A Miopia dos CSO's

Por Jordan M. Bonagura

Antes de começar a ler este artigo, imagine como seria gerir a sua empresa sem as informações de seus clientes, ou ainda, imagine como seria se os seus concorrentes tivessem essas informações...

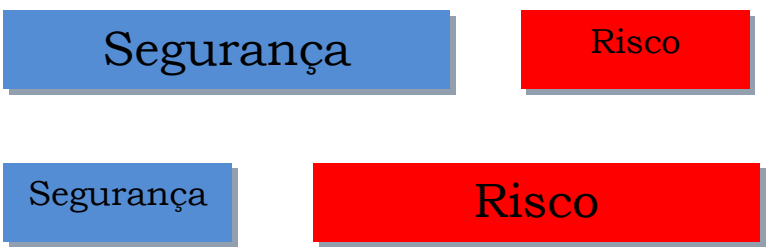
Pois é, já está mais do que claro para o mercado a importância das informações para as empresas. A base de informações de seus clientes e os conhecimentos que estas empresas adquirem ao longo de sua existência são fundamentais e de grande vantagem competitiva nesta nova era corporativa.

Tendo isto em mente, percebe-se a importância da implementação de políticas específicas, cujo objetivo é a criação de um alicerce para a segurança das informações.

Com o crescente aumento dos incidentes relacionados à segurança, tornou-se complexa a administração da área de TI e automaticamente criou-se uma demanda para um novo tipo de profissional, o CSO.

Este passou a ser o responsável pelas áreas de risco, segurança da informação e também pela definição e implementação das estratégias/políticas de segurança que esta empresa deverá adotar. Tais políticas estão diretamente relacionadas com a intenção de minimização dos riscos e conseqüentes impactos negativos que poderão interferir no negócio.

A figura abaixo demonstra a relação direta do aumento da segurança com a diminuição do risco, ou seja, basicamente, quanto maior a segurança de um ambiente, menor o risco.

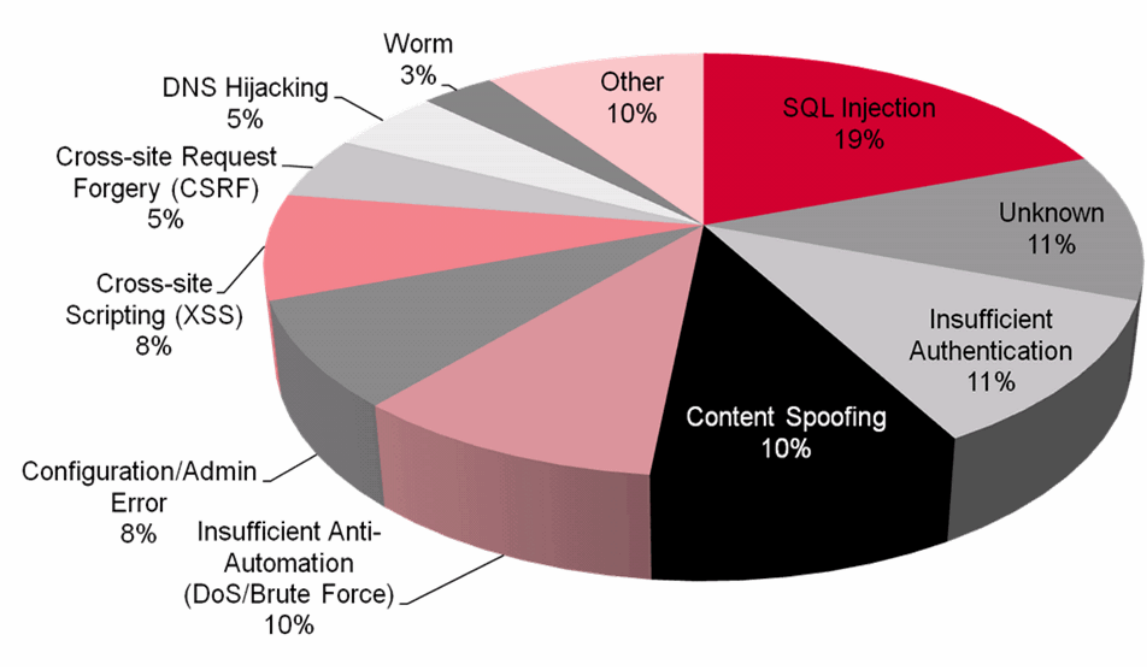


Contudo, a grande questão a ser tratada neste caso não aborda a necessidade de bons profissionais, de informação segura e/ou do desenvolvimento de boas políticas de segurança, mas sim, do processo construtivo pelo qual toda empresa passa no momento de criar e estruturar tais políticas.

A visão *"in box"* utilizada no momento da geração destas políticas, não é, muitas vezes, suficiente para contemplar toda a gama de vulnerabilidades existentes na empresa.

Quando analisamos o gráfico publicado pela Breach Security Labs em agosto de 2009 no "The Web Hacking Incidents Database 2009", que demonstra quais foram as vulnerabilidades mais utilizadas pelos hackers durante o primeiro semestre de 2009, automaticamente e obviamente nos deparamos com um alto percentual de uma vulnerabilidade cujo principal objetivo é a obtenção de dados (SQL Injection (19%)). Digo obviamente, pois conforme citado anteriormente, a informação é um dos bens mais valiosos de uma organização.

Quais as vulnerabilidades que os hackers têm usado?



Fonte: Breach Security Labs

Análises deste tipo são de extrema importância para o CSO, pois através destas é possível aprimorar e atualizar os mecanismos de controles lógicos (Firewalls, Anti Vírus, IDS/IPS etc), e assim minimizar os risco em relação as vulnerabilidades já conhecidas e

contempladas na política da organização, e mais do que isto, considerar novas formas de exploração destas vulnerabilidades.

