Bem-vindo

Quando era criança, alguma vez imaginou vir a ser um magistral defensor do universo — reconhecer uma ameaça, proteger os inocentes, procurar os malfeitores e levá-los à justiça?

Sabia que pode fazer disso uma carreira?

* Guru da cibersegurança
* Perito forense em cibersegurança
* Perito na segurança das informações
* Pirata informático com ética

Todos estas funções podem fazer parte do seu trabalho no emocionante, dinâmico e altamente exigente campo da cibersegurança.

A página de apoio ao aluno inclui uma ligação para a página de Facebook da NetAcad e para a nossa página no LinkedIn. Aí também encontra: [Recursos e atividades adicionais](https://static-course-assets.s3.amazonaws.com/CyberSec2/pp/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) para cada capítulo.

# Uma comunidade global

Ao participar na Networking Academy está a juntar-se a uma comunidade global ligada por objetivos e tecnologias comuns. Escolas, institutos, universidades e outras entidades em mais de 160 países participam no programa. Clique [aqui](https://www.youtube.com/watch?v=ajRgZaNLC1A) para ver um vídeo sobre como é que a Cisco Networking Academy está a mudar o mundo.

Procure a página oficial da Cisco Networking Academy no Facebook© e no LinkedIn©. No site Facebook, pode encontrar e interagir com outros alunos da Networking Academy de todo o mundo. No site da Cisco Networking Academy no LinkedIn pode encontrar anúncios de emprego e ver como é que os outros estão a comunicar as suas competências de forma eficaz.

# Mais do que apenas informação

O ambiente de aprendizagem da netacad.com é uma parte importante da experiência geral do curso para alunos e formadores na Networking Academy. Estes materiais de curso online incluem textos do curso e multimédia interativa relacionada, laboratórios em suporte de papel e muitos tipos diferentes de questionários. Todos estes materiais fornecem comentários importantes para o ajudar a avaliar os seus progressos ao longo do curso.

O material neste curso engloba um vasto leque de tecnologias que facilitam o modo como as pessoas trabalham, vivem, se divertem e aprendem através da comunicação por voz, vídeo e outros dados. A rede e a Internet afetam as pessoas de forma diferente em diferentes partes do mundo. Embora tenhamos trabalhado com instrutores de todo o mundo para criar estes materiais, é importante que trabalhe com o seu instrutor e com outros colegas alunos para que o material neste curso seja aplicável à situação no local onde se encontra.

# Método de ensino

O E-doing é uma filosofia do design baseada no princípio de que as pessoas aprendem melhor ao fazerem. O currículo inclui atividades de e-doing integradas e altamente interativas destinadas a ajudar a estimular a aprendizagem, aumentar a retenção do conhecimento e enriquecer a experiência como um todo – e isto facilita muito a compreensão do conteúdo.

Descrição geral do curso

O foco deste curso é explorar o campo da cibersegurança, como o seu nome indica. Neste curso irá fazer o seguinte:

* Aprender as noções básicas para se manter protegido online.
* Conhecer diferentes tipos de ataques e de software maligno e como é que as organizações se protegem a si próprias contra estes ataques.
* Explorar oportunidades de carreira na cibersegurança.

No final deste curso estará mais sensibilizado para a importância de se manter protegido online, as potenciais consequência dos ciberataques e possíveis oportunidades de carreira na cibersegurança.

# Capítulo 1: A necessidade de cibersegurança

Este capítulo explica o que é a cibersegurança e por que motivo a procura de profissionais de cibersegurança está em crescimento. Explica em que consiste a sua identidade e dados online, onde se encontram e por que motivo têm interesse para os cibercriminosos.

Este capítulo debate igualmente o que são dados organizacionais e por que têm de estar protegidos. Debate ainda quem são os ciberatacantes e o que pretendem. Os profissionais de cibersegurança têm de ter as mesmas competências que os ciberatacantes, mas têm de trabalhar dentro dos limites da legislação local, nacional e internacional. Os profissionais da cibersegurança também têm de utilizar as suas competências de forma ética.

Este capítulo também inclui conteúdo que explica resumidamente a ciberguerra e o motivo pelo qual os países e os governos necessitam de profissionais de cibersegurança para ajudar a proteger os cidadãos e as infraestruturas.

# O que é a Cibersegurança?

A rede de informações eletrónicas ligadas tornou-se parte integrante da vida quotidiana. Todos os tipos de organizações como, por exemplo, instituições médicas, financeiras e pedagógicas, recorrem a esta rede para trabalhar de forma eficaz. As organizações utilizam a rede através da recolha, do processamento, do armazenamento e da partilha de grandes quantidades de informação digital. À medida que é recolhida e partilhada mais informação digital, a proteção desta informação torna-se ainda mais vital para a segurança nacional e para a estabilidade económica.

A cibersegurança é o esforço contínuo para proteger estes sistemas em rede, e todos os dados contra o seu uso não autorizado ou que sejam danificados. A nível pessoal, é necessário proteger a sua identidade, os seus dados e os seus dispositivos informáticos. A nível empresarial, todos têm a responsabilidade de proteger a reputação, os dados e os clientes da organização. A nível estatal, estão em jogo a segurança nacional, a segurança dos cidadãos e o seu bem-esta

# A sua identidade online e offline

Quanto mais tempo é passado online, a sua identidade, tanto online como offline, pode afetar a sua vida. A sua identidade offline é a pessoa com quem os seus amigos e familiares interagem no dia a dia em casa, na escola ou no trabalho. Eles conhecem as suas informações pessoais, tais como o seu nome, a sua idade ou o local onde vive. A sua identidade online é quem você é no ciberespaço. A sua identidade online é a forma como você se apresenta aos outros online. Esta identidade online deve revelar apenas uma quantidade limitada de informações sobre si.

Deve ter cuidado ao escolher um nome de utilizador ou um alias para a sua identidade online. O nome de utilizador não deve incluir informações pessoais. Deve ser adequado e respeitoso. Este nome de utilizador não deverá fazer com que outras pessoas pensem que é um alvo fácil para cibercrimes ou atenção indesejada.

# Os seus dados

Quaisquer informações sobre si podem ser consideradas como dados a seu respeito. Estas informações pessoais podem identificá-lo de forma exclusiva como indivíduo. Estes dados incluem as fotografias e as mensagens que troca com familiares e amigos online. Outras informações, tais como o nome, número de segurança social, data e local de nascimento ou o nome de solteira da mãe, são informações conhecidas por si e utilizadas para identificá-lo. Informações médicas, académicas, financeiras e sobre a situação laboral também podem ser utilizadas para identificá-lo online.

**Registos médicos**

Sempre que consulta um médico, são adicionadas mais informações aos seus registos de saúde eletrónicos (RSEs). A receita prescrita pelo seu médico de família torna-se parte do seu RSE. O RSE inclui informações sobre a sua saúde física, mental e outras informações pessoais que podem não estar relacionadas com dados médicos. Por exemplo, se tiver recebido aconselhamento psicológico em criança numa altura em que ocorreram grandes mudanças na família, esta informação constará dos seus registos médicos. Além do seu historial médico e informações pessoais, o RSE também pode incluir informações sobre a sua família.

Dispositivos médicos, tais como pulseiras de fitness, utilizam a plataforma na cloud para permitir a transferência, o armazenamento online e a apresentação de dados como frequências cardíacas, pressões sanguíneas e glicémias. Estes dispositivos podem gerar uma vasta quantidade de dados clínicos que podem tornar-se parte dos seus registos médicos.

