WORLD ECONOMIC FORUM

EMPENHADO EM MELHORAR O ESTADO DO MUNDO

Moldando o futuro da Segurança Cibernética e da Confiança Digital

Guia de Segurança Cibernética para Líderes no Mundo Digital de Hoje

Outubro de 2019

Fórum Econômico Mundial
91-93 route de la Capite
CH-1223 Colônia / Genebra Suíça
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
E-mail: contact@weforum.org
www.weforum.org

Índice

Prefácio

Rob Wainwright
Parceiro Sênior da Deloitte

Tenho o prazer de apresentar este importante guia, que é o produto da colaboração conjunta entre o Fórum Econômico Mundial e vários de seus parceiros. Os desafios de segurança cibernética que todas as empresas enfrentam na economia digital interconectada de hoje atingiram novos níveis de complexidade e escala. As ameaças são propagadas por meio de formas novas e inovadoras de malwares, ao comprometer as cadeias de suprimentos globais e por meio sofisticados de atuantes estatais criminosos e hostis. Essas e outras características estão no centro de uma economia cibercriminosa em expansão e difícil de combater.

O Cibernético está em toda parte e não irá desaparecer. As empresas globais perceberam que não conseguem se safar dos desafios cibernéticos nem encontrar uma solução definitiva para remover as ameaças. O desenvolvimento de níveis mais robustos de resiliência cibernética hoje é a ordem do dia, e isso envolve tanto o desenvolvimento de uma nova cultura e mentalidade quanto a adoção de diferentes processos e tecnologias. A cibertecnologia traz novas demandas aos responsáveis pela administração dos negócios de segurança cibernética em empresas e organizações.

Portanto, este guia vem em boa hora, pois mostra os princípios de como a resiliência cibernética na era digital pode ser formada através de uma liderança eficaz e planejada. Desde as etapas necessárias para se parecer mais com um líder de negócios e desenvolver melhores padrões de higiene cibernética, até os elementos essenciais do gerenciamento de crises, o guia oferece um excelente manual de segurança cibernética para líderes nesse espaço. Com base na minha longa experiência de trabalho nos setores de inteligência e de aplicação da lei, bem como na minha exposição atual aos conselhos e equipes executivas de muitas empresas globais como parceira da Deloitte, todos os elementos aqui são relevantes e oportunos.

A recomendação para promover parcerias internas e externas é uma das mais importantes, na minha opinião. A natureza dinâmica da ameaça, principalmente em termos de como ela reflete o crescimento recente de uma economia criminal integrada, exige que construamos uma arquitetura global de cooperação cibernética melhor. Essa cooperação deve incluir plataformas mais eficazes para o compartilhamento de informações dentro e entre setores, liberando os benefícios da integração e análise de dados para criar melhores níveis de reconhecimento de ameaças e capacidade de resposta para todos. Soluções de tecnologia e modelos de governo estão disponíveis para atingir esse objetivo, tudo dentro de condições fortes e responsáveis de privacidade e segurança dos dados.

Nesta e em outras áreas prioritárias destacadas aqui, exigimos a liderança dos setores público e privado para conduzir essa importante mudança. Isso nos levará a um futuro cibernético melhor e mais confiante. Para os líderes de segurança cibernética envolvidos, a leitura deste guia é uma ótima maneira de começar.

Sumário Executivo

Os Ataques Cibernéticos são um dos 10 principais riscos globais de maior preocupação para a próxima década, de acordo com o Fórum Econômico Mundial ***Relatório Global de Riscos 2019***, com fraude e roubo de dados em 4º lugar e Ataques Cibernéticos em 5º. Globalmente, seu custo potencial pode chegar a US$ 90 trilhões em impacto econômico líquido até 2030/1 se os esforços de segurança cibernética não acompanharem o ritmo crescente da conectividade, de acordo com o Atlantic Council e a Zurich Insurance Group, entre outros. Embora os líderes governamentais e corporativos estejam profundamente engajados na promoção de estratégias eficazes de segurança cibernética e os gastos globais em segurança continuem se acelerando, o número anual de Ataques Cibernéticos atingiu o nível mais alto de todos os tempos no ano passado.

Os 10 principais riscos em termos de **Probabilidade**

1. Eventos climáticos extremos
2. Falha na mitigação e adaptação às mudanças climáticas
3. Desastres naturais
4. Fraude ou roubo de dados
5. **Ataques cibernéticos**
6. Desastres ambientais causados pelo homem
7. Migração involuntária em larga escala
8. Perda de biodiversidade e colapso do ecossistema
9. Crises Hídricas
10. Bolhas Financeiras em uma grande economia

Os 10 principais riscos em termos de **Probabilidade**

1. Falha na mitigação e adaptação às mudanças climáticas
2. Armas de destruição em massa
3. Eventos climáticos extremos
4. Crises Hídricas
5. Desastres naturais
6. Perda de biodiversidade e colapso do ecossistema
7. **Ataques cibernéticos**
8. Colapso da Infraestrutura crítica de informações
9. Desastres ambientais causados pelo homem
10. Propagação de doenças infecciosas

Há uma enorme gama de orientações na comunidade de segurança cibernética, desde padrões bem aceitos do governo e da indústria para segurança da informação em todo o mundo, incluindo ISO, NIST e muitos outros. No entanto, a aplicação das orientações continua aquém do necessário para garantir uma defesa eficaz contra ataques cibernéticos. O Centro do Fórum Econômico Mundial para Segurança Cibernética trabalhou com seus parceiros para considerar as atuais barreiras à adoção dessas práticas, em um esforço para fornecer alguns elementos essenciais para as organizações que desejam melhorar sua capacidade de defesa contra ataques.

Este guia é destinado a executivos seniores responsáveis por definir e implementar a estratégia e governança de segurança cibernética e resiliência em sua organização. A segurança cibernética é responsabilidade de todos em uma organização, não apenas do diretor de segurança da informação. É essencial que as principais partes interessadas no C-Suite, como Diretores de Informações, Diretores de Tecnologia, Diretores Digitais, Diretores Financeiros e outros executivos da empresa, entendam suas responsabilidades em relação à segurança cibernética.

Nós nos esforçamos para tornar este trabalho relevante para pequenas e grandes empresas, embora reconhecendo que alguns dos elementos prescritos podem ser mais pertinentes para empresas maiores com uma variedade maior de sistemas, funções e processos integrados.

Este guia é apenas uma parte de um portfólio mais amplo de trabalhos realizados pelo Centro do Fórum Econômico Mundial para Segurança Cibernética e por nossos parceiros. Por exemplo, o documento *Ferramentas e princípios do conselho para promover a Resiliência Cibernética* publicado pelo Fórum Econômico Mundial em 2017 definiu o tom no nível estratégico e executivos de organizações menores também podem querer consultar o *Kit de Ferramentas da Aliança Global de Segurança Cibernética para Pequenas Empresas*.

