Segurança da Informação

Resumo

Esse artigo tem como objetivo, apresentar os conceitos gerais de segurança da informação, e de algumas das principais técnicas utilizadas para os mais diversos fins. Além de colocar como o mundo vê esse importante tema da atualidade.

Abstract

This paper aims to present the general concepts of information security, and some of the main techniques used for different purposes. In addition to putting the world sees this important topical issue.tecnology.

Introdução

É imprescindível a importância da Segurança da Informação nos tempos modernos, onde os dados e informações são preciosos, seja para um nível empresarial, ou para simples usuários que mantém os mais diversos tipos de arquivos em seus computadores. De pessoas más intencionadas que possuem conhecimentos suficientes para conseguir praticar invasões de sistemas, de que é preciso se proteger.
Existem diversas técnicas complexas ou não, para que essas pessoas com intenções errôneas possam explorar os mais diferentes tipos de sistemas e obter informações que não deveriam ser acessados por pessoas sem autorização. Neste artigo, você verá, com alguns detalhes algumas dessas técnicas, saber para que servem e como funcionam. Também vamos tomar conhecimento de como o mundo está agindo quanto a esse tema importante, o que está acontecendo, e o que aconteceu para tomar tamanha amplitude. Saber de como o nosso país enfrenta essa realidade, políticas que foram empregadas, leis que foram sancionadas.
Salientar também, o mercado da segurança computacional, qual profissão seguir e como adentrar neste meio.

1.Conceito de Segurança da Informação

Segurança da Informação como o próprio nome sugere, são os artifícios usadas para garantir a proteção do recurso valioso que é a informação, o conjunto de dados, que dá sentido a grandes ou pequenas empresas. Já imaginou, se o Facebook, perde os dados de todos seus usuários, o estrago que isso causaria? Não só na economia, mas de outras muitas formas.
Existem 3 atributos básicos da Segurança da Informação:

Confidencialidade: É necessário que uma informação só seja acessada por quem tem direito a isso. Ninguém não autorizado, pode de maneira alguma, saber do que se trata tal informação. Imaginem uma senha de banco, somente o titular da conta pode ter conhecimentos desses dados, um roubo dessa senha, poderia causar prejuízos. A palavra "secreto", resume bem o significado deste atributo.

Integridade: A informação deve ter garantias que não será alterada, violada sem autorização ou de forma indevida. A originalidade do que for gravado deve ser mantida em todos os sentidos. Por exemplo, você envia um e-mail para seu chefe, mas, de alguma

forma a mensagem é alterada chegando algo indevido para o destinatário. Isso causaria sérios problemas pessoais e também por parte da informação perdida.

Disponibilidade: A informação deve estar disponível a todo e qualquer momento, considerando que, quando o usuário necessite do uso da mesma, receba rapidamente o retorno. Considerando uma requisição no mundo empresarial, onde a chegada ou saída de uma informação seja retroagida, a pessoa que precisa destas, ficará de mão atadas, prejudicando todo andamento do processo que ali se passa.

Estes três princípios devem ser garantidos, para que o sistema esteja dentro do que a Segurança da Informação pede.

1.Atributos da Segurança da Informação

Existe esse cuidado para proteção dos dados, pois há o lado oposto, destinado a obter informações que não deveriam ser acessadas por pessoas não autorizadas.
Partindo da primordia que não existe sistema 100% seguro, afinal, as buscas por vulnerabilidades são intensas, mesmo com os recursos de defesa também atualizando conjuntamente é um confronto bem nivelado.
É partir das descobertas de vulnerabilidades, e as formas de como explora-las que funciona a quebra da segurança da informação. E algumas dessas técnicas já estão espalhadas pela internet, ensinando como usá-las, tornado o uso possível para qualquer simples usuário que queira praticar. Obviamente não se restringe a usuários comuns, existem pessoas dedicadas e até mesmo já profissionais que usam ativamente, a todo tempo, seja por bem ou por mal a habilidade de quebrar a segurança.

