Fundamentos da segurança cibernética

Visão geral da segurança cibernética

O que é a segurança cibernética?

15 Minutos

Visão geral do módulo

Este módulo se concentra em alguns fundamentos sobre segurança cibernética para você começar no curso. Você aprenderá sobre estes tópicos:

- O que é segurança da informação e segurança cibernética?
- Objetivos da segurança da informação, usando a tríade CIA
- Elementos-chave da segurança cibernética
- Risco e os métodos para gerenciar riscos
- Equívocos comuns sobre o setor de segurança cibernética
- Importância das leis e considerações éticas para o setor de segurança cibernética

Depois de concluir este módulo, os alunos devem ser capazes de:

- Comparar e contrastar os cinco principais tipos de grupos de agentes de ameaças
- Descrever tipos comuns de ataques cibernéticos
- Explicar a estrutura geral de um ataque cibernético típico, discutindo cada etapa da estrutura da Lockheed Martin Cyber Kill Chain
- Usar a matriz MITRE ATT&CK para identificar táticas e técnicas do invasor
- Resumir como funciona a economia do crime cibernético
- Definir engenharia social e descrever técnicas comuns de engenharia social
- Descrever inteligência de código aberto (OSINT) e fontes comuns que os invasores usam
- Listar as técnicas típicas de escaneamento técnico e discutir as informações que cada uma fornece
-

Resumir os detalhes e as lições aprendidas com vários ataques cibernéticos de alto perfil

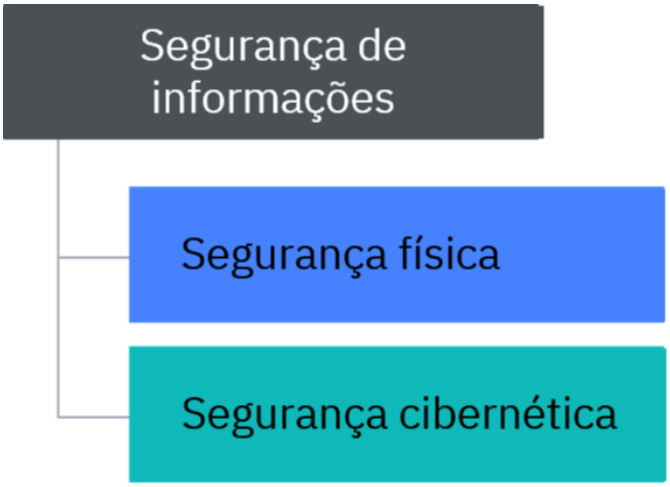
Segurança de informações

Vamos começar pensando sobre o que é segurança cibernética e o que estamos tentando realizar. A maioria das definições de segurança cibernética tende a se concentrar na **tecnologia**. Portanto, uma definição típica seria "segurança dos sistemas digitais" ou "segurança das comunicações". Essas definições tendem a ficar confusas muito rapidamente. Por exemplo:

- E se um fraudador enviar um e-mail a uma pessoa afirmando ser do banco e solicitar o número de identificação pessoal (PIN) dela. Isso é uma preocupação da segurança cibernética?
- E se um investigador particular ligar para um funcionário de uma empresa para pedir que ele imprima alguns arquivos confidenciais e deixe os papéis na sala de correspondência para a coleta. Isso é uma preocupação da segurança cibernética?

No mundo real, a maioria dos ataques geralmente tem alguns **elementos digitais**, mas também alguns **fatores humanos** e, ocasionalmente, **elementos físicos** a serem considerados. Lembre-se disso. Não devemos nos concentrar somente nos elementos digitais, porque isso limita nosso processo de raciocínio e oferece maior flexibilidade aos invasores em potencial.

Vamos considerar um novo conceito chamado **segurança de informações**. A segurança de informações foca no **valor das informações que devemos proteger** e não em como protegê-las. O diagrama a seguir mostra os elementos físicos e digitais que fazem parte da segurança de informações.



- **A segurança física** é a prática de proteger fisicamente ativos, como edifícios, câmeras de segurança, equipamentos e propriedades, contra ameaças físicas, como roubo, vandalismo, incêndios e desastres naturais.
- **A segurança cibernética** é a prática de proteger e recuperar redes, dispositivos e programas de qualquer tipo afetados por ataques cibernéticos maliciosos.
- Uma boa segurança integra essas duas coisas, trabalhando em conjunto para os mesmos objetivos.

