Unidade VII

7 TESTE DE INVASÃO E SEGURANÇA EM TECNOLOGIAS EMERGENTES

Após a implantação dos dispositivos tecnológicos de segurança, o grande problema para os administradores de rede é saber se esses dispositivos estão efetivamente protegendo as informações que trafegam na rede. Pensando nisso, podem recorrer a testes de invasão, que permitem verificar na prática se os dispositivos tecnológicos estão atendendo a seu propósito.

7.1 Teste de invasão

De acordo com Weidman (2014, p. 30),

> [...] testes de invasão ou pentesting (não confundir com testes de caneta esferográfica ou de canetas-tinteiro) envolvem a simulação de ataques reais para avaliar os riscos associados a potenciais brechas de segurança. Em um teste de invasão (em oposição a uma avaliação de vulnerabilidades), os pentesters não só identificam vulnerabilidades que poderiam ser usadas pelos invasores, mas também exploram essas vulnerabilidades, sempre que possível, para avaliar o que os invasores poderiam obter após uma exploração bem-sucedida das falhas.

Notícias sobre organizações de grande porte que foram alvo de um ciberataque são muito comuns nos dias atuais. Com mais frequência do que se espera, os invasores não usam a mais recente vulnerabilidade zero-day (vulnerabilidade que ainda não foi corrigida pelos fornecedores de software); eles atacam utilizando vulnerabilidades existentes há muito tempo e, na maioria das vezes, com a correção publicada.

Organizações de grande porte, com orçamentos consideráveis aplicados em segurança, tornam-se vítimas de injeção de SQL em seus sites, de ataques de engenharia social contra seus funcionários, de senhas fracas em serviços disponíveis pela internet, e assim por diante. Em outras palavras, as organizações estão perdendo dados proprietários e expondo informações pessoais de seus clientes em consequência de brechas de segurança que poderiam ter sido corrigidas. Quando aplicamos um teste de invasão, descobrimos esses problemas antes que um invasor o faça e fornecemos recomendações sobre como corrigi-los e evitar vulnerabilidades futuras.

O escopo dos testes de invasão varia de cliente para cliente, assim como de tarefa para tarefa. Algumas organizações adotam posturas excelentes quanto à segurança, ao passo que outras têm vulnerabilidades que permitiriam aos invasores violar o perímetro e obter acesso aos sistemas internos.

Às vezes, é necessário ser responsável também pela avaliação de uma ou mais aplicações web personalizadas. Isso pode exigir ataques de engenharia social para verificar a capacidade de obter acesso à rede interna do cliente. Determinados testes de invasão requerem que se atue como alguém de dentro – um funcionário mau-caráter ou descontente ou um invasor que já tenha violado o perímetro. Outras situações demandam um teste de invasão externo, em que se deve simular um ataque por meio da internet. Algumas organizações podem querer avaliar a segurança da rede wireless de seus escritórios. Em certos casos, você pode até efetuar uma auditoria nos controles de segurança físicos da organização.

7.2 Etapas de um teste de invasão

Os testes de invasão têm início com a etapa de **preparação** (pre-engagement), que envolve definir, por exemplo, os objetivos do teste e o mapeamento do escopo (a extensão e os parâmetros do teste). Quando o pentester e a organização chegam a um acordo, o teste tem início.

Na **coleta de informações** (intelligence gathering), o pentester procura informações sobre a organização disponíveis publicamente e identifica maneiras em potencial de conectar-se com os sistemas dela.

Na **modelagem de ameaças** (threat modeling), o pentester usa as informações coletadas para determinar o valor de cada descoberta e o impacto sobre o cliente caso a descoberta permita que alguém invada um sistema. Essa avaliação possibilita ao pentester desenvolver um plano de ação e métodos de ataque.

Na **análise de vulnerabilidades** (vulnerability analysis), o pentester começa a examinar ativamente as vulnerabilidades a fim de determinar até que ponto é possível que suas estratégias de exploração de falhas tenham êxito. Os exploits que não funcionarem poderão desativar serviços e disparar alertas de detecção de invasão, o que arruinaria as chances de efetuar uma exploração de falhas bem-sucedida. Com frequência, durante essa etapa, o pentester executa scanners de vulnerabilidade, que usam bancos de dados e uma série de verificações ativas para obter um palpite melhor a respeito de quais vulnerabilidades estão presentes no sistema de um cliente. Embora os scanners sejam ferramentas eficazes, eles não podem substituir totalmente o raciocínio crítico. Portanto, também devem ser realizadas análises manuais.

A **exploração de falhas** (exploitation) é com certeza a etapa mais interessante. Nesse momento, o pentester executa exploits contra as vulnerabilidades descobertas (às vezes, usando uma ferramenta como o Metasploit), numa tentativa de acessar os sistemas do cliente. Algumas vulnerabilidades são muito fáceis de ser exploradas – por exemplo, fazer logon com senhas default.

Na **pós-exploração de falhas** (post exploitation), começam os testes de invasão. O que determinada invasão realmente significaria para a organização? Invadir um sistema legado, sem patches (correções), que não faça parte de um domínio, que não esteja relacionado a alvos muito valiosos, que não contenha nenhuma informação de interesse para um invasor não seria o mesmo que invadir um controlador de domínio ou um sistema de desenvolvimento do cliente. Na pós-exploração de falhas, o pentester reúne informações sobre o sistema invadido, procura arquivos de interesse, tenta elevar o nível de seus privilégios, e assim por diante. Pode fazer, por exemplo, um dump dos hashes de senha para ver

se é possível revertê-los ou usá-los para acessar sistemas adicionais. Também pode tentar empregar o computador explorado para atacar sistemas que não estavam anteriormente disponíveis a ele.