Observando as barreiras à adoção das melhores práticas de segurança cibernética, é evidente que as abordagens atuais dificultam a implementação de boas práticas abrangentes em toda a extensão dos ambientes digital e operacional nas organizações. Em outro aspecto, as ferramentas e processos de segurança geralmente são configurados uma vez e depois esquecidos, consequentemente se tornando redundantes

rapidamente em um cenário de ameaças em constante evolução. Os sistemas devem ser atualizados continuamente para acompanhar o fluxo da atividade comercial, a fim de proteger efetivamente contra vulnerabilidades recém-descobertas. Terceiro, embora as organizações tenham muitas ferramentas para automatizar tarefas de segurança, elas geralmente não podem ser usadas juntas de maneira totalmente automatizada. Isso resulta em um cenário complexo de ferramentas de segurança, lacunas e vulnerabilidades e, finalmente, na incapacidade de implantar uma abordagem automatizada holística. Por fim, outro grande desafio é o grande volume de trabalho envolvido no acompanhamento de alertas de segurança e incidentes que não podem ser automatizados. Existe uma dependência importante de seres humanos para desempenhar funções de segurança, em particular para avaliar as implicações mais estratégicas de alertas e incidentes. A escassez de talentos em segurança cibernética, no entanto, significa que essa função geralmente tem poucos recursos. Para compensar esses desafios, as organizações precisam considerar a terceirização de alguns dos serviços mais avançados, complexos e onerosos para os prestadores de serviços, dependendo do perfil de risco, para melhorar os contratos de cobertura e nível de serviço.

O papel dos líderes de resiliência cibernética de uma organização é apoiar a missão de sua organização, garantindo que os riscos cibernéticos sejam gerenciados em um nível aceitável. Não inviável para qualquer organização esperar que seu papel seja alcançar segurança sem falhas, ou mesmo que isso seja possível. Nenhuma empresa é imune a ameaças cibernéticas e as organizações precisam assumir que uma violação ocorrerá. O objetivo final é a resiliência, a capacidade de identificar e minimizar com rapidez e eficiência o impacto de um incidente para permitir que uma organização continue sua missão da maneira mais eficaz possível.

Na era digital, as organizações devem adaptar continuamente suas medidas de segurança cibernética proporcionalmente ao número crescente e à sofisticação das ameaças que enfrentam. De acordo com uma pesquisa realizada em 2018 por Willis Towers Watson e pela Unidade de Inteligência da The Economist (EIU, em inglês) 2 de 452 membros do conselho de grandes empresas, executivos e diretores do C-Suite com responsabilidade pela resiliência cibernética, um terço das empresas pesquisadas passou por um grande incidente cibernético que interrompeu suas operações e os executivos citam o tamanho do risco financeiro e de reputação como o motivo mais importante para a supervisão do conselho. Enquanto cerca de 45% das empresas norte-americanas confiavam na restauração após uma violação, esse número diminuiu para 30% para as empresas europeias e apenas 21% para as empresas asiáticas. Para agravar esse problema, foi relatado que, em média, apenas 1,7% da receita total foi gasta em resiliência cibernética.

Os princípios a seguir são os fundamentos que uma organização deve implementar para incorporar a segurança cibernética no DNA corporativo e como parte de um programa abrangente de segurança cibernética no exercício de diligências devidas para resiliência cibernética. Eles levam em conta as diretrizes e os padrões existentes e têm como objetivo servir como um guia prático de resiliência cibernética para executivos ao avaliar a gestão de riscos cibernéticos em sua organização.

10 Princípios para líderes

Princípio 1
Pense como um Líder de Negócios

Princípio 2
Promova parcerias internas e externas

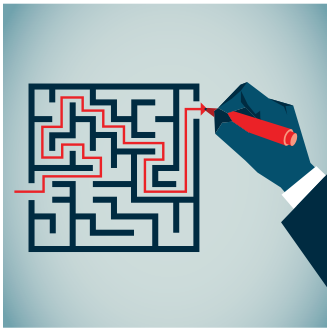
Princípio 3
Construa e pratique uma ampla Higiene Cibernética

Princípio 4
Proteja o acesso à ativos de suma importância

Princípio 5
Proteja seu domínio de e-mail contra Phishing

Princípio 6
Aplique uma abordagem de confiança zero para proteger sua cadeia de suprimentos

Princípio 7
Prevenir, monitorar e responder à ameaças cibernéticas



Princípio 8
Desenvolva e pratique um plano abrangente de Gerenciamento de Crises

Princípio 9
Crie um plano resistente de recuperação de desastres para ataques cibernéticos

Princípio 10
Crie uma cultura de Segurança Cibernética

Princípio 1: Pense como um Líder de Negócios

No contexto da Quarta Revolução Industrial, quase todas as empresas estão se transformando adotando tecnologias líderes e modelos de negócios inovadores baseados em dados. Nesta onda massiva e sem precedentes de transformação digital, as operações de segurança cibernética são um elemento vital do sucesso de todas as empresas. Hoje, as responsabilidades de um líder em segurança cibernética incluem educar a diretoria e a liderança executiva sobre a importância da gestão de riscos cibernéticos. Embora o setor de segurança cibernética tenha uma tendência a incutir medo para vender produtos, os líderes em segurança cibernética devem se concentrar em colocá-la como um componente integrante de sua estratégia e sucesso nos negócios.

Na última década, o papel e o significado da segurança cibernética dentro de uma organização - em geral e o dos líderes em segurança cibernética em particular - evoluíram imensamente. Os líderes de segurança cibernética são líderes de negócios, primeiro e acima de tudo, e, portanto, devem se posicionar, assim como suas equipes e operações como facilitadores de negócios.

Transformar a segurança cibernética de uma função de suporte em uma função de habilitação de negócios requer uma visão mais ampla e um conjunto de habilidades de comunicação mais forte do que o exigido anteriormente. Como parte integrante do sucesso comercial de hoje, a segurança cibernética influencia diretamente a reputação da empresa, o valor das ações, a receita, o valor da marca, o relacionamento com o cliente e o tempo de comercialização do produto, entre outros parâmetros. Consequentemente, os líderes na era digital devem:

- Promover a transparência e a confiança
- Desenvolver o pensamento crítico, a criatividade e a capacidade de resolver problemas, não apenas da equipe segurança cibernética, mas de toda a organização
- Possuir forte perspicácia comercial para converter os riscos técnicos em riscos da estratégia comercial, para que um público não técnico possa entender as ameaças potenciais às operações comerciais
- Entender os negócios e o setor em que atuam, para entender as ameaças cibernéticas exclusivas da organização e usar o idioma familiar à Diretoria e outros executivos da organização.
- Ser proficientes em falar o idioma comercial ao se comunicar sobre segurança cibernética para influenciar a gerência sênior e o Conselho de Administração
- Alinhar os objetivos da estratégia de segurança cibernética com a estratégia de negócios

O Centro do Fórum Econômico Mundial para Segurança Cibernética está tentando mudar a narrativa cibernética, que até agora era principalmente motivada pelo medo, destacando as oportunidades positivas para construir confiança na transformação digital.

