COMO APRENDER SEGURANÇA DE VERDADE

06/12/2013

Continuando a séria de artigos que estou escrevendo a pedido da 4Linux, gostaria de discutir um pouco a respeito do aprendizado de segurança da informação.

Continuando a séria de artigos que estou escrevendo a pedido da 4Linux, gostaria de discutir um pouco a respeito do aprendizado de segurança da informação.

Muitas vezes me perguntam o que fazer para de fato entender os conceitos envolvidos em segurança e como se livrar dos direcionamentos dados por empresas em suas próprias tecnologias.

Minha resposta poderá parecer um pouco extremista, mas creio que a única forma de se entender segurança de verdade esteja no entendimento real da tecnologia de informação utilizada. As ameaças à segurança da informação armazenada, gerada ou manipulada em um computador, estão sob as mesmas restrições que quaisquer elementos computacionais, ou seja, não existem milagres, apenas o que um computador pode ou não fazer.

Em minha opinião (e compartilhei tal opinião em diversas palestras, tanto no Brasil quanto no exterior) é de que existe um desiquilíbrio entre quem compra e quem vende segurança da informação. Esse desiquilíbrio foi muito bem explicado pelo economista George Akerlof [1] em seu paper 1729879058***"The Market for Lemons: Quality Uncertainty and the Market Mechanism"***. O desequilíbrio - chamado de assimetria daqui em diante - no caso de segurança da informação é relacionado ao entendimento das tecnologias e dos problemas que as mesmas visam resolver. Neste caso, vemos que as empresas de segurança definem quem são seus "experts" e os clientes, por não terem acesso a mesma base de conhecimento e as mesmas informações, acabam por aceitar que tais vendedores são de fato "experts" no assunto.

Infelizmente remover este tipo de assimetria é extremamente difícil , e como discutido no artigo mencionado, é algo que um participante do mercado em si não conseguiria fazer sozinho por meio de fatores econômicos. Com isso cabe a outros elementos participarem, e aqui já estendo o debate gerado no artigo anterior, sobre o papel do governo:

- Incentivos governamentais em educação apropriada -> Difíceis de se evitar o lobby das empresas. Também é difícil formar os educadores;

- Influência da comunidade Open Source -> Pra mim a melhor forma. A comunidade Open Source já é amplamente ativa quando o assunto é desenvolvimento de tecnologias e possui boa parte do conhecimento necessário para o entendimento de segurança da informação. Também não possui os interesses comerciais e esta disposta a contribuir. A melhor forma do governo contribuir seria portanto investindo nestas comunidades;

- Acadêmicos -> Alguns professores já conseguiram sair do paradigma publicação como sendo a maior prioridade e entendem que o sistema precisa ser melhorado [2]. Exceções terão de existir para que o conhecimento seja trazido para a academia e então replicado;
E com isso volto a questão inicial: como uma pessoa pode fazer para aprender segurança e se desenvolver nesta carreira?
Primeiramente, minha resposta sempre envolve fazer com que a pessoa entenda o que é segurança da informação, e tentar desmistificar o que são pesquisas na área e o que são os "hackers":

- Segurança da Informação: uma área que envolve diversoss ramos do conhecimento humano, entre eles a computação (também envolve, por exemplo, ciências comportamentais, para se entender e evitar ataques de engenharia social, segurança física pois a informação também está em meios físicos e assim por diante);

- A segurança da informação computacional (comumente o interesse das pessoas que me perguntam) envolve também diversas áreas da computação:

- Sistemas Operacionais;

- Banco de Dados;

- Redes de Computadores;

- Programação;

- Saber do que se gosta e escolher de acordo é o principal elemento para o sucesso;

- A computação, e segurança da informação em especial, é uma área em constante desenvolvimento, portanto estar "antenado" é fundamental;

- Não existe a melhor ou pior parte, ou a parte menos interessante e a mais interessante, as pessoas têm suas próprias preferências. O generalista em geral acaba sendo o cliente desinformado. O ideal é se especializar e, então, expandir seu conhecimento para as partes que influenciem também sua

tarefa: por exemplo, se você prefere a parte de segurança de código, eventualmente terá algum conhecimento de redes quando for desenvolver aplicativos que utilizem este tipo de ambiente.

