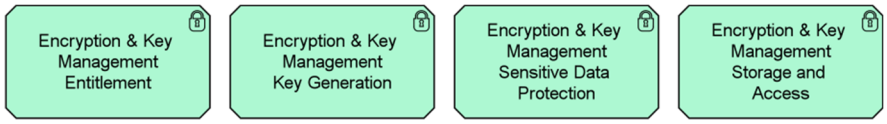

Figura 4: Controles para encriptação e gerenciamento de chaves CSA

8. **Implementar**: A etapa final é desenhar a implementação destas medidas de controle como parte da sua arquitetura, processos e sistemas. Por exemplo, você terá que descobrir como você realiza o registro de usuários (a primeira medida na Figura 4). Você pode comparar o custo da implementação destas medidas com os riscos que você está correndo. Eles realmente valem isto, ou você está protegendo ativos de baixo valor com controles extensivos caros?

A análise de risco mostrada acima é, naturalmente, algo a ser feito por especialistas em avaliação de riscos e modeladores, e pode parecer complicado para os não iniciados. Os resultados podem, no entanto, ser apresentados através de mapas de calor amigáveis como o mostrado na Figura 5. O mapa de calor mostra como a alta capacidade das ameaças (por exemplo, hackers habilidosos) combinado com a pouca força dos controles resulta em um nível de vulnerabilidade muito alto. As outras duas vulnerabilidades neste mapa de calor são, provavelmente, menos urgentes.

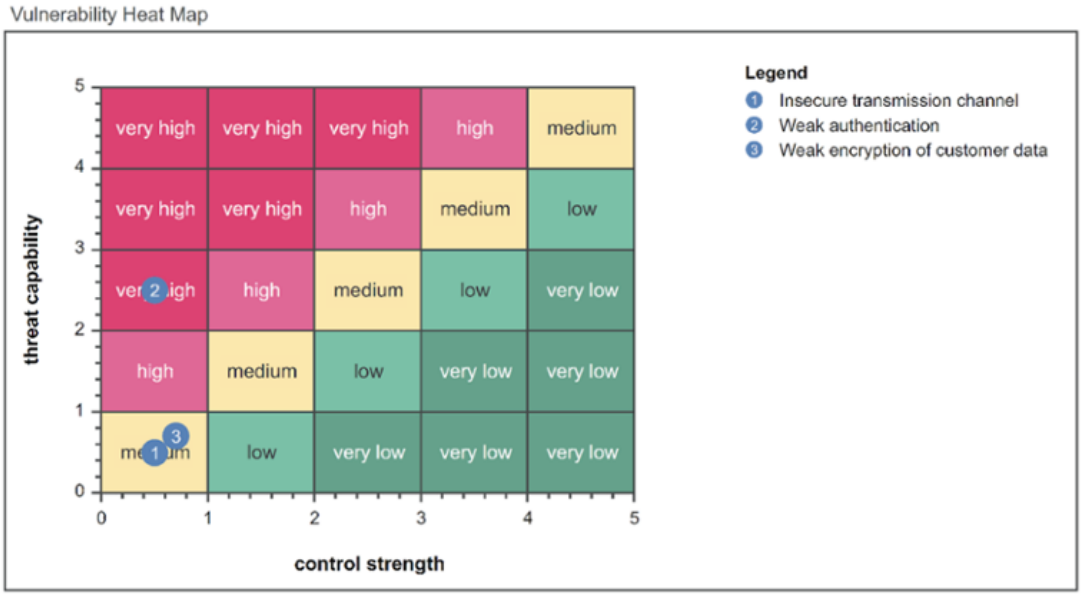

Figura 5: Mapa de calor mostrando o posicionamento de risco das vulnerabilidades

Esta análise ajuda a gerência a priorizar investimentos na melhoria da segurança como, neste exemplo, implementar regras relacionadas com o tamanho das senhas, ou instituir a autenticação de múltiplos fatores. Assim, sua organização ganha espaço no orçamento para investir naquilo que realmente conta. Lembre-se que a arquitetura de segurança é uma preocupação contínua. O gerenciamento de risco é, também, um processo contínuo e interativo.

O processo esboçado aqui deveria ser executado regularmente para avaliar novas vulnerabilidades e ameaças, e para manter suas políticas, princípios e controles atualizados com a estratégia da sua organização e com as demandas regulatórias. Mais ainda, o fato que você tenha um processo de gerenciamento de risco como este é, em si, demandado por vários frameworks regulatórios.

Embutir isto em seus processos regulares de arquitetura e desenho fornece para você uma abordagem de segurança por desenho - uma forma muito mais efetiva de melhorar a resiliência da sua organização do que simplesmente implementar algumas medidas de segurança após o evento de segurança cibernética. Não existe garantia de que nada sairá errado. De qualquer forma, ter uma abordagem para análise e mitigação de risco baseada em modelo, como apresentado aqui, se provará ser um grande investimento na segurança cibernética, continuidade do negócio e resiliência da sua organização onde (e quando) isto realmente importa.