EXEMPLO

Vamos pensar nisso pela perspectiva de um cliente. Imagine que você foi a uma empresa de viagens e compartilhou os detalhes de seu passaporte para reservar uma viagem ao exterior. E se um funcionário da empresa enviar acidentalmente por e-mail os detalhes de seu passaporte para a pessoa errada ou deixar papéis impressos com esses detalhes em uma pasta esquecida num trem? O resultado é o mesmo. Suas informações privadas foram comprometidas. Na segurança de informações, a **ênfase está no resultado,** em vez de no método exato utilizado.

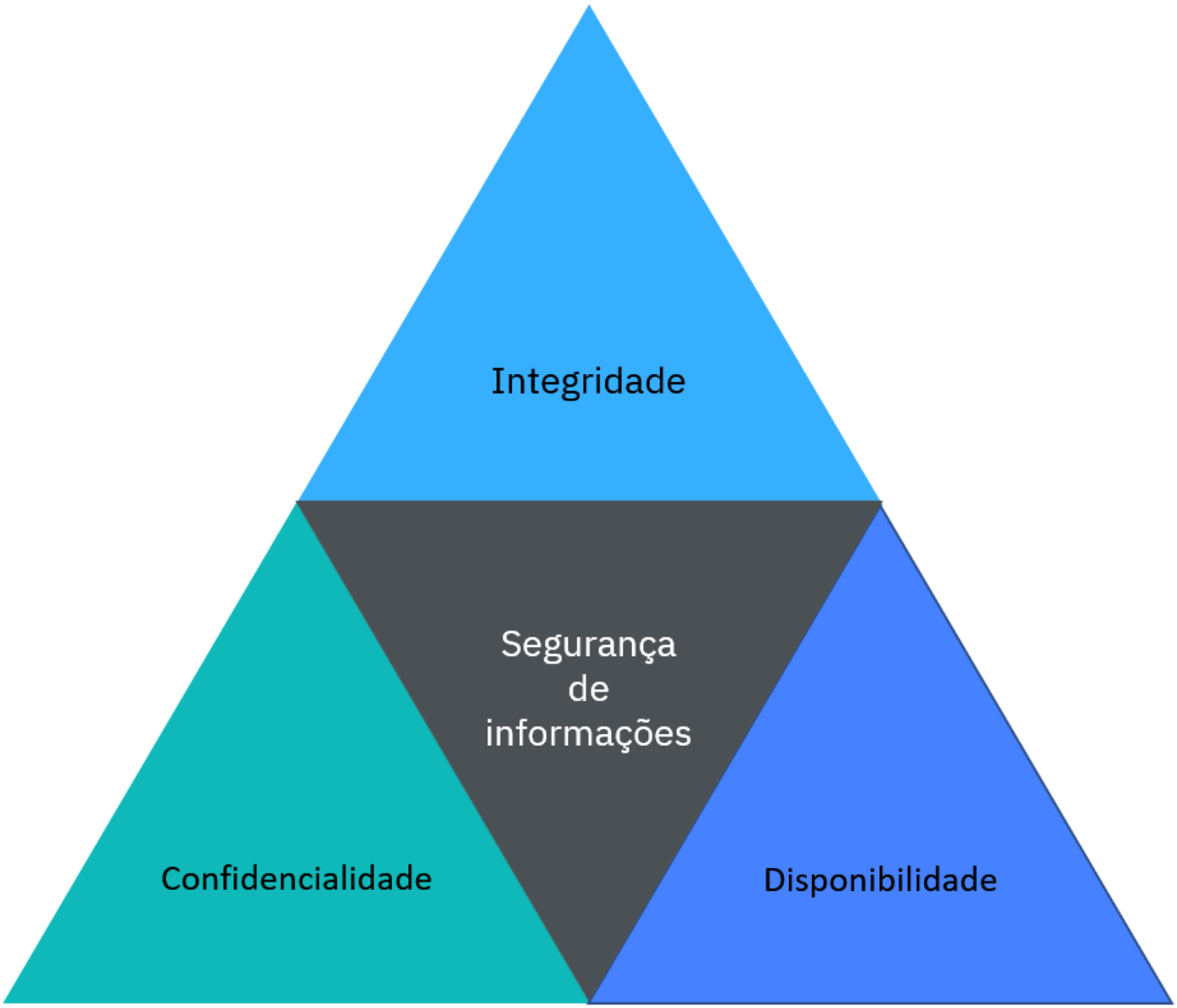
O que os profissionais da segurança cibernética estão tentando realizar?

De acordo com o **National Institute of Standards and Technology (NIST) (https://csrc.nist.gov/glossary/term/information_security)**, a **segurança de informações** é "a proteção das informações e dos sistemas de informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer confidencialidade, integridade e disponibilidade".

