

1

Por que Segurança da Informação

Para começar

Este capítulo tem como proposta apresentar os conceitos básicos da segurança da informação.

Em uma linguagem bastante simples e didática, detalhamos algumas ameaças e buscamos mostrar como estas ameaças interagem conosco e como podemos melhorar a segurança de informações da sociedade. As informações apresentadas formam a base necessária para entender tudo o que envolve o assunto, bem como suas definições e modos de uso. Assim compreenderemos de maneira simples o que parece ser de alta complexidade e estaremos mais bem preparados para as oportunidades do mercado de trabalho ou para continuarmos estudando sobre o assunto.

1.1 Conceitos gerais

Você já deve ter ouvido falar em vírus que causam prejuízos de milhões de dólares, hackers que capturam informações de cartões de crédito de instituições financeiras e sites de grandes empresas que foram atacados e tiveram seu acesso interrompido por razões políticas. Já deve ter ouvido falar também em informações secretas de governos, ou empresas, que foram divulgadas por hackers.

De certa maneira, essas situações podem parecer os principais problemas enfrentados pela segurança da informação. Contudo, tais atividades não são as únicas preocupações de uma empresa, ou de um profissional de segurança, no que diz respeito às tarefas diárias ou mensais de segurança.

Embora os vírus e os hackers apareçam em muitas manchetes de jornais, o gerenciamento de segurança é, dentro do núcleo de informática, o responsável pela segurança da informação de uma empresa, e mesmo não aparecendo nas manchetes dedicam-se a evitar os ataques como os noticiados na mídia.

O gerenciamento de segurança inclui a gestão de riscos, as políticas de segurança e a educação de segurança de todos os funcionários. São estes três componentes principais que servem como base do programa de segurança de qualquer empresa.

O universo da gestão de segurança da informação envolve determinação de objetivos, escopo, políticas, prioridades, padrões e estratégias.

Os objetivos da segurança da informação baseiam-se na identificação adequada dos ativos de informação de uma empresa, atribuindo valores para estes ativos, desenvolvimento, documentação e implementação de políticas de segurança, procedimentos, normas e diretrizes, que devem fornecer integridade, confidencialidade e disponibilidade da informação.

1.2 Princípios fundamentais de segurança

Existem vários objetivos, uns pequenos e outros grandes, em um programa de segurança. Mas os três princípios centrais em todo e qualquer programa de segurança da informação são: *confidencialidade, integridade e disponibilidade*, também conhecidos como a tríade CIA.

Confidencialidade

Confidencialidade é a capacidade de garantir que o nível necessário de sigilo seja aplicado em cada junção de dados em processamento. Além disso, trata-se da prevenção contra a divulgação não autorizada dos mesmos.

Os atacantes podem burlar os mecanismos de confidencialidade por meio de monitoramento de rede (chamado surf de ombro¹), engenharia social, e roubar arquivos de senhas.

A confidencialidade pode ser fornecida por meio de técnicas de criptografia de dados e da forma como eles são armazenados e transmitidos, assim como por meio de acompanhamento de tráfego de rede, controle de acesso rigoroso, classificação de dados e treinamento de pessoal sobre os procedimentos adequados na utilização de informações na empresa.

Integridade

A integridade é a garantia de rigor e confiabilidade das informações e sistemas e de que não ocorrerão modificações não autorizadas de dados.

¹ Surf de ombro é quando uma pessoa olha por cima do ombro de outra pessoa e observa a sua digitação ou os dados que aparecem na tela.

Os mecanismos de hardware, software e comunicação devem trabalhar de maneira conjunta para manter e processar dados corretamente e movimentar dados para os destinos desejados sem qualquer alteração não autorizada ou não esperada.

Os sistemas da empresa e a rede devem ser protegidos contra interferências e contaminações externas ao seu ambiente tecnológico.

Disponibilidade

É a capacidade que os sistemas e as redes devem ter para executar e disponibilizar os dados de forma previsível e adequada às necessidades da empresa.

Eles devem estar aptos a recuperar quedas de disponibilidade de forma rápida e segura e a garantir que a produtividade das operações da empresa não seja afetada significativamente.

A disponibilidade de sistemas pode ser afetada por falhas de equipamentos ou de softwares.

Backups, também conhecidos como cópias de segurança, devem estar disponíveis para uma rápida recuperação de sistemas e dados críticos na empresa.