Na última etapa do processo, a **geração de relatórios** (reporting), o pentester informa as descobertas significativas, diz o que se está fazendo corretamente, indica maneiras de melhorar a postura quanto à segurança, explica como conseguiu invadir o sistema etc.

Escrever um bom relatório de teste de invasão é uma arte que exige prática para ser dominada. É preciso apresentar as descobertas de forma clara para todos, da equipe de TI, responsável pela correção de vulnerabilidades, até a alta gerência, que aprova as alterações com os auditores externos. Devemos evitar, por exemplo, termos técnicos em excesso; caso sejam necessários, devem ser explicados. Um bom recurso é mencionar os dados privados que puderam ser acessados ou alterados. Uma afirmação como "Fui capaz de ler seu e-mail" gera repercussão em quase todos.

O relatório do teste de invasão deve incluir tanto um sumário executivo quanto um relatório técnico.

O sumário executivo descreve os objetivos do teste e oferece uma visão geral das descobertas. O público-alvo são os executivos responsáveis pelo programa de segurança. Esse sumário deve incluir:

- **Histórico**: descrição do propósito do teste e definição de qualquer termo que possa não ser familiar aos executivos, vulnerabilidades e medidas de prevenção.
- **Postura geral**: visão geral da eficiência do teste e dos problemas encontrados, como a ausência de gerenciamento de patches.
- **Perfil do risco**: classificação da postura da empresa quanto à segurança. Deve-se incluir uma explicação sobre a classificação ou utilizar a matriz de risco da organização (caso exista).
- **Descobertas gerais**: sinopse dos problemas identificados, junto com as estatísticas e as métricas sobre a eficiência de qualquer medida de prevenção implantada.
- **Resumo das recomendações**: visão geral das tarefas necessárias para corrigir os problemas descobertos no teste de invasão.
- **Mapa estratégico**: apresentação de objetivos de curto e de longo prazo ao cliente para melhorar sua postura quanto à segurança.

O relatório técnico, como o próprio nome indica, oferece detalhes técnicos sobre o teste. Ele deve incluir:

- **Introdução**: inventário dos detalhes, como escopo e contatos.
- **Coleta de informações**: detalhes das descobertas da etapa de coleta de informações. De particular interesse são os rastros do cliente (footprint) deixados na internet.

- **Análise de vulnerabilidades**: detalhes das descobertas da etapa de análise de vulnerabilidades.
- **Exploração de falhas**: detalhes das descobertas da etapa de exploração de falhas.
- **Pós-exploração de falhas**: detalhes das descobertas da etapa de pós-exploração de falhas.
- **Risco/exposição**: descrição quantitativa do risco identificado. Essa seção traz uma estimativa das perdas caso as vulnerabilidades identificadas sejam exploradas por um invasor.
- **Conclusão**: visão geral final do teste.

7.2.1 Coleta de informações

O objetivo dessa etapa é conhecer o máximo possível do cliente. O executivo revela informações demais no Twitter? O administrador do sistema escreve para listservs de arquivos perguntando a respeito de como garantir a segurança de uma instalação de Drupal? Quais softwares são executados nos servidores web? Os sistemas voltados para a internet estão ouvindo mais portas do que deveriam?

Também começamos a interagir com nossos sistemas-alvo, procurando conhecê-los bem, mas sem atacá-los de forma ativa. Usamos o conhecimento adquirido nessa fase na etapa de modelagem de ameaças, na qual pensamos como um invasor e desenvolvemos planos de ataque com base nas informações coletadas.

Embora nos permita aprender bastante sobre a organização e a infraestrutura do objeto de análise, a coleta de informações mantém-se como uma espécie de alvo em movimento. Não é viável estudar a vida on-line de todos os funcionários. Além disso, diante de uma enorme quantidade de informações coletadas, poderá ser difícil discernir dados importantes de ruído.

Se um executivo tuitasse com frequência sobre um time esportivo favorito, haveria chances de o nome desse time ser a base da senha de seu webmail. Essa informação, no entanto, também poderia ser irrelevante.

Ao contrário dos dados de inteligência obtidos a partir de fontes secretas – por exemplo, ao vasculhar lixos e bancos de dados ou usar engenharia social –, a Osint (open source intelligence) é coletada a partir de fontes legais, como registros públicos e mídia social. O sucesso de um teste de invasão, com frequência, depende do resultado da etapa de coleta de informações.

7.2.2 Descoberta de vulnerabilidades

Antes de começar a lançar exploits, precisamos fazer um pouco mais de pesquisa e análise. Ao identificar vulnerabilidades, devemos procurar, de forma ativa, problemas que levem a algum comprometimento na etapa de exploração de falhas. Embora algumas empresas de segurança executem somente uma ferramenta automatizada de exploração de falhas e esperem pelo melhor, um estudo das vulnerabilidades feito por um pentester habilidoso proporcionará resultados mais satisfatórios do que qualquer ferramenta por si só.

Depois de obter informações sobre o alvo e a superfície de ataque, podemos desenvolver cenários para atingir os objetivos do teste de invasão.

Imagine, por exemplo, que o servidor FTP na porta 21 anunciou-se como vsftpd 2.3.4. Vsftpd é a abreviatura de very secure FTP daemon. Pode-se dizer que um produto que se autodenomina very secure (muito seguro) está pedindo para ter problemas. De fato, em julho de 2011, veio à tona a notícia de que o repositório do vsftpd havia sido invadido. Os binários do vsftpd tinham sido substituídos por uma versão contendo um backdoor, o qual podia ser acionado por meio de um nome de usuário com uma carinha sorridente. Isso fazia com que um root shell fosse aberto na porta 6200. Depois que se descobriu o problema, os binários com o backdoor foram removidos e o vsftpd 2.3.4 oficial foi restaurado. Ainda que a presença do vsftpd 2.3.4 não confirme que nosso alvo é vulnerável, definitivamente é uma ameaça a ser considerada. O teste de invasão torna-se mais fácil se pegamos carona com um invasor que já tem o controle de um sistema.