**Registos escolares**

À medida que avança no seu percurso académico, o seu registo escolar pode incluir informações acerca das suas notas e classificações de testes, assiduidade, cursos frequentados, prémios e obtenção de diplomas, a par de registos disciplinares. Este registo também pode incluir informações de contacto, registos de saúde e vacinação, bem como registos de educação especial, incluindo programas de educação individualizada (PEIs).

**Registos profissionais e financeiros**

O seu registo financeiro pode incluir informações sobre os seus rendimentos e despesas. Os registos fiscais podem incluir registos de pagamento de salários, extratos de cartões de crédito, a sua notação de crédito e outras informações bancárias. As suas informações de emprego podem incluir o seu emprego anterior e o desempenho.

# Onde estão os seus dados?

Todas estas informações são a seu respeito. Existem diversas leis que protegem a sua privacidade e dados no seu país. Mas sabe onde estão os seus dados?

Durante uma consulta, a conversa que tem com o médico é registada na sua ficha médica. Para efeitos de faturação, estas informações podem ser partilhadas com a seguradora para garantir uma faturação adequada e a qualidade. Agora, uma parte do seu registo médico relacionada com a consulta também estará na posse da seguradora.

Os cartões de fidelidade de lojas podem ser uma forma conveniente de poupar dinheiro nas suas compras. Contudo, a loja está a compilar um perfil das suas compras e irá utilizar essas informações para uso próprio. O perfil demonstra que um comprador compra regulamente uma determinada marca de dentífrico com um determinado sabor. A loja utiliza esta informação para dirigir ao comprador ofertas especiais do parceiro de marketing. Ao utilizar o cartão de fidelidade, a loja e o parceiro de marketing têm um perfil do comportamento de compras de um cliente.

Quando partilha fotografias online com os seus amigos, sabe quem pode ter uma cópia das fotografias? As cópias das fotografias encontram-se nos seus próprios dispositivos. Os seus amigos podem ter transferido cópias dessas fotografias para os respetivos dispositivos. Se as fotografias forem partilhadas publicamente, alguns estranhos também podem ter cópias das mesmas. Estes podem transferir ou efetuar capturas de ecrã dessas fotografias. Uma vez que as fotografias foram publicadas online, também estão guardadas em servidores localizados em várias partes do mundo. Agora, as fotografias já não se encontram apenas nos seus dispositivos informáticos.

# Os seus dispositivos informáticos

Os seus dispositivos informáticos não armazenam apenas os seus dados. Estes dispositivos tornaram-se agora num portal para os seus dados e geram informações a seu respeito.

A não ser que tenha optado por receber extratos em papel de todas as suas contas, utiliza os seus dispositivos computacionais para aceder aos dados. Se quiser uma cópia digital do extrato de cartão de crédito mais recente, utiliza os seus dispositivos computacionais para aceder ao Web site da entidade emissora do cartão de crédito. Se quiser pagar a sua fatura de cartão de crédito online, acede ao Web site do banco para transferir o montante através dos seus dispositivos computacionais. Além de lhe permitirem aceder às suas informações, os dispositivos informáticos também podem gerar informações a seu respeito.

Com todas estas informações a seu respeito disponíveis online, os seus dados pessoais tornaram-se lucrativos para os piratas informáticos.

# Eles querem o seu dinheiro

Se tiver alguma coisa de valor, os criminosos vão querê-la.

As suas credenciais online são valiosas. Estas credenciais permitem que os ladrões acedam às suas contas. Pode pensar que as milhas de passageiro frequente que obteve não são valiosas para os cibercriminosos. Pense novamente. Depois de cerca de 10 000 contas da American Airlines e da United Airlines terem sido pirateadas, os cibercriminosos reservaram voos e upgrades gratuitos através destas credenciais roubadas. Embora as companhias aéreas tenham devolvido as milhas de passageiro frequente aos clientes, isto demonstra o valor das credenciais de início de sessão. Um criminoso também pode tirar partido das suas relações. Pode aceder às suas contas e à sua reputação online para ludibriá-lo no sentido de transferir dinheiro para os seus amigos ou familiares. O criminoso pode enviar mensagens a indicar que os seus familiares ou amigos precisam que lhes transfira dinheiro para que possam regressar a casa do estrangeiro depois de terem perdido a carteira.

Ao tentarem ludibriá-lo para lhes entregar dinheiro, a imaginação dos criminosos não tem limites. Eles não lhe roubam apenas dinheiro: também podem roubar a sua identidade e arruinar a sua vida.

# Eles querem a sua identidade

Além de roubarem o seu dinheiro para proveito monetário a curto prazo, quando roubam a sua identidade, os criminosos pretendem obter lucros a longo prazo.

À semelhança das despesas médicas que são cada vez mais elevadas, o roubo de identidade médica também está a aumentar. Os ladrões de identidade podem roubar o seu seguro de saúde e utilizam os seus benefícios médicos para proveito próprio, e estes procedimentos médicos encontram-se agora nos seus registos médicos.

Os procedimentos de declaração anual de impostos podem variar de país para país, contudo, os cibercriminosos veem este período como uma oportunidade. Por exemplo, os cidadãos dos Estados Unidos têm de entregar a respetiva declaração até ao dia 15 de abril de cada ano. O Serviço da Receita Interna (IRS, Internal Revenue Service) não compara a declaração fiscal com as informações fornecidas pela entidade patronal antes do mês de julho. Um ladrão de identidade pode entregar uma declaração fiscal falsa e obter o reembolso. Os contribuintes legítimos irão aperceber-se da situação quando as respetivas declarações forem rejeitadas pelo IRS. Com a identidade roubada, podem ainda abrir contas de cartão de crédito e contrair dívidas em seu nome. Isto será prejudicial para a sua notação de crédito e dificultará a sua obtenção de empréstimos.

As credenciais pessoais também podem permitir o acesso a dados empresariais e governamentais.

# Tipos de dados organizacionais

**Dados tradicionais**

Os dados empresariais incluem informações pessoais, propriedades intelectuais e dados financeiros. As informações pessoais incluem materiais de candidatura, folhas de pagamento, cartas de oferta, contratos de trabalho e quaisquer informações utilizadas na tomada de decisões de emprego. A propriedade intelectual como, por exemplo, patentes, marcas comerciais e novos planos de produtos, permitem que uma empresa tenha vantagem económica sobre os seus concorrentes. Esta propriedade intelectual pode ser considerada um segredo comercial; a perda destas informações pode ser desastrosa para o futuro da empresa. Os dados financeiros, tais como declarações de rendimentos, balanços e demonstrações de fluxo de caixa dão uma perceção do estado da empresa.

**Internet of Things e Big Data**

Com o aparecimento da Internet of Things (IoT), existem muito mais dados para gerir, salvaguardar e proteger. A IoT é uma vasta rede de objetos físicos, tais como sensores e equipamento, que se estende muito além da rede informática tradicional. Todas estas ligações, mais o facto de termos expandido a capacidade e os serviços de armazenamento através da Cloud e da virtualização, conduzem ao crescimento exponencial dos dados. Estes dados deram origem a uma nova área de interesse na tecnologia e nos negócios, denominada “Big Data”. Com a velocidade, o volume e a variedade de dados gerados pela IoT e as operações de negócio diárias, a confidencialidade, a integridade e a disponibilidade destes dados é vital para a sobrevivência da organização.