O ataque a sistemas é cotidiano, a todo momento algum computador, servidor, site está sendo testado (testes de penetração). E esses ataques são diferentes, tem suas peculiaridades, suas formas especificas de agir. Citamos aqui, alguns dos mais usados, mais conhecidos, como:

Fingerprint e Footerprint – Se trata do levantamento de informações do sistema alvo. É a fase do pré-ataque, é onde é decidido os caminhos que serão seguidos, o tipo de ataque que será usado. Nessa fase não se restringe somente a informações dos sistemas, mas também das pessoas envolvidas nele. Caso o alvo seja um site quaisquer, é de extrema importância saber quem o administra, levantar o máximo de informações possíveis, também não descartando o site, onde através de softwares e serviços disponibilizados gratuitamente como o Whois e o Nmap é possível descobrir detalhes restritos do site, como por exemplo, servidor usado, informações sobre banco de dados, portas abertas, esse tipo de informação que auxilia diretamente na invasão.
Para melhor entendimento é possível se fazer uma analogia com uma casa que será roubada. Antes de mais nada, é preciso fazer um estudo da casa, sua estrutura, suas proteções, seus habitantes. Somente após estar com tudo em mãos, se parte para invasão de fato.

Vírus/Malwares/Trojans – Embora tenha nomes e particularidades diferentes, ambos possuem uma característica em comum, causar danos. Cada qual possui um código malicioso por trás, com objetivos diversos, seja prejudicar o hardware, roubar informações, monitorar o computador, modificar o sistema operacional de forma a prejudica-lo, dentre outros, quase sempre afetando diretamente o sistema ou quem o usa. Vendo essa descrição, logo se conclui que esses "vermes", ferem os princípios da segurança. Para distinção, uma breve descrição de algumas pragas, que afetam milhares de computadores, e muitas das vezes passam despercebidos.

Malware – Programas com códigos maliciosos, com funções para causar danos em um sistema.
Vírus – É um tipo de Malware. Vírus podem se espalhar através de outros softwares e/ou arquivos, desde que seja executado pelo usuário. Ele pode-se propagar pelo sistema, se auto copiando para outros arquivos.
Worms – São mais inteligentes que os vírus, possuem a capacidade de espalharem por autonomia própria, usam do computador que o está hospedando, e procura contaminar mais vítimas (por e-mail, softwares de comunicação, etc).
Trojans – Disfarçam, tomam forma de um software funcional qualquer, e a partir disso, infecta o computador. Tem como funcionalidades principais o acesso remoto e obter informações como senhas e outros dados.
Spyware – São softwares espiões, que monitoram as atividades do usuário no computador.
Rootkit – Causam impacto direto no sistema operacional, alteram registros, modificam dlls, dentre outras formas de prejudicar o sistema.

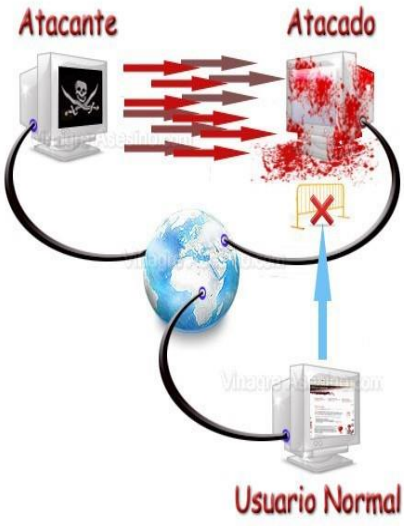
Existem outros tipos, mas são derivações dos já citados, os ditos acimas são os principais, e com eles pode-se perceber os problemas, que arquivos maliciosos podem causar.

Sniffing – Técnica utilizada para monitorar redes através de softwares denominados sniffers, como este tipo de programa pode-se enxergar todo o fluxo de informações que se trafega na rede do alvo. Uma dos famosos sniffers é o wireshark, que permite capturar e navegar interativamente pelo tráfego de uma rede em tempo de execução. Pessoas maliciosas utilizam desse tipo de ataque, para pegar nos pacotes da rede, senhas, informações valiosas e afins, e além do mais, pode também obter não só o

acesso, mas permissão para editar, apagar um determinado objeto detectado. Todavia, também é um facilitador para administradores de redes e outros profissionais que se envolvem com redes de computadores, pois, pode detectar possíveis problemas, intrusos, dentre outras diversas funcionalidades.