Aspectos ambientais como calor, frio, umidade, eletricidade estática e produtos contaminantes podem afetar a disponibilidade de sistemas e dados.

Como veremos a seguir, os ataques de negação de serviços (DoS) são os mais populares métodos que hackers utilizam para perturbar e afetar a disponibilidade de informações e sistemas e, conseqüentemente, a produtividade destes sistemas. Estes ataques são feitos para reduzir ou bloquear o acesso de usuários a recursos de sistemas e informações, normalmente em sites de grandes e médias empresas.

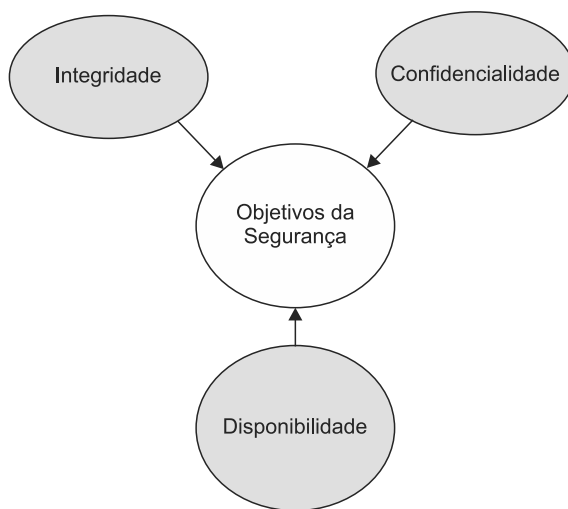


Figura 1.1 – CIA, a tríade de segurança.

A seguir falaremos sobre os principais conceitos da segurança da informação e por que ela é tão importante para os negócios de uma empresa e para você. Antes disso, porém, temos

de conhecer alguns conceitos da área de tecnologia da informação, que são fundamentais para entendê-los corretamente.

Nosso objetivo, aqui, é mostrar a você, leitor, como conseguir um ambiente seguro para a informação.

1.3 Informação

O que é informação?

Ao longo dos anos de experiência no desenvolvimento de sistemas de informação, observamos que existe uma grande dificuldade das pessoas em geral para entenderem a diferença entre *informação* e *dados*.

A *informação* acrescenta algo ao conhecimento de uma realidade analisada. Por exemplo, a dosagem que um paciente precisa receber de um determinado remédio é uma *informação*.

O *dado* é uma representação, um registro de uma informação.

Esse *dado* pode ser registrado fisicamente em um papel (receita médica), em um disco de computador ou através de um impulso elétrico etc.

Esse registro pode ser o gerador de uma série de processos que influenciam a realidade observada (salvar a vida de um paciente, tocar um alarme etc.).

O tratamento das informações dá origem a vários tipos de *dados*, porém o *dado* deve registrar apenas os aspectos realmente relevantes da *informação*. Ou seja, o endereço do fabricante do remédio, por exemplo, não tem qualquer interesse para um sistema de controle que mantém a vida dos pacientes em um CTI.

Podemos concluir, então, que em um sistema de informações estão todas as informações necessárias ao objetivo do sistema (manter a vida do paciente).

Os *dados* originados dessas informações serão processados pelo que denomina *sistema de informações*.

Porém, por definição, os computadores não processam informações, mas sim *dados*.

Informação	Dado
Hoje está muito quente.	Temperatura atual de 38 °C.

1.4 Sistema de informação

Um sistema de informação é em princípio a automação de todos os processos manuais sobre os dados de uma determinada área ou empresa.

Um *sistema de informações* é baseado na premissa apresentada graficamente na Figura 1.2.

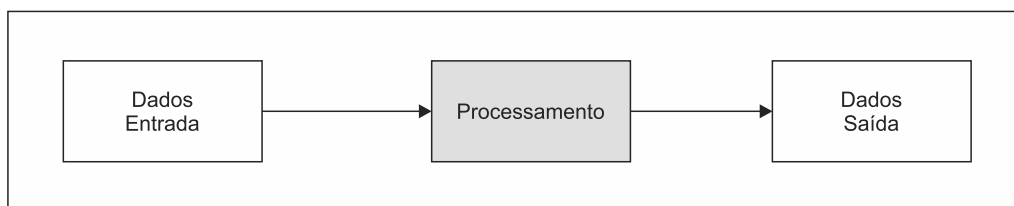


Figura 1.2 – Sistema de informações.