# Confidencialidade, integridade e disponibilidade

Confidencialidade, integridade e disponibilidade, conhecidas como a tríade CID (Figura 1), é uma diretriz de segurança das informações para uma organização. A confidencialidade assegura a privacidade dos dados, restringindo o acesso através da criptografia e autenticação. A integridade assegura que a informação é precisa e confiável. A disponibilidade assegura que a informação seja acessível a pessoas autorizadas.

**Confidencialidade**

Outro termo para confidencialidade seria privacidade. As políticas das empresas devem restringir o acesso à informação a pessoal autorizado e assegurar que apenas tais indivíduos autorizados possam visualizar estes dados. Os dados podem ser compartimentados segundo o nível de segurança ou sensibilidade da informação. Por exemplo, um programador de Java não deve ter acesso à informação pessoal de todos os funcionários. Além disso, os funcionários devem receber formação no sentido de compreenderem as melhores práticas na proteção de informação sensível, a fim de se protegerem, tanto a si próprios como a empresa, contra ataques. Os métodos para garantir a confidencialidade incluem a criptografia de dados, ID de nome de utilizador e palavra-passe, autenticação de dois fatores e minimização da exposição de informações sensíveis.

**Integridade**

A integridade corresponde à precisão, consistência e confiabilidade dos dados durante o ciclo de vida completo dos mesmos. Os dados têm de permanecer inalterados durante o tráfego e não serem modificados por entidades não autorizadas. As permissões de ficheiros e o controlo de acesso de utilizadores podem impedir o acesso não autorizado. É possível utilizar o controlo de versão para impedir modificações acidentais por utilizadores autorizados. Têm de estar disponíveis cópias de segurança para restaurar quaisquer dados danificados e é possível utilizar hash de soma de controlo para verificar a integridade dos dados durante a transferência.

É utilizada uma soma de controlo para verificar a integridade de ficheiros ou de cadeias de carateres depois da transferência dos mesmos de um dispositivo para outro na sua rede local ou na Internet. As somas de controlo são calculadas com funções hash. Algumas somas de controlo comuns são MD5, SHA-1, SHA-256 e SHA-512. Uma função hash utiliza um algoritmo matemático para transformar os dados num valor de comprimento fixo que representa os dados, conforme representado na Figura 2. O valor do hash está presente apenas para comparação. A partir do valor do hash, não é possível obter diretamente os dados originais. Por exemplo, se se esquecer da sua palavra-passe, não é possível recuperá-la a partir do valor do hash. É necessário repor a palavra-passe.

Depois de transferir um ficheiro, pode verificar a integridade do mesmo verificando os valores do hash a partir da origem com o que gerou através de uma calculadora de hash. Ao comparar os valores do hash, pode assegurar que o ficheiro não foi adulterado ou danificado durante a transferência.

**Disponibilidade**

Ao realizar a manutenção do equipamento, reparações de hardware, a atualização dos sistemas operativos e do software e criar cópias de segurança garante a disponibilidade da rede e dos dados para os utilizadores autorizados. Devem ser previamente estabelecidos planos para uma rápida recuperação de desastres naturais ou provocados pelo homem. O equipamento ou software de segurança como, por exemplo, as firewalls, evita a ocorrência de tempos de indisponibilidade devido a ataques, tais como negação de serviço (DoS). A negação de serviço ocorre quando um ataque tenta sobrecarregar recursos de modo a que os serviços fiquem indisponíveis para os utilizadores.

# As consequências de uma falha de segurança

Não é possível proteger uma organização de todos os ciberataques possíveis, por vários motivos. As competências necessárias para configurar e manter a rede segura podem ser dispendiosas. Os atacantes continuarão sempre a encontrar novas formas de atingir as redes. Eventualmente, em algum momento, um ciberataque avançado e orientado será bem-sucedido. A prioridade será, então, a prontidão com que a sua equipa de segurança consegue responder ao ataque para minimizar a perda de dados, o tempo de indisponibilidade e a perda de receitas.

Agora, sabe que quaisquer dados publicados online podem permanecer online para sempre, mesmo que tenha conseguido apagar todas as cópias na sua posse. Se os seus servidores tiverem sido pirateados, as informações pessoais confidenciais podem ter sido tornadas públicas. Um pirata informático (ou um grupo de pirataria informática) pode vandalizar o Web site da empresa, publicando informações falsas, e arruinar a reputação da empresa que levou anos a construir. Os piratas informáticos também podem desativar o Web site da empresa, levando à perda de receitas da empresa. Se o Web site estiver desativado durante períodos de tempo mais longos, a empresa pode aparentar pouco fiável e, possivelmente, perder credibilidade. Se o Web site ou a rede da empresa tiver sofrido uma falha, pode ocorrer a divulgação de documentos confidenciais, a revelação segredos comerciais e o roubo de propriedade intelectual. A perda de todas estas informações pode impedir o crescimento e a expansão da empresa.

O custo monetário de uma falha vai muito além da substituição de quaisquer dispositivos perdidos ou roubados, do investimento na segurança existente e do reforço da segurança física do edifício. A empresa pode ter a responsabilidade de contactar todos os clientes afetados acerca da falha e pode ter de preparar-se para contencioso. Com toda esta incerteza, os funcionários podem optar por deixar a empresa. A empresa poderá ter de concentrar-se menos no crescimento e mais na reparação da sua reputação.

# Exemplo de falha de segurança 1

O gestor de palavras-passe online LastPass detetou atividade incomum na sua rede em julho de 2015. Constatou-se que diversos endereços de e-mail, lembretes de palavra-passe e hashes de autenticação tinham sido roubados por piratas informáticos. Felizmente para os utilizadores, os piratas informáticos não conseguiram obter os cofres de palavras-passe encriptados de nenhum utilizador.

Embora tenha ocorrido uma falha de segurança, o LastPass conseguiu, ainda assim, proteger as informações das contas dos utilizadores. O LastPass requer autenticação por verificação de e-mail ou autenticação multifator sempre que é efetuado um novo início de sessão a partir de um dispositivo ou de um endereço IP desconhecido. Os piratas informáticos também teriam de conhecer a palavra-passe principal para aceder à conta.

Os utilizadores do LastPass também têm alguma responsabilidade na proteção das suas próprias contas. Os utilizadores devem utilizar sempre palavras-passe principais complexas e alterá-las periodicamente. Os utilizadores devem ter sempre cuidado com ataques de phishing. Um exemplo de um ataque de phishing seria se um atacante enviasse e-mails falsos alegando pertencer à LastPass. Os e-mails solicitariam aos utilizadores que clicassem numa ligação incorporada e alterassem a palavra-passe. A ligação apontaria para uma versão fraudulenta do Web site, utilizada para roubar a palavra-passe principal. Os utilizadores nunca devem clicar nas ligações incorporadas num e-mail. Os utilizadores também devem ter cuidado com o respetivo lembrete de palavra-passe. O lembrete de palavra-passe não deve revelar as suas palavras-passe. Acima de tudo, os utilizadores devem ativar a autenticação multifatores sempre que esteja disponível em qualquer Web site que a disponibilize.

Se tanto os utilizadores como os fornecedores de serviços utilizarem as ferramentas e os procedimentos adequados para proteger as informações dos utilizadores, os dados dos utilizadores podem manter-se protegidos mesmo em caso de falha de segurança.