Brute Force – O ataque de força bruta, faz diversos testes combinatórios, e randômicos, num espaço de tempo, até que se esgote as possibilidades ou o sistema seja violado. O objetivo é descobrir um campo de senha, ou algo relacionado. O programa que realiza o ataque, simulará diversas possibilidades para senha ou outra coisa (logins, códigos, falsificar autenticações) que deseja ser descoberto, usando combinações de caracteres especificados pelo atacante. É um processo que pode ser muito demorado, dependendo da complexidade da senha (considerando este o objetivo), podendo ficar por anos e anos fazendo testes (obviamente usando recursos de processamento). Pode usar uma lista de palavras especificas para agilizar o teste, utilizando apenas palavras relacionadas com o alvo, assim os testes são feitos apenas com as palavras que estão nesta lista. Este método não é muito eficaz, os sistemas atuais, na maioria das vezes, forçam o usuário a utilizarem de "senhas fortes", justamente para inutilizar esse tipo de quebra de confidencialidade.

DOS/DDOS – São ataques de negação de serviço, tem por objetivo sobrecarregar um determinado servidor, fazendo com que este cai com tanto tráfego que é direcionado para ele. Este tráfego pode ser enviado de um só computador (DOS) , ou utilizando de várias máquinas, conhecidas como zombies, sobre o comando do atacante (DDOS). No DDOS o atacante irá comandar as máquinas zombies, fazendo que estás enviem seu tráfego para o serviço alvo, quando mais a quantidade de computadores à mercê do atacante, maior a efetividade do ataque, podendo derrubar grandes servidores. Esses zombies não funcionam por livre e espontânea vontade, geralmente são máquinas infectadas por vírus, que se tornam "escravas", sendo forçada a enviar tráfego, que o usuário comum não está enviando por conta própria.



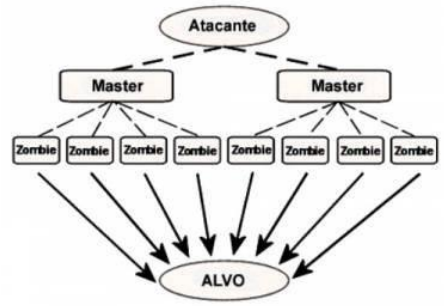


Imagem 1 Imagem 2

Imagem 1 - http://piratadafaja.blogspot.com.br/2011/11/como-fazer-um-ataque-dos-na-linha-de.html
Imagem 2 - http://www.noticiastecnologia.com.br/ataques-dos-anonymous-entenda-como-funciona-osistema-para-derrubar-os-grandes-sites

Este ataque é muito usado devido a sua facilidade de ser feito. Muitos programas como T50 (criado por um brasileiro) e LOIC facilitam muito quem quer fazer o ataque. Além disso, muitos serviços não estão preparados para este tipo de ataque.
Um grande exemplo é quando grandes empresas como a Visa, MasterCard e Paypal que em 2010 caíram perante o DDOS. É importante salientar, que o objetivo desse ataque é derrubar um serviço especifico, e não roubo de dados.

Engenharia Social – Este é um tipo de "ataque" que não necessariamente precisa de softwares, ou recursos computacionais para ser executado. Ele está ligado ao ser humano, ao usuário, este que é a maior vulnerabilidade de um sistema. Usa do poder de enganação, persuasão para obter informações sigilosas. Abusa do fator psicológico, meche com a mente da vítima. Kevin Mitcnick, um famoso hacker, foi um dos responsáveis pela popularização do termo, ele usava de diversas técnicas para ludibriar as pessoas, com fins de diversão ou alcançar algum objetivo. Kevin escreveu o livro A Arte de Enganar, com várias histórias reais, que auxiliam no desenvolvimento do "pensar", ligado a segurança da informação.
Um outro grande exemplo é o filme Prenda-me se for capaz, que mostra a engenharia social funcionando na prática. Com o filme, pode-se ver que essa técnica não fica somente na tentativa de conseguir informações em armazenadas em computadores, muito pelo contrário, pode agir em qualquer segmento social, desde que aplicada corretamente.