Princípio 2: Promova parcerias internas e externas

A segurança cibernética é um trabalho de equipe. Ao fornecer veículos para o diálogo e a tomada de decisões, as parcerias internas permitem que as equipes de segurança da informação se tornem mais ágeis e responsivas às necessidades dos negócios. O número de parcerias em potencial aumentou e continuará a crescer à medida que o escopo do risco das informações se amplia para incluir uma série de preocupações regulatórias e de privacidade, bem como ameaças tradicionais à segurança. O momento de desenvolver essa parceria é antes de uma crise, não após uma violação da segurança cibernética.

Hoje, as equipes de segurança da informação precisam formar parcerias com muitos grupos internos na condução de várias funções, incluindo decisões de gerenciamento de riscos, resposta a incidentes e monitoramento.

Um líder em segurança cibernética precisa desenvolver uma visão, objetivos e KPIs (Indicadores-chave de desempenho) compartilhados com executivos de negócios para garantir que os prazos de entrega sejam cumpridos, enquanto oferece um produto altamente seguro e utilizável aos clientes, de acordo com a tolerância a riscos definida pela organização.

A tolerância ao risco identifica os limites de quanto risco uma entidade está preparada a aceitar. A conscientização do risco residual e a operação dentro de uma tolerância a riscos oferecem à administração maior garantia de que a empresa permanece dentro de sua apetência por riscos. Essa garantia, por sua vez, proporciona um maior grau de conforto para que a empresa alcance seus objetivos estratégicos.

Para garantir que os negócios em geral cumpram os requisitos legais e regulamentares, os líderes de segurança cibernética precisam incluir os executivos jurídicos e de privacidade como principais partes interessadas na jornada de segurança da organização.

Essas parcerias podem incluir estruturas formais, como comitês diretores e conselhos de revisão de riscos, bem como entidades informais e específicas. Sejam formais ou informais, as parcerias internas são essenciais para criar confiança e, portanto, devem ser criadas, mantidas e gerenciadas de acordo com as necessidades específicas da organização, com uma definição clara das partes envolvidas e das autoridades de tomada de decisão.

Além de construir parcerias internamente, está se tornando cada vez mais importante estabelecer parcerias com organizações externas para compartilhar informações sobre questões relacionadas à segurança, como ameaças e práticas recomendadas. Compartilhar informações de segurança traz benefícios consideráveis para gerenciar os riscos associados a ameaças cibernéticas ou adotar novas tecnologias. Isso é baseado na confiança; quanto mais confiável o relacionamento, mais sensível é a natureza das informações que podem ser compartilhadas.

Um elemento essencial para estimular o compartilhamento de informações é aumentar a proteção regulatória para as vítimas, de modo a incentivar as partes afetadas a compartilhar informações sobre Ataques Cibernéticos e violações sem medo da repercussão. Também é essencial conhecer as principais agências e funcionários das jurisdições em que os negócios são realizados. A aplicação da lei e o governo podem ser parceiros-chave na prevenção e na resposta.

O Centro do Fórum Econômico Mundial para Segurança Cibernética reúne partes interessadas do setor público e privado em comunidades de propósito e ação para enfrentar alguns dos desafios mais urgentes que os líderes de segurança cibernética enfrentam.

Princípio 3: Construa e pratique uma ampla Higiene Cibernética

A implementação eficaz e consistente de uma forte segurança cibernética poderia potencialmente mitigar a maioria dos ataques cibernéticos da última década. A exploração de vulnerabilidades conhecidas existentes em um servidor, aplicativo ou dispositivo de terminal, bem como a engenharia social - entendida como a manipulação psicológica de pessoas para executar ações ou divulgar informações confidenciais - são os principais pontos de entrada para um ataque cibernético, entre outros. Os princípios básicos de segurança a seguir são elementares e cruciais para criar uma forte higiene de segurança em uma organização:

- **Desenvolver um sistema detalhado de gerenciamento de inventário e configuração**
  Um entendimento claro e completo da cadeia de fornecimento de dados em uma organização é fundamental para a construção de uma higiene cibernética forte. As organizações devem desenvolver e manter sistemas atualizados de gerenciamento de inventário e configuração que registrem todos os dispositivos operacionais e de TI da empresa, aplicativos e suas configurações, bem como conjuntos de dados confidenciais na cadeia de fornecimento de dados da organização. Os sistemas devem incluir os recursos de monitoramento, configuração e status dos dispositivos, conjuntos de dados e aplicativos.

- **Desenvolva uma forte estratégia de correção**
  As empresas de hoje funcionam com uma infraestrutura heterogênea composta de vários componentes. Qualquer sistema crítico desatualizado representa vários níveis de risco, dependendo de como pode ser explorado e de como está conectado à rede mais ampla. Toda organização precisa garantir que cada componente através do qual qualquer fluxo de dados tenha um status de correção atualizado de acordo com uma avaliação da vulnerabilidade baseada em risco. A estratégia de correção deve incluir varreduras automatizadas dos ambientes em busca de vulnerabilidades, implantações automatizadas de correção e recursos de alerta. A implementação de tal estratégia para sistemas de controle industrial é um grande desafio, já que os sistemas antigos que têm um ciclo de vida muito longo podem não mais ser mais suportados. Um plano de renovação, além de controles compensadores, será essencial para proteger esses sistemas críticos contra ameaças cibernéticas.

- **Implementar forte autenticação em toda a organização**
  Os vetores de ameaças atuais, como o preenchimento de credenciais, por exemplo, abusam de credenciais de usuário fracas e falta de mecanismos de contestação de credenciais para obter acesso fraudulento às contas de usuário. A autenticação por multifator é um impedimento e reforço comprovados da postura de segurança, mitigando ataques cibernéticos que tentam aproveitar as credenciais de usuário comprometidas. O investimento em tecnologias que permitem a criação de senhas fortes e o gerenciamento contínuo de senhas também são impedimentos comprovados. Elas são altamente recomendadas porque geram altos retornos para uma sólida higiene cibernética.

  A FIDO Alliance (Fast Identity Online) e o World Wide Web Consortium (W3C) criaram um padrão aberto que permite a substituição de uma autenticação fraca baseada em senha por uma autenticação forte baseada em hardware para fazer a transição para um futuro sem senha.

- **Proteger o Active Directory**
  Um Active Directory é a principal plataforma de identidade para muitas empresas e deve ser considerado um componente crítico em uma infraestrutura. As empresas devem começar a implantar o Modelo de Camada recomendado pela Microsoft o Administrative Tier Model.

- **Aplicar mecanismos de segurança de dados para processos comerciais críticos**
  Todos os dados confidenciais, incluindo credenciais, devem ser criptografados, em repouso e em trânsito. No caso de uma violação de dados, os arquivos críticos devem resultar apenas na obtenção de dados ilegíveis. Grandes quantidades de informações pessoais continuam vazando na dark web após violações de dados direcionadas a empresas que geralmente falham na implementação de controles básicos de segurança cibernética, como criptografia de dados e proteção das chaves de criptografia para impedir que os cibercriminosos os acessem e os monetizem.