Então, tudo que compõe as caixinhas do desenho, na realidade, faz parte de um *sistema de informações*:

- » O que entra (por exemplo, dados, informações, eventos, entre outros) é um requisito;
- » Para que seja executado, o processamento a ser realizado tem regras, fórmulas, normas, critérios, arquivos, tabelas etc., que compõem os chamados requisitos funcionais de sistemas de informação;
- » A saída desse processamento também é composta de dados e informações, ou de disparo de eventos.

Um sistema de informação deve ser considerado sempre como um composto de um componente social e de um conjunto de dados e processamentos automatizados destes dados por meio de tecnologias computacionais.

O componente social inclui pessoas, processos, tarefas, informações e documentos. O segundo componente consiste nos meios tecnológicos (máquinas, computadores, redes de comunicação, linguagens de programação, telas de interfaces) que se interligam com o chamado componente social.

As pessoas e os processos que rotineiramente executam, e também os dados e documentos que criam, alteram, apagam e consultam, fazem parte do sistema de informações, compondo algo maior que simplesmente um software. Afinal, além de possuir o hardware e o software, também possui e realiza os processos que dependem de atividades e tarefas que são muitas vezes executadas fora dos computadores por pessoas.

A importância do conjunto social reside no fato de que os sistemas de informação, para ter a eficácia desejada, dependem diretamente da interação das pessoas que os criam e desenvolvem, de quem os acessa e utiliza. Eles não nascem do nada, não fazem nada sem a interferência humana.

Uma das preocupações da segurança da informação é proteger os elementos que compõem a informação e seus meios de comunicação e manipulação.

Sistemas de informação são também utilizados em empresas para dar apoio à tomada de decisões, atuando, além do processamento das transações rotineiras de negócio, também no planejamento e no controle operacional, no planejamento gerencial. E, finalmente, servem de base para as estratégias e políticas de uma empresa.

Lembre-se

“Informação é o resultado do tratamento dos dados existentes acerca de alguém ou de alguma coisa.”

1.5 O que são bancos de dados

Um banco de dados pode ser definido como um conjunto de dados devidamente relacionados.

Podemos compreender como dados os objetos que podem ser armazenados e que possuem um significado implícito. Porém o significado do termo banco de dados é mais restrito.

Um banco de dados possui as seguintes propriedades:

- » É uma coleção lógica coerente de dados com um significado inerente; uma disposição desordenada dos dados não pode ser referenciada como banco de dados.
- » Ele é projetado, construído e preenchido com valores de dados para um propósito específico; um banco de dados possui um conjunto predefinido de usuários e de aplicações.
- » Ele representa algum aspecto do mundo real, chamado de minimundo; qualquer alteração efetuada no minimundo é automaticamente refletida no banco de dados.

Antes somente era considerado banco de dados uma coleção lógica coerente de dados com um significado inerente e disposta de forma ordenada. Uma disposição desordenada de dados, por sua vez, não era considerada um banco de dados.

Hoje, entretanto, dados não estruturados e até mesmo desordenados são considerados banco de dados, pois caracterizam o que se denomina dados não estruturados. São, ainda, considerados extremamente importantes, afinal, o contexto das redes sociais é formado por esse tipo de estrutura de dados. Basta que estes dados estejam armazenados e sob o controle de softwares chamados sistemas gerenciadores de bancos de dados.

Podem ser considerados bancos de dados: arquivos de texto, planilhas eletrônicas e estruturas de sistemas gerenciadores de bancos de dados. Estas últimas são armazenadas em forma de tabelas relacionadas entre si e representam objetos de um determinado negócio de uma empresa.

Os bancos de dados são importantes porque os sistemas de informação processam os dados ali armazenados. Ou seja, eles registram, alteram, disponibilizam para visualização e os deletam. Estes dados, portanto, se transformam em informação com um valor para uma empresa, isto é, ativos digitais. Eles passam, assim, a ter valor financeiro para a manutenção e a existência dos negócios de qualquer tipo de organização, seja privada ou pública.

1.6 Log

Quando o capitão de um navio escreve o diário de bordo (em inglês *log*), ele registra os principais fatos ocorridos na embarcação. Ele está na realidade fazendo este registro para a qualquer momento da navegação revisar o que aconteceu durante o período.

Da mesma maneira, os sistemas de uma rede, entre eles os gerenciadores de banco de dados, realizam constantemente o log de toda e qualquer operação ocorrida continuamente. Dessa maneira, eles garantem que todas as informações sejam registradas, informando quem acessou, quando, como, o valor da informação e que operação foi realizada.