# Exemplo de falha de segurança 2

O fabricante de brinquedos de alta tecnologia para crianças, Vtech, sofreu uma falha de segurança na sua base de dados em novembro de 2015. Esta falha poderia afetar milhões de clientes em todo o mundo, incluindo crianças. A falha de dados expôs informações sensíveis, incluindo nomes de clientes, endereços de e-mail, palavras-passe, fotografias e registos de chat.

Um brinquedo tablet tinha-se tornado num novo alvo para os piratas informáticos. Os clientes tinham partilhado fotografias e utilizado as funcionalidades de chat através dos tablets de brincar. A informação não foi protegida adequadamente e o Web site da empresa não suportava a comunicação SSL segura. Embora a falha não tenha exposto quaisquer informações de cartão de crédito nem dados de identificação pessoal, a preocupação com o ato de pirataria informática foi de tal ordem que levou à suspensão da empresa da bolsa de valores.

A Vtech não protegeu devidamente as informações dos clientes e foi exposta durante a falha. Embora a empresa tenha informado os clientes que as respetivas palavras-passe tinham sido protegidas por hash, ainda era possível que os piratas informáticos as decifrassem. As palavras-passe na base de dados foram codificadas utilizando a função hash MD5, mas as perguntas e respostas de segurança estavam armazenadas em texto simples. Infelizmente, a função hash MD5 tem vulnerabilidades conhecidas. Os piratas informáticos podem determinar as palavras-passe originais ao compararem milhões de valores de hash pré-calculados.

Com as informações expostas nesta falha de dados, os cibercriminosos poderiam utilizá-las para criar contas de e-mail, solicitar créditos e cometer crimes antes de as crianças terem idade escolar. No caso dos pais destas crianças, os cibercriminosos poderiam apoderar-se das contas online porque muitas pessoas reutilizam as palavras-passe em diferentes Web sites e contas.

A falha de segurança não só teve impacto sobre a privacidade dos clientes como arruinou a reputação da empresa, conforme indicado pela própria empresa quando a sua presença na bolsa de valores foi suspensa.

Para os pais, é uma chamada de atenção para estarem mais atentos à privacidade online dos filhos e para exigirem uma melhor segurança dos produtos para crianças. Para os fabricantes de produtos ligados em rede, significa que têm de ser mais veementes na proteção dos dados e da privacidade dos clientes, agora e no futuro, à medida que o panorama dos ciberataques se desenvolve.

# Tipos de atacantes

Os atacantes são indivíduos ou grupos que tentam explorar vulnerabilidades para proveito pessoal ou financeiro. Os atacantes estão interessados em tudo, desde cartões de crédito a desenhos de produtos e qualquer bem de valor.

**Amadores** – Por vezes, estas pessoas designam-se por “miúdos dos scripts”. Normalmente, são atacantes com pouco ou nenhum conhecimento que, muitas vezes, utilizam ferramentas ou instruções encontradas na Internet para iniciar ataques. Alguns deles são apenas curiosos, enquanto outros tentam demonstrar os seus conhecimentos e provocar danos. Podem utilizar ferramentas básicas, mas os resultados podem, contudo, ser devastadores.

**Piratas informáticos** – Este grupo de atacantes invade computadores ou redes para obter acesso. Consoante a intenção da invasão, estes atacantes são classificados como bem intencionados, de intenção neutra ou mal intencionados. Os atacantes bem intencionados invadem redes ou sistemas informáticos para descobrir fraquezas, a fim de melhorar a segurança destes sistemas. Estas invasões são realizadas com autorização prévia e todos os resultados são comunicados ao proprietário. Por outro lado, os atacantes mal intencionados tiram partido de qualquer vulnerabilidade para proveito pessoal, financeiro ou político ilegal. Os atacantes de intenção neutra encontram-se entre os bem intencionados e os mal intencionados. Os atacantes de intenção neutra podem encontrar uma vulnerabilidade no sistema e comunicar essa vulnerabilidade aos proprietários do sistema, caso essa ação coincida com a sua agenda. Alguns piratas informáticos de intenção neutra publicam os factos relativos à -vulnerabilidade na Internet para que outros atacantes possam explorá-la.

A figura fornece detalhes sobre os termos pirata informático bem intencionado, mal intencionado e de intenção neutra.

**Piratas informáticos organizados** – Estes piratas informáticos incluem organizações de cibercriminosos, ativistas da pirataria informática, terroristas e piratas informáticos patrocinados pelo estado. Geralmente, os cibercriminosos são grupos de criminosos profissionais centrados no controlo, no poder e na riqueza. Os criminosos são altamente sofisticados e organizados e podem até fornecer o cibercrime como um serviço a outros criminosos. Os ativistas da pirataria informática fazem declarações políticas para sensibilizar para questões importantes para os mesmos. Os atacantes patrocinados pelo estado recolhem informações ou cometem atos de sabotagem em nome do respetivo governo. Geralmente, estes atacantes são altamente especializados e bem financiados, e os seus ataques centram-se em objetivos específicos vantajosos para o respetivo governo.

Clique [aqui](http://www.watchguard.com/tips-resources/hacker-profiles.asp) para ver representações pictóricas de perfis de piratas informáticos.

Ameaças internas e externas

**Ameaças à segurança interna**

Os ataques podem ter origem no interior ou no exterior de uma organização, conforme indicado na figura. Um utilizador interno como, por exemplo, um funcionário ou parceiro contratado, pode, de modo acidental ou intencional:

* Manusear dados confidenciais de forma incorreta
* Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede
* Facilitar ataques externos, ligando suportes de dados USB infetados ao sistema informático empresarial
* Convidar acidentalmente à entrada de software maligno na rede através de e-mails ou Web sites malignos

As ameaças internas também têm o potencial de provocar danos maiores do que as ameaças externas, porque os utilizadores internos têm acesso direto ao edifício e aos dispositivos da infraestrutura do mesmo. Os funcionários possuem igualmente conhecimentos sobre a rede empresarial, os respetivos recursos e dados confidenciais, bem como dos diferentes níveis de privilégios de utilizador ou administrativos.

**Ameaças à segurança externa**

Algumas ameaças externas de amadores ou atacantes especializados podem explorar vulnerabilidades em dispositivos de rede ou informáticos ou utilizar engenharia social para obter acesso.

# Questões jurídicas na cibersegurança

Os profissionais de cibersegurança têm que ter os mesmos conhecimentos que os piratas informáticos, especialmente os piratas informáticos mal intencionados, para realizarem a devida proteção contra ataques. Uma diferença entre um pirata informático e um profissional de cibersegurança consiste no facto de que o profissional de cibersegurança tem de trabalhar dentro dos limites da lei.

**Questões legais pessoais**

Não tem sequer de ser funcionário para estar sujeito às leis de cibersegurança. Na sua vida privada, pode ter a oportunidade e os conhecimentos para piratear o computador ou a rede de terceiros. Existe um velho ditado que sugere que, só porque podemos fazer algo, não significa que devemos fazê-lo. Tenha em mente este ditado. A maioria dos piratas informáticos deixa pistas, quer saibam quer não, e estas pistas podem conduzir até ao pirata informático.

Os profissionais de cibersegurança desenvolvem muitas competências que podem ser utilizadas para o bem ou para o mal. Os que utilizam as suas competências dentro do sistema legal, para proteger infraestruturas, redes e privacidade, são sempre bastantes solicitados.

**Questões legais empresariais**

Na maioria dos países estão em vigor algumas leis relativas à cibersegurança. Podem estar relacionadas com infraestruturas críticas, redes e privacidade empresarial e individual. As empresas estão obrigadas a cumprir estas leis.