Princípio 4: Proteja o acesso à ativos de suma importância

É necessário fazer investimentos para aumentar ou escalar os sistemas de gerenciamento de identidade e acesso para atender aos novos desafios “sem perímetro” e na nuvem. Conceitos que promovem maior mobilidade e agilidade dos negócios também introduzem novas complexidades no sistema de gerenciamento de identidade e acesso de uma organização. A adoção de novas estratégias e tecnologias adaptadas às demandas de uma organização é essencial para proteger ativos críticos.

Nem todo acesso do usuário é criado da mesma forma. Ao definir as funções e políticas para cada usuário dentro de uma organização, o “princípio de acesso menos privilegiado” deve prevalecer. Por exemplo, um engenheiro de projetos não precisa acessar os dados financeiros de uma organização e um gerente financeiro não precisa acessar o repositório de códigos de produção da organização. A criação de um forte sistema de gerenciamento de identidade e acesso começa com uma única referência confiável de todos os usuários e suas funções dentro de uma organização. É essencial ter processos fortes e sistemas automatizados em vigor para garantir mecanismos apropriados de aprovação de direitos de acesso, inclusive para encerramento de acesso após a saída de um funcionário ou no final de um compromisso com um terceiro.

Por exemplo, um administrador de banco de dados dentro de uma organização pode exigir acesso a um repositório de dados para executar determinadas funções críticas ao seu trabalho. A gestão robusta do acesso de usuário privilegiado é fundamental nos casos de múltiplas funções nas organizações e para evitar combinações tóxicas. Deve haver um mecanismo de acesso em camadas para que um usuário privilegiado obtenha acesso a um sistema de suma importância. Cada camada deve ser reforçada com um mecanismo de autenticação multifator diferente, com base na sensibilidade das informações.

Por fim, mecanismos abrangentes de alerta e auditoria devem ser um requisito obrigatório para todo sistema de gerenciamento de identidades e acessos. Eles devem ser atualizados regularmente com base nos requisitos novos e variáveis da organização. Estes não devem ser definidos uma vez e depois esquecidos. Além disso, é necessário aderir a um processo de revisão regular, à medida que os projetos são concluídos e os requisitos de acesso mudam.

Princípio 5: Proteja seu domínio de e-mail contra Phishing

O e-mail é um dos meios de comunicação mais valiosos e amplamente utilizados, e a maioria das empresas depende fortemente deste meio. O protocolo de envio de e-mail pela Internet (SMTP) foi criado há quase 40 anos sem incluir segurança e é suscetível a uma ampla gama de ataques. O e-mail é o ponto de entrada mais comum, onde uma empresa média recebe mais de 90% do malware detectado por esse canal.[3]

As campanhas de phishing direcionadas, especificamente, podem ser mais bem-sucedidas falsificando o endereço de e-mail do remetente para representar uma organização ou pessoa confiável. Isso pode levar o destinatário a ceder credenciais ou infectar seu computador executando malware enviado por e-mail. Recomenda-se aumentar a conscientização do usuário sobre como evitar a fraude por e-mail, mas ainda é insuficiente – é necessário fazer mais.

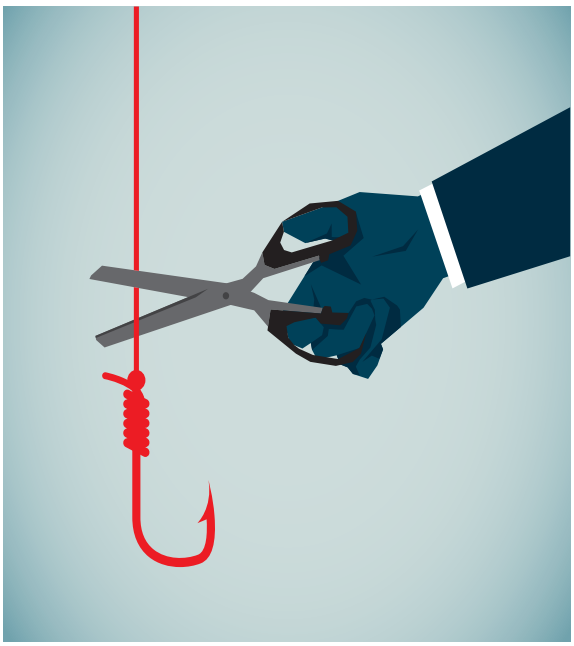
A redução do risco de violação por e-mail é possível por meio das seguintes medidas:

- Treinar todos os funcionários no reconhecimento de e-mails de phishing, especialmente a liderança da empresa e os departamentos que lidam com informações confidenciais, pois geralmente são os principais alvos de phishing; talvez essa seja a medida mais eficaz para proteger sua organização contra phishing
- Manter-se informado sobre as técnicas de phishing à medida que novos golpes são constantemente desenvolvidos, inclusive por telefone ("vishing") e mensagem de texto ("smishing")
- Implementar um filtro de e-mail para identificar e separar e-mails de spam, verificar hiperlinks e anexos em busca de conteúdo malicioso e implementar regras específicas de acordo com as políticas de sua empresa
- Implantar um software antimalware atualizado em todos os dispositivos de terminal, pois eles geralmente possuem algum tipo de recurso antiphishing
- Aderir a práticas robustas de segurança cibernética, as quais reduzirão significativamente o risco de um problema por meio de um e-mail de phishing
- Implementar o padrão gratuito DMARC (*Domain-based Message Authentication, Reporting & Conformance*), que ajuda remetentes e destinatários a trabalharem juntos para melhor proteger e-mails e proteger usuários e marcas contra violações caras e prejudiciais

A implementação do DMARC, em particular, ajuda a:

- Reduzir o risco na empresa, bloqueando os e-mails de spear-phishing antes que eles cheguem aos usuários
- Proteger outras organizações, reduzindo o risco de receber e-mails de spear-phishing que usurpam seus domínios
- Ser notificado em tempo real sobre novas campanhas de e-mail de spear-phishing, que podem colocar sua empresa ou comunidade em risco

A Global Cybersecurity Alliance fornece diretrizes simples sobre como as organizações podem implementar o DMARC com maior facilidade.



Princípio 6: Aplique uma abordagem de confiança zero para proteger sua cadeia de suprimentos

Quase 50% das empresas falham ao avaliar o nível de risco cibernético de seus fornecedores de hardware e software.[4] Hackers trabalharão proativamente para identificar e explorar o elo mais fraco de uma cadeia de valor, por isso, uma abordagem de confiança zero para proteger a cadeia de suprimentos deve ser a norma.

A alta velocidade de novos aplicativos em desenvolvimento junto da adoção de plataformas de código aberto e nuvem não têm precedentes. As organizações geralmente não conseguem resolver bugs ou problemas de configuração de versões anteriores de seus aplicativos de software, pois a demanda por novas versões é sempre urgente. Para isso, a equipe de segurança precisa adotar novas técnicas que permitam aos desenvolvedores escrever códigos seguros desde o início, em vez de descobrir falhas de segurança durante as revisões de código ou já na produção.