Portando, os **objetivos** da segurança de informações são frequentemente definidos com a **tríade CIA** como um bom ponto de partida. A CIA, do inglês, é um recurso mnemônico representando os seguintes objetivos: **confidencialidade ("C", de confidentiality)**, **integridade ("I", de integrity)** e **disponibilidade ("A", de availability)**.

Confidencialidade *Informações são privadas*	Confidencialidade significa impedir que essas informações caiam nas mãos de pessoas que não têm autorização para acessá-las.
Integridade *Informações não devem ser alteradas*	Integridade significa garantir que as informações permaneçam precisas e consistentes, garantindo que pessoas não autorizadas não possam fazer mudanças nelas.
Disponibilidade *Informações devem poder ser acessadas quando necessário*	Disponibilidade significa o acesso oportuno e confiável e o uso das informações quando necessário.

A tríade CIA é um modelo para ajudar a guiar políticas de segurança de informações dentro de uma empresa.



Diferentes empresas e cenários podem priorizar objetivos diferentes em relação a outros.

EXEMPLO

Vejamos alguns exemplos para contextualizar os objetivos da segurança de informações.

- **Confidencialidade** pode ser o objetivo mais importante para as agências de inteligência do governo. Pense no quanto elas se esforçam para manter as informações em sigilo, usando criptografias sob medida ou até mesmo maletas que afundariam, se jogadas na água, a fim de proteger o conteúdo interno.
- **Integridade** pode ser o objetivo mais importante para os bancos. Como quando USD 10 são gastos em uma pizza. Não existiria nenhuma preocupação com a confidencialidade desta transação. No entanto, se a transação for alterada e o preço mudar para USD 10.000, sérios problemas financeiros podem acontecer. Caso isso aconteça em escala com seu banco, ele poderá deixar de funcionar como resultado de uma perda de confiança.
- **Disponibilidade** pode ser o objetivo mais importante para um website. Como quando você tem um blog. Você não ficaria particularmente preocupado com a confidencialidade ou com um editor ajudando você a corrigir a ortografia. Você quer que ele esteja lá e esteja disponível a qualquer momento que você desejar atualizar e publicar algo.

Qual é a sua opinião?

Vejamos como os objetivos da segurança de informações podem se relacionar à sua vida cotidiana avaliando ativos que você provavelmente valoriza. Na segurança cibernética, um **ativo** é definido como algo que tem valor para o proprietário. Os ativos podem ser digitais, como um programa, ou físicos, como um servidor. Informações confidenciais, como bancos de dados, pesquisas ou registros, também podem ser chamadas de **ativos de informação**.

Considere sua conta bancária pessoal, sua biblioteca de fotos, sua conta de mídia social e seu telefone celular. **Como uma perda de confidencialidade, integridade e disponibilidade afetaria você em cada um desses ativos?** Use esta escala de 1 a 5 para digitar sua classificação nos campos fornecidos.

1) Consequência baixa: você não teria um impacto perceptível no dia a dia.

3) Consequência média: você teria um impacto secundário, que resultaria em algumas horas de tempo perdido.

5) Consequência alta: você teria um impacto gigantesco e que mudaria sua vida, podendo durar por meses ou anos.

O **maior valor** será calculado automaticamente para que seja possível comparar como você valoriza seus ativos e prioridades.

> EXEMPLO
>
> Já existe um exemplo sendo exibido para você: um comentário em um debate on-line. Nesse exemplo:
>
> - Uma perda de **confidencialidade** é considerada irritante, mas terá apenas um impacto secundário e a classificação correspondente à opção **2**.
> - Uma perda de **integridade** causada por outra pessoa editando o comentário pode causar uma discussão, o que levaria à perda de tempo fazendo atualizações. Portanto, a integridade recebe uma classificação correspondente à opção **3**.
> - Por fim, se o comentário on-line desaparecer completamente ou se tornar inacessível, praticamente não haverá impactos. Portanto, uma perda de **disponibilidade** receberá uma classificação correspondente à opção **1**.

Agora, usando o sistema de classificação acima, conclua suas avaliações.

	Confidencialidade	Integridade	Disponibilidade	Maior valor
Comentário em um debate on-line	2	3	1	**3**
Conta bancária				
Biblioteca de fotos				
Conta em mídia social				
Telefone celular				

Ao terminar, será possível ver que certos ativos são mais importantes para você do que outros. Eles devem

corresponder aos **Maiores valores** exibidos. Alguma de suas avaliações de valor surpreende você?

Do ponto de vista da segurança, é sensato priorizar suas proteções em relação aos ativos mais importantes para você. Por exemplo, a senha de seu gerenciador de senhas pode ter mais de 20 caracteres e ser mantida em sigilo, enquanto uma senha da rede Wi-Fi doméstica pode ocasionalmente ser compartilhada com amigos e familiares!

