Segurança na Web: Uma Janela de Oportunidades

Uma mensagem do OWASP Brasil ao Governo Brasileiro

Março de 2011

Sumário Executivo

O OWASP (Open Web Application Security Project)[1] é uma comunidade mundial e aberta, focada em melhorar a segurança dos sistemas de software e conta com diversos capítulos em cidades brasileiras. Este documento apresenta a visão da comunidade brasileira do OWASP sobre como o governo brasileiro pode atuar para melhorar a segurança na Internet.

Neste documento, apresentamos sugestões e recomendações a respeito de políticas públicas, legislação e outras atividades que acreditamos que poderiam contribuir para a melhoria do ambiente de segurança na internet brasileira.

As recomendações são divididas conforme o foco de cada órgão:

- legisladores
- defesa do consumidor
- controle
- ensino e pesquisa
- todos os órgãos públicos

As recomendações não tem dependências entre si, mas acreditamos que a máxima eficácia ocorre com a implementação de todas as recomendações. A melhoria da segurança na Internet brasileira poderia trazer diversas vantagens competitivas para o país, como a atração de investimentos, capacitação de mão-de-obras e o desenvolvimento de uma indústria capaz de exportar produtos e serviços de alto valor agregado.

Os especialistas brasileiros participantes do OWASP estão dispostos a contribuir para que o país avance na direção certa e podem servir de corpo consultivo ou de ligação com especialistas estrangeiros, caso seja necessário. O OWASP não tem fins lucrativos e os especialistas envolvidos trabalham como voluntários.

[1] http://www.owasp.org

A insegurança na Web

A Internet é hoje uma realidade na vida da maioria das pessoas, como mostra a evolução das estatísticas de quantidades de usuários. O IBGE indicava em 2009 que 27,4% dos domicílios brasileiros tinham acesso à Internet e que 67,9 milhões de pessoas eram usuárias de Internet nesse mesmo ano[2]. As pesquisas também indicam um crescimento acelerado do número de internautas, com um aumento de 112,9% entre 2005 e 2009.

As alternativas de acesso à Internet também se diversificaram e agora incluem desde os tradicionais telecentros e *lan houses*, até os acessos via celulares, passando pelos acessos discados e de banda larga. Assim, a gama de usuários vai desde o usuário casual, que acessa a partir de um computador público, aos usuários "sempre conectados", que acessam do computador ou do celular a todo instante e onde quer que estejam.

Qualquer que seja a frequência ou a modalidade de acesso, é inegável que a Internet hoje faz parte do cotidiano das pessoas. As empresas também dependem cada vez mais da Internet como ferramenta de negócio. Mesmo desconsiderando negócios que existem exclusivamente na Internet, hoje é muito difícil encontrar alguma organização que não dependa do uso da Internet de alguma forma. Com o advento da Nota Fiscal Eletrônica, a Internet ganha uma importância ainda maior no dia-a-dia das empresas.

Também o governo brasileiro tem investido no uso de estratégias de e-gov, ou governo eletrônico, que consistem em prover serviços à população através da Internet. O exemplo mais importante nesta área é, sem dúvida, o Imposto de Renda da Pessoa Física, que em 2011 passou a ser aceito somente em formato eletrônico. Outro exemplo de larga escala é o SiSU - Sistema de Seleção Unificada do Ministério da Educação. Outros serviços, embora não sejam propriamente serviços disponíveis na Internet, têm características semelhantes e têm o potencial de parar o país, como o Sistema de Pagamentos Brasileiro (SPB), mantido pelo Banco Central.

O Poder Judiciário também caminha a passos largos em sua informatização e na utilização da Internet para prover serviços aos cidadãos. Exemplos são a larga utilização de processos eletrônicos[3] e as consultas de andamentos pela Internet. Muitos tribunais estudam formas de permitir a juntada de documentos e a abertura de processos por meio eletrônico, principalmente via Internet.