Práticas de segurança por padrão devem ser incorporadas ao ciclo de vida completo do projeto e ao desenvolvimento do produto, incluindo codificação, arquitetura do sistema, configuração e na definição do processo para avaliação contínua dos riscos.

As organizações devem descartar a convicção de que a segurança do perímetro, obtida com firewalls ou proteção antivírus, seja suficiente. Elas precisam adotar uma abordagem de confiança zero que não suponha que uma empresa pode estar a salvo dentro dos limites de sua própria rede corporativa "segura". Uma abordagem de confiança zero coloca o controle sobre os próprios ativos de dados e aumenta a visibilidade de como são usadosem um ecossistema corporativo digital. A segurança cibernética é tão forte quanto seu elo mais fraco.

Seguir as etapas abaixo ajudará a assegurar o nível de cuidado devido a toda a cadeia de suprimentos:

- Limitar o acesso conforme a necessidade
- Conduzir a devida diligência nos antecedentes dos fornecedores com acesso
- Revisar a linguagem de contratos existentes; entender as práticas de segurança cibernética de fornecedores já existentes
- Vincular contratualmente os fornecedores às políticas e normas de segurança
- Auditar fornecedores terceirizados com base na importância e localização dos negócios; os fornecedores devem estar dispostos a cooperar para manter um nível de segurança que seja bom o suficiente de acordo com normas organizacionais
- Exigir que os fornecedores que processam dados confidenciais comuniquem incidentes cibernéticos em até 72 horas após a ocorrência

O Centro do Fórum Econômico Mundial para Segurança Cibernética vem trabalhando com a comunidade de investimentos para desenvolver um conjunto de princípios de alto nível e uma estrutura de due diligence padrão. Este trabalho tem como objetivo fornecer orientação sobre como investidores podem não apenas avaliar e comparar as empresas de seu portfólio de investimentos e seu nível de preparo em segurança cibernética, mas também influenciar a nova tecnologia em desenvolvimento em uma possível empresa-alvo, ao priorizar segurança e privacidade por projeto e padrão. O compromisso do investidor em priorizar a segurança em novas tecnologias garantirá que a superfície geral de ataque seja reduzida, diminuindo o número de vulnerabilidades.

Princípio 7: Prevenir, monitorar e responder a ameaças cibernéticas

Apesar da crescente pressão dos ataques cibernéticos direcionados, com criminosos cibernéticos elevando o nível de suas operações usando modelos de negócios mais sofisticados, como ransomware como serviço e DDoS-for-Hire, e monetizando esses esforços com criptomoedas, as equipes de segurança seguem identificando quase dois terços de todas as tentativas de violação, em média.[5] No entanto, essas ocorrências ocultam uma discrepância no desempenho entre as organizações. Embora muitas organizações tenham bom desempenho em indústrias e mercados mais maduros, algumas estão claramente enfrentando a crescente pressão de ataques.

Novos vetores e técnicas de ataque modificam continuamente o cenário de ameaças. Os sistemas de detecção ficam desatualizados rapidamente se não evoluírem no ritmo da inovação e requerem aprimoramento contínuo, com contribuições de diversas fontes. Ao mesmo tempo, novas técnicas de detecção com base em tecnologias de aprendizado de máquina e inteligência artificial devem ser aplicadas para permitir que os sistemas de detecção possam consumir essa ampla variedade de dados, executar regressões e análises para, finalmente, produzir sinais de alta fidelidade que indiquem uma anomalia ou atividade suspeita de forma proativa para mais investigações.

As equipes de inteligência de ameaças devem realizar buscas proativas em toda a infraestrutura da organização, além de manter as equipes de detecção informadas das tendências mais recentes. As organizações devem monitorar ameaças cibernéticas, interna e externamente, e investigar regularmente se há vulnerabilidade em sistemas críticos e com acesso à Internet. Além disso, precisarão monitorar a Internet, mídias sociais e a dark web para obter dados e informações roubados sobre executivos e operações comerciais importantes que poderiam ser usados para engenharia social, ataques de spear-phishing e campanhas golpistas. O Mitre Attack Framework oferece uma base de conhecimento de táticas e abordagens comuns usadas pelos adversários.

A questão não é se, mas quando haverá uma violação significativa e, portanto, qual será o nível de sucesso da empresa no gerenciamento é inevitavelmente crítico.

A chave aqui é desenvolver uma abordagem com base em risco robusta para avaliar riscos e responder a ataques cibernéticos, que seja personalizada ao contexto comercial da organização. Os serviços de segurança implementados devem ser adequados ao objetivo e adaptados às necessidades da organização nas três dimensões:

- As pessoas e organização que operacionalizarão esses serviços
- Os processos e procedimentos para gerenciá-los efetivamente
- As tecnologias que serão adquiridas e implementadas

Embora grandes organizações possam contratar especialistas internos em segurança cibernética para gerenciar alguns serviços complexos (incluindo testes de intrusão, exercícios red/blue team, um centro de operações de segurança, busca a ameaças e outros), pequenas e médias empresas devem considerar a terceirizar esses serviços a um prestador de serviços de segurança gerenciado, para reduzir a complicação e os custos da formação e treinamento de uma organização interna e aquisição de hardware e software necessários. Esses serviços terceirizados também costumam oferecer melhores contratos de nível de serviço e cobertura, que se tornam essenciais ao lidar com organizações criminosas que trabalham 24 horas por dia. Ao considerar a terceirização de serviços de segurança, as empresas precisam fazer a devida diligência, se envolver com prestadores de serviços respeitáveis e confiáveis e firmar contratos de nível de serviço detalhados.

Uma abordagem tripla mitigará os riscos cibernéticos no ecossistema corporativo em constante expansão:

Prevenir. Estratégias preventivas permanecem muito importantes e devem evoluir continuamente, desde suas políticas de segurança e programas de conscientização até os controles de acesso reais que eles implementam. Uma abordagem multicamadas com base em riscos fortalecerá a proteção de ativos críticos e minimizará o risco de invasão.

Detectar. A prevenção não é infalível devido à natureza evolutiva das ameaças cibernéticas, portanto é essencial ter mecanismos de detecção adequados. A seleção e implantação de controles apropriados para detecção e notificação pontual de comprometimentos é essencial. Os controles de detecção devem ser projetados para monitorar os ativos críticos que armazenam e processam informações confidenciais ou são vitais para as operações da organização.

Resposta. A detecção é inútil sem resposta. As organizações precisam abordar a segurança cibernética como vantagem competitiva e responder de com eficácia e prontidão a um incidente de segurança, de forma a mitigar o impacto nos negócios, conter as redes e dispositivos infectados e investigar a origem do ataque para determinar o vetor de infecção e paciente zero. O monitoramento dos eventos coletados dos diversos ativos de infraestrutura e aplicativos terá que ser ampliado para rastrear e alertar sobre qualquer atividade anormal.