O registro de *log* permite, em caso de perda de dados, que os sistemas de informação possam recuperar estes dados a partir do momento anterior à ocorrência da perda, para auditar as operações realizadas. Ou seja, validar quem acessou, o que foi feito sobre os dados e quando.

A existência de *log* é de extrema importância, como veremos no decorrer do livro, para os processos de segurança da informação.

Amplie seus conhecimentos

Os sistemas gerenciadores de bancos de dados possuem características em suas estruturas de dados, possuem também linguagens e regras para que as informações sejam extraídas dos mesmos, e os sistemas de informações utilizam dados para entrada que, processados, registram nos bancos de dados e os apresentam e disponibilizam para consultas por meio da linguagem SQL. Todas as operações realizadas com utilização de sistemas gerenciadores de bancos de dados são registradas em logs.

Pesquise em livros sobre Fundamentos de Bancos de Dados, ou na internet alternativamente, sobre o funcionamento e como são criados e mantidos os dados em sistemas gerenciadores de banco de dados e procure conhecer quais são os fatores relevantes em segurança da informação no tocante a banco de dados.

De nada servirá um sistema de segurança, por mais completo que seja, se os usuários, por exemplo, permitirem o acesso não autorizado ou fornecerem seu nome de usuário e senha a pessoas de fora da empresa, ou até a colegas da própria empresa, que não estejam habilitadas para tal fim, deixando aberta uma porta para ataques ou vazamentos de informações.

No mundo real, os aspectos sociais podem interferir diretamente no funcionamento de um sistema de informação.

Os procedimentos de operação e os acessos de um sistema de informação podem ser alterados ou refeitos em consequência direta de alguns aspectos sociais e de negócio, com objetivo de disponibilizar a existência de um maior controle dos acessos e das operações permitidas a usuários e realizadas sobre os dados que são objeto do sistema. Regulando assim a forma como são utilizados e manipulados.

Tudo o que é feito sobre dados depende do ambiente social em que estes dados estão disponibilizados e controlados.

1.7 Sociedade e segurança da informação

Atualmente estamos, e precisamos estar, conectados. Ao ler um artigo na *Info Exame* sobre a internet, “?Não, Caiu!”, observamos o quanto estamos dependentes do “*estar conectado*”.

Temos a necessidade de ler e-mails, acessar dados de trabalho na empresa, efetuar pesquisas, ou mesmo ver um mapa para localizar um endereço ou um local aonde queremos chegar.

“Vivemos na internet e da internet”, diz Dagomir Marquezi, colunista da Info Exame.

É muito importante saber que, quanto mais interconectado nós, ou uma empresa, estivermos maior será a complexidade por onde trafegam e onde estão armazenadas as informações. E, conseqüentemente, maior deverá ser a preocupação com o nível de segurança a ser implantado para garantir os três princípios básicos da segurança: confidencialidade, integridade e disponibilidade.

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2005, p. 2)

Não seria exagerado afirmar que as informações na sociedade dependem cada vez mais dos sistemas de informação e da utilização de computadores pessoais e equipamentos móveis. E, por isso, interpretamos a segurança da informação como assunto diretamente relacionado com a tecnologia da informação.



Figura 1.3 – Hacker.

Diariamente, lemos e ouvimos notícias sobre ataques realizados por piratas digitais.

São os hackers e crackers, que aparecem em centenas pelo mundo e realizam ataques a sites de empresas e organizações governamentais. Eles invadem sites de bancos, grandes redes de comércio virtual, entidades internacionalmente conhecidas como FBI, NSA, sites de governos estrangeiros, entre outros.

Hacker é uma pessoa que estuda, em profundidade, como modificar os aspectos internos de dispositivos de tecnologia da informação, programas e redes de computadores.

Com o aprimoramento desses conhecimentos, um hacker, com certa facilidade, consegue obter domínio e penetrar em equipamentos de rede, sistemas de informação, causando efeitos extremamente danosos a empresas e pessoas. Ele, inclusive, consegue superar as barreiras que são criadas para impedir o acesso e controle externo de sistemas de informação e de bancos de dados que são utilizados por este sistema.

Às vezes, o conceito de **hacker** se confunde com um outro tipo de estudioso com as mesmas capacidades, mas com objetivos diferentes. Trata-se dos crackers.