Em alguns casos, se transgredir as leis sobre cibersegurança durante o seu trabalho, é a empresa que pode ser punida e pode perder o seu emprego. Noutros casos, pode ser processado, multado e, possivelmente, condenado.

Em geral, se não tiver a certeza se uma ação ou um comportamento possa ser ilegal, parta do princípio de que é ilegal e não a realize. A sua empresa pode ter um departamento jurídico ou um funcionário no departamento de recursos humanos que pode responder às suas questões antes de cometer qualquer ato ilegal.

**Lei e cibersegurança internacional**

A área da legislação sobre cibersegurança é muito mais recente do que a própria cibersegurança. Tal como mencionado anteriormente, a maioria dos países tem algumas leis em vigor e mais estarão para vir.

A legislação internacional sobre cibersegurança ainda é bastante recente. A Parceira Multilateral Internacional Contra Ciberameaças (International Multilateral Partnership Against Cyber Threats, IMPACT) é a primeira parceria público-privada internacional centrada nas ciberameaças. [A IMPACT](http://www.impact-alliance.org/home/index.html) é uma parceria entre governos, indústrias e instituições académicas de todo o mundo, dedicada a melhorar as capacidades globais ao lidar com ciberameaças. A figura representa o Web site da IMPACT

Questões éticas na cibersegurança

Além de trabalharem dentro dos limites da lei, os profissionais de cibersegurança também têm de demonstrar um comportamento ético.

**Questões éticas pessoais**

Uma pessoa pode agir de forma pouco ética e não ser sujeita a ação penal, multas ou pena de prisão porque, tecnicamente, a ação pode não ter sido ilegal. Contudo, isso não significa que o comportamento seja aceitável. Um comportamento ético é bastante fácil de determinar. É impossível enumerar todos os comportamentos pouco éticos que podem ser observados numa pessoa com conhecimentos de cibersegurança. Abaixo, encontram-se apenas dois. Pergunte-se o seguinte:

* Será que gostaria de descobrir que alguém invadiu o meu computador e alterou imagens nos meus sites de redes sociais?
* Será que gostaria de descobrir que um técnico de informática a quem confiei a reparação da minha rede revelou aos colegas algumas informações pessoais minhas que obteve ao trabalhar na minha rede?

Se a sua resposta a alguma destas perguntas foi “não”, não proceda dessa forma com terceiros.

**Questões éticas empresariais**

A ética são códigos de comportamento que, por vezes, são reforçados pela legislação. Na cibersegurança existem muitas áreas que não são abrangidas pela legislação. Isto significa que fazer algo que é tecnicamente legal pode, ainda assim, não ser o procedimento mais ético. Na medida em que várias áreas da cibersegurança não são (ou ainda não são) abrangidas pela legislação, muitas organizações profissionais de TI criaram códigos de ética para as pessoas do setor. Segue-se uma lista de três organizações com Códigos de Ética:

* O CyberSecurity Institute (CSI) publicou um código de ética que poderá ler [aqui](http://csisite.net/training/ethicsconduct.htm).
* A Information Systems Security Association (ISSA) tem um código de ética que poderá encontrar [aqui](http://www.issa.org/?page=CodeofEthics).
* A Association of Information Technology Professionals (AITP) tem um código de ética e uma norma de conduta que poderá encontrar [aqui](http://www.aitp.org/?page=EthicsConduct).

A Cisco possui uma equipa que se dedica exclusivamente à conduta comercial ética. Aceda [aqui](http://csr.cisco.com/pages/governance-and-ethics) para ler mais acerca desta conduta. Este [site](http://investor.cisco.com/investor-relations/governance/code-of-conduct/default.aspx) contém um e-book sobre o Código de Conduta Comercial da Cisco, bem como um ficheiro .pdf. Em ambos os ficheiros, encontra-se uma “Árvore de Decisões Éticas”, conforme indicado na figura. Mesmo que não trabalhe para a Cisco, as perguntas e respostas que se encontram nesta árvore de decisões podem aplicar-se facilmente ao seu local de trabalho. De um ponto de vista legal, em geral, se não tiver a certeza se uma ação ou um comportamento possa ser ilegal, parta do princípio de que é ilegal e não a realize. No departamento de recursos humanos ou no departamento jurídico da sua empresa, alguém poderá esclarecer a sua situação antes de realizar qualquer procedimento que seria considerado pouco ético.

Pesquise online para encontrar outras organizações relacionadas com TI com códigos de ética. Tente determinar o que todas têm em comum.

# O que é a ciberguerra?

O ciberespaço tornou-se noutra dimensão importante da guerra, na qual os países podem travar conflitos sem os combates tradicionais com tropas e máquinas. Isto permite que os países com presença militar mínima sejam tão fortes como outros países no ciberespaço. A ciberguerra é um conflito baseado na Internet que envolve a penetração nos sistemas informáticos e nas redes de outros países. Estes atacantes têm os recursos e os conhecimentos para iniciarem ataques maciços baseados na Internet contra outros países para provocarem danos ou perturbarem serviços como, por exemplo, desativarem uma rede elétrica.

Um exemplo de um ataque patrocinado pelo estado envolveu o software maligno Stuxnet que foi concebido para danificar a central de enriquecimento nuclear do Irão. O software maligno Stuxnet não pirateou computadores específicos para roubar informações. Foi concebido para danificar equipamento físico que era controlado por computadores. Recorreu a codificação modular que foi programada para realizar uma tarefa específica dentro do software maligno. Utilizou certificados digitais roubados de modo a que o ataque parecesse legítimo para o sistema. Clique em Play (Reproduzir) para ver um vídeo sobre o Stuxnet.

Clique [aqui](https://static-course-assets.s3.amazonaws.com/CyberSec2/pp/course/files/1.4.1.1%20Video%20-%20Breaking%20Down%20Stuxnet.pdf) para ler a transcrição deste vídeo.

Clique [aqui](https://vimeo.com/25118844) para ver outro vídeo para saber mais sobre o Stuxnet.

# A finalidade da ciberguerra

A principal finalidade da ciberguerra consiste em obter uma vantagem sobre os adversários, quer sejam países ou concorrentes.

Um país pode invadir continuamente a infraestrutura de outro país, roubar segredos de defesa e recolher informações sobre tecnologia para reduzir o desfasamento nas suas indústrias e poder militar. Além da espionagem industrial e militar, a ciberguerra pode envolver a sabotagem da infraestrutura de outros países e custar vidas nos países atingidos. Por exemplo, um ataque pode perturbar a rede elétrica de uma grande cidade. O trânsito sofreria perturbações. A troca de bens e serviços é interrompida. Os doentes não podem receber os cuidados necessários em situações de emergência. O acesso à Internet também pode sofrer perturbações. Ao afetar a rede elétrica, o ataque pode afetar a vida quotidiana dos cidadãos comuns.

Além disso, os dados sensíveis comprometidos podem dar aos atacantes a possibilidade de chantagem a funcionários governamentais. As informações podem permitir que um atacante se faça passar por um utilizador autorizado para aceder a informações ou equipamentos sensíveis.

Se o governo não se conseguir defender contra os ciberataques, os cidadãos podem perder a confiança na capacidade que o governo tem de protegê-los. A ciberguerra pode desestabilizar um país, perturbar o comércio e afetar a confiança dos cidadãos no governo, sem nunca ocorrer qualquer invasão física ao país atingido.