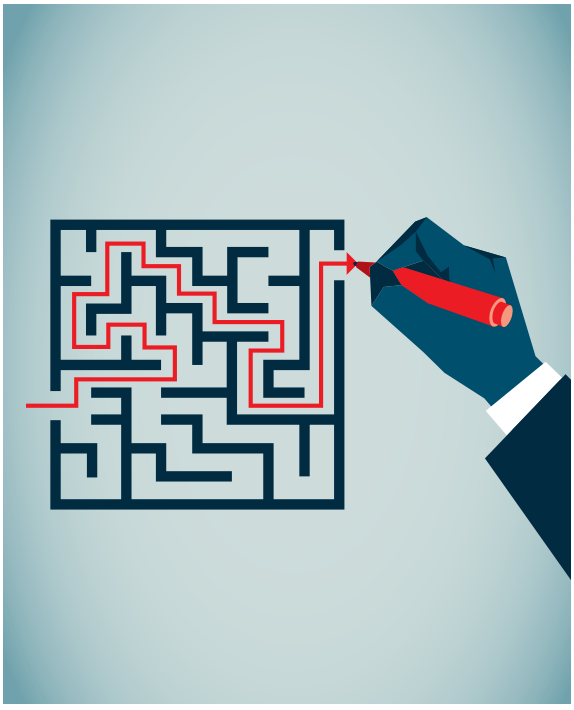
Princípio 8: Desenvolva e pratique um plano abrangente de Gerenciamento de Crises

A gestão de crises é um elemento crítico de qualquer programa de segurança no mundo atual, onde um incidente de segurança não é mais uma questão de se, mas quando. Uma organização de segurança comum que se concentra exclusivamente em análise e mitigação de riscos pode não estar bem posicionada para gerenciar uma crise. Assim, a formação de uma equipe exclusiva, apta a gerenciar crises, é o primeiro componente.

Proteger uma empresa inteira é uma tarefa extremamente difícil, principalmente porque tudo é uma prioridade. Qualquer possível vulnerabilidade pode se tornar o próximo ponto de ataque a comprometer os negócios. Por isso, muitas organizações se concentram principalmente em como se prevenir e defender, porém não se concentram o bastante em institucionalizar o manual de gestão de crises para toda a organização.

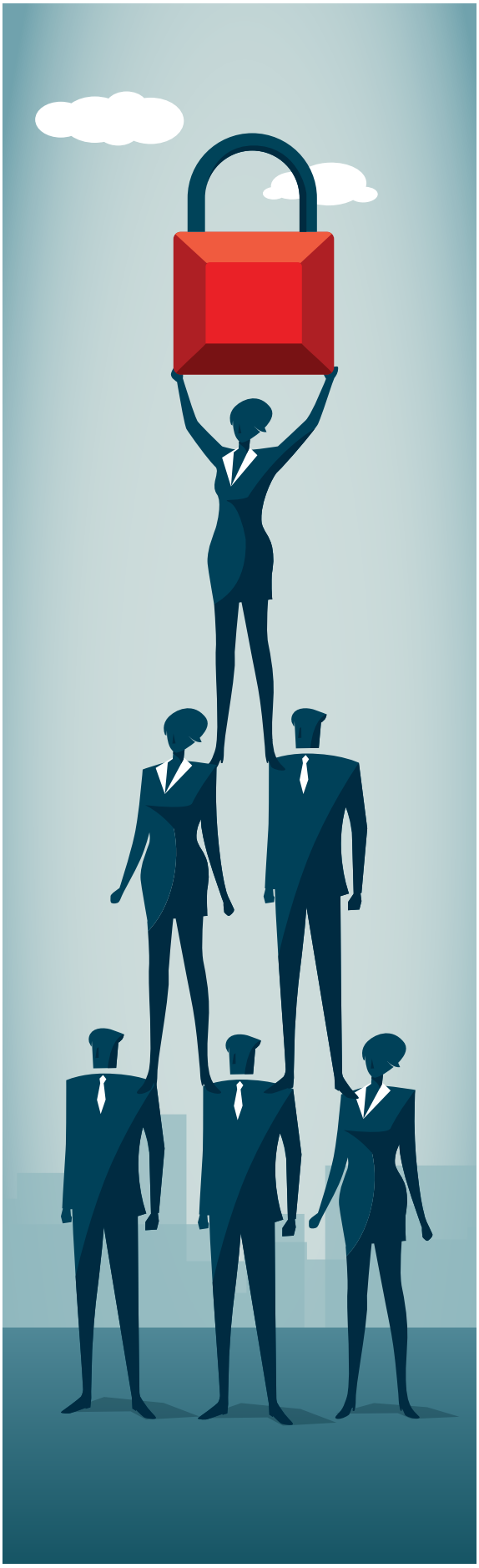
Os aspectos a seguir são vitais ao elaborar um plano de gestão de crises:

- Desenvolver uma equipe multifuncional. O escopo da equipe varia entre a liderança executiva e inclui os departamentos de operações, financeiro, jurídico, comunicação, seguros, recursos humanos e tecnologia
- Quando há uma crise, um plano altamente detalhado é vital para coordenar indivíduos com diferentes funções e responsabilidades rumo a um objetivo e ação coletiva comuns. Esse plano precisa abranger todo o espectro de atividades da empresa, desde as ferramentas a serem usadas para gerenciamento de casos e comunicação interna até as salas de conferência que devem ser reservadas em caso de crise
- Considerar vias de comunicação alternativas, incluindo mecanismos de comunicação alternativos que não dependam da infraestrutura principal da empresa (que pode ficar indisponível durante um ataque cibernético)
- Manter sempre um backup com cópias impressas de procedimentos, contatos e outras documentações críticas à operação
- Convocar especialistas técnicos, jurídicos e de relações públicas terceirizados e seguradoras durante uma grande crise, para fornecer visões imparciais
- Identificar e manter uma lista facilmente disponível dos principais contatos de execução da lei e reguladores aplicáveis, caso seja preciso comunicar-se com essas autoridades
- Assegurar o cumprimento de leis regulatórias globais ao documentar seu plano de gestão de crises
- Concentrar-se no alcance, motivações e objetivos de possíveis ataques (por ex., espionagem, negação de serviço, ganhos financeiros, etc.).
- Praticar exercícios e simulações teóricas frequentes, para garantir a prontidão em caso de crise
- Se a organização não se comunicar, outros o farão, e muitos “especialistas” ficarão felizes em especular
- Considerar que a ocorrência de violações pode ser particularmente elevada durante a inatividade das operações e permanecer vigilante durante esses períodos (por ex., fora do horário comercial, durante feriados)
- Evitar o excesso de confiança na tecnologia para embasar seu plano; sistemas e comunicações podem não estar disponíveis durante um incidente cibernético



A pontualidade é tão importante quanto transparência e simplicidade na formação de um sólido relacionamento de confiança com clientes, acionistas, reguladores e outros interessados. No passado recente, houve inúmeros exemplos terríveis de empresas que falharam em comunicar incidentes de segurança a seus clientes ou que comunicaram apenas quando exigido por um órgão regulador. Em certos casos, como a violação de dados do Yahoo em 2016, a demora na comunicação de um incidente permite que os invasores usem indevidamente os dados comprometidos do cliente, mesmo antes que o cliente seja notificado. Em contrapartida, o ataque cibernético à Norsk Hydro que atingiu a gigante da manufatura de alumínio em março de 2019 destacou os benefícios de um plano de comunicação e resposta a incidentes perfeitamente orquestrado que resultou em ações com preços mais altos. Estes são bons exemplos para garantir a pontualidade das comunicações de incidentes de segurança.