- Hackers: são pessoas como quaisquer outras, mas que possuem um nível de curiosidade e busca de aprendizado que os diferenciam. Em geral os hackers são pessoas bastante práticas, portanto, tendem a quebrar regras que não fazem sentido e apenas atrapalham atividades (sejam elas em empresas, em casa, ou simplesmente algo que tenham vontade). A maioria das pessoas de segurança não se tornam hackers e nem deveriam almejar tal coisa. O mito foi criado simplesmente pela ignorância das pessoas de fora da comunidade.

Dito tudo isso, a pergunta ainda não foi respondida, e deve ser por isso que até hoje não havia de fato parado para escrever sobre o assunto. A base que deve ser criada é fundamental para chegarmos ao meu ponto:

- Open Source: desenvolva, participe, entenda.

Muitas pessoas vão dizer que alguém pode se interessar em trabalhar com sistemas Microsoft, ou que os mesmos são a maior parte do mercado, que em Open Source não existe dinheiro etc. As pessoas que dizem isso são, semdúvidas, aquelas que compram sem saber, apesar de realmente pensarem que sabem. Elas são as mesmas que participam dos testes conduzidos pelos fabricantes e acham que estão testando o que precisam. São aquelas que definem os requerimentos de segurança, mas não têm de verdade a menor ideia do que estão fazendo e são a maior razão para vermos o número de incidentes crescendo ao invés de diminuir, apesar dos investimentos serem enormes.

Desmistificando o meu ponto:

1-) O Open Source lhe propicia o aprendizado rápido, real entendimento das implementações e objetivos de um sistema, desafios na proteção da informação, limitações e áreas de estudo;

2-) O Open Source lhe permite utilizar diferentes tecnologias e praticar as limitações das mesmas;

3-) Talvez o mais importante dos pontos para aqueles que desejam se iniciar na profissão, mas apenas veem oportunidades de vagas monótonas (como operadores de soluções de segurança e não como engenheiros das mesmas):

- Compartilhe o que aprendeu, as pessoas e empresas veem isso;

- Inove, divulgue, debata;

Pode parecer ilusão minha pensar assim, não é mesmo? Mas o leitor se surpreenderia com o número de vezes que fui conversar em uma empresa e as pessoas de lá conheciam o meu trabalho. Não pelo que fiz em meus trabalhos anteriores, mas pelo que divulguei para comunidade durante meu tempo livre.

Todas as vezes que me perguntam sobre a carreira, as pessoas também mencionam treinamentos e livros. Sou um viciado em livros, pra mim todos os livros são bons:

1-) Se o livro possui informações erradas, e eu as absorvo sem de fato testá-las, eu que sou um péssimo estudante. Saibam a diferença entre LER e ESTUDAR. Ler significa simplesmente sentar e ver o que está escrito. A absorção é mínima e você confia totalmente no autor. ESTUDAR significa praticar o que se lê. Validar, duvidar, provar.

2-) Se o livro possui apenas informações que já sei, não precisarei ESTUDAR, apenas LER, mas ainda assim aprendo novas formas de expor o meu ponto de vista, facilitando assim a comunicação no futuro: e acreditem, isso fará diferença na carreira (justamente pelo ponto de poder palestrar e divulgar suas pesquisas, lhe dando ainda mais visibilidade)

Hoje em dia existe excesso de informações, então, como regra, quando eu estudo crio uma árvore mental (mindmap e softwares do tipo podem lhe ajudar no começo):

- Não desvio do meu ponto de aprendizado a menos que seja um item fundamental para meu aprendizado;

- Itens não relacionados entram em uma nova parte da árvore, para leitura/estudo posterior;

Se eu tiver de recomendar um website, eu recomendaria este: http://www.phrack.org (muito bom para quem deseja entender mais sobre a área de pesquisas em segurança da informação).