Como Comunicar sobre Segurança Cibernética

Como prometido anteriormente, vamos voltar ao tema da comunicação sobre segurança cibernética. Nós daremos algumas dicas sobre como envolver mais o negócio, o que realmente funciona quando tratamos de construir a consciência da segurança, bem como algumas práticas a evitar.

Para começar a discussão, é realmente necessário comunicar sobre a arquitetura de riscos e segurança? Se sim, para quem? E o que? Bem, a comunicação é, de fato, integral ao processo, e você deveria pensar nos tomadores de decisão como seu público-alvo, uma vez que o negócio precisa estar bem-informado se as decisões certas devem ser tomadas. Como arquitetos corporativos tentando construir processos e padrões de segurança cibernética, você precisa envolver e informar não apenas a gerência, mas todo o resto da organização também.

O que você comunica também importa e é mais difícil de decidir, uma vez que as diferenças entre os tomadores de decisão do negócio são enormes. Interesses pessoais, experiência, níveis de educação e área profissional são todas variáveis importantes. Apesar disso, gostaríamos de oferecer uma lista de melhores práticas que com certeza ajudarão você a definir uma boa abordagem.

1. O risco não machuca; o impacto sim!

Normalmente, gerentes de risco e arquitetos de segurança tentam ganhar a atenção de seus gerentes e executivos de duas maneiras. Um método popular é mirar no medo e na dor. Eles comunicam o impacto potencial dos riscos no negócio. Alternativamente, alguns profissionais apresentam o ganho potencial de ser bem-sucedido em segurança, e.g. maior confiança dos clientes. Em geral, vender o medo supera vender o ganho de estar seguro. Isso é conhecido como "aversão à perda"[2]: as pessoas preferem evitar as perdas a buscar ganhos equivalentes.

2. Use metáforas

Metáforas são extremamente efetivas para comunicar conceitos complexos para os seus gerentes de negócio. Por exemplo, você pode simplificar a discussão comparando a segurança da informação com seguros. Todo mundo tem alguma forma de seguro. Muitas pessoas têm mais seguros do que realmente precisam. Naturalmente, a maioria das pessoas espera jamais precisar deles, mas eles compram de qualquer forma, apenas para se sentir seguros caso algo ruim aconteça.

Outra boa metáfora é o trânsito. Alguns gerentes gostam de dirigir em alta velocidade. Eles sabem que as coisas podem dar errado e eles poderiam acabar sendo penalizados de alguma forma, mas muitas vezes eles estão dispostos a aceitas este risco. Alguns gerentes jamais dirigem acima do limite legal de velocidade, porque eles sabem que podem sofrem multas ou até mesmo ter a carteira de motorista suspensa. Outros, usam aplicativos para saber onde a polícia está localizada. Quando você usa metáforas o risco se torna mais fácil de entender do que usando a terminologia abstrata da segurança cibernética. Isso ajuda você a defender a importância do gerenciamento de riscos.

3. Mostre exemplos concretos

Somente uma pequena parcela dos ataques (talvez poucos porcentos) são divulgados para o público. Mesmo assim, estes casos podem realmente ajudar as pessoas a internalizar quais são as consequências potenciais das falhas de segurança. Use isso! E seja esperto em relação a isso; escolha casos da sua própria indústria e/ou país para garantir que você atinja o alvo.

[2] https://en.wikipedia.org/wiki/Loss_aversion

4. Teste a segurança

Muitos profissionais têm que ficar em pé em frente ao edifício da empresa todo mês quando mais um treinamento de incêndio acontece. Verdade, isso é um inconveniente, mas todos nós entendemos que isso tem um propósito claro. O teste na vida real de problemas cibernéticos é feito por meio de testes de penetração, por exemplo. Mas nem o negócio em si, e especialmente sua direção, raramente são afetados por estes testes.

Tente organizar experiências envolvendo teste real de vazamentos de segurança, ataques e interrupção dos serviços. Isto não apenas fornece informações relevantes para você, mas também ajuda a dar um senso de urgência sobre este tópico para as partes interessadas.

5. Use comunicação específica para a parte interessada

O "negócio" não é uma pessoa. Ele é feito de um público amplo englobando os empregados do chão-de-fábrica, líderes de equipe, partes interessadas não-técnicas, semi-técnicas e técnicas, os membros da Diretoria e talvez até mesmo seus parceiros de terceirização. Estes grupos têm diferentes necessidades de informação e precisam de estilos de comunicação diferentes. Defina estratégias de comunicação que mostrem as informações de segurança corretas para as pessoas certas, por meio dos canais adequados e no formato correto. Apenas não ofenda os gerentes apresentando informação que foi simplificada em excesso!