---

[2] http://www.ibge.gov.br/home/presidencia/noticias/noticia_visualiza.php?id_noticia=1708

[3] http://www.conjur.com.br/2007-mar-21/lei_processo_eletronico_forca_modernizacao_justica

No aspecto comunicação, a Internet também se incorporou e também alterou a rotina de milhões de pessoas. O email, ou correio eletrônico, já é quase tão popular quanto o telefone. Os sistemas de mensagens instantâneas, como MSN Messenger ou Google Talk, são utilizados por grande parte da população como ferramentas de trabalho ou para o lazer. As rede sociais, como Facebook, Orkut ou Twitter, são uma realidade na vida de pessoas e empresas e ganham importância como ferramentas de formação de comunidades e também para os negócios.

Embora esteja se tornando essencial para a sociedade, a Internet é uma infraestrutura inerentemente insegura. Projetada na década de 1960 para resistir a um ataque nuclear, a Internet é capaz de continuar operando mesmo que ocorra uma catástrofe em parte da rede. No entanto, esta infraestrutura depende de uma grande quantidade de programas de computador, o chamado *software*. O software é que define as regras de funcionamento dos computadores, celulares e demais componentes da Rede Mundial.

Assim como em toda atividade humana, o desenvolvimento de software está sujeito a erros. Os erros existentes em um software podem levar a falhas, incluindo falhas de segurança. Laurence Lessig, professor de Direito da Universidade de Harvard, definiu que “Code is law”, ou seja, o software é a lei que rege a Internet. Como consequência, as "leis" que regem a Internet contém falhas e estas falhas podem causar problemas para a segurança dos usuários da rede.

Falhas de segurança na Internet são comuns e costumam fazer parte do noticiário. Vários são os casos divulgados pela polícia de criminosos que se utilizam da Internet para cometer seus crimes. Em grande parte dos casos, os crimes são possíveis devido à falta de sistemas que apresentem um nível adequado de segurança. As fraudes bancárias são talvez o maior exemplo de exploração de falhas de segurança, mas as fraudes a outros tipos de sites e sistemas existem e podem causar danos à população.

A dependência da sociedade em serviços via Internet é tanta que a mera indisponibilidade de alguns desses serviços (muitas vezes causada por indivíduos mal intencionados utilizando técnicas que exploram falhas de segurança da infraestrutura de Internet) é manchete nos telejornais, como a indisponibilidade de sistemas governamentais de grande porte (Denatran, IRPF[4], SiSU[5]).

O CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, é o órgão do Comitê Gestor da Internet no Brasil que coleta informações sobre ataques à Internet brasileira. As estatísticas do CERT.br[6] mostram que a quantidade de ataques a redes brasileiras aumentou de 3107 em 1999 para 358343 em 2009, um aumento de 100 vezes em 10 anos.

---

[4] http://noticias.uol.com.br/cotidiano/2011/03/02/apos-pane-sistemas-do-detran-e-do-ir-estao-estaveis-diz-serpro.jhtm

[5] http://oglobo.globo.com/educacao/vestibular/mat/2010/03/17/enem-nova-falha-no-sistema-frustra-estudantes-916087399.asp

[6] http://www.cert.br/stats/incidentes/

A situação da segurança na Internet é delicada e tende a se agravar a medida que a sociedade passa a depender cada vez mais dessa infraestrutura. Numa analogia com recente crise do mercado financeiro (crise dos subprimes do mercado imobiliário americano), temos um ecossistema pujante de aplicações e sites na Internet cuja base não é solida o bastante. O risco da base desse ecossistema ruir é real, assim como aconteceu com o mercado financeiro, e as consequências poderiam ser devastadoras para toda a sociedade. Assim como no caso dos mercados financeiros, solidificar as bases da infraestrutura é importante e o custo é certamente menor do que esperar que aconteça uma crise antes de agir.

