Ingresso.com: Como não lidar com segurança da informação

05 OCTOBER 2014 on Português, Portuguese, Information Security, Segurança da Informação

Este artigo foi originalmente postado em http://marcoagner.com/posts/ingresso.com-como-nao-lidar-com-seguranca-da-info em 03 de maio de 2014

Neste post, mostro falhas de segurança críticas no site do serviço Ingresso.com e espero
trazer benefícios e mais conhecimento às pessoas de outras áreas fora de engenharia/ciência da computação, especialmente, aos clientes da empresa citada.
E, espero que a empresa resolva os problemas citados de uma vez por todas de forma transparente para o bem de todos envolvidos.

As falhas achadas são críticas por três motivos: expõem informações de clientes, coloca em risco o principal serviço oferecido e são muito simples
(leia-se praticamente obrigatórias) de serem tratadas antes de um sistema entrar em ambiente de produção.
Apesar de ter achado e reportado outras falhas (como o indevido tratamento de formulários), explicito apenas duas, pois são tão simples a ponto de poderem ser exploradas por um leigo desavisado ou curioso, logo, foge do escopo deste post mostrar
falhas mais avançadas e que necessitam de um certo grau de conhecimento específico.

Vale ressaltar que, em um grande ambiente empresarial, é compreensível que ocorra problemas com a segurança de sistemas e isto não
acarreta, automaticamente, na descredibilidade de uma empresa inteira. Muitas pessoas de áreas e especialidades

muito divergentes estão
envolvidas nas operações e muitos problemas de comunicação ocorrem, especialmente quando se trata dos serviços de atendimento ao cliente que, geralmente, são terceirizados; Adicione problemas específicos de cada equipe e infortúnios praticamente imprevisíveis... e, *voilà*, eis uma receita para grandes problemas.
Logo, o mais importante a se levar em consideração em casos do tipo é a capacidade da empresa de correr atrás dos danos causados de forma transparente com todas as partes envolvidas,
corrigir as falhas encontradas rapidamente e seguir em frente gerando valor se a mesma tiver a devida resiliência para tal.

Eu entrei em contato com a empresa, pela primeira vez, em 24 de janeiro de 2014 por e-mail, quando recebi uma resposta interessante:

> *"Olá, Marco. Explico que o site Ingresso.com utiliza modernos protocolos de segurança HTTP SSL seguro, para garantir a confidencialidade dos dados e*
> *segurança das transações realizadas via web. O site também é certificado pela VeriSign, empresa conceituada em segurança na internet.*
> *Os usuários podem clicar no selo na parte inferior esquerda de nossa página para confirmar em tempo real que nosso site foi aprovado pela*
> *VeriSign com respeito a proteger informações confidenciais com a criptografia SSL. Apesar dos mecanismos de segurança, recomenda-se que*

> *os consumidores mantenham sempre antivírus instalados em suas máquinas e devidamente atualizados para evitar a ação de programas espiões.*
> *Colocamo-nos a disposição para quaisquer esclarecimentos."*

O último contato com a equipe de atendimento por telefone envolveu um momento de quase cumplicidade entre mim e a atendente:

> *"[...] nosso site é seguro." - Atendente.*
>
> *"Lourdes. Confie em mim, Lourdes... O site de vocês não é seguro." - Eu.*

... Mas, tragicomicamente, não deu certo e ficou no quase. Por fim, a resposta final era de que eu deveria enviar meus "questionamentos" (segundo o atendimento) por e-mail para a empresa, apesar de eu ter explicado que já havia enviado e, obtido respostas insatisfatórias e nenhuma alteração dos problemas. *(em todas as ligações, me perguntaram se o problema tinha a ver com um tal de "e-mail da Copa" que explico no final do que se trata)*

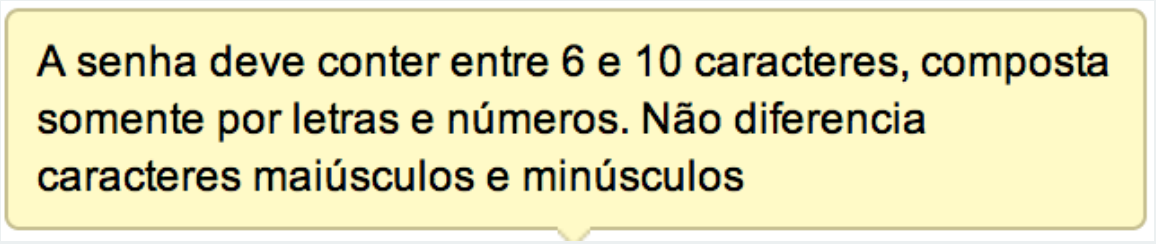
Reportar falhas de segurança em um site que lida com dados de milhões de clientes NÃO deve ser tão complicado. Estou falando do site que,
neste momento, segura o posto 480 (passível a variações) de maior tráfego entre sites brasileiros segundo o Alexa.
Problemas como este não são banais para serem tratados com descaso e nem monstros escondidos no armário da empresa para serem tratados com

medo de reconhecer que existem e que devem ser devidamente tratados, afinal, problemas não costumam sumir pelo simples fato de serem ignorados.