Um dos riscos específicos que gostaria de abordar rapidamente, é o de que existem pessoas responsáveis por esta administração, e estas estão sujeitas a falhas.

Muitos podem questionar que para tanto existem políticas criadas e que estas são seguidas a risca por seus colaboradores, porém vale lembrar que da mesma maneira que mecanismos físicos e lógicos precisam ser atualizados, políticas também precisam ser revistas continuamente e os colaboradores responsáveis por sua administração e execução precisam ser constantemente treinados.

Tudo parece bem agora, certo?

Infelizmente não! Lembre-se da bíblia: *"o homem tolo que construiu o seu castelo sobre a areia..."*

O grande problema é que toda a política de segurança é desenvolvida sob uma visão *"in box",* no entanto, uma série de vulnerabilidades conhecidas pelo mercado, muitas vezes estão disponíveis "out box", ou seja, só enxerga, quem não vive a situação. Se o CSO estiver baseado simplesmente na sua política não conseguirá ver o que ela não contempla, ou seja, será prisioneiro de sua pseudo-segurança.

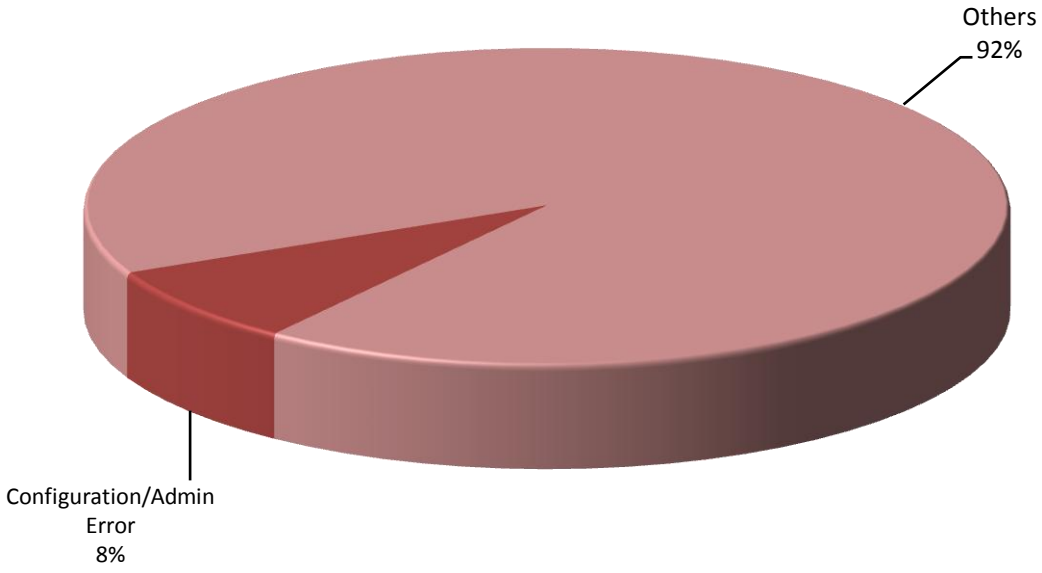
É isto que chamo de miopia do CSO. Acreditar que com sua política definida consegue controlar o todo, quando na verdade controla o todo de sua política, porém esta não garante a segurança de sua empresa, pois, como vimos, foi criada sobre um padrão conhecido pela equipe e não contempla vulnerabilidades existentes no mercado e ainda não conhecidas "in box".

Mas o que quero dizer com isto?

Quero dizer que: "Muitas vezes esconde-se a chave embaixo do tapete e simplesmente se esquece de trancar a porta..."

Um dos grandes problemas desta miopia é quando tratamos, por exemplo, dos riscos relacionados aos erros de configuração e administração (Configuration/Admin Error (8%)) demonstrado no gráfico abaixo:

Quais as vulnerabilidades que os hackers têm usado?



Fonte: Adaptado de Breach Security Labs

Este tipo de erro, além de ser considerado uma vulnerabilidade, pode muitas vezes potencializar a facilidade de identificação e conseqüente exploração de outras vulnerabilidades. Um exemplo prático disto é a listagem de diretórios de um servidor web exibindo arquivos de configuração de banco de dados.

Calma! Nem tudo esta perdido...

Muitas vezes fica difícil buscar o “out box” quando se está 100% do tempo focado no “in box”, e ainda mais sobre a idéia de que se está controlando tudo. Uma recomendação que julgo ser de grande valia é a contratação de consultorias especializadas (Pentest), que poderão avaliar vulnerabilidades não conhecidas pela empresa e diferentes formas

de exploração de algumas vulnerabilidades já contempladas na política de segurança atual.

Esta visão se faz importante porque tais consultorias não vivem o dia a dia desta empresa, e, portanto não tem sua visão limitada pela roda viva de suas rotinas.

Com atitudes como esta, pode-se diminuir significativamente os problemas decorrentes deste tipo de miopia gerencial.

Fique Atento, Fique Seguro!

Jordan M. Bonagura é cientista da computação com pós-graduações nas áreas de gestão estratégica de negócios, inovação e docência (metodologia de ensino e pesquisa).

Atua como consultor empresarial e pesquisador na área de segurança da informação com ênfase na busca de novas vulnerabilidades e suas formas de exploração.

Docente na área de tecnologia da informação em diversas instituições, dentre elas o Instituto Brasileiro de Tecnologia Avançada (Veris/IBTA).

Como docente das instituições que atua, ministra treinamentos *"in company"*, em diversas organizações de renome nacional, dentre as quais destaca-se o Instituto Nacional de Pesquisas Espaciais (INPE).