O Brasil foi bem menos afetado pela crise do subprime do que outros países já que havia construído uma base sólida para seu mercado financeiro. É hora de aprendermos com essa experiência e nos prepararmos também em outros setores importantes da nossa economia e do nosso cotidiano.

O Projeto OWASP

O OWASP (Open Web Application Security Project)[7] é uma comunidade mundial e aberta, focada em melhorar a segurança dos sistemas de software. Existem mais de 80 Capítulos locais do OWASP ativos em todas as regiões do globo, sendo 8 deles no Brasil, que congregam os principais especialistas mundiais em segurança de aplicações.

Sendo uma comunidade aberta, o OWASP se dedica a capacitar as organizações para que sejam capazes de conceber, desenvolver, adquirir, operar e manter sistemas que sejam confiáveis. Todas as ferramentas, documentos, fóruns, e os capítulos do OWASP são gratuitos e abertos a qualquer pessoa interessada em melhorar a segurança de aplicações.

O OWASP é um novo tipo de organização. Nossa liberdade com relação a pressões comerciais permite-nos fornecer informações imparciais, práticas e econômicas sobre a segurança de aplicações. O OWASP não é afiliado a qualquer empresa de tecnologia, apesar de apoiar o uso informado de tecnologias comerciais de segurança. Como muitos projetos de software open-source, o OWASP produz diversos tipos de materiais de uma maneira colaborativa e aberta.

Os projetos desenvolvidos incluem documentos e ferramentas importantes no cenário da segurança de aplicações e também importantes congressos nessa área. Todos os projetos do OWASP são publicados com licenças de software livre ou Creative Commons[8].

O OWASP não tem fins lucrativos e seus associados participam em suas atividades de forma voluntária. Toda a arrecadação do projeto advém de doações e é utilizada no suporte a suas atividades e de sua infraestrutura.

[7] http://www.owasp.org

[8] http://www.creativecommons.org.br/

O que pode ser feito?

Tendo em vista a importância do tema, é imperativo que o governo brasileiro atue no desenvolvimento de um mercado capaz de produzir software com um nível de segurança adequado ao seu uso e à criticidade das informações que processa ou armazena. Em seguida, listamos algumas recomendações do que pode ser feito para melhorar o panorama da segurança de software no Brasil.

Nós acreditamos que as ações aqui propostas tem o potencial para melhorar a segurança dos sistemas utilizados por milhões de pessoas e também para fomentar uma indústria pujante, capaz de colocar o Brasil na vanguarda mundial, gerando prosperidade para o país.

Por legisladores

O atual mercado de software apresenta incentivos que privilegiam as funcionalidades em detrimento da segurança. Como consequência, todos acabam vítimas da falta de segurança existente hoje no ambiente da Internet. É necessário que o governo atue de forma a criar incentivos para a adoção de práticas seguras no desenvolvimento de sistemas e para responsabilizar pessoas e organizações que não tratem adequadamente os aspectos de segurança de aplicações.

Algumas sugestões de ações são:

Permitir e incentivar pesquisas sobre ataques e defesas cibernéticas

As punições aos criminosos digitais são extremamente necessárias e a posição defendida pelo OWASP não é a criação de mecanismos para a proteção de atividades ilegais ou nocivas à sociedade. No entanto, o OWASP percebe que algumas iniciativas de legislar a respeito de crimes eletrônicos podem também dificultar atividades legítimas e necessárias de pesquisas de vulnerabilidades de segurança.

Entendemos que a legislação deve focar na intenção, criminalizando atividades que objetivem causar danos à sociedade e permitindo atividades de pesquisa, que beneficiam a sociedade pela criação de conhecimento crucial para a melhora da segurança dos sistemas.

Requerer a publicação de avaliações de segurança

A disseminação de informações a respeito de vulnerabilidades de segurança é essencial para permitir que a sociedade se proteja de ataques que explorem estas falhas. Hoje sabemos que os criminosos digitais participam de redes de troca de informações e têm amplo acesso a descrições de falhas e novas técnicas de ataque. Ou seja, os criminosos tem hoje mais acesso às informações do que as equipes responsável pela manutenção da segurança das redes de provedores, empresas ou do governo.