Alguns cursos de testes de invasão excluem totalmente o scan de vulnerabilidades e argumentam que um pentester habilidoso pode descobrir tudo o que um scanner também pode. O fato é que o scanner continua sendo uma ferramenta valiosa, especialmente porque muitos testes de invasão são realizados numa janela de tempo menor do que qualquer um gostaria de ter. No entanto, se um dos objetivos de sua avaliação for evitar a detecção, você deverá pensar duas vezes antes de usar um scanner.

Muito embora as ferramentas tenham um bom grau de eficácia, nenhuma delas chega nem perto da análise manual para verificar se uma vulnerabilidade pode levar a um comprometimento, e não há melhor maneira de se aperfeiçoar do que praticando.

Como exemplo, podemos analisar uma porta que não costuma aparecer em scans automatizados: a porta 3232. Se tentarmos efetuar o scan dessa porta com um scanner convencional, perceberemos que haverá uma falha. Esse comportamento sugere que o programa que está ouvindo foi projetado para ouvir um dado de entrada em particular e que ele tem dificuldade de processar qualquer outra informação. Isso é interessante para o pentester, porque mostra que o programa não está validando a entrada de forma adequada.

Observação

Existem diversas ferramentas automatizadas de exploração de vulnerabilidades. Os testes serão mais eficientes se o responsável unir a tecnologia com sua experiência, pois algumas ameaças estão além do ambiente tecnológico das redes.

7.2.3 Captura de tráfego

Antes de partir para a exploração de falhas, devemos usar ferramentas de monitoração, como o Wireshark, para efetuar o sniffing e a manipulação do tráfego e obter informações úteis de outros computadores da rede local. Num teste de invasão interno, quando estivermos simulando uma ameaça interna ou um invasor que tenha conseguido acessar a periferia do sistema, capturar o tráfego de outros

sistemas da rede poderá nos proporcionar informações adicionais interessantes (nomes de usuário e senhas, por exemplo), que nos ajudarão a explorar as falhas. O problema, nesse caso, é que a captura de tráfego pode gerar uma quantidade excessiva de dados potencialmente úteis, o que dificulta a continuidade do processo.

De modo diferente dos hubs, os switches enviam tráfego somente para o sistema desejado. Portanto, numa rede com switches, não podemos ver todo o tráfego de e para o controlador de domínio sem enganar a rede para que ela nos envie esse tráfego. A maioria das redes com as quais você vai se deparar em testes de invasão provavelmente será uma rede com switches; até mesmo alguns hardwares de redes legadas que dizem ser hubs podem ter a funcionalidade de switches.

As redes virtuais parecem agir como hubs porque todas as suas máquinas virtuais compartilham um dispositivo físico. Se o tráfego for capturado em modo promíscuo numa rede virtual, você poderá ver o tráfego de todas as máquinas virtuais e o do computador host, mesmo que um switch esteja sendo usado no lugar de um hub no ambiente. Para simular uma rede não virtualizada, desative o **use promiscuous mode** (usar modo promíscuo) em todas as interfaces no Wireshark. Com isso, você terá de se esforçar um pouco mais para capturar o tráfego das máquinas virtuais alvo.

7.2.4 Ataque a senhas

Segundo Weidman (2014, p. 247), as senhas, geralmente,

> representam o ponto que oferece a menor resistência em atividades de testes de invasão. Um cliente com um programa robusto de segurança pode corrigir a falta de patches do Windows e evitar a existência de softwares desatualizados, porém os usuários em si não podem ser corrigidos.

As empresas estão despertando para os riscos inerentes à autenticação baseada em senhas. Ataques de força bruta e palpites embasados representam ameaças a senhas fracas. Muitas organizações utilizam a biometria ou uma autenticação de dois fatores para atenuar os riscos. Até mesmos os web services, como o Gmail e o Dropbox, oferecem autenticação de dois fatores, em que o usuário fornece, além da senha, um segundo valor – por exemplo, os dígitos de um token eletrônico. Se a autenticação de dois fatores não estiver disponível, o uso de senhas fortes é obrigatório para garantir a segurança da conta. Senhas fortes são longas, utilizam caracteres diversos e não se baseiam em palavras dicionarizadas.

Os usuários podem ser forçados pela empresa a criar senhas fortes. No entanto, à medida que as senhas se tornam mais complexas, também se tornam mais difíceis de lembrar. Em razão disso, aumenta a probabilidade de que os usuários guardem a senha no computador, no smartphone ou até mesmo num papel para recados, pois é mais fácil lembrar-se dela dessa maneira. Obviamente, essa atitude coloca em risco a segurança proporcionada pelo uso de uma senha forte.

Outro pecado capital consiste em usar a mesma senha para vários sites. Imagine, por exemplo, um CEO que emprega num fórum web comprometido a mesma senha que usa para o acesso corporativo a

documentos financeiros. Esse processo de reutilização é algo para ter em mente ao realizar ataques a senhas. Você poderá encontrar as mesmas senhas sendo usadas em vários sistemas e sites.

O gerenciamento de senhas constitui um problema difícil para a equipe de TI e é provável que continue a ser um caminho frutífero para os invasores, a menos que (ou até que) a autenticação baseada em senhas seja completamente substituída por outro modelo.