Na segurança cibernética, as empresas tomam essas decisões o tempo todo.

Elementos importantes da segurança cibernética

10 Minutos

Existem muitas maneiras de proteger ativos de informações e decidir a melhor abordagem é uma consideração importante em segurança cibernética.

> **EXEMPLO**
> Imagine ter um quadro de alto valor que precisa ser protegido. Uma opção seria contratar seguranças para ficarem ao lado do quadro e vigiá-lo constantemente. Outra opção pode ser exigir que todos os possíveis visitantes de seu quadro façam um depósito monetário ou busquem a confirmação do seguro. Por fim, é possível optar por um sistema de segurança com laser de detecção de movimento, câmeras de segurança e sensores de movimento para detectar pessoas desconhecidas. Cada uma dessas opções tem diversas vantagens e desvantagens. Como em todos os grandes filmes policiais, confiar em somente uma opção pode não ser suficiente.

Há três elementos principais de segurança cibernética a serem considerados:

Essas são as áreas que um invasor pode atacar e é nelas que as empresas devem concentrar seus esforços de segurança cibernética. Vamos examiná-las mais adiante nesta lição.

Pessoas

Por mais intuitivo que possa ser para um mercado altamente digital, as pessoas são a parte mais importante da segurança cibernética. Primeiramente, as pessoas são os usuários finais dos sistemas digitais e, em segundo lugar, elas geralmente são responsáveis pelo design e pela manutenção desses sistemas. A ação humana é, sem dúvida, a

principal causa de incidentes de segurança cibernética. Quando as empresas projetam um sistema seguro, elas devem fazer isso tendo as pessoas em mente.

Um exemplo comum desse erro é o caso de fadiga de alerta. Se as pessoas receberem muitas notificações ou alarmes, elas ficarão dessensibilizadas. Bons sistemas são desenvolvidos para antecipar e levar em consideração o comportamento humano.

Processo

No mundo dos negócios, a maioria das atividades segue um conjunto de etapas claramente definido. Esses processos podem ajudar na segurança cibernética, considerando a segurança em cada etapa, ou dificultar a segurança cibernética, sendo frustrantes para o usuário final.

Imagine um processo que leva o usuário a preencher uma pesquisa de 20 perguntas sempre que desejar denunciar atividades suspeitas. Muitos usuários, que poderiam contribuir com informações úteis, podem ser dissuadidos e desistir do processo.

Bons processos têm os seguintes atributos:

- Eles são **extremamente claros e fáceis**. Durante o processo, deve ser óbvio o que fazer em todas as etapas. Os processos não devem usar jargões desnecessários ou ser escritos de maneira ambígua.
- Eles são **acessíveis ou conhecidos**. Todos os usuários que poderiam vir a seguir um processo devem saber como acessá-lo. Um bom exemplo disso são as evacuações de incêndio em edifícios. A maioria das pessoas sabe onde estão os pontos de evacuação mais próximos devido a uma boa sinalização.
- Eles são **consistentes**. Os processos não devem contradizer uns aos outros, se possível. Se um processo tem muitas exceções ou desvios, aumenta a complexidade. Mais adiante no curso, aprenderemos sobre como os criminosos cibernéticos podem explorar isso durante seus ataques.

Tecnologia

A tecnologia é toda a infraestrutura subjacente.

Na segurança cibernética, isso geralmente abrange elementos como criptografia de dispositivo, defesas de perímetro de rede e tecnologias anti-malware.

Nos negócios, bons usos da tecnologia resolvem problemas sem criar novos para seus usuários.

Um exemplo de boa segurança técnica é o software de gerenciamento de dispositivos, que pode rastrear os status de correções de software e aplicar atualizações. Isso geralmente é uma ferramenta essencial para grandes empresas. Se isso for feito corretamente, a tecnologia não será invasiva e os usuários serão protegidos de maneira passiva. Se isso for mal feito, os usuários podem tentar desativar o software completamente. Esse mesmo exemplo aplica-se a usuários de dispositivos, como você.

A tabela a seguir mostra alguns avanços tecnológicos de segurança, suas desvantagens percebidas e algumas desvantagens de sua introdução da perspectiva do usuário.