Num paralelo com o setor de aviação, onde as falhas são investigadas a fundo e os resultados das investigações são publicados, é importante que as falhas encontradas em sistemas informatizados e os descritivos dos ataques sofridos pelas organizações públicas e privadas sejam amplamente divulgados, permitindo a toda a sociedade aprender com os problemas já ocorridos de forma a evoluir o estado da segurança dos sistemas dos quais dependemos.

Criar uma agência para tratar os aspectos de divulgação de falhas de segurança

Com a publicação de leis exigindo a divulgação das falhas de segurança, será importante regular esta atividade. Sugerimos a criação de uma agência governamental especializada para regular e gerir as atividades de troca de informações sobre vulnerabilidades de segurança de forma ética e responsável, inclusive com poder para punir pessoas e organizações que atuem de forma nociva à sociedade.

Exigir o cumprimento de requisitos mínimos de segurança em contratos governamentais

O poder de compra do Estado não pode ser ignorado e deve ser usado em favor da sociedade. Com relação à segurança de software, o governo pode definir critérios mínimos de segurança e exigir qualificação e o uso de técnicas de proteção nos sistemas fornecidos ao governo. Um aspecto importante é a possibilidade de responsabilizar os fornecedores em caso de falhas na segurança dos sistemas.

Responsabilizar organizações que não tratem com diligência os aspectos de segurança de aplicações

Assim como os fornecedores governamentais, quaisquer organizações devem ser legalmente responsáveis pela segurança dos sistemas que operam ou comercializam. A legislação deve prever a possibilidade de punição para as organizações que não tomarem providências adequadas para garantir a segurança de seus sistemas. Os fornecedores das tecnologias utilizadas devem ter responsabilidade solidária e objetiva, nos moldes do Código de Defesa do Consumidor.

Exigir que a administração pública tenha acesso às atualizações de segurança de qualquer software durante a sua vida útil

É imperativo que os sistemas utilizados pelos órgãos públicos estejam atualizados com todas as correções de segurança, de forma que não sejam afetados por vulnerabilidades já conhecidas.

Desta forma, é necessária legislação que determine que a administração pública tenha acesso às correções de segurança dos sistemas que utilizar enquanto durar a vida útil desses sistemas e independentemente da existência de contratos de manutenção.

Exigir a abertura do código fonte de aplicativos utilizados pela administração pública cuja vida útil tenha terminado

É bastante comum que fabricantes de software restrinjam o tempo de vida útil de seus sistemas, principalmente por causa do lançamento de novas versões desses mesmos sistemas. Ao final da vida útil definida para um software, os fabricantes deixam de publicar atualizações e correções de segurança, o que aumenta o risco das organizações que ainda dependem dessas versões.

É também bastante comum em órgãos governamentais o uso de sistemas que já foram abandonados pelos fabricantes mas que atendem às necessidades de administração pública. Para permitir que o governo se proteja em caso de falhas nesses sistemas, é necessária a criação de legislação que obrigue os fabricantes a tornar disponível o código fonte desses sistemas para que a administração pública tenha a possibilidade de realizar as manutenções de segurança necessárias, uma vez que o próprio fabricante não vai mais manter o sistema. O fabricante pode também escolher disponibilizar a versão mais atual do software, desde que não haja custo para o erário.

Eliminar licenças de software que isentam os fabricantes da responsabilidade com a segurança de seus produtos

Muitas das licenças de software utilizadas atualmente restringem a responsabilidade do fabricante do software em caso de falhas de segurança. É importante haver legislação que impeça um fabricante de software de se eximir da responsabilidade pela segurança dos produtos que comercializa.

Para evitar distorções no mercado de software, a responsabilidade dos fabricantes pode ser limitada ao valor pago pelo sistema.