Com tantas formas de invadir um sistema, ter acesso a informações de maneira indevida, é necessário também defesas que garantam que os princípios da segurança sejam compridos, garantam a segurança da informação de fato. Um destes meios de proteção é a **Criptografia.** Esse mecanismo age embaralhando senhas convencionais de forma que, mesmo que o atacante tenha acesso a senha, ele não conseguirá decifrar a senha real, barrando-se na embaralhada. Existem muitos algoritmos de criptografia, sendo os mais comuns md5 e sha-1, responsáveis por essa mistura, cada qual diferenciando seus métodos. Resultado dessa mistura é chamado de hash, ou seja, a senha criptografada. Não existe o reverso de um hash. É uma área da matemática, envolve cálculos complexos, sempre buscando a melhor forma de se conseguir uma criptografia inquebrável. Não somente senhas são passiveis de criptografia, mas também arquivos, diretórios, dispositivos de armazenamento, ou até mesmo uma máquina inteira.
Não podemos dizer que algo criptografado não pode ser quebrado, porém a dificuldade para tal é extrema. Técnicas como a brute force podem ser usadas, mas vale lembrar sua ineficácia. O maior adversário da criptografia são sites como o *https://hashkiller.co.uk/* que geram senhas criptografadas e armazenam em seu enorme banco de dados, que podem ser consultados. Por esse motivo, é importante o uso de "senhas fortes".

Um caso muito conhecido da criptografia aqui no Brasil é de Daniel Dantas, um famoso banqueiro que criptografou seu computador usando PGP (ferramenta líder de mercado) e o Truecrypt (ferramenta que pode ser encontrada gratuitamente na internet), onde supostamente existiam provas de vários crimes cometidos. A polícia (especialista na área) em posse do computador não conseguiu descriptografar a máquina (nem mesmo com a ajuda do FBI). Casos como esse provam o poder da criptografia.

Além da criptografia, que é um mecanismo que exige um certo conhecimento para se protege, existem alguns bons comportamentos e softwares que podem ajudar a manter um sistema seguro, seja o seu computador pessoal ou de uma pequena/grande empresa.

Antivírus – Ferramentas que detectam e eliminam arquivos maliciosos (vírus). Monitora o computador e alguns também toda navegação na internet, assim se algo de errado é encontrado, é imediatamente bloqueado. Existem diversos softwares no mercado, alguns grátis, outros pagos.

Firewall – É uma barreira de "fogo", que age diretamente no trafego da rede, e se algo de estranho aparece é bloqueado. Monitora todo o fluxo de dados, podendo assim fazer o bloqueamento de conteúdo malicioso. É nativo nos sistemas operacionais modernos, podendo também ser configurado da maneira desejada. Mesmo já presento nos sistemas, há também firewalls comerciais, com proteções mais amplas, um mercado que atende principalmente o setor empresarial.

Independentemente de ter ou não uma defesa, o que mais importa é como o usuário vai fazer uso de sua máquina. É necessário tomar os devidos cuidados ao navegar pela internet, baixar arquivos, acessar sites, tomar precaução de onde irá seu clique. Agindo corretamente, juntamente com os recursos de proteção, as chances de ter a segurança quebrada diminui bruscamente.

2. Cenário Mundial

Não é de hoje que segurança é um tema que atrai atenção, antigamente informações de guerra, ou quais que eram de importância de pessoas com poder, passavam por métodos engenhos para serem escondidas e protegidas das pessoas erradas. Porém toda essa atração nem sempre foi assim. Essa atenção foi difundida principalmente depois que Edward Snowden em 2013 vazou vários arquivos confidenciais da NSA, tornando claro, vigilância que acontece na rede mundial de computadores. Além disso casos mundiais, como da Playstation Network (77 milhões de pessoas sem acesso), Epsilon (60 milhões de e-mails vazados, Target (110 milhões de dados vazados) que repercutiram mundialmente na mídia, ajuda a afirmar que dados estão sendo roubados, sistemas estão sendo invadidos.