Avanço tecnológico	Benefício de negócios	Desvantagem percebida	Respostas indesejadas do usuário
Gerenciamento automatizado de correções	Todo o software está atualizado	Interrupções no uso do dispositivo	O usuário não desliga os dispositivos

Avanço tecnológico	Benefício de negócios	Desvantagem percebida	Respostas indesejadas do usuário
Senhas obrigatórias de alta complexidade	Mais difícil para os invasores adivinharem senhas	Tedioso de usar	S3NH4!
As senhas obrigatórias expiram após 30 dias	As senhas não podem ser comprometidas por longos períodos de tempo	Previsivelmente repetitivo	SenhaJan para SenhaFev
E-mails criptografados	Os invasores não podem ler e-mails em movimento	Configuração e complexidade adicionais	Desativação do recurso de criptografia

É possível notar a importância, para as empresas, da educação dos usuários sobre por que exatamente a tecnologia foi introduzida e por que as desvantagens percebidas podem ser necessárias.

Qual é a sua opinião?

Reflita sobre as perguntas a seguir. Digite suas respostas nas caixas. Refletir e digitar uma resposta é uma boa maneira de processar seus pensamentos. Suas respostas serão visualizadas somente por você e serão salvas somente em seu curso. Certifique-se de clicar em **Salvar o texto**.

Pense em algum momento no qual você avaliou sua própria segurança digital pessoal para seu computador e/ou seus dispositivos.

1. Em termos de **pessoas**, você tentou se informar com o propósito de melhorar sua postura de segurança?

Salvar o texto Salvar o texto Salvar o texto Salvar o texto

2. Em termos de **processo**, você iniciou novos processos, como ativar a autenticação de dois fatores para cada login?

Salvar o texto

3. Em termos de **tecnologia**, você comprou ou usou uma nova tecnologia para ajudar a melhorar sua segurança

pessoal?

Salvar o texto

Agora tente aplicar o que você aprendeu nesta lição. Agora, tente aplicar o que você aprendeu nesta lição. Suas respostas são apenas para você e serão salvas neste curso apenas para seu acesso. Certifique-se de selecionar **Salvar texto** depois de terminar cada resposta.

Explique como cada elemento-chave da segurança cibernética se aplica aos exemplos a seguir.

Conta bancária on-line

Pessoas:

Salve o Texto Salve o Texto Salve o Texto Salve o Texto

Salve o Texto Salve o Texto Salve o Texto Salve o Texto

Salve o Texto

Processo:

Seu texto foi salvo. Clique em "X" para continuar. ✖

Tecnologia:

Seu texto foi salvo. Clique em "X" para continuar.

Notebook pessoal

Pessoas:

Seu texto foi salvo. Clique em "X" para continuar.

Processo:

Seu texto foi salvo. Clique em "X" para continuar.

Tecnologia:

Seu texto foi salvo. Clique em "X" para continuar.

Gestão de risco

10 Minutos

Os riscos fazem parte da vida cotidiana e são algo com o qual todos estamos instintivamente familiarizados. Um **risco** é a possibilidade de algo acontecer e ter uma consequência negativa. A gestão de riscos é um dos pontos mais importantes para a maioria das empresas e para muitos mercados, como o de seguros. Empresas sólidas entendem e gerenciam riscos de maneira eficaz, o que proporciona a elas uma vantagem competitiva.

Nesta lição, exploraremos alguns conceitos importantes sobre o risco e como ele se aplica à segurança cibernética.

Valorização de riscos

Os riscos não são todos igualmente importantes. Certos riscos podem exigir atenção urgente, enquanto outros podem ser ignorados. Riscos mais significativos são conhecidos como **riscos altos**. Essa é uma equação básica para calcular o valor de um risco:

Valor de risco = consequência x probabilidade

Consequência é o impacto e os danos associados.

Probabilidade é com que frequência o impacto do risco ocorre.

Idealmente, por razões matemáticas, seria ótimo se tivéssemos boas informações estatísticas para todos os riscos. Se, por exemplo, soubermos em um determinado ano que 1 em cada 10 carros terá um pneu furado, o valor do risco associado poderá ser facilmente calculado.

> **EXEMPLO**
>
> Um exemplo da equação do valor de risco aplicada ao cenário anterior de pneus furados pode ser o seguinte. Um indivíduo pode perder a produtividade de um dia como resultado de um pneu furado no caminho para o trabalho. A *consequência* desse risco seria a perda de um dia de trabalho. Embora essa consequência incomode, lembre-se, a *probabilidade* do risco é baixa: 1 em 10 carros em um ano. Isso significa que podemos avaliar o valor geral do risco como baixo.

Na segurança cibernética, é difícil medir diretamente a probabilidade devido à constante evolução da tecnologia e ao envolvimento de invasores externos. Como regra geral, a probabilidade de uma empresa ser atacada depende, em parte, dos três atributos a seguir:

Probabilidade = capacidade do adversário x motivação do adversário x severidade da vulnerabilidade

Um **adversário** é um termo geral usado para descrever uma entidade que deseja comprometer um sistema de informação. Mais adiante nesse curso, você aprenderá mais sobre como os adversários podem ser categorizados. Isso permitirá que você designe valores para seus recursos e motivações.