# Capítulo 1: A necessidade de cibersegurança

Neste capítulo, explicou-se as funcionalidades e as características da cibersegurança. Explicou-se o motivo pelo qual a procura de profissionais de cibersegurança continuará a aumentar. O conteúdo explica por que motivo a sua identidade e os seus dados pessoais online são vulneráveis aos cibercriminosos. São dadas algumas sugestões sobre a forma como pode proteger a sua identidade e os seus dados pessoais online.

Este capítulo debateu igualmente os dados organizacionais: o que são, onde estão e por que têm de estar protegidos. Explicou quem são os ciberatacantes e o que pretendem. Os profissionais de cibersegurança têm de ter as mesmas competências que os ciberatacantes. Os profissionais de cibersegurança têm de trabalhar dentro dos limites da lei local, nacional e internacional. Os profissionais da cibersegurança também têm de utilizar as suas competências de forma ética.

Por último, este capítulo explicou brevemente a ciberguerra e o motivo pelo qual os países e os governos necessitam de profissionais de cibersegurança para ajudar a proteger os cidadãos e as infraestruturas.

Se quiser continuar a explorar os conceitos apresentados neste capítulo, consulte a página [Recursos e atividades adicionais](https://static-course-assets.s3.amazonaws.com/CyberSec2/pp/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) nos Recursos do aluno.

# Capítulo 2: Ataques, conceitos e técnicas

Este capítulo aborda as formas como os profissionais de cibersegurança analisam o que aconteceu após um ciberataque. Explica as vulnerabilidades do hardware e do software de segurança, bem como as diversas categorias de vulnerabilidades de segurança.

São debatidos os diferentes tipos de software maligno (conhecido como malware) e os sintomas de malware. São abordadas as diversas formas pelas quais os atacantes podem infiltrar-se num sistema, bem como os ataques de negação de serviço.

Os ciberataques modernos são, na sua maioria, considerados ataques mistos. Os ataques mistos utilizam várias técnicas de infiltração e ataque a um sistema. Quando não é possível impedir um ataque, é da responsabilidade de um profissional de cibersegurança reduzir o impacto desse ataque.

# Encontrar vulnerabilidades de segurança

Vulnerabilidades de segurança são qualquer tipo de defeito de software ou de hardware. Depois de tomarem conhecimento de uma vulnerabilidade, os utilizadores mal intencionados tentam explorá-la. Um *exploit (exploração)* é o termo utilizado para descrever um programa escrito para tirar partido de uma vulnerabilidade conhecida. O ato de utilizar um exploit contra uma vulnerabilidade designa-se por ataque. O ataque tem como objetivo a obtenção de acesso a um sistema, aos dados que aloja ou a um recurso específico.

**Vulnerabilidades de software**

As vulnerabilidades de software são normalmente introduzidas por erros no sistema operativo ou no código de uma aplicação e, apesar de todos os esforços que as empresas realizam para encontrar e corrigir vulnerabilidades de software, é comum surgirem novas vulnerabilidades. A Microsoft, a Apple e outros produtores de sistemas operativos lançam patches e atualizações quase todos os dias. As atualizações de aplicações são igualmente comuns. Aplicações como browsers, aplicações móveis e servidores Web são frequentemente atualizados pelas empresas ou organizações responsáveis pelos mesmos.

Em 2015, foi descoberta uma grande vulnerabilidade denominada SYNful Knock no Cisco IOS. Esta vulnerabilidade permitiu aos atacantes obterem o controlo de routers de nível empresarial, tais como os routers descontinuados Cisco 1841, 2811 e 3825. Os atacantes conseguiram, assim, monitorizar toda a comunicação de rede e infetar outros dispositivos de rede. Esta vulnerabilidade foi introduzida no sistema quando foi instalada uma versão alterada do IOS nos routers. Para evitar este tipo de situações, verifique sempre a integridade da imagem do IOS transferida e limite o acesso físico do equipamento apenas a pessoal autorizado.

As atualizações de software têm o objetivo de manterem os sistemas atualizados e evitar a exploração de vulnerabilidades. Embora muitas empresas tenham equipas de teste de penetração que se dedicam a pesquisar, encontrar e corrigir vulnerabilidades de software antes que possam ser exploradas, alguns investigadores de segurança de terceiros também são especializados em encontrar vulnerabilidades em software.

O Project Zero da Google é um excelente exemplo dessa prática. Após a descoberta de diversas vulnerabilidades em vários softwares utilizados por utilizadores finais, a Google formou uma equipa permanente dedicada a encontrar vulnerabilidades de software. Poderá encontrar a Google Security Research [aqui](https://code.google.com/p/google-security-research/issues/list?can=1).

**Vulnerabilidades de hardware**

Muitas vezes, as vulnerabilidades de hardware são introduzidas por defeitos na conceção, i.e., no design do hardware. A memória RAM, por exemplo, é constituída por condensadores instalados muito próximos uns dos outros. Descobriu-se que, devido à proximidade, a aplicação de alterações constantes a um destes condensadores pode influenciar os condensadores adjacentes. Com base nesse defeito de design, foi criado um exploit denominado Rowhammer. Ao reescrever repetidamente a memória nos mesmos endereços, o exploit Rowhammer permite a obtenção de dados de células de memória de endereços próximos, mesmo que as células estejam protegidas.

As vulnerabilidades de hardware são específicas de modelos de dispositivo e, normalmente, não são exploradas através de tentativas aleatórias de comprometimento. Embora os exploits de hardware sejam mais comuns em ataques altamente direcionados, a proteção contra malware tradicional e uma segurança física são a proteção suficiente para o utilizador comum.

# Categorização de vulnerabilidades de segurança

A maioria das vulnerabilidades de segurança de software enquadra-se numa das seguintes categorias:

**Capacidade da memória intermédia excedida –** Esta vulnerabilidade ocorre quando são escritos dados além dos limites de uma memória intermédia. As memórias intermédias são áreas da memória atribuídas a uma aplicação. Ao alterar dados para além dos limites de uma memória intermédia, a aplicação acede a memória atribuída a outros processos. Tal pode levar a uma falha do sistema, ao comprometimento de dados ou disponibilizar escalamento de privilégios.

**Entrada não validada –** Os programas trabalham frequentemente com entrada de dados. Estes dados que entram no programa podem incluir conteúdo maligno, concebido para forçar o programa a comportar-se de forma indesejada. Considere um programa que recebe uma imagem para processamento. Um utilizador mal intencionado pode criar um ficheiro de imagem com dimensões de imagem inválidas. As dimensões criadas de forma mal intencionada podem forçar o programa a atribuir memórias intermédias de tamanhos incorretos e inesperados.

**Condições de corrida –** Esta vulnerabilidade ocorre quando a saída de um evento depende de saídas ordenadas ou temporizadas. Uma condição de corrida torna-se uma fonte de vulnerabilidade quando os eventos ordenados ou temporizados não ocorrem pela ordem ou dentro da temporização correta.

**Fraquezas em práticas de segurança –**Os sistemas e dados sensíveis podem ser protegidos por técnicas como a autenticação, autorização e criptografia. Os programadores não devem tentar criar os seus próprios algoritmos de segurança, pois é provável que estes introduzam vulnerabilidades. Aconselha-se vivamente que os programadores utilizem bibliotecas de segurança que já tenham sido criadas, testadas e verificadas.

**Problemas de controlo de acesso –**O controlo de acesso é o processo que controla a ação de cada elemento e vai desde a gestão do acesso físico a equipamento à indicação de quem tem acesso a um recurso como, por exemplo, um ficheiro, e o que é possível fazer com o mesmo, como ler ou alterar o ficheiro. Muitas vulnerabilidades de segurança são criadas pelo uso indevido de controlos de acesso.