Em caso de incidente de segurança, é importante informar aos clientes que a permanência é limitada ao incidente e não as possíveis consequências para as vítimas. Muitas vezes, as organizações comunicam-se publicamente com seus clientes sobre um possível comprometimento dos dados, sem perceber que essa comunicação é uma oportunidade para que os criminosos cibernéticos enganem os clientes. Frequentemente, ondas de ataques de phishing sofisticados são lançadas visando clientes de empresas que recentemente tenham comunicado uma violação de segurança. Notícias de uma violação geralmente exigem que os clientes realizem determinadas ações, como, por exemplo, fornecer informações para verificar se foram afetados pelo incidente.



Princípio 9: Crie um plano resistente de recuperação de desastres para ataques cibernéticos

À medida que a sociedade se torna mais dependente da tecnologia e os ataques cibernéticos se proliferam, é essencial que todas as organizações, independentemente do porte, estejam prontas para o pior. Uma grande violação de ativos críticos pode ter impacto desastroso na reputação, operações e finanças de organizações incapazes tomar medidas abrangentes para se proteger.

Incêndios, tempestades, apagões e outros eventos físicos são imprevisíveis, mas geralmente têm uma natureza bem compreendida. As ameaças à segurança, por outro lado, são imprevisíveis e, dada a natureza de rápido avanço dos crimes cibernéticos, geralmente não são bem compreendidas. Isso significa que as estratégias de recuperação de segurança devem ser analisadas e atualizadas com mais frequência que as estratégias de recuperação de desastres. Além disso, os líderes de segurança cibernética precisam integrar a equipe de recuperação de desastres e devem ser consultados antes que um desastre seja declarado como resultado de um ataque cibernético.

Um plano de recuperação de desastres e continuidade deve ser adaptado aos cenários de incidentes de segurança, para proteger a organização de possíveis ataques cibernéticos e instruir como reagir em caso de violação de dados. Além disso, pode reduzir o tempo necessário para identificar violações e restaurar serviços críticos para a empresa.

Siga estas melhores práticas para elaborar seu plano:

- **Defina seus ativos principais**

  Para defender sua empresa de ataques, é preciso primeiro saber o que está protegendo. Quais são os principais ativos que causariam prejuízos à sua empresa e às partes interessadas caso fossem invadidos? Reúna sua equipe de gerenciamento para discutir essas possíveis perdas e como mitigar a ameaça

- **Identifique soluções de recuperação**

  Após definir os ativos mais importantes de sua empresa, o próximo passo é determinar os meios de recuperação em caso de violação de dados e ataque cibernético. Os planos de recuperação ou de mitigação permitem que a empresa permaneça em níveis aceitáveis. Por exemplo, podem incluir salvar dados em um disco, servidor ou armazenamento em nuvem de backup – ou talvez replicar totalmente os dados em uma instalação externa segura

- **Desenvolva e divulgue a governança**

  Em caso de emergências, é importante saber quem é responsável por declarar oficialmente um desastre e aprovar uma cadeia de comunicação.

- **Revise e pratique seu plano com frequência**

  Para que seu plano funcione efetivamente conforme planejado, é importante repassá-lo com os funcionários regularmente, para que todos entendam o que fazer quando deparados com uma violação de dados ou um grande ataque cibernético. Certifique-se de atualizar o plano de acordo com novas políticas adicionadas e mudanças de pessoal e assegure que seja praticado com exercícios e simulações teóricos.[6]

Além de um plano de recuperação de desastres e continuidade, pode ser útil considerar o seguro cibernético. Embora o custo total da detecção de violação de dados esteja aumentando à medida que os ataques cibernéticos ficam mais sofisticados, o seguro de responsabilidade cibernética ajuda a reduzir esses custos.

Princípio 10: Crie uma cultura de Segurança Cibernética

O tradicional paradigma de segurança corporativa, geralmente expresso como um fosso ao redor do castelo, descrevia uma barreira de tecnologia que isolava e protegia os trabalhadores atrás dela. Atualmente, no entanto, um número crescente de interações de usuários com o mundo externo ignora os perímetros físicos e de rede e os controles de segurança que eles oferecem. Essas interações ocorrem em sites externos e redes sociais, laptops em cafeterias e residências e continuamente em dispositivos pessoais, como smartphones e smartwatches.

Esse ambiente em mudança não significa que o perímetro de segurança desapareceu. Em vez disso, foi transferido para os usuários e seus diversos terminais. Consequentemente, a identidade tornou-se o novo perímetro. Todos os dias, os usuários tomam decisões que podem ter tanto impacto na segurança quanto os controles técnicos que utilizamos.

Manter uma organização segura é o trabalho de todos os funcionários: vetores de ataque de vias principais, como phishing, por exemplo, são aproveitados por muitos invasores. Isso coloca os usuários na primeira linha de defesa e reconhece a função crítica que todos os funcionários desempenham na segurança da organização. É importante que as regras de segurança e a tecnologia fornecida permitam que os usuários executem seu trabalho e ajudem a manter a organização segura. De acordo com a pesquisa IBM X-Force, em 2018, 43% dos registros comprometidos estavam associados a erros humanos e configuração incorreta de serviços de TI[7], e 75% desses incidentes envolviam más intenções, com a negligência sendo responsável pelo restante. Portanto, as organizações devem levar em conta que a maioria das violações de dados é cometida por agentes internos. Isso pode ocorrer através da divulgação não intencional de informações confidenciais, clicar em um link de phishing, negligência no uso de unidades USB não seguras, redes WIFI, uso de senhas fracas ou reutilizadas ou de práticas inadequadas de compartilhamento de senhas.

As práticas a seguir ajudarão a promover uma cultura de segurança cibernética mais forte:

- Desenvolva a conscientização de usuários e treinamentos adaptados ao contexto empresarial e a diferentes grupos de usuários da organização.
- Implemente uma divulgação eficiente de campanhas de conscientização, aproveitando formas diversas e inovadoras para melhorar o engajamento e alcance em toda a organização.
- Incentive os funcionários a participarem da campanha de conscientização e denunciarem atividades suspeitas. Por exemplo, o setor de aviação tem mantido consistentemente altos padrões de segurança, implementando programas eficazes de treinamento e conscientização para sensibilizar todos os funcionários a denunciarem incidentes e depois investigá-los. Uma abordagem similar deve ser adotada para incidentes de segurança cibernética.
- Aplique sanções contra grandes infratores ou reincidentes, conforme o código de conduta da organização

O conhecimento básico sobre segurança deve se tornar popular, e as organizações devem formar parcerias com os sistemas educacionais acadêmicos e do governo, para elaborar um programa de ensino adaptado às reais necessidades de seu setor, a fim de preparar uma força de trabalho de segurança cibernética equipada com as habilidades necessárias para a era digital.