Algumas pessoas julgam que sou contra treinamentos por eu dificilmente recomendar algum. Na verdade pelo contrário. Eu entendo que treinamentos são a forma mais rápida de se receber uma informação já processada, preparada. Mas, as pessoas esperam mais do que deveriam, e as empresas oferecem menos do que poderiam:

1-) As pessoas esperam que em um treinamento vão aprender tudo que precisam para desempenhar a função:

- A prática é essencial para entendimento real de quaisquer itens aprendidos, pois diversas dúvidas surgiram apenas com o uso de algo aprendido em situações fora do controle do ambiente de treinamento;

- O treinamento possui uma carga horária limitada e visa condensar as informações essenciais do assunto. Mesmo que tal carga horária seja apropriada, não irá e nem deveria cobrir tudo que existe e exceções. Isso apenas se obtém com a prática;

2-) As empresas oferecem menos do que poderiam:

- Infelizmente muitas empresas oferecem treinamentos com instrutores que jamais praticaram o item ensinado: isso faz com que as melhores lições a serem absorvidas em um treinamento, que são as reais, sejam perdidas. Um instrutor que apenas segue o material irá falhar em oferecer exemplos reais da experiência que envolvam o aluno e que fazem com que a aplicabilidade do conteúdo seja ainda melhor;

- O material desenvolvido muitas vezes não recebe o investimento correto e em diversas situações a carga horária é menor do que deveria ser para um apropriado ensino do conteúdo, mas ainda assim sobram horas de conteúdo em que o instrutor acaba sendo prolixo com itens que são claramente desperdício de tempo, por exemplo, em um treinamento avançado sobre um software, aprender a instalar tal software);

A melhor forma de se escolher o treinamento adequado e de se saber se você realmente precisa de um treinamento sobre o assunto é:

1-) Verifique a experiência do instrutor no tópico a ser ensinado. Por exemplo, se você vai ter aulas sobre exploração de software, verifique quantos exploits o instrutor já divulgou, quantas falhas já encontrou e assim por diante. Procure, por exemplo, diferenciar carreiras similares, para evitar ser confundido: Por exemplo, uma pessoa que divulga falhas em software ou uma pessoa que escreve um exploit, não é um pentester (pessoa que testa a segurança de empresas);

2-) Valide que o material do treinamento é apropriado. Peça informações para a empresa sobre o conteúdo, como o mesmo foi desenvolvido, quem o desenvolveu, quando foi atualizado, se houveram revisões, e etc;

3-) E mais importante: tenha certeza que você possui os pré-requisitos para aquele treinamento. Lembre-se sempre que o interesse é mais seu em

aprender do que da empresa em ensinar (não importa quão honesta seja tal empresa).

Se você gostar deste artigo e ele lhe incentivar a fazer algo, não exite em me enviar um e-mail com um link para seu projeto.

[1] Akerlof, George. "The Market for Lemons: Quality Uncertainty and the Market Mechanism". 1970.
[2] Bratus, Sergey. "Pwnie Awards: Sergey Bratus nomination". Link: http://pwnies.com/nominations/. Acessado em: 10/20/2013.

Sobre o autor

Rodrigo Rubira Branco (BSDaemon), atua como pesquisador sênior no centro de excelência em segurança da Intel . Foi fundador do projeto Dissect || PE de análise de malware e palestrante em diversas conferências nacionais e internacionais, tais como Blackhat, Defcon, Hack in The Box, XCon e Hackito.

Membro do comitê técnico de diversas conferências (Blackhat Brasil, Hackito e Nosuchcon, por exemplo) também foi palestrante principal (keynote) em eventos fora do Brasil e em território nacional. É organizador do evento Hackers to Hackers (H2HC), maior e mais antigo evento de pesquisas em segurança da informação na América Latina. Atuou em diversas empresas, tais como Check Point (como Chief Security Research) e Qualys (como Diretor de Pesquisas de Vulnerabilidades e Malware). Também é conselheiro do Instituto Coaliza.

Em 2011 foi homenageado pela Adobe como um dos contribuidores principais em vulnerabilidades nos produtos da empresa. Brasileiro convicto (apesar de ter morado em Israel, Dubai e atualmente nos Estados Unidos), é membro do Comitê Técnico da RENASIC, ligada ao Centro de Defesa Cibernética (CDCiber) do Departamento de Defesa Brasileiro.