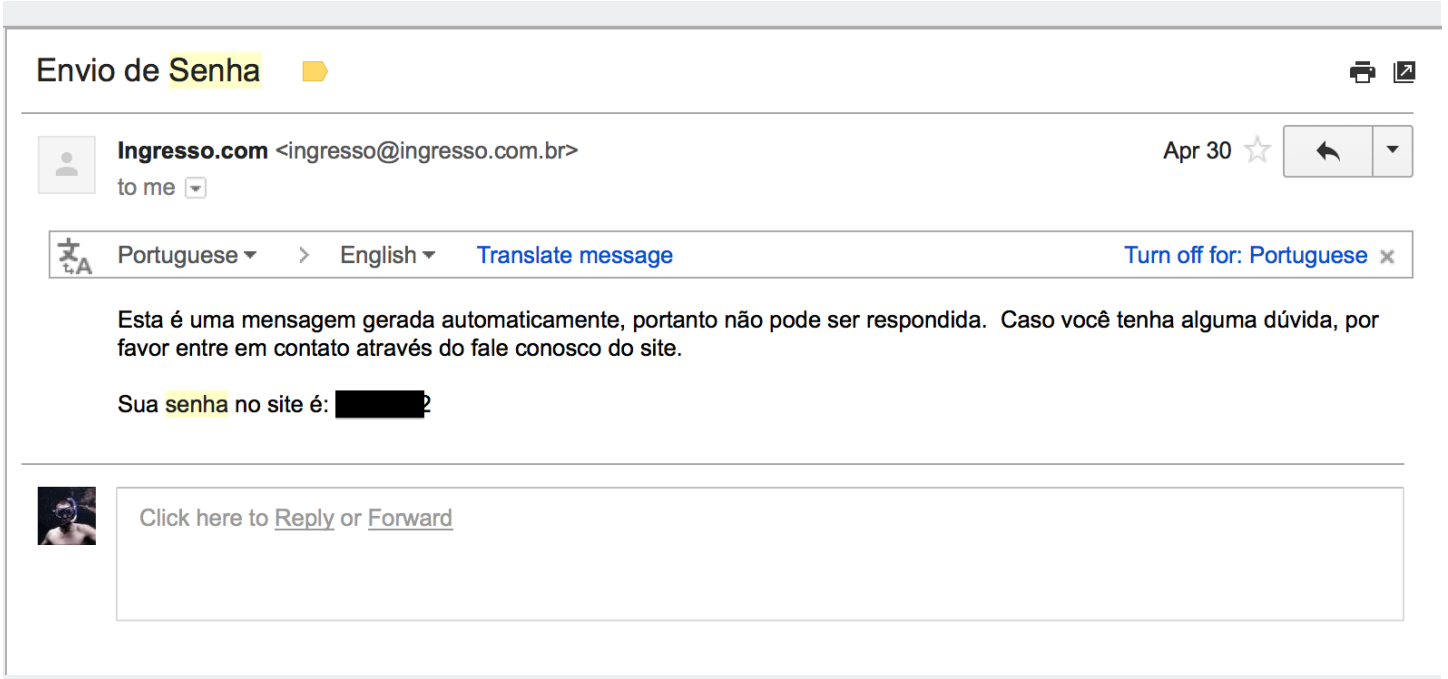
As falhas que escolhi postar...

1. Senhas guardadas em "plain text":

Sim, eu sou cliente da Ingresso.com e sempre que me registro em algum serviço na internet faço uso de uma senha genérica e de pouca importância para mim, peço recuperação de senha e verifico se me retornam a senha em puro "plain text" como eu escrevi. Porém, eu já tinha quase certeza de que as senhas eram guardadas em "plain text" devido às restrições "sem sentido" impostas no registro dela:



Eis que chega por e-mail a vergonha para o desenvolvedor que permite isso:



Muitos usuários podem ver isso como uma facilidade benéfica sem saber o verdadeiro risco por trás desta péssima prática e, talvez, se perguntem:

> *"Porque será que existem outros serviços chatos que me fazem registrar uma nova senha? Deve ter algum motivo..."*

... Ou não. Afinal, não é obrigação do cliente entender da segurança dos dados da aplicação pela qual ele paga.

E para os que não tem a obrigação de saber porque senhas "plain text" são ruins, uma rápida (muito resumida) explicação: Quando um website guarda as suas senhas no formato em que você escreveu no banco de dados é a mesma coisa que guardar a sua senha
e ficar esperando alguém simplesmente pegar ela como

está para usar - seja alguém mal-intencionado de dentro ou alguém de fora que
se aproveite de diversas possíveis falhas a serem exploradas. Basicamente, antes de ser armazenada no banco de dados, a sua senha deve
passar por um função hash que é um algoritmo utilizado para transformar qualquer tamanho de dado (no caso, a sua senha) em uma espécie de "representação" de tais dados com um tamanho fixo e que não
pode ser revertida. Além disso, mesmo se os dados de entrada mudarem muito pouco o hash resultante será completamente diferente do hash resultante
dos dados antes da pequena mudança como neste exemplo:

```
hash('suasenha') ==
'5df1bf8c658bcb1e77258754d0529912f6c93ab26788f52160c27aa0
9e95a938efa1035c5071b3f10377405af0607ee48ad1501c6353204d3
787b7912601bb5b'
True

hash('suasenha2') ==
'63b79454bb906a505efbe263d8b7fbfed92b9be6de16b3eb29c85ff9
3b51993875272e8c91487522fc8a751b910751131842ff8eb53f7cf35
b5e9bc6f938e066'
True
```

Apenas "hashear" a senha ainda não é suficiente para as práticas de segurança da informação atuais, porém, isso já atende à representação desejada para o post.