Segundo a definição correta, hacker é aquele indivíduo que se preocupa em utilizar seu conhecimento para detectar e melhorar falhas e vulnerabilidades de sistemas de informação e redes de computadores.

Por outro lado, os crackers, com seu conhecimento e nenhuma preocupação em manter o funcionamento de sistemas de informações, são os atacantes de sistemas preocupados principalmente em deixar uma “marca”, bloquear acessos, roubar informações ou simplesmente destruir completamente um sistema.

Cracker (quebrador) deveria ser utilizado somente para identificar aqueles indivíduos que praticam a quebra (ou cracking) de um sistema de informações e de sua segurança, de forma ilegal e antiética.

Entretanto, vulgarmente o termo hacker ficou associado às pessoas que têm o domínio especializado e profundo de sistemas operacionais, redes e linguagens de programação, em nível de como se dão os processamentos internos em computadores. São eles que invadem sites, criam vírus e quebram a segurança de sistemas.

Nesse caso, o mais correto seria utilizarmos craker como o substantivo que define os mal-intencionados e hacker como os bem-intencionados.

Quando alguém deseja baixar um software e utilizá-lo como cópia pirata, esta pessoa procura normalmente um crack (quebra) para este software, ou seja, um código que quebra a segurança da licença de uso deste software. Assim, ela poderá utilizá-lo sem ter adquirido e pago os direitos de licenciamento pelo seu uso.

Fica claro, então, que craker é quem pratica o roubo de dados e altera sistemas de informação. Enquanto isso, quem busca identificar vulnerabilidades e criar proteções para elas são os hackers.

Infelizmente popularizou-se o termo hacker. Contudo, para não nos distanciarmos tanto do senso comum, chamaremos, neste livro, de hackers todos que atacam redes e sistemas de informação.

Mark Zuckerberg, criador do Facebook, começou sua carreira como um hacker. Ele invadia o banco de dados dos alunos da Universidade de Harvard com o objetivo de fornecer uma forma mais simples de as pessoas se conectarem entre si, alterando o chamado Anuário Online que continha dados sobre os estudantes da Universidade. O site alterado combinou os elementos de um anuário comum já existente com mais funções para os perfis, permitindo que os estudantes buscassem uns aos outros de acordo com cursos, organizações sociais e dormitórios. Assim nasceu o TheFacebook.

Procure, portanto, pesquisar mais sobre como o Facebook foi criado, sobre a trajetória de Zuckerberg, um hacker que mudou e criou uma das maiores corporações de negócios da internet nos dias de hoje.

No Google, há diversos sites com curiosidades e histórias da carreira de Zuckerberg e como ele se tornou uma referência para o assunto.

Antigamente acreditava-se que os hackers eram pessoas que queriam se vingar de alguma empresa, ou adolescentes que queriam ser aceitos por grupos de hackers (ou script kiddies)² e saíam apagando tudo que encontravam. Ou, ainda, eram grandes especialistas de linguagens de programação que eram contratados por algumas empresas para fazerem espionagem industrial, invadindo redes e sistemas de empresas concorrentes.

Hoje em dia ainda existe, por exemplo, a superstição de que empresas que produzem antivírus possuem em suas equipes hackers para criar vírus e disseminá-los em âmbito mundial. Com isso, elas criariam e distribuiriam as chamadas “vacinas” contra estes mesmos vírus.

1.7.1 Notícias de segurança da informação

Diariamente sabemos de uma novidade bombástica no universo virtual da internet.

Em 2013, um dos assuntos que mais chamou atenção quanto ao acesso a informações de pessoas e empresas foi o caso Snowden:

Ex-agente da Agência de Segurança Nacional dos Estados Unidos (NSA), Edward Snowden revelou que ele mesmo espionava e acompanhava, para a NSA, tudo o que eu, você ou praticamente qualquer outra pessoa fazem na internet.

Chamado de Prism, este sistema secreto (?) receberia a colaboração de empresas de telefonia e também de algumas das maiores companhias digitais do mundo, como Facebook, Microsoft®, Apple® e Google®.

Snowden denunciou as práticas de espionagem em uma entrevista porque, segundo ele, “quem deve decidir se os governos devem – ou não – investigar o que as pessoas comuns fazem na internet são os próprios cidadãos”.