Assim como usamos scans automatizados para descobrir vulnerabilidades, podemos usar scripts para tentar descobrir credenciais válidas e fazer logon automaticamente em serviços. Utilizaremos ferramentas projetadas para automatizar ataques on-line a senhas ou para fornecer palpites de senha até o servidor responder com um logon bem-sucedido. Essas ferramentas, que se valem da técnica denominada **de força bruta**, procuram todas as combinações possíveis de nome de usuário e senha e, se houver tempo suficiente, elas vão descobrir credenciais válidas.

O problema com a força bruta é que, à medida que senhas mais fortes são usadas, o tempo necessário para descobri-las passa de horas para anos, e até mesmo para um tempo maior que a duração natural de uma vida. Provavelmente, descobriremos credenciais funcionais mais facilmente se fornecermos, a uma ferramenta automatizada de logon, palpites embasados sobre as senhas corretas. Por serem mais simples de lembrar, palavras dicionarizadas costumam ser empregadas por muitos usuários, apesar dos avisos de segurança. Usuários um pouco mais conscientes, no entanto, colocam números ou sinais de pontuação na senha.

Uma lista de palavras deve ser desenvolvida antes da utilização de uma ferramenta para adivinhar senhas. Se não souber o nome da conta do usuário cuja senha você quer quebrar, ou se quiser simplesmente fazer o cracking do máximo possível de contas, forneça uma lista de nomes de usuário a ser percorrida pela ferramenta.

Para criar uma lista de nomes de usuário, determine o esquema usado pelo alvo do teste para nomes de usuário. Por exemplo, se estiver tentando invadir as contas de e-mail dos funcionários, descubra o padrão seguido pelos endereços de e-mail. Esse padrão corresponde a **primeironome.sobrenome**, somente a **primeironome** ou é algo diferente? Existem bons candidatos a nomes de usuário em listas de primeiro nome e sobrenome comuns. Evidentemente, haverá mais chances de os palpites terem êxito se você puder descobrir o nome dos funcionários de seu alvo.

Se uma organização usar a inicial do primeiro nome seguida de um sobrenome como esquema para o nome de usuário, e ela tiver um funcionário chamado Carlos Silveira, **csilveira** provavelmente será um nome de usuário válido.

Observação

Pesquisas revelam que 60% dos usuários de redes corporativas utilizam senhas fracas, que facilitam ataques de força bruta. Testes de invasão são eficazes para verificar se a norma está sendo cumprida.

7.2.5 Exploração de falhas do lado da organização

Em testes de invasão, é comum descobrir serviços vulneráveis ouvindo portas, senhas default que não foram alteradas, servidores web mal configurados, e assim por diante.

Em organizações que investem bastante tempo e esforço em segurança, por sua vez, as chances de haver esse tipo de vulnerabilidade são bem menores. Essas organizações podem, por exemplo, instalar todos os patches de segurança assim que disponibilizados, efetuar auditorias periódicas em senhas e remover as que correm o risco de ser facilmente adivinhadas ou quebradas, bem como controlar as permissões de cada usuário.

Mesmo assim, apesar da implantação das melhores e mais recentes tecnologias de segurança e do emprego de equipes de segurança contra cracking, organizações de destaque (alvos valiosos para os invasores) continuam sendo invadidas.

Nos ataques do lado da organização, em vez de atacar diretamente um serviço que esteja ouvindo uma porta, serão criados vários arquivos maliciosos que, quando abertos num software vulnerável no computador-alvo, resultem em comprometimento.

Conforme se executam ferramentas, análises manuais e pesquisas, as possibilidades de exploração de falhas diminuem gradualmente, até restar um número limitado de problemas nos sistemas-alvo. Os problemas correspondiam até então a problemas do lado do servidor, ou seja, serviços que estavam ouvindo portas. O que resta são softwares potencialmente vulneráveis e que não estão ouvindo uma porta, isto é, softwares do lado da organização.

Softwares como navegadores web, visualizadores de documento e players de música estão sujeitos aos mesmos problemas que os servidores web, os servidores de e-mail e os demais programas baseados em rede.

Como os softwares do lado da organização não estão ouvindo a rede, não podemos atacá-los diretamente, porém o princípio geral é o mesmo. Se enviarmos um dado de entrada não esperado a um programa para acionar uma vulnerabilidade, poderemos sequestrar sua execução da mesma maneira que fizemos com programas do lado do servidor. Como não é possível enviar dados de entrada diretamente a programas do lado do cliente pela rede, devemos convencer um usuário a abrir um arquivo malicioso.

À medida que a segurança é levada mais a sério e as vulnerabilidades do lado do servidor tornam-se mais difíceis de descobrir do ponto de vista da internet, a exploração de falhas do lado do cliente está se tornando a chave para obter acesso até mesmo a redes internas cuidadosamente protegidas. Os ataques do lado do cliente são ideais em equipamentos (estações de trabalho e dispositivos móveis) que não estão diretamente ligados à internet.

No entanto, o sucesso de ataques do lado da organização depende de nosso exploit ser baixado e aberto num produto vulnerável, concretizando assim o ataque.

Saiba mais

Para obter mais informações sobre testes de invasão, acesse:

THE PENETRATION testing execution standard. 2014. Disponível em: <http://www.pentest-standard.org/index.php/Main_Page>. Acesso em: 5 jul. 2018.

7.3 Segurança em tecnologias emergentes

A implantação de novas tecnologias quase sempre representa redução de custos ou melhora significativa de desempenho. Nesse cenário, porém, a segurança da informação costuma ficar em segundo plano, cabendo aos administradores de rede trazer à tona discussões sobre o impacto das novas tecnologias.

7.3.1 Computação em nuvem

A computação em nuvem (cloud computing), uma tecnologia antiga que ganhou força em 2008, nada mais é do que utilizar, armazenar e desenvolver dados, informações ou aplicações, das mais variadas formas, independentemente do local ou da plataforma, através da internet.