Vulnerabilidade são possíveis fraquezas em um sistema que podem ser exploradas para comprometê-lo. Por exemplo, uma vulnerabilidade pode ser uma página da web que não autentica um usuário corretamente.

EXEMPLO

Um exemplo dessa segunda equação pode ser o seguinte. Vamos imaginar que um banco esteja sendo alvo de uma gangue criminosa interessada em roubar detalhes e senhas de login bancário de usuários.

- O **recurso do adversário** pode ser avaliado como *médio* porque os criminosos poderiam usar uma variedade de ferramentas e desenvolver suas próprias ferramentas, se necessário.
- A **motivação** pode ser avaliada como *alta* porque eles poderiam tentar diversos ataques ao longo de um período de tempo.
- Uma **vulnerabilidade** pode ser avaliada como *alta* porque é relativamente fácil de explorar. Por exemplo, certas vulnerabilidades publicaram descrições on-line que permitem que os invasores espelhem ataques com facilidade.

Nota: o uso dos termos de classificação "baixo", "médio" e "alto" é um exemplo de análise qualitativa do risco. Em um mundo ideal, usaríamos números ou porcentagens exatas, no entanto, pode ser difícil encontrá-las. Portanto, as estimativas são muitas vezes tudo o que temos.

Resposta de risco

Depois que uma empresa avalia todos os seus riscos, a ênfase é colocada na gestão ou na resposta de risco. Em geral, existem quatro respostas a um risco que uma empresa pode escolher. A tabela a seguir as descreve.

Aceitar	A empresa aceita o risco em sua forma atual. Essa é uma decisão que será tomada por um indivíduo sênior da empresa, chamado de "proprietário do risco".
Reduzir	A empresa pode decidir que um risco é muito grande para ser aceito e tem como objetivo reduzi-lo de alguma forma. Isso pode acontecer através da redução da probabilidade ou consequência.
Transferir	A empresa pode querer que terceiros aceitem o risco, ou parte dele, em vez de aceitarem eles mesmos. Isso é feito via seguradora.
Rejeitar	A empresa pode decidir que um risco é muito alto e pode retirar-se para não ser afetada por ele. Isso terá impactos comerciais significativos, como desligar sites ou evitar mercados.

EXEMPLO

Vamos ilustrar essas quatro respostas a um risco. Imagine que você está pensando em iniciar um negócio de panificação em casa. Existe o risco de a sua cozinha ser danificada se o forno pegar fogo durante o processo de cozimento. Estas são diversas respostas para esse risco.

- **Aceitação**: é possível olhar para o risco e, com fé em suas capacidades na cozinha, concluir que é improvável que algo dê errado. Se o seu cozimento der errado, será possível consertar sua cozinha e você estará preparado para fazer isso.
- **Redução**: você decide que prefere que sua cozinha e forno não sejam colocados em um alto nível de risco e decide reduzir o risco. É possível reduzir a probabilidade de incidentes relacionados ao fogo instalando um detector de fumaça para fornecer um aviso prévio. É possível reduzir a consequência de um incêndio instalando um sistema anti-incêndio. Ambas as opções terão um custo pequeno, mas você acredita que elas valem a pena.
- **Transferência**: você vai à sua seguradora e faz upgrade de seu seguro para cobrir incêndios relacionados à comida caseira. Eles realizam a própria avaliação do risco. Juntos, vocês concordam em um custo a ser pago para cobrir o risco. Se sua cozinhe pegar fogo, eles cobrirão os custos. Esse acordo inicialmente incorre em um custo, mas limita sua responsabilidade.
-

> **Rejeição**: você decide que o risco de incêndio relacionado ao forno é muito alto. Seria possível mudar as receitas para fazer bolos sem usar um forno ou nem mesmo começar seu negócio.

Como é possível ver neste exemplo, há muitas coisas a considerar, mesmo em um exemplo simples. Empresas com tecnologia de TI em rápida mudança enfrentam muitos riscos em constante evolução. A gestão de risco é uma ocupação em tempo integral em muitas empresas e orienta muitas decisões estratégicas e táticas.

Apetite de risco

Um **apetite de risco** é o nível de risco que uma empresa está disposta a aceitar.

- Uma empresa terá um apetite de risco *alto* se estiver disposta a aceitar um alto nível de risco.
- Uma empresa terá um apetite de risco *baixo* se estiver disposta a aceitar um baixo nível de risco.