² Script Kiddies significa garoto dos scripts, em tradução literal. É um termo depreciativo atribuído aos grupos de crackers inexperientes que desenvolvem atividades relacionadas com segurança da informação, utilizando-se do trabalho intelectual dos verdadeiros especialistas técnicos. Eles não possuem conhecimento de programação e não estão interessados em tecnologia, e sim em ganhar fama ou outros tipos de vantagens pessoais.

A divulgação deste fato alertou pessoas e organizações de vários países para uma prática de ações de espionagem, as quais já se desconfiava estarem sendo realizadas há muito tempo.

Depois de as denúncias terem sido feitas e documentos terem sido apresentados, comprovando as ações de monitoramento realizadas, “caiu a ficha” de todo mundo. Sim, estamos sendo monitorados em quase tudo o que fazemos na internet.

Explicaremos tudo o que envolve o Prism e sua privacidade, leitor, ao navegar na internet. Isto nos ajudará a entender o porquê da necessidade e importância tão grande de segurança da informação, assim como por que regras, políticas e ferramentas de segurança podem ser eficientes de fato.

Em artigo publicado no site TecMundo, Lucas Karasinski explicou detalhadamente como funciona, ou funcionava, o Prism, este sistema de monitoramento de atividades na internet no mundo inteiro.

Segundo Lucas, o jornal americano *Washington Post* e o inglês *The Guardian* apresentaram dois artigos que impressionaram e revelaram muito sobre o grau de segurança das nossas informações e de governos e empresas ao redor do mundo.

Este assunto obviamente foi o sistema Prism, um projeto de colaboração secreta entre NSA, FBI e quase todas as empresas de tecnologia em que confiamos e usamos diariamente.

O Prism forneceu ao governo dos Estados Unidos acesso sem precedentes a informações pessoais, pelo mundo, há pelo menos seis anos. Mas qual é o significado disso, exatamente? Para Lucas Karasinski:

O Prism é na verdade uma sigla para um programa real do governo dos Estados Unidos. De acordo com documentos vazados, ele entrou em ação em 2007, e só ganhou força desde então.

A sua finalidade é monitorar potenciais comunicações estrangeiras valiosas que podem passar pelos servidores dos Estados Unidos, mas parece que na prática seu alcance é bem maior.

Os relatos iniciais sugeriam que o processo funcionava da seguinte maneira: as empresas anteriormente mencionadas (e talvez até outras) recebiam uma diretiva do procurador-geral e do diretor de inteligência nacional.

Elas davam acesso aos seus servidores através da Unidade de Tecnologia de Interceptação de Dados do FBI, a qual por sua vez os retransmitia para os escritórios de tecnologia da NSA.

Ainda existem, como você deve imaginar, filtros para ajudar a lidar com a quantidade de dados recebidos diariamente, os trilhões de bits e bytes que fazem sua identidade e vida online.

Alguma coisa para garantir que apenas os caras maus estão sendo vigiados (será?), e não os cidadãos honestos. Existe sim um filtro, e é ridículo: um analista da NSA precisa ter 51% de certeza de que um assunto é “externo”. Depois disso, carta branca.

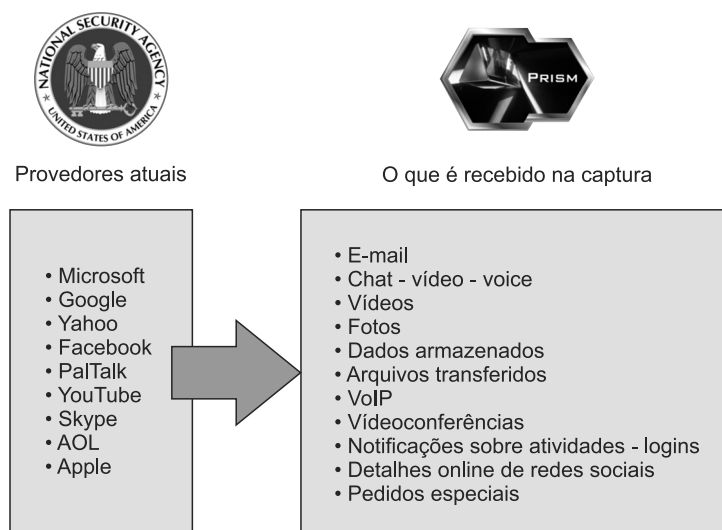


Figura 1.4 – Dados Coletados pelo Prism.

O que é mais preocupante sobre o PRISM não é a coleta de dados.

É o tipo de dado coletado.