Uma guerra hoje não é somente feita com armas, soldados, pelo contrário, ela saiu do meio físico e passa também a fazer parte do meio tecnológico. Computadores protegem segredos de estados, computadores controlam lançamento de bombas, tais exemplos confirmam o porquê das grandes potências mundiais investirem não só em armamento, mas também na proteção de seus sistemas, principalmente onde estão seus maiores segredos. Quando se fala em segurança nacional, tenha certeza que a informação está envolvida nesse contexto. Contudo não só defesa, mas também ataque, grandes nações, abusam da espionagem, o controle de dados é de suma importância para continuar no topo, pesquisas para o desenvolvimento da espionagem global estão sendo feitas para manter o controle.

Falando em Brasil, é deprimente quando se coloca segurança da informação em pauta.
Alvo de ataques contínuos e espionagens de grandes países, não se dá o verdadeiro valor para pesquisas no ramo, sendo quase nula a proteção de estado. É comum ver sites do governo sendo invadidos, e-mails e outras informações sendo vazadas.

No país vigora uma lei, sancionada em 2012, depois do escândalo envolvendo Carolina Dieckman (que leva o nome da lei) que teve fotos intimas vazadas na internet. Em suma a lei diz a respeito de invasões:

"Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita"

Alvo de críticas de especialistas, não é algo que de firmeza, não chega nem perto do que o país precisa. Muito pelo contrário, é facilmente "quebrada" num tribunal com um certo conhecimento.

Outra lei, bem atual (2014) muita contestada é o marco civil da internet. Esta estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Garante proteção à privacidade de usuário, liberdade de expressão e retirada de conteúdo do ar, garantia de neutralidade de rede e regulamentação da mesma.
Com ela não afeta muito diretamente a vida do usuário, que continua se conectado normalmente, mas agora tendo um artificio que garante seus direitos.

É baseado nessas leis, que o cenário nacional vai se baseando. Ainda bem degradado e caminhando a passos curtos, vem-se desenvolvendo.

3. Cenário Profissional

O mercado de segurança da informação é bem amplo e diversificado (mundialmente falando), são várias as áreas que uma pessoa pode escolher para trabalhar. É possível essa amplitude, pois está diretamente ligado com outros setores da tecnologia da informação, como: banco de dados, infraestrutura e servidores, aplicações web/mobile, desenvolvimento de software e afins. Sendo assim um profissional pode-se especializar na proteção de um determinado setor. Também é comum a consultoria/analise de segurança e cargos mais de administração e gerência da segurança.

Para chegar num nível profissional é necessário muito estudo. Certificações é algo quase que obrigatório para alguém que quer seguir neste ramo. CompTIA, CEH[1], ECSA[2], LPT[3], certificações CISCO são algumas das mais pedidas no mercado, existindo diversas mais especificas para a função que deseja desempenhar.

Conclusão

Claramente a segurança da informação tem um grande impacto não só na tecnologia, mas sim no mundo inteiro. A cada segundo do dia, alguém está tentando fazer algum ataque em algum sistema, seja como forma de trabalho (bem) ou para obter dados (mal). Com esse fato, as empresas e pessoas com dados sigilosos precisam estar preparadas, precisam estar com o máximo de segurança, para evitar possíveis catástrofes. Vivemos num mundo onde a informação tem extremo valor, quem as tem, possui uma grande responsabilidade de mantê-las conforme os atributos primordiais de segurança dizem.

1- Certified Ethical Hacker
2- EC- Council Certified Security Analyst
3- Licensed Penetration Teste

Referências

http://culturadigital.br/marcocivil/
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojansworms-e-saiba-como-se-proteger.html