O e-mail que acessamos por meio de um navegador está na nuvem, desde sempre. A partir de 2008, porém, foram desenvolvidas soluções comerciais que, além de facilitar a administração, também reduziram os custos.

Com a computação em nuvem, os aplicativos e os arquivos não precisam mais estar instalados ou armazenados no computador do usuário ou num servidor próximo. Esse conteúdo pode ficar na nuvem, isto é, na internet.

Ao fornecedor das aplicações cabem as tarefas de gerenciamento e manutenção dos dados (armazenamento, atualização, backup, escalonamento etc.). Os clientes e/ou as organizações não precisam preocupar-se com nenhum desses aspectos; podem apenas acessar e utilizar os dados.

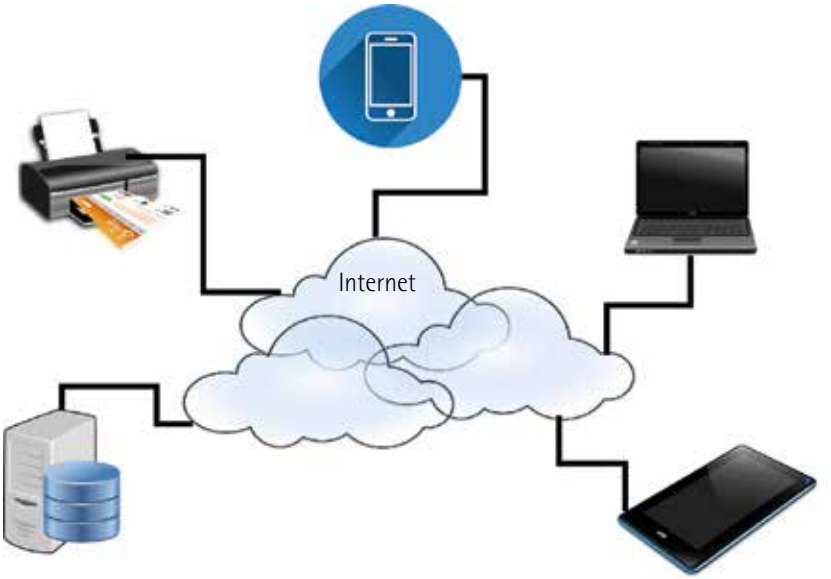

Figura 33 – Utilização da nuvem

Um exemplo prático dessa situação é o Office 365, da Microsoft, que disponibiliza aos usuários acesso aos recursos do pacote Office de forma inteiramente on-line. Basta ao usuário conectar-se à internet, pagar o serviço e criar uma conta e uma senha; o acesso será fornecido por meio de qualquer navegador.

Devido às vantagens oferecidas e à constante ampliação da computação em nuvem, bem como ao aumento da velocidade de conexão, os serviços estão migrando para a nuvem num caminho quase sem volta, não sendo possível aos administradores negar o seu uso ou simplesmente ignorar o fato de que as organizações vão utilizá-la, restando a eles determinar uma forma segura de realizar a migração. No caso específico da implantação de serviços em nuvem, a primeira preocupação dos administradores relaciona-se com a disponibilidade das informações.

É muito provável que executivos adotem serviços em nuvem por acreditarem que possam trazer benefícios. O maior apelo, como sempre, seria o financeiro, mas existem outros.

Quadro 27 – Benefícios da computação em nuvem

Benefício	Descrição
Diversidade	As aplicações podem ser acessadas independentemente do sistema operacional ou do equipamento utilizado.
Redução de custos com atualização do parque e segurança da informação	A estrutura para executar a aplicação (hardware, procedimentos de backup, controles de segurança, manutenção etc.) deixa de ser uma preocupação.
Unicidade de informações em qualquer lugar	O trabalho colaborativo torna-se mais fácil, pois todos os usuários acessam as aplicações e os dados de um mesmo lugar: a nuvem.
Disponibilidade	Dependendo do fornecedor, uma alta disponibilidade computacional pode ser oferecida. Caso um servidor pare de funcionar, os demais que integram a estrutura continuam a oferecer o serviço.
Controle de gastos	O usuário controla melhor os gastos porque contrata somente o que vai usar.

Diversos serviços estão disponíveis em nuvem. Os mais comuns são:

- **Software as a service (SaaS)**: formato de serviço em que o contratante não necessita adquirir uma licença de uso para a instalação ou mesmo investir em computadores; ele simplesmente contrata os serviços de um software por assinatura e paga um valor pelo uso dele por um tempo definido em contrato.

- **Platform as a service (PaaS)**: solução que, na maioria das vezes, inclui todos ou quase todos os recursos necessários ao trabalho, como armazenamento, banco de dados, escalabilidade (aumento automático da capacidade de armazenamento ou processamento), suporte a linguagens de programação e segurança.

- **Database as a service (DaaS)**: oferecida a clientes que desejam serviços para armazenar e acessar volumes de dados. A vantagem está na flexibilidade para expandir o banco de dados e compartilhar as informações com outros sistemas.

- **Infrastructure as a service (IaaS)**: muito semelhante ao PaaS, mas destinado à estrutura de hardware ou de máquinas virtuais, com o usuário tendo acesso inclusive a recursos do sistema operacional.

- **Testing as a service (TaaS)**: disponibiliza um ambiente de teste para aplicações e sistemas desenvolvidos pelo cliente, até mesmo com simulação do comportamento deles em nível de execução.

Quando os administradores de rede se deparam com a implantação de um ou mais desses serviços em nuvem, devem estar cientes de que os problemas de segurança não deixam de existir, apenas mudam de endereço. A análise do aspecto de segurança dependerá de qual formato de nuvem a organização adotou: público, privado ou híbrido.