Quase todos os controlos de acesso e práticas de segurança podem ser ultrapassados se o atacante tiver acesso físico ao equipamento alvo. Por exemplo, independentemente das permissões que definir para um ficheiro, o sistema operativo não pode impedir que uma pessoa contorne o sistema operativo e leia os dados diretamente do disco. Para proteger o computador e os dados que contém, é necessário restringir o acesso físico e utilizar técnicas de criptografia para proteger contra roubo ou corrupção de dados.

# Tipos de software maligno

O software maligno, ou malware, é qualquer código que possa ser utilizado para roubar dados, contornar controlos de acesso, provocar danos ou comprometer um sistema. Seguem-se alguns tipos comuns de software maligno:

**Spyware –** Este software maligno é concebido para monitorizar e espiar o utilizador. O spyware inclui frequentemente monitores de atividade, registo do que é digitado e captura de dados. Numa tentativa de ultrapassar medidas de segurança, o spyware modifica muitas vezes as definições de segurança. Frequentemente, o spyware vem incluído em software legítimo ou inclui trojans.

**Adware –** O software suportado por publicidade é concebido para apresentar automaticamente anúncios. Muitas vezes, é instalado adware com algumas versões de software. Algum adware é concebido apenas para apresentar anúncios, mas também é comum conter spyware.

**Bot –**Derivado da palavra “robot”, um bot é software maligno concebido para realizar automaticamente uma ação, geralmente online. Embora a maioria dos bots seja inofensiva, uma utilização crescente dos mesmos são os botnets. Muitos computadores são infetados com bots programados para esperar silenciosamente por comandos fornecidos pelo atacante.

**Ransomware –**Este software maligno é concebido para manter cativo um sistema informático ou os dados que contém, até que seja realizado um pagamento (de um resgate). Normalmente, o ransomware funciona cifrando (encriptando) dados no computador com uma chave desconhecida pelo utilizador. Outras versões de ransomware podem tirar partido de vulnerabilidades específicas do sistema para bloquear o sistema. O ransomware é propagado através de um ficheiro descarregado ou de alguma vulnerabilidade de software.

**Scareware –**Este tipo de software maligno é concebido para persuadir o utilizador a realizar uma ação específica com base no medo. O scareware imita janelas de pop-up que se assemelham a janelas de caixa de diálogo do sistema operativo. Estas janelas apresentam mensagens falsificadas que indicam que o sistema está em risco ou que requer a execução de um programa específico para regressar ao funcionamento normal. Na realidade, não foram avaliados nem detetados quaisquer problemas e, se o utilizador concordar e autorizar a execução do programa indicado, o sistema será infetado com software maligno.

**Rootkit –** Este software maligno é concebido para modificar o sistema operativo a fim de criar uma backdoor. Os atacantes utilizam a backdoor para aceder remotamente ao computador. A maioria dos rootkits tira partido de vulnerabilidades de software para realizar o escalamento de privilégios e modificar ficheiros do sistema. Também é comum que os rootkits modifiquem elementos forenses e ferramentas de monitorização do sistema, tornando-os muito difíceis de detetar. Muitas vezes, um computador infetado por um rootkit tem de ser totalmente limpo e reinstalado.

**Vírus –**Um vírus consiste num código executável maligno que é anexado a outros ficheiros executáveis, muitas vezes, a programas legítimos. A maioria dos vírus requer ativação pelo utilizador final e pode ser ativado a uma hora ou data específica. Os vírus podem ser inofensivos e apresentar apenas uma imagem ou podem ser destrutivos, tais como os que modificam ou eliminam dados. Os vírus também podem ser programados para gerar mutações, a fim de evitar a deteção. Atualmente, a maioria dos vírus é propagada através de memórias USB, discos óticos, partilhas de rede ou e-mail.

**Trojan –**Um trojan, ou cavalo de troia, consiste em software maligno que realiza operações malignas sob a aparência de uma operação pretendida. Este código malicioso explora os privilégios do utilizador que o executa. Muitas vezes, os trojans encontram-se em ficheiros de imagem, ficheiros de vídeo ou jogos. Um trojan difere de um vírus na medida em que se une a ficheiros não executáveis.

**Worms –**Worms são códigos maliciosos que se replicam, explorando vulnerabilidades em redes de modo independente. Geralmente, os worms tornam as redes lentas. Enquanto um vírus requer a execução de um programa host (hospedeiro), os worms podem ser executados de forma independente. Após a infeção inicial, já não requerem a participação do utilizador. Uma vez infetado um host, o worm consegue propagar-se muito rapidamente por toda a rede. Os worms partilham padrões semelhantes. Todos possuem uma vulnerabilidade de ativação, uma forma de se propagarem e todos contêm um payload.

Os worms são responsáveis por alguns dos ataques mais devastadores na Internet. Conforme indicado na Figura 1, em 2001, o worm Code Red infetou 658 servidores. No período de 19 horas, o worm havia infetado mais de 300 000 servidores, conforme indicado na Figura 2.

**Man-In-The-Middle (MitM) –**O MitM permite que o atacante assuma o controlo de um dispositivo sem conhecimento do utilizador. Com esse nível de acesso, o atacante pode intercetar e capturar informações do utilizador antes de serem enviadas para o destino pretendido. Os ataques MitM são amplamente utilizados para roubar informações financeiras. Existem muitos softwares malignos e técnicas que disponibilizam funcionalidades de MitM aos atacantes.

**Man-In-The-Mobile (MitMo) –**Uma variante de man-in-the-middle, MitMo é um tipo de ataque utilizado para assumir o controlo de um dispositivo móvel. Uma vez infetado, o dispositivo móvel pode ser instruído para extrair informações sensíveis do utilizador e enviá-las aos atacantes. ZeuS, um exemplo de exploit com funcionalidades de MitMo, permite que os atacantes capturem silenciosamente mensagens SMS de verificação em 2 passos enviadas aos utilizadores.

Sintomas de software maligno

Independentemente do tipo de software maligno com que um sistema tenha sido infetado, estes são sintomas comuns de software maligno:

* Ocorre um aumento da utilização da CPU.
* Ocorre uma redução da velocidade do computador.
* O computador congela ou fica bloqueado frequentemente.
* Ocorre uma redução da velocidade de navegação na Internet.
* Existem problemas inexplicáveis com ligações de rede.
* Ocorre a modificação de ficheiros.
* Ocorre a eliminação de ficheiros.
* Estão presentes ficheiros, programas ou ícones do ambiente de trabalho desconhecidos.
* Existem programas desconhecidos em execução.
* Alguns programas desligam-se ou reconfiguram-se automaticamente.
* São enviados e-mails sem conhecimento ou autorização do utilizador.

Engenharia social

A engenharia social é um ataque de acesso que tenta manipular indivíduos para realizarem ações ou divulgarem informações confidenciais. Muitas vezes, os engenheiros sociais baseiam-se na vontade que as pessoas têm de ajudar, mas também tiram partido das suas fraquezas. Por exemplo, um atacante pode contactar um funcionário autorizado relativamente a um problema urgente que requer o acesso imediato à rede. O atacante pode apelar ao orgulho do funcionário, invocar autoridade utilizando técnicas de citação de nomes ou apelar à cobiça do funcionário.