Por órgãos de defesa do consumidor

Nosso entendimento é que a proteção das informações dos clientes faz parte das práticas necessárias de proteções do consumidor, assim como o fornecimento de sistemas livres de defeitos, em especial defeitos que possam comprometer a segurança de seus usuários. Assim, as entidades

de defesa do consumidor podem e devem atuar de forma a melhorar o panorama de segurança para os consumidores.

Sugerimos as seguintes ações:

Atuar para restringir o uso de licenças de software abusivas

Esta ação é similar e complementar ao item "Eliminar licenças de software que isentam os fabricantes da responsabilidade com a segurança de seus produtos", descrito acima.

Exigir que os fabricantes divulguem informações inteligíveis sobre o nível de segurança de seus produtos e/ou serviços

Assim como os fabricantes de produtos eletro-eletrônicos precisam divulgar as informações sobre consumo de energia de seus produtos, o consumidor tem o direito de saber sobre as características e o nível de segurança proporcionado pelos sistemas informatizados que utiliza.

É imperativa a criação de um sistema que permita aos consumidores verificar o nível de segurança provido como parte de seu processo de decisão de consumo. Tal sistema permitiria diminuir as externalidades perversas do mercado de software e criaria incentivos para que os produtores de software melhorem a segurança de seus produtos, além de atender ao Código de Defesa do Consumidor que, em seu art. 31[9], determina que as ofertas de produtos ou serviços devem apresentar informações sobre os riscos que apresentam à segurança dos consumidores.

Hoje existem poucos mecanismos capazes de transformar os dados sobre a segurança de sistemas em informações que o consumidor final seja capaz de compreender. Os mecanismos existentes atualmente precisam ser aprimorados para que possam fornecer informações melhores aos consumidores.

Exigir um nível adequado de segurança de sistemas que lidem com dados que possam afetar a privacidade dos consumidores ou cidadãos

Muitas organizações coletam dados de seus clientes durante seus relacionamentos de negócio, mas nem sempre protegem esses dados de forma adequada. É necessária a definição de procedimentos mínimos de proteção das informações coletadas dos consumidores e a responsabilização das organizações públicas ou privadas que não protegerem as informações adequadamente. Os vazamentos de informações pessoais devem ser passíveis de punição e devem ser amplamente divulgados. Em particular, todas as pessoas potencialmente afetadas pelo vazamento devem ser alertadas do fato e de suas possíveis consequências.

[9] http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm

Definir que os consumidores devem ser informados dos possíveis usos dos dados inseridos em sistemas ou sites

Não apenas as organizações devem proteger os dados que coletam dos consumidores, mas também os consumidores devem saber todos os possíveis usos das informações coletadas. Assim, é necessário que todas as organizações públicas e privadas tenham a obrigação de divulgar todos os usos possíveis para os dados coletados, inclusive usos futuros. Qualquer alteração na política de uso dos dados deve ser previamente informada e explicitamente aceita pelos consumidores.

Estabelecer campanhas de conscientização de segurança para os consumidores

Além das ações que exijam que os fabricantes de software ajam de forma responsável para com os consumidores, é importante também capacitar os usuários de sistemas informatizados dos riscos inerentes ao uso desses sistemas.

Assim como é importante a realização de campanhas de conscientização de segurança no trânsito ou de controle de doenças como a dengue, é importante conscientizar os internautas sobre os riscos e atitudes que advém de um mundo cada vez mais conectado. As campanhas devem tratar de temas como os riscos de informar dados pessoais em sites desconhecidos ou dos cuidados que cada pessoa deve ter com seu computador pessoal para evitar que este se torne uma arma nas mãos de criminosos digitais.