Qual é a sua opinião?

Reflita sobre esta pergunta e digite sua resposta na caixa. Refletir e digitar uma resposta é uma boa maneira de processar seus pensamentos. Sua resposta será visualizada somente por você e será salva somente em seu curso. Certifique-se de clicar em **Salvar o texto**.

Pense em um risco que você encontrou recentemente em sua vida.

Qual foi o risco e sua resposta? Você aceitou, reduziu, transferiu ou rejeitou esse risco?

Seu texto foi salvo. Clique no "X" para continuar. ✖

Agora tente aplicar o que você aprendeu nesta lição. Agora, tente aplicar o que você aprendeu nesta lição. Suas respostas são apenas para você e serão salvas neste curso apenas para seu acesso. Certifique-se de selecionar **Salvar texto** depois de terminar cada resposta.

Pense em um evento de vida que você experimentou que envolveu um risco de segurança cibernética. Alguns exemplos incluem abrir uma conta bancária, criar uma nova conta de mídia social ou configurar uma rede doméstica de internet.

Qual era o risco?

Seu texto foi salvo. Clique em "X" para continuar. ✖

Qual foi a sua resposta ao risco? Explique como você aceitou, reduziu, transferiu ou rejeitou o risco.

Seu texto foi salvo. Clique em "X" para continuar.

Equívocos comuns

5 Minutos

Existem muitos conceitos errados sobre segurança cibernética no mundo hoje. Eles variam de clichês irrealistas de Hollywood sobre o processo de ataque a um sistema de computador a estereótipos desatualizados de pessoas que trabalham no mercado. Vamos examinar alguns equívocos comuns e esclarecer algumas coisas.

Avalie cada conceito errado para desmistificá-lo.

Todo mundo que trabalha com segurança cibernética tem experiência em TI.

Embora a maioria dos cargos em segurança cibernética dependa parcial ou totalmente da TI, nem todos dependem absolutamente desse conhecimento. Você já deve ter notado que a segurança cibernética abrange muitas coisas e que há demanda por talentos em muitas áreas. As habilidades variam do gerenciamento e da comunicação com pessoas à matemática e à ciência de dados. Ter um conjunto diversificado de experiências e habilidades também ajuda as equipes a abordarem os problemas de novas maneiras e isso é muito valioso.

Todos os hackers são criminosos.

O termo hacker refere-se historicamente a alguém que gosta de adaptar as coisas e descobrir como elas funcionam. Essa definição se confundiu com pessoas que tentaram ilegalmente obter acesso a sistemas de computadores com a intenção de sequestrar suas operações. Hoje, existem milhares de hackers que trabalham em uma variedade de cargos de TI e contribuem para o entendimento dos sistemas de TI de maneira legal, como parte de muitas empresas. Sua curiosidade e motivação são inestimáveis para garantir que os sistemas de TI sejam construídos de maneira segura.

Não posso atuar em segurança cibernética.

Devido às áreas em constante evolução na segurança cibernética e ao amplo escopo, há lugar para todos. A diversidade de cargos requer uma grande diversidade de habilidades. Essas habilidades podem variar de análise estratégica e antecipação do cenário dos negócios de TI em evolução à vigilância e à paciência nos cargos de monitoramento de sistema. Lembre-se de que há muito aprendizado e treinamento disponíveis.

Sou muito velho ou muito jovem para trabalhar nesse mercado.

Um bom teste decisivo para a diversidade de uma equipe é verificar quantas décadas são cobertas pela composição da equipe. Uma boa equipe terá uma gama diversificada de experiências e visões de vida. A segurança cibernética precisa examinar os problemas com novas pessoas e com uma visão experiente. Se você acha que as abordagens são ótimas ou ruins, provavelmente, você tem metade da solução e uma ótima opinião para agregar ao diálogo.

Qual é a sua opinião?

Reflita sobre esta pergunta e digite sua resposta na caixa. Refletir e digitar uma resposta é uma boa maneira de processar seus pensamentos. Sua resposta será visualizada somente por você e será salva somente em seu curso. Certifique-se de clicar em **Salvar o texto**.

Até agora, qual suposição você tem sobre o mercado de segurança cibernética? Ao final do curso, é possível revisitar esta seção para ver se você ainda acredita nisso.

Seu texto foi salvo. Clique no "X" para continuar.

Leis e ética

10 Minutos

O crime cibernético é um conceito completamente novo, tendo se desenvolvido apenas nos últimos 30 anos. Antes disso, as pessoas que usavam computadores maliciosamente tinham de ser processadas usando uma combinação de atos de roubo e telegrafia, que não eram aplicáveis.