Quando falamos de **nuvem pública**, referimo-nos ao fornecimento de determinados serviços em plataformas distantes, gerenciadas por um terceiro, que são acessadas pela internet. A **nuvem privada** apresenta os mesmos benefícios – tanto que os usuários não percebem a diferença entre ela e a anterior –, porém os equipamentos e sistemas utilizados para constituí-la ficam dentro da infraestrutura da própria corporação. Um terceiro formato, a **nuvem híbrida**, une os outros dois: as nuvens privadas ficam com as atividades mais críticas ao negócio ou que sofrem imposição legal, e as nuvens públicas com tudo o que não for crítico ou imposto pela lei, proporcionando assim segurança, desempenho e redução de custos.

No que se refere à segurança das informações disponibilizadas em nuvem, cada formato de nuvem requer um cuidado específico. Para as nuvens privadas, os princípios de segurança seguem os modelos estudados até aqui, como autenticação e configuração de dispositivos.

No caso das nuvens públicas, as preocupações são as mesmas, mas a configuração e a manutenção ficam a cargo de um terceiro. Isso, porém, não diminui a responsabilidade pelos ativos ali presentes. Deve-se ver a situação por uma esfera jurídica. Cabe ao contratante estabelecer um contrato muito bem redigido, em que constem:

- todas as necessidades de segurança quanto a confidencialidade, integridade e principalmente disponibilidade das informações;

- as multas (de no mínimo duas vezes o valor do ativo de informação) para o vazamento de informações ou a indisponibilidade do serviço, mesmo que temporária;

- as auditorias (presenciais ou remotas) e os testes de invasão que serão realizados.

As nuvens híbridas parecem mais eficazes quando se pensa em segurança da informação, e elas realmente o são. Isso por um motivo bem óbvio: porque ao terceiro são confiadas apenas as informações menos importantes, enquanto o restante permanece protegido pelas políticas de segurança da organização e é devidamente gerenciado por ela mesma.

Para ter uma nuvem híbrida protegida, os responsáveis devem estar atentos aos princípios de classificação da informação e de análise de riscos estudados antes, inclusive na elaboração de um contrato.

Lembrete

Os benefícios da computação em nuvem são diversidade, redução de custos com atualização do parque e segurança da informação, unicidade de informações em qualquer lugar, disponibilidade e controle de gastos.

7.3.2 Criptomoeda e blockchain

Para entender a aplicabilidade do blockchain, precisamos analisar o conceito e o funcionamento da criptomoeda, também conhecida como moeda digital, que chegou ao conhecimento público em 2008, por meio de Satoshi Nakamoto, pseudônimo que durante muito tempo não se soube se pertencia a uma pessoa ou a um grupo. Em 2016, o australiano Craig Steven Wright assumiu a criação da mais famosa moeda criptográfica, o bitcoin.

Incialmente, as moedas criptográficas eram usadas como alternativa de pagamento para atos ilícitos, como compra de drogas, encomenda de assassinatos, tráfico de armas e lavagem de dinheiro, tudo sempre através da darknet. Essas atividades eram realizadas com moeda criptografada pela impossibilidade de rastrear tanto a origem do recurso quanto a fonte de fornecimento dos produtos. Esse caráter ilegal deixou marginalizado o seu emprego por pessoas comuns, o que manteve a cotação do ativo em patamares relativamente baixos. A partir de 2013, porém, o verdadeiro potencial de negociação desse ativo veio à tona quando estabelecimentos comerciais e pessoas comuns começaram a fazer transações com criptomoedas.

Atualmente, existem mais de cem tipos de criptomoeda disponíveis. Para facilitar a compreensão de como ela funciona, vamos nos basear na estrutura do bitcoin, a mais utilizada e a mais rentável até o momento. Antes de apresentar tecnicamente o o bitcoin, devemos responder algumas perguntas

básicas. Por exemplo: o bitcoin é uma moeda ou um ativo? Alguns afirmam que é uma moeda, pois é possível fazer transações com ele, como compra e venda de produtos e serviços. Já os bancos centrais de diversos países consideram-no um ativo e de alto risco. O bitcoin é virtual ou ele existe fisicamente? Sim, ele existe fisicamente.

O bitcoin é a composição de uma programação aritmética complexa, que requer grande processamento e que gera um número único, o qual é registrado sequencialmente numa cadeia de blocos, o blockchain. No início, esse número era gerado com certa facilidade. Depois, a sequência numérica aumentou, assim como a concorrência, e o tempo de processamento foi ficando praticamente inviável para amadores.

Uma vez gerado, o número ficará na cadeia de blocos e na relação de confiança criptografada. Apenas a pessoa que o gerou poderá transferir sua posse mediante a inserção de uma senha única. Daí em diante, funcionará a lei da oferta e da procura: quanto mais pessoas estiverem dispostas a ter a moeda, maior será sua valorização em relação a outras moedas ou outros ativos financeiros. As moedas criptográficas têm valorização incompatível com os modelos monetários atuais. Por isso, é impossível prever sua alta ou sua baixa por meio dos indicadores de mercado, o que as torna um ativo de alto risco e sem garantias.

As criptomoedas em si não alteram o cotidiano de um administrador de rede – a não ser que a capacidade de processamento de seus equipamentos seja desviada por algum cracker para executar ações ligadas a elas. A estrutura que sustenta as criptomoedas é extremamente segura e confiável nos quesitos de transferência de propriedade e gestão. Estamos falando agora do blockchain.