6. Não use jargões, e se for realmente necessário, use jargões de negócio

Arquitetos entendem a distinção entre modelos conceituais, lógicos e físicos, e consideram os métodos que precisam ser aplicados. Mas os gerentes são indiferentes a isso. O único jargão em que eles são fluentes é o jargão dos seus próprios negócios. Dinheiro, velocidade e risco é o jargão a ser usado na sala da diretoria. Então, quando você estiver defendendo o seu caso, tenha certeza de relacionar as medidas com potenciais perdas financeiras ou de imagem. É bem provável que isso ajude você a engajar os membros da diretoria no assunto da segurança da informação.

7. Torne isso pessoal

A principal mensagem que deveria estar entranhada na mente dos gerentes de negócio depois de uma reunião de conscientização sobre segurança da informação deveria ser: "Este é um problema sério". Ou mais concretamente: "Isso afeta a mim/minha posição/meu pessoal/meus clientes/minha carreira". Discutir estes tópicos somente em grandes reuniões não ajudará realmente a receber retorno e entender se a mensagem foi recebida. Não fale *para* os gerentes e executivos que você gostaria de ter ao seu lado na sua jornada pela segurança da informação, fale *com* eles!

Aqui estão algumas abordagens que, na nossa experiência, funcionam muito bem para construir a conscientização sobre a segurança da informação:

- *O que isso tem a ver comigo*? Embora os interesses da organização como um todo a respeito da segurança da informação sejam compreendidos pela maioria dos empregados, os interesses pessoais ainda parecem falar mais alto para alguns. Tente explorar este fato dizendo o que elas têm a perder, como reputação, confiança, continuidade do negócio, dinheiro, dados, tempo, ou o que seja mais relevante para elas.
- *E se isso fosse na nossa empresa*? Perguntar para as pessoas o que elas fariam se fosse a sua empresa enfrentando problemas de segurança da informação é uma ótima forma de conseguir respostas honestas. Isso é uma questão pessoal, que leva as pessoas a pensar no desafio maior, não nas suas pequenas atividades.
- *O herói da segurança do mês*: Recompensar o bom comportamento é um mecanismo simples e ainda assim bastante efetivo. Reconheça aqueles que realizam bem com recompensas simples, e um elogio da gerência pode fazer uma grande diferença.
- *Mensagem em gotas vs inundação*: É uma prática ruim inundar sua audiência com uma enorme quantidade de informação uma ou duas vezes por ano. Ao invés disso, compartilhar mensagens curtas regularmente (ao invés de grandes mensagens raramente) funciona muito melhor para manter a segurança no topo das mentes das pessoas. Continue lembrando as pessoas sobre a sua visão e sempre repita o que você espera que as pessoas façam.
- *Torne real*: Uma demonstração de ataque pode jogar alguma luz na discussão. Não é necessário mostrar a parte técnica, apenas a parte onde você mostra qual foi o dano.

Criar a conscientização é realmente um desafio, mas com as melhores práticas mencionadas acima as coisas podem ficar um pouco mais fáceis. A suíte de ferramentas da BiZZdesign ajuda você a alavancar seus modelos, dados e portfólios de arquitetura existentes para lhe fornecer um início mais rápido quando buscando melhorar sua segurança de dados e garantir a conformidade regulatória.

Nossa abordagem integrada ajuda você a investir em segurança onde isso realmente conta, e evitar as penalidades e o risco de reputação de não-conformidades ou, pior, vazamentos de dados. Quer saber mais sobre como nossa plataforma pode ajudar você a melhorar sua segurança cibernética? Entre em contato conosco e marque uma demonstração do BiZZdesign Enterprise Studio.

Sobre a BiZZdesign

A BiZZdesign é uma fornecedora líder de software e serviços de transformação empresarial baseada na Holanda. Fundada em 2000, como uma cisão comercial de um instituto de P&D, hoje a empresa possui presença global é reconhecida pelos analistas de mercado como um líder de mercado. O principal produto da BiZZdesign, o Enterprise Studio, é utilizado pelas maiores empresas mundiais e organizações governamentais através dos cinco continentes, onde ele desempenha um papel fundamental na habilitação exitosa da mudança dos negócios.

Sobre a Centus

A Centus é uma empresa de consultoria de negócios e transformação empresarial baseada em Belo Horizonte. Fundada em 2013, a empresa é focada na disseminação de conhecimentos sobre arquitetura corporativa, gerenciamento de decisões, transformação de negócios e a linguagem ArchiMate. Nossos principais produtos são plataformas de gerenciamento de decisões e de modelagem e repositório de arquitetura corporativa, contando com a parceria e o apoio de empresas líderes nos seus mercados, como a BiZZdesign.

Para mais informações, por favor visite bizzdesign.centus.com.br ou www.bizzdesign.com.