Seguem-se alguns tipos de ataques de engenharia social:

* **Pretexting** – Ocorre quando um atacante contacta um indivíduo e lhe mente no sentido de obter acesso a dados privilegiados. Um exemplo envolve um atacante que finge necessitar de dados pessoais ou financeiros para confirmar a identidade do destinatário.
* **Tailgating** – Ocorre quando um atacante segue rapidamente uma pessoa autorizada para uma localização segura.
* **Troca por troca (Quid pro quo)** – Ocorre quando um atacante solicita informações pessoais a uma entidade em troca de algo como, por exemplo, uma oferta.

# Decifração da palavra-passe de Wi-Fi

A decifração da palavra-passe de Wi-Fi é o processo de descoberta da palavra-passe utilizada para proteger uma rede sem fios. Eis algumas técnicas utilizadas na decifração de palavras-passe:

**Engenharia social** – O atacante manipula uma pessoa que conhece a palavra-passe no sentido de a divulgar.

**Ataques de força bruta** – O atacante experimenta várias palavras-passe possíveis numa tentativa de adivinhar a palavra-passe. Se a palavra-passe for um número de 4 algarismos, o atacante terá de experimentar cada uma das 10 000 combinações. Geralmente, os ataques de força bruta envolvem um ficheiro de lista de palavras. Trata-se de um ficheiro de texto que contém uma lista de palavras retiradas de um dicionário. Um programa experimenta então cada palavra e combinações comuns. Na medida em que os ataques de força bruta são demorados, as palavras-passe complexas demoram muito mais tempo a adivinhar. Algumas ferramentas de força bruta para palavras-passe incluem o Ophcrack, L0phtCrack, THC Hydra, RainbowCrack e Medusa.

**Interceção de rede –**Ao escutar e capturar pacotes enviados na rede, um atacante pode conseguir descobrir a palavra-passe se esta for enviada sem criptografia (em texto simples). Se a palavra-passe estiver cifrada, o atacante pode, ainda assim, conseguir revelá-la através de uma ferramenta de decifração de palavras-passe.

# Phishing

O phishing ocorre quando uma entidade maliciosa envia um e-mail fraudulento pretendendo ser originário de uma fonte legítima e fiável. A mensagem tem a intenção de ludibriar o destinatário a fim de instalar software maligno no dispositivo ou partilhar informações pessoais ou financeiras. Um exemplo de phishing é um e-mail forjado para parecer ter sido enviado por uma loja, no qual se pede ao utilizador para clicar numa ligação para reclamar um prémio. A ligação pode apontar para um site falso onde são solicitadas informações pessoais ou pode instalar um vírus.

Spear phishing é um ataque de phishing altamente direcionado. Embora tanto o phishing como o spear phishing utilizem e-mails para chegar às vítimas, os e-mails de spear phishing são personalizados para um indivíduo específico. O atacante pesquisa os interesses do alvo antes de enviar o e-mail. Por exemplo, um atacante descobre que o alvo tem interesse em automóveis e que está a pensar comprar um modelo de automóvel específico. O atacante inscreve-se no mesmo fórum de discussão sobre automóveis de que o alvo é membro, falsifica uma oferta para venda de um automóvel e envia um e-mail ao alvo. O e-mail contém uma ligação para fotografias do automóvel. Quando o alvo clica na ligação, é instalado software maligno no computador do alvo.

# Exploração de vulnerabilidades

A exploração de vulnerabilidades é outro método de infiltração comum. Os atacantes irão analisar os computadores para obterem informações acerca dos mesmos. Segue-se um método comum de exploração de vulnerabilidades:

**Passo 1**. Recolha de informações sobre o sistema alvo. Este procedimento pode ser realizado de várias formas, tais como um analisador de portas ou engenharia social. O objetivo é obter o máximo de informações possível sobre o computador alvo.

**Passo 2**. Uma das informações relevantes obtidas no passo 1 pode ser o sistema operativo, a respetiva versão e uma lista de serviços em execução.

**Passo 3**. Quando o sistema operativo e a versão do alvo já são conhecidos, o atacante procura quaisquer vulnerabilidades conhecidas dessas versão do SO ou de outros serviços do SO.

**Passo 4**. Quando for encontrada uma vulnerabilidade, o atacante procura um exploit previamente escrito para utilizar. Se não tiverem sido escritos quaisquer exploits, o atacante pode considerar a escrita de um.

A Figura 1 representa um atacante a utilizar o **Whois**, o qual é uma base de dados pública da Internet que contém informações sobre nomes de domínio e respetivos inscritos. A Figura 2 representa um atacante a utilizar a ferramenta **Nmap**, um analisador de portas popular. Com um analisador de portas, um atacante pode sondar portas de um computador alvo para obter informações sobre os serviços que estão em execução nesse computador.

**Ameaças persistentes avançadas**

Uma forma de conseguir a infiltração é através de ameaças persistentes avançadas (APAs). Estas consistem numa operação multifaseada, a longo prazo, furtiva e avançada contra um alvo específico. Dada a sua complexidade e o nível de conhecimentos necessário, geralmente, uma APA é bem financiada. Uma APA é direcionada a organizações ou países por motivos comerciais ou políticos.

Geralmente relacionada com espionagem baseada em rede, a APA tem a finalidade de implementar software maligno personalizado num ou vários sistemas do alvo, não sendo detetado. Ao envolver múltiplas fases de operação e vários tipos personalizados de software maligno que afetam diversos dispositivos e realizam funções específicas um atacante individual, muitas vezes, não possui os conhecimentos, os recursos ou a persistência necessários para realizar APAs.

# DoS

Os ataques de negação de serviço (Denial-of-Service, DoS) são um tipo de ataque de rede. Um ataque DoS resulta numa espécie de interrupção do serviço de rede para utilizadores, dispositivos ou aplicações. Existem dois tipos principais de ataque DoS:

**Quantidade esmagadora de tráfego –** Ocorre quando uma rede, um host (hospedeiro) ou uma aplicação recebe uma quantidade enorme de dados a uma velocidade que não consegue processar. Esta situação provoca um abrandamento da transmissão ou da resposta, ou o bloqueio de um dispositivo ou serviço.

**Pacotes com formatação maliciosa –** Ocorre quando um pacote com formatação maliciosa é enviado a um host ou a uma aplicação e o recetor não consegue processá-lo. Por exemplo, um atacante reencaminha pacotes com erros que não podem ser identificados pela aplicação ou reencaminha pacotes com formatação incorreta. Esta situação faz com que o dispositivo recetor funcione de forma muito lenta ou bloqueie.

Os ataques DoS são considerados um risco grave, na medida em que podem interromper facilmente a comunicação e provocar perdas significativas de tempo e dinheiro. Estes ataques são relativamente fáceis de realizar, mesmo por um atacante com poucos conhecimentos.

# DDoS

Um ataque DoS distribuído (Distributed DoS Attack, DDoS) é semelhante a um ataque DoS, mas tem origem em múltiplas fontes coordenadas. Por exemplo, um ataque DDoS pode ocorrer da seguinte forma:

Um atacante constrói uma rede de hosts infetados, denominada botnet. Os hosts infetados são designados por zombies. Os zombies são controlados por sistemas de controladores.

Os computadores zombies analisam constantemente e infetam mais hosts, criando mais zombies. Quando está preparado, o pirata informático dá ordem aos sistemas de controlo para que façam com que a botnet de zombies realize um ataque DDoS.

Clique em Play (Reproduzir) na figura para ver as animações de um ataque DDoS.