Desenvolvido para alicerçar as operações com bitcoins, o blockchain pode ser definido como uma estrutura composta de um banco de dados compartilhado, no qual cada integrante é capaz de ler tudo, sem que haja controle por parte de uma única entidade ou controle de quais integrantes podem escrever. Grosso modo, podemos entender o blockchain como um registro ou um livro-razão distribuído, que providencia uma forma de gravar e compartilhar informações dentro de determinada estrutura (comunidade/serviço). No blockchain, existem dois tipos de registro: transações individuais e blocos.

Algumas caraterísticas que transformaram o blockchain em objeto de estudo da segurança da informação:

- **Inovação**: o blockchain pode modificar o sistema de pagamento e transferência de informações e serviços.
- **Autonomia**: os participantes da cadeia de confiança gerada pelo blockchain não necessitam de permissão para fazer transações entre si.
- **Transparência**: ao realizar uma transação entre si, os participantes do blockchain devem validá-la, atualizando seus blocos.
- **Imutabilidade e integridade**: uma vez concretizada a transação, os dados inseridos no blockchain nunca mais serão modificados, o que garante a integridade do processo.
- **Robustez**: por ter natureza distribuída, o blockchain é mais fortificado; a cadeia se sustenta por si só.

- **Desempenho**: o blockchain demanda verificação da assinatura, execução do algoritmo de consenso e viabilização da redundância.

- **Descentralização**: por meio do blockchain, deixa de existir a figura centralizadora que valida a transação.

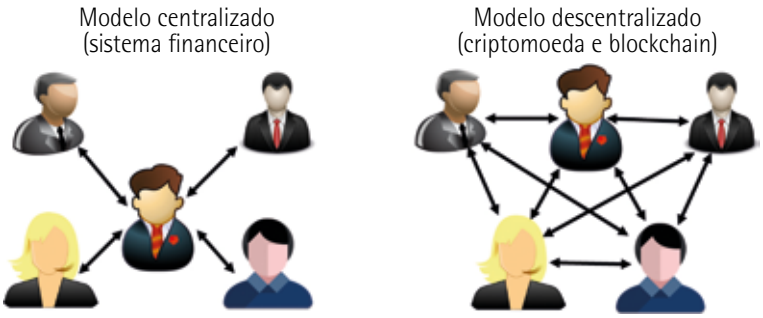

Figura 34 – Comparativo entre o modelo de transação centralizado e o descentralizado

Para assegurar o processo, o blockchain utiliza três técnicas. Sempre que ocorrer uma transação na cadeia de blocos, ela deverá ser ponto a ponto. Apesar de todos validarem, autenticarem e conhecerem a origem e o destino, o uso dessa técnica se justifica porque as inserções no bloco precisam ser únicas e sequenciais. Outra técnica é a criptografia através de chaves públicas e privadas, ou seja, a criptografia assimétrica. Além disso, para cada transação, desenvolve-se um hash, a fim de encurtar a chave criptografada e acelerar o processo.

Tudo funciona assim: João quer fazer uma transação com Maria. Para isso, com a senha de acesso, ele entra em sua carteira no blockchain. Depois de combinar com Maria quais informações ou valores devem ser transferidos, João solicita o número da carteira de Maria na cadeia de blocos para efetivar a transferência. Maria, também conectada a sua carteira por meio de uma senha individual, deve aceitar o processo. Feito isso, gera-se um número único sequencial no blockchain, dentro da cadeia de confiança em que João e Maria estão inseridos. Nesse momento, a transação circula entre todos os membros da cadeia de confiança, de modo que todos tomem ciência e atualizem suas cadeias, porque se está gerando um novo número de transação para aquela cadeia. Depois que todos os integrantes estiverem cientes e com suas cadeias atualizadas, a transação será validada e o número sequencial será inserido na cadeia eternamente.

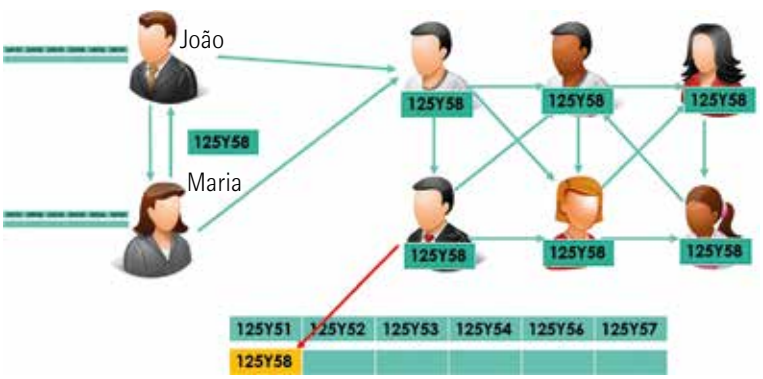

Figura 35 – Relação de confiança no blockchain

Quando analisamos o processo da relação de confiança das cadeias de blocos, podemos nos perguntar de que forma ele afeta o cotidiano de um administrador de rede. Se considerarmos a estrutura que o mantém, perceberemos que o blockchain pode influenciar quase todos os setores que transferem informações de um ponto a outro, como o sistema financeiro, o sistema hospitalar e os departamentos governamentais.

Abre-se então um leque de oportunidades para o desenvolvimento de plataformas seguras, que permitam tratar de assuntos comuns entre concorrentes de mercado, obtendo-se benefícios como:

- redução de custos de infraestrutura;
- melhoria na auditabilidade dos registros para fins internos e regulatórios;
- ampliação da segurança sistêmica;
- aumento da agilidade nas operações de colaboração;
- eliminação de intermediários e entidades centralizadoras do ramo de atividade;
- realização de negócios com não clientes em qualquer lugar do mundo.

Exemplos de aplicação do blockchain começam a aparecer ao redor do mundo, em diversos ramos de atividade. Vejamos o caso da Islândia e o de Dubai, nos Emirados Árabes Unidos.