Hoje, um amplo conjunto de leis internacionais foi criado para governar o uso de tecnologias de computação e a proteção das informações que residem nelas. Todos são afetados por essas leis e é importante que todos os profissionais de segurança cibernética tenham uma compreensão básica delas.

Esta lição fornecerá uma rápida visão geral dos tipos comuns de leis e a importância de considerar a ética.

Nota importante

Leis não são as mesmas em todo o mundo. Elas podem variar bastante de acordo com o país. Deve-se verificar e cumprir as leis relevantes para o país de residência e/ou ao qual se viaja. Alguns governos desenvolveram leis mais proibitivas do que outros, portanto, uma ação legal em um pode ser ilegal em outro.

Em caso de dúvida, procure aconselhamento jurídico.

Tipos comuns de leis de uso indevido de computadores

Vamos revisar alguns recursos ou conceitos comuns refletidos em todo o mundo nas leis de uso indevido de computadores.

Uso ou controle não aprovado de um dispositivo de computador

- Muitas leis proíbem o acesso ou o uso não autorizado ou não aprovado de um dispositivo de computação.
- Essa barreira abrangente significa que o sequestro de computadores por meio de material técnico ou da imposição de acesso à conta de uma pessoa é banido.
- Essas leis podem se aplicar a pessoas que contornam controles quebrados, como a autenticação.

> EXEMPLO
> Colocar uma tela de login falsa em um website para roubar um conjunto de senhas de usuário e usá-las para espionar a conta de alguém.

Impedir o uso legítimo por outros

- Essas leis tentam cobrir ataques à disponibilidade de recursos de computador, como recursos de rede.
- Ações que degradam a qualidade do serviço para terceiros ou o impedem totalmente geralmente serão cobertas por essas leis.

EXEMPLO

Sobrecarregar um servidor ou comutador de rede enviando muitos pacotes de informações para processamento.

Ajudar outros criminosos ou projetar malware

- Essas leis se referem a ajudar outras pessoas a cometerem crimes de uso indevido de computador como cúmplice.
- Uma dessas maneiras de ajudar os outros pode ser criando um software malicioso, conhecido como malware.
- Essas leis devem ser usadas para ajudar a acabar com gangues criminosas.

EXEMPLO

Produzir um programa que permita acesso remoto a uma máquina sem o conhecimento do proprietário.

Além das leis relativas ao uso indevido de computadores, você descobrirá que alguns crimes cibernéticos se sobrepõem às leis de proteção de dados e às leis tradicionais de propriedade. Se um crime cibernético resultar em roubo de propriedade intelectual, isso poderá ser examinado como um caso de roubo.

A regra de ouro antes de tentar qualquer coisa na segurança de TI é obter as permissões corretas do proprietário antes de experimentar um dispositivo. Também é importante saber exatamente o que está sendo feito para evitar efeitos colaterais não intencionais.

Discussão sobre ética

Como as leis variam em todo o mundo, a ética também. Há um grande debate sobre muitos aspectos da ética na segurança cibernética. Por exemplo, é permitido que as empresas deixem arquivos de armadilha dentro de sua infraestrutura aguardando que um invasor os ative? Muitos poderiam argumentar que isso é eticamente válido, embora, sob a maioria das estruturas legais, seria discutido que tal ação é ilegal, uma vez que os arquivos seriam considerados malware. Além disso, há os dilemas éticos sobre o uso de técnicas do setor de segurança para atacar criminosos. Uma retaliação poderia ser justificável ou defensável? E as regras para ações militares ou governos?

É possível notar que existem dilemas éticos que existem desde o início do setor. Esses debates são um bom sinal de um mercado saudável atingindo sua maturidade e da integridade de seus participantes, que consideram essas questões importantes.

Para ilustrar a complexidade das leis e da ética da segurança cibernética, esse diagrama mostra como as áreas de legalidade e ética podem ser vistas como *sobrepostas*.

Atividade

Faça uma pesquisa rápida na Internet por leis de computadores em seu país. Existem leis sobre computadores a serem seguidas? Se sim, quais são elas?

Digite sua resposta na caixa. Sua resposta será visualizada somente por você e será salva somente em seu curso. Certifique-se de clicar em **Salvar o texto**.

Seu texto foi salvo. Clique no "X" para continuar. ✖

Faça uma pesquisa rápida na Internet sobre as leis de informática em seu país e, em seguida, liste e descreva algumas dessas leis. Quando terminar, lembre-se de selecionar Salvar texto.

Seu texto foi salvo. Clique em "X" para continuar. ✖

Preferências de Cookies