O Centro Econômico Mundial para Segurança Cibernética está trabalhando com seus parceiros para solucionar a deficiência de habilidades de segurança cibernética, por meio do trabalho com líderes globais para encontrar formas modulares de combater a escassez de habilidades de segurança cibernética e ajudar países com economias digitais emergentes a estimular seu setor de tecnologia.

Conclusão

Troels Oerting
Presidente do Conselho Consultivo do Fórum Econômico Mundial de Segurança Cibernética

Os líderes de segurança cibernética de hoje são uma espécie diferente dos líderes do passado. A natureza da função mudou rapidamente de uma posição voltada à tecnologia para uma responsabilidade de liderança nas empresas, e essa evolução está longe de seu fim.

Uma estratégia bem-sucedida de segurança cibernética e sua implementação dependem da cultura da organização. Segurança cibernética, privacidade e confiança digital têm base no sucesso da organização em integrar a segurança como um elemento inerente do seu DNA.

A importância de promover um ambiente de segurança e conscientização de riscos, responsabilidade conjunta e resiliência a riscos cibernéticos só aumentará. Líderes de segurança cibernética capazes de ir além do nível tático e técnico têm maior chance de obter credibilidade e apoio entre os líderes de toda a empresa, incluindo os líderes do conselho, diretoria executiva e unidades de negócios.

Na Quarta Revolução Industrial, todas as empresas estão passando por uma digitalização transformadora de seus setores, o que dará acesso a novos mercados e também esperança de um mundo melhor e mais próspero.

Essa transformação digital é alimentada por avanços tecnológicos disruptivos, como 5G, IA, computação em nuvem e a conexão do mundo físico com o digital por meio das tecnologias de IoT, que conectam tudo, geram petabytes de dados e aumentam a superfície de ataque e a quantidade de vetores.

Essa explosão de conectividade oferece às empresas grandes oportunidades de aumentar a eficiência operacional, melhorar a satisfação e a experiência do cliente. Contudo, ela traz uma ressalva: À medida que os dados do cliente, a propriedade intelectual e o valor da marca evoluem, se tornam novos alvos de roubo, afetando diretamente o valor para os acionistas e o desempenho da empresa. Como resposta, os líderes empresariais precisam que os líderes de segurança cibernética assumam um papel de liderança mais sólido e estratégico. Inerente a essa nova função está o dever de ir além da função de monitores e agentes de conformidade, para integrar-se melhor aos negócios, gerenciar riscos de informações de forma mais estratégica e trabalhar rumo a uma cultura de responsabilidade conjunta por riscos cibernéticos em toda a empresa.

Ao avaliar riscos cibernéticos, os líderes de segurança cibernética são agora chamados a avaliar o impacto nos negócios e ter métricas para avaliar a conformidade operacional e regulatória e o impacto financeiro. Como no mundo físico, a segurança perfeita não existe no mundo digital e são necessárias contrapartidas. As empresas e principais partes interessadas precisam tomar decisões mais bem informadas sobre o apetite de risco de sua organização, para definir uma postura boa o bastante em relação à segurança cibernética. Isso envolveria a avaliar o cenário de ameaças, motivos e táticas de invasores, bem como a identificar de ativos digitais críticos, vulnerabilidades conhecidas para priorizar o nível apropriado de controles necessários em relação a pessoas, processos e tecnologias.

Uma segurança cibernética robusta tornou-se fundamental para um ecossistema de negócios e indústria resilientes. Com uma gestão de riscos cibernéticos eficaz, as empresas podem chegar a futuros mais inteligentes, rápidos e conectados, promovendo o crescimento dos negócios. À medida que as ameaças cibernéticas aos negócios continuam a evoluir, líderes dos setores público e privado terão que enfrentá-las no mundo digital e físico, para mitigar qualquer possível dano a indivíduos e evitar a interrupção de serviços críticos.

Fatores Contribuintes

O Fórum Econômico Mundial gostaria de agradecer aos parceiros e colaboradores desta publicação:

Kelly Bissel	Diretor Executivo, Accenture Security, Accenture, EUA
Craig Froelich	Diretor de Segurança da Informação, Bank of America, EUA
Paul Gillen	Diretor Executivo, Chefe de Operações de Segurança e Vice-Diretor de Segurança, Barclays, Reino Unido
Rob Wainwright	Parceiro Sênior, Deloitte, Holanda
Rosa Kariger	Diretor Global de Segurança da Informação, Iberdrola, Espanha
Jim Alkove	Vice-Presidente Executivo, Segurança, Salesforce, EUA
Anthony Dagostino	Diretor Global de Risco Cibernético (2016-2019), Willis Towers Watson, EUA
Peter Foster	Presidente Global de FINEX (Riscos Financeiros, Executivos e Profissionais) e Soluções para Riscos Cibernéticos, Willis Towers Watson, EUA
Paige Adams	Diretor de Segurança da Informação do Grupo, Zurich Insurance Group, EUA

Do Fórum Econômico Mundial

Georges de Moura	Diretor de Soluções Industriais, Centro de Segurança Cibernética; Autor Principal
Troels Oerting	Presidente do Conselho Consultivo, Centro de Segurança Cibernética

O Fórum também deseja agradecer a contribuição de Algirde Pipikaite e Amy Jordan, Líderes do Projeto, no Centro de Segurança Cibernética.

Notas Finais

1. Nota da Zurich Insurance Group. A mitigação do risco cibernético pode representar uma diferença de US$ 120 trilhões para a economia global até 2030. https://www.zurich.com/en/media/news-releases/2015/2015-0910-01 (acesso em 23/10/19)

2. Infográfico: Informações globais sobre invasões cibernéticas e confiança organizacional https://www.willistowerswatson.com/en-BE/Insights/2018/07/infographic-global-insights-on-cyber-intrusionsand-organisational-confidence (acesso em 23/10/19)

3. 2019 Verizon Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/ (acesso em 23/10/19)

4. Global Cyber Risk Perception Survey. https://www.marsh.com/us/insights/research/globalcyber-risk-perception-survey.html (acesso em 23/10/19)

5. 2018 State of Cyber Resilience report. https://www.accenture.com/pl-en/insights/security/2018-state-of-cyber-resilience-index (acesso em 23/10/19)

6. Healthcare Business and Technology. https://www.healthcarebusinesstech.com/cyber-attacksrecovery-plan/ (acesso em 23/10/19)

7. IBM 2018 Cyber Security Intelligence Index. https://www.ibm.com/security/data-breach/threatintelligence (acesso em 23/10/19)

WORLD ECONOMIC FORUM

EMPENHADO EM MELHORAR O ESTADO DO MUNDO

O Fórum Econômico Mundial, comprometido com a melhoria do mundo, é a Organização Internacional de Cooperação Público-Privada.

O Fórum envolve os principais líderes políticos, empresariais e outros da sociedade para definir agendas globais, regionais e das indústrias.

Fórum Econômico Mundial
91-93 route de la Capite CH-
1223 Cologny/Genebra, Suíça

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org