A Islândia tem 1,3 milhão de habitantes. O governo desse país implantou uma estrutura de blockchain para o sistema de saúde, unificando e armazenando todos os prontuários médicos da população. Esse sistema inclui planos de saúde, pacientes, médicos e outros. Como ele funciona na prática? Imagine que você passe mal, fique desacordado e seja inicialmente socorrido por uma ambulância. Assim que você for identificado, o paramédico terá acesso a todas as suas informações clínicas, como alergias, doenças preexistentes, exames realizados, o nome do seu médico e o hospital em que ele está atendendo naquele momento. Quando os primeiros procedimentos de atendimento são inseridos no sistema, ainda na ambulância, o prontuário é atualizado, alertando seu médico, que fica pronto para recebê-lo, uma vez que a ambulância, assim que o localizou, já se direcionou para onde ele está.

Em Dubai, uma cidade com 2,9 milhões de habitantes, todos os serviços públicos municipais utilizam o blockchain para minimizar o desperdício de tempo. Um exemplo: geralmente, quando um cano de água é comprometido numa rua qualquer, a empresa responsável pela manutenção é acionada e o conserto é feito. O único problema é que essa empresa conserta o cano, mas não a rua, que fica esburacada até a empresa responsável pelo asfaltamento corrigir essa situação. Com o blockchain, assim que é emitida a solicitação, todos os envolvidos ficam a par do estágio do conserto, podendo assim trabalhar em conjunto, o que diminui o tempo de resposta.

A área financeira também está aderindo ao blockchain, transformando uma ameaça em oportunidade. Plataformas para a transferência internacional de recursos e para a compra e venda de ações, por exemplo, estão sendo a cada dia testadas e implementadas.

Quanto à segurança, estudos comprovam que as cadeias de blockchain também estão expostas a riscos, os quais são maiores nas cadeias de blockchain públicas do que nas corporativas ou particulares, fechadas na estrutura de transmissão da organização.

Podem-se indicar cinco riscos principais para as cadeias de blocos:

- **Risco cibernético e de informação**: associado à possibilidade de ação de crackers, que objetivam furtar informações dentro da cadeia.
- **Risco de arquitetura e design**: ligado ao desenvolvimento incorreto da cadeia de blocos, o que pode levar à exploração de vulnerabilidades.
- **Risco de conformidade de TI**: relacionado às melhores práticas e normas internas, e até mesmo a legislações, que podem inviabilizar a utilização do blockchain.
- **Risco de terceiros**: vinculado à escolha dos fornecedores da solução – os quais, em sua maioria, são startups de tecnologia, que podem simplesmente desaparecer do mercado, deixando-o sem suporte – e dos participantes de sua cadeia de confiança, que devem estar atentos aos princípios da segurança da informação.
- **Risco de integração**: concernente às novas tecnologias empregadas na organização, que podem representar um problema de segurança, permitindo a ação de crackers nas estruturas adaptadas.

7.3.3 Internet das coisas

O conceito de internet das coisas (em inglês, internet of things – IoT) foi empregado em 1992 para definir algo que se estava viabilizando por meio do IPv6, o qual multiplicou o número de endereços IP válidos na internet. A partir desse momento, começaram estudos para introduzir tudo na internet, desenvolvendo assim uma rede de objetos físicos, veículos, prédios e outros elementos que dispõem de tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.

Atualmente, esse conceito já está incorporado em nosso cotidiano, com a ligação das coisas físicas (câmeras de segurança, televisores, geladeiras, casas, automóveis etc.) à grande rede, à internet.

Para os administradores de rede, está cada vez mais difícil encaixar a segurança da informação – e, por que não dizer, a segurança física – dentro desse cenário, extremamente instável e em constante mudança.

Tudo o que aprendemos sobre segurança deve adaptar-se a essa nova realidade, na qual, por exemplo, funcionários conectados a uma rede corporativa podem realizar reuniões de qualquer lugar do mundo, mesmo dentro de veículos ou através de celulares, processando e gerando informações importantes e confidencias, que requerem o mesmo grau de proteção daquelas que estão nos servidores corporativos na organização.

Essas práticas, ao mesmo tempo que facilitam muito o cotidiano, representam um pesadelo para a segurança da informação, porque as pessoas vêm se preocupando menos com a segurança de suas ações e criando muitas vulnerabilidades. Os administradores de rede devem, portanto, procurar brechas e introduzir variadas soluções de proteção. A observação da política, das normas e da legislação também é fundamental. Considerando a hipótese de nada disso funcionar, deve existir ainda um bom plano de recuperação.

Resumo

Nesta unidade, abordamos os testes de invasão, os quais permitem trazer à tona erros de projeto, vulnerabilidades não mapeadas e ferramentas de proteção ultrapassadas, que crackers ou funcionários insatisfeitos poderiam vir a explorar.

Vimos todas as etapas de um teste de invasão: preparação, coleta de informações, modelagem de ameaças, análise de vulnerabilidades, exploração de falhas, pós-exploração de falhas e geração de relatórios. Em relação à última etapa, consideramos as informações que devem constar num sumário executivo e num relatório técnico.

Discutimos ainda as tecnologias emergentes e os desafios que propõem. Sua natureza inovadora exige dos administradores de rede uma busca constante pelo aperfeiçoamento e pelo conhecimento. Tecnologias como computação em nuvem e internet das coisas vieram para quebrar paradigmas e impor transformações nos atuais modelos de gestão.

Uma das tecnologias examinadas foi o blockchain, empregado não apenas no contexto das criptomoedas, mas também no âmbito das políticas governamentais. Vimos exemplos disso no sistema de saúde da Islândia e no sistema de serviços públicos municipais de Dubai.