De acordo com o artigo do *Washington Post*, isso inclui:

...conversas por vídeo e áudio, fotografias, e-mails, documentos e logs de conexão... [Skype®] podem ser monitorados por áudio quando um dos lados da conversa é em um telefone convencional, e para qualquer combinação de 'áudio, vídeo, chat, e transferência de arquivos' quando os usuários do Skype® se conectam por um computador.

O disponibilizado pelo Google inclui Gmail, chats de voz e vídeo, arquivos do Google Drive, bibliotecas de fotos e vigilância de termos de busca em tempo real.

Veja o quanto de suas informações estão acessíveis nesta situação.

A mesma profundidade similar de acesso também se aplica ao Facebook, Microsoft e ao resto.

Para sermos mais claros: isso abrange praticamente qualquer coisa que você já tenha feito online, e ainda inclui pesquisas no Google® enquanto você está digitando.

Quando a NSA monitora registros de telefone, ela só coleta os metadados deles. Isso significa quem e para quem a chamada foi feita, e de onde ela foi feita, e outras informações gerais.

É importante entender que, até onde sabemos, o conteúdo das conversas não era monitorado ou registrado.

Em contraste, o PRISM pelo noticiário geral que se tem acesso permite acesso total não apenas ao fato de que um e-mail foi enviado – ele permite acesso ao conteúdo destes e-mails e chats.

E observe que, como veremos em capítulo específico de controles de segurança, os e-mails enviados por qualquer pessoa são normalmente criptografados, o que impediria outros de os lerem

sem chave para decodificá-los. Entretanto, isso acontece porque todas as pessoas utilizam as chamadas chaves públicas que são mais simples de serem decodificadas.

De acordo com a fonte do *Washington Post*, eles podem “literalmente vigiá-lo enquanto você digita”. Eles podem estar fazendo isso com você, agora mesmo.

1.7.2 As tendências em segurança

Com o crescimento do uso de sistemas de informação, comércio eletrônico e tecnologia digital, as empresas e as pessoas estão se vendo obrigadas a pensar mais na segurança de suas informações para superar ameaças e golpes, a que estamos expostos todos os dias.

Assim, podemos entender que a segurança da informação veio para minimizar possíveis ataques aos sistemas empresariais e domésticos.

Simplificando, a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro dos princípios de confidencialidade, integridade e disponibilidade.

Os problemas de segurança da informação são em geral provocados por pessoas mal-intencionadas que buscam algum tipo de vantagem, seja ela monetária, política, intelectual etc.

Existe alguma maneira rápida e eficiente de se descobrir uma senha?

Simplesmente perguntar? Ou observar alguém digitando a senha e decorar?

Por mais incrível que isso possa ser, é esta a forma mais simples, mais usada e provavelmente a mais eficiente de se obter informações: simplesmente chegar e perguntar.

Nos próximos capítulos falaremos sobre os ataques e golpes que deram origem a uma área específica da segurança da informação tanto em empresas quanto em nossos computadores, smartphones e tablets.

1.7.3 Mais notícias para você

EA sofre ataque DDoS³, e servidores da Origin ficam fora do ar (6 de jan. de 2014).

Este ataque de negação de serviço certamente foi realizado ao servidor da EA (Electronic Arts), o que derruba os servidores da Origin, e pelo tipo de ataque deve ter impedido os jogadores online no mundo de acessar os serviços desta plataforma de distribuição de games.

Com este ataque, os jogadores no mundo inteiro ficaram durante um tempo impossibilitados de fazer login no serviço de games online e, óbvio, não podiam jogar os

³ Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service) é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Falaremos um pouco mais sobre o assunto mais à frente.

games desta empresa em diversos equipamentos de videogame, incluindo o PC, Xbox 360 e Xbox One, ou até realizar compras na loja online deste site.

Claro que, com um ataque deste, após a realização de manutenção, tudo voltou a funcionar normalmente.

Fonte: Olhar Digital. Acesso em: 3 jan. 2014.

No final de 2013, uma das maiores redes de varejo dos Estados Unidos, em plena época de compras de Natal, viu os dados de cartões de crédito de milhares de clientes serem vazados após os sistemas da empresa terem sido invadidos por hackers. O ataque foi amplamente divulgado em todas as mídias.

Fique de olho!