Por órgãos de controle

Os órgãos de controle podem e devem exigir dos setores que regulam a adoção de práticas adequadas de segurança de aplicações. Esses órgãos deveriam definir regulamentos que favoreçam o uso de técnicas de segurança no desenvolvimento de sistemas. Assim, as ações sugeridas são:

Definir claramente as responsabilidades com relação aos aspectos de segurança de aplicações

Toda organização deve ser responsável pela segurança dos seus sistemas e esta responsabilidade deve ser claramente definida. Os órgãos de controle devem, sempre que possível, incluir a responsabilidade de manter a segurança dos sistemas de informação como parte de seus regulamentos. Deve haver previsão de punição em casos em que não haja segurança adequada nos sistemas.

Verificar e auditar para garantir que práticas adequadas de segurança são adotadas

Sempre que possível, as auditorias ou verificações realizadas devem incluir itens que permitam avaliar se as práticas de segurança de aplicações foram adotadas adequadamente. Entendemos que as

auditorias são uma oportunidade para melhorar as práticas adotadas pelas organizações e os órgãos de controle devem se preparar para exigir a manutenção de níveis adequados de segurança nos sistemas das entidades auditadas.

Existem alguns modelos que podem balizar as práticas de auditoria de segurança de sistemas, como o SSE-CMM (Systems Security Engineering Capability Maturity Model)[10], o OWASP ASVS (Application Security Verification Standard)[11] ou o SAMM (Software Assurance Maturity Model)[12]

Inserir os aspectos de segurança de aplicações em seus regulamentos e/ou recomendações setoriais

Muitos órgãos de controle publicam regulamentos ou recomendações para os setores que regulam. É importante que estes regulamentos ou recomendações incluam aspectos de segurança de aplicações e que indiquem claramente a necessidade de incluir os requisitos de segurança em contratos com os fornecedores.

Facilitar a criação de um mercado de seguros para a segurança de aplicações

Assim como é importante a responsabilização por falhas na manutenção de níveis adequados de segurança, é igualmente importante a criação de um mercado de seguros para a segurança de aplicações.

Um mercado de seguros possibilita a transferência de parte dos riscos ligados à segurança para uma seguradora, ao mesmo tempo que tende a aumentar os custos de seguro para as entidades que não possuem um tratamento adequado dos aspectos de segurança dos seus sistemas. Junto com mecanismos de responsabilização, um mercado de seguros funcionando adequadamente produz incentivos para que as organizações aumentem o seu nível de segurança.

Requerer o uso de conexões criptografadas (SSL) para aplicações web

Muitos dos ataques existentes atualmente só são possíveis porque algumas organizações não usam nem mesmo os mecanismos de segurança disponíveis. Um desses mecanismos é o protocolo SSL, que permite a codificação dos dados transmitidos entre o navegador do usuário e os servidores do sistema web de forma segura, garantindo o sigilo e a autenticidade das informações.

Assim, uma medida simples e efetiva para melhorar a segurança dos sistemas web é exigir que os dados sejam transmitidos de forma segura pela Internet.

---

[10] http://www.sse-cmm.org/

[11] http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

[12] http://www.opensamm.org/

Por órgãos de ensino e pesquisa

A capacitação de mão de obra é essencial para fazer o país avançar em uma área intimamente ligada à tecnologia. Para que haja um mercado de segurança de aplicações pujante, é necessária a formação de um contingente adequado de especialistas, tanto nos aspectos de ataque quanto nos aspectos de defesa da infraestrutura. A formação de uma força de trabalho adequada deve ser dar pela inclusão da área de segurança nos conteúdos das universidades e também pela formação de pesquisadores capazes de propor novas técnicas e metodologias que avancem esta área do conhecimento. Também é necessária uma interação das instituições de ensino e pesquisa com a indústria para o repasse e produtização de tecnologias.

As ações sugeridas para instituições de ensino e pesquisa são:

Inclusão das boas práticas de segurança de aplicações no conteúdo dos cursos

É essencial que todos os profissionais de tecnologia da informação tenham conhecimento das práticas básicas de segurança e a inclusão dessas informações nos conteúdos dos cursos da área é a melhor forma de atingir esse objetivo.