Ameaças virtuais criadas para tirar vantagem da confiança de usuários em sistemas, aplicativos e redes pessoais alcançaram níveis alarmantes, apontou relatório de segurança da CISCO®. Ainda segundo este fabricante de equipamentos de rede e segurança, as vulnerabilidades e ameaças chegaram ao nível mais alto desde que começou o rastreamento no ano de 2000.

A quantidade de alertas de segurança aumentou 14% no ano passado.

Trojans (falaremos sobre eles a seguir) foram os malwares encontrados com mais frequência, com 27% do total detectado no ano passado. Nos dispositivos móveis, programas mal-intencionados estavam em lojas não oficiais dos sistemas operacionais destes dispositivos.

Há dois anos aproximadamente os principais jornais e meios de comunicação mundiais divulgaram notícias sobre um desconhecido site chamado de WikiLeaks.

O conteúdo apresentado pelo site (documentos secretos de vários países) causou grande repercussão no mundo inteiro. Chegou-se, inclusive, a falar no início da primeira ciberguerra da história. Entretanto, este mesmo conteúdo, de caráter político, colocou em situação constrangedora alguns países no que diz respeito aos direitos humanos, trazendo a público questionamentos sobre como muitos países se posicionam frente a este fato.

O WikiLeaks foi fundado em 4 de outubro de 2006, na Suécia, e construído sob a plataforma de MediaWiki, similar ao da Wikipédia.

O conteúdo do site tem a opção de edição restrita a um seleto grupo de editores, cujo principal editor era o jornalista e ciberativista australiano Julian Assange. Era ele quem publicava a maior parte dos documentos, tornando-se famoso em 2010 com a divulgação de arquivos secretos do governo dos Estados Unidos da América, como documentos relativos à Guerra do Afeganistão e à Guerra do Iraque. Como característica comum, muitos desses documentos denunciavam graves violações aos direitos humanos.

Para especialistas, até mesmo o conteúdo de um site como o WikiLeaks pode ser objeto de uma inclusão de dados fraudulenta. Isso acontecerá se alguma informação for ali postada e esta mesma informação for adulterada visando apenas causar impacto na população e na comunidade internacional, sem ter fundamento verídico.

Continuaremos estudando o que afeta a segurança da informação e buscaremos conhecer melhor as ameaças e problemas que tanto causam.

Existem diferentes áreas de segurança que afetam umas às outras e que são objeto do contexto geral denominado segurança da informação.

A segurança física está inter-relacionada com a segurança da informação, a segurança dos bancos de dados, e no topo desta cadeia encontra-se a segurança do sistema operacional.

À segurança implica diretamente na forma como as operações com sistemas são utilizadas nas empresas.

Tecnologia, hardware, pessoas e procedimentos importam em conjunto como fatores para a segurança da informação, assim como aspectos ambientais, entre eles: terremotos, enchentes, raios, quedas de energia, incêndios etc.

Nos próximos capítulos estudaremos as vulnerabilidades para a segurança da informação.

Vamos recapitular?

Neste capítulo, apresentamos os conceitos básicos da segurança da informação, inclusive mostramos a diferença entre informação e dado. Além disso, demos exemplos de casos graves de violação de segurança.

Mostramos também que existem duas denominações para designar as pessoas que executam estas violações, apesar de uma ser a mais utilizada.

Falamos também que não são somente pessoas que causam problemas para a segurança da informação. Devemos levar em conta aspectos físicos, climáticos e os chamados lógicos, provocados por especialistas ou não.



Agora é com você!

- 1) Pesquise em livros, jornais, revistas e na internet um caso recente de indisponibilidade de informações, perda de confidencialidade ou invasão de sites, e faça uma descrição resumida de três parágrafos sobre o fato ocorrido e quais danos foram causados por violação destes princípios de segurança da informação.
- 2) Assista a um seriado de televisão em que alguém acessa dados, por exemplo do FBI, e responda qual dos princípios está sendo violado no seu entendimento.
- 3) Violação de acesso (acesso não autorizado) com utilização de senha de um amigo ou colega viola qual princípio, conforme apresentado no início deste capítulo?
- 4) Qual a denominação para quem acessa dados não autorizados, destrói dados ou rouba informação de redes, sistemas e computadores?
- 5) O sistema Prism da agência americana NSA, tão comentado nas notícias, violou ao interceptar mundialmente mensagens e conversas na internet qual dos princípios da segurança da informação?
- 6) Demonstre com três exemplos que não estejam no livro a diferença entre informação e dado, no formato da tabela a seguir:

Informação	Dado
------------	------