Os estudantes dos níveis básico e médio também precisam aprender sobre os perigos do mundo virtual. Nesses níveis de ensino, o foco deve ser nos riscos envolvidos no uso de sistemas ou sites web, como redes sociais ou sites de comércio eletrônico. Os aspectos éticos do uso da Internet também devem ser enfatizados.

Definição de cursos avançados para formação de mão-de-obra na área

Além das práticas básicas que devem ser de conhecimento de todos os profissionais da área, é necessária a formação de especialistas em segurança de software para que o país possa desenvolver uma indústria de segurança pujante e geradora de riquezas para o país.

Fomentar e financiar pesquisas sobre segurança de aplicações

A geração de conhecimento na área também é essencial para que o país possa assumir a vanguarda mundial em segurança de aplicações. E a única forma de aumentar a geração de conhecimento é fomentar e financiar pesquisas na área, sejam elas desenvolvidas por entidades públicas ou privadas.

O fomento da geração de conhecimento e tecnologias nas empresas é de suma importância para a criação no país de um mercado de segurança de aplicações capaz de criar produtos e tecnologias avançados e inovadores.

Promover a formação de profissionais capazes de atuar com ética e responsabilidade

Todo o processo de formação de profissionais e pesquisadores na área de segurança deve priorizar os aspectos éticos e a atuação responsável. A formação ética deve ser parte essencial da formação desses profissionais.

Por todos os órgãos públicos

Qualquer órgão público pode contribuir para melhorar o atual estado de coisas, seja com conscientização e capacitação, seja utilizando o seu poder de compra de forma a favorecer empresas que tratem adequadamente os aspectos de segurança de aplicações.

As ações sugeridas para todos os órgãos públicos são:

Financiar validações e correções de segurança para sistemas de código aberto

Muitos órgãos públicos usam sistemas de código aberto como parte de sua infraestrutura de tecnologia da informação. Assim, é essencial para essas organizações que estes sistemas de código aberto sejam seguros e confiáveis. Os órgãos públicos deveriam investir na avaliação da segurança dos sistemas de código aberto que adotam, na correção das falhas de segurança encontradas e na divulgação responsável tanto das falhas quanto das correções.

Desta forma, os órgãos públicos prestam um serviço à sociedade com a melhora da segurança de seus próprios sistemas e dos sistemas de terceiros.

Promover o uso de tecnologias e metodologias de segurança de aplicações

Todo órgão público deveria exigir e promover o uso de tecnologias e metodologias de desenvolvimento seguro de aplicações, tanto internamente quanto por seus fornecedores.

Deve ser de responsabilidade de cada órgão garantir que seus sistemas tenham um nível adequado de segurança e que as técnicas adequadas são utilizadas no desenvolvimento dos seus sistemas informatizados.

Promover e permitir testes de segurança de forma responsável mas aberta

Os testes de segurança são uma das principais ferramentas para encontrar falhas de segurança em sistemas informatizados. Todo órgão público deveria estabelecer um programa que permita a pesquisadores de segurança realizar testes em seus sistemas com o objetivo de encontrar as falhas e saná-las com a maior brevidade possível.

Ressaltamos que os testes devem ser feitos de forma ética e responsável e devem ser encarados como uma forma de colaboração para a melhoria dos sistemas governamentais. Acreditamos que os criminosos digitais já realizam seus próprios testes nos sistemas de forma velada, ao contrário dos pesquisadores com legitimas intenções de melhoria dos sistemas. Essa realidade dá uma vantagem aos criminosos com relação aos responsáveis pela segurança dos sistemas. A melhor forma de equilibrar essa disputa é facilitar a atuação dos pesquisadores e profissionais de segurança de forma a permitir que as falhas sejam encontradas e divulgadas de forma adequada ao invés de servirem como moeda de troca nos submundos digitais.

Promover treinamento e conscientização dos gestores para os desafios da segurança na web

Todos os órgãos públicos devem se preocupar com a segurança de seus sistemas e esta preocupação deve fazer parte do direcionamento dado pela alta administração de cada órgão. Assim, é importante que os gestores de todos os órgãos participem de sessões de treinamento e conscientização neste sentido.

O Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República tem feito um excelente trabalho de conscientização dos funcionários públicos federais e este trabalho deve ser valorizado e levado às esferas estadual e municipal.

Vantagens competitivas para o Brasil

A área de tecnologia é uma atividade econômica de alto valor agregado e com a capacidade de geração de riqueza para o país. Com o apoio e liderança do governo, o Brasil tem o potencial para se tornar um líder mundial na área de segurança de aplicações, podendo inclusive gerar divisas pela exportação de produtos e serviços de alto valor agregado através da criação de novos negócios.

Por se tratar de uma atividade intensiva em mão-de-obra, há também a possibilidade de geração de empregos no país para profissionais altamente capacitados. A existência de profissionais capacitados em segurança favorece também a soberania nacional, já que esse conhecimento é crucial em caso de conflitos cibernéticos, ou guerra eletrônica.

O desenvolvimento de uma área intimamente ligada à informática tem também o potencial de fomentar o desenvolvimento de áreas afins, aumentando a capacidade tecnológica do país.

A melhora do ambiente online para negócios tende a melhorar a imagem do país no exterior, de forma que o Brasil passe a ser considerado um porto seguro para negócios, tanto na Internet quanto fora dela. Um ambiente de negócios favorável pode atrair investimentos internacionais, em especial investimentos para negócios diretamente ligados à Internet ou de empresas de desenvolvimento de software.

Como o OWASP pode ajudar?

O OWASP é uma comunidade internacional e congrega os maiores especialistas no assunto a nível global, além de uma boa quantidade de especialistas brasileiros, incluindo funcionários públicos. Todos os materiais e sistemas desenvolvidos pelo OWASP estão livremente disponíveis para que o governo brasileiro utilize da forma que considerar mais adequada e a comunidade pode também ajudar no desenvolvimento de materiais ou ferramentas para atender às necessidades específicas de órgãos governamentais.

Os materiais e guias desenvolvidos pelo OWASP podem ser traduzidos para o português de forma a servirem de subsídio no desenvolvimento de legislação ou regulamentação. O OWASP possui guias de boas práticas e padrões que podem ser utilizados como insumo ao desenvolvimento de documentos brasileiros alinhados com as melhores práticas internacionais.

Os especialistas brasileiros participantes do OWASP estão dispostos a contribuir para que o país avance na direção certa e podem servir de corpo consultivo ou de ligação com especialistas estrangeiros, caso seja necessário. O OWASP não tem fins lucrativos e os especialistas envolvidos trabalham como voluntários.

Contatos

Em Português:

Lucas de Carvalho Ferreira
Líder - Capítulo do OWASP em Brasília, DF
email: lucas.ferreira@owasp.org
endereço: rua Boa Vista, 18 - Núcleo Bandeirante, DF - CEP 71730-055

Em Inglês:

Kate Hartmann
Diretora de Operações
email: kate.hartmann@owasp.org
endereço: 9175 Guilford Road, Suite 300 - Columbia, MD 21046 - Estados Unidos

Capítulos do OWASP no Brasil:

Brasília:

Lucas C. Ferreira (lucas.ferreira@owasp.org)

Campinas:

Fernando Amatte (famatte@owasp.org) ou Ricardo Makino (makino@owasp.org)

Curitiba:

Eduardo Neves (eduardo.neves@owasp.org)

Goiânia:

Eduardo Jorge (eduardo.jorge@owasp.org)

Paraíba:

Magno Rodrigues (magno.logan@owasp.org)

Porto Alegre:

Gustavo Barbato (lgbarbato@owasp.org)

Recife:

Felipe Ferraz (felipe.ferraz@owasp.org) ou Rodrigo Assad (rodrigo.assad@owasp.org)

São Paulo:

Wagner Elias (wagner.elias@owasp.org)