Para quem quiser saber mais pode começar procurando por "salted hash", "key stretching" e "key derivation functions".

Não existe essa história de senha boa ou segura quando ela é armazenada em "plain text" no banco de dados.

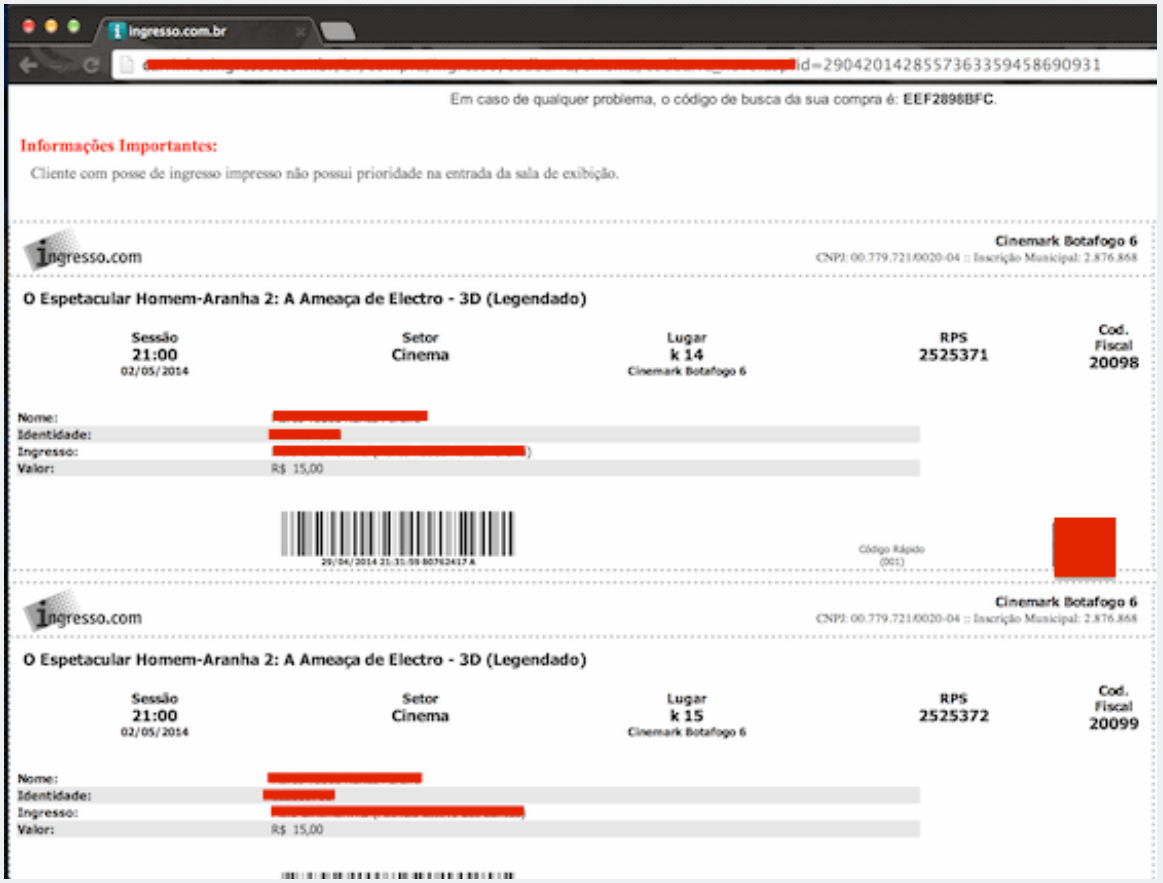
2. Acesso aos ingressos e números de documentos de clientes:

Eu acho o serviço prestado pela Ingresso.com útil e eu sou cliente deles. Para ter uma certa segurança sem perder a facilidade do serviço, eu uso
um cartão de crédito com limite máximo de 500 reais e políticas de bloqueio bastante severas em compras claramente inseguras; com o intuito
de evitar maiores problemas em caso de fraudes em serviços que estão apenas esperando o primeiro bandido entrar pela porta de trás ou da frente
como ocorre nesta segunda falha. E, tenho certeza, de que pararei de usar assim que houver uma alternativa equivalente e mais segura caso eles não resolvam os problemas... e tenho dúvida sobre se o ideal
da minha parte seria apenas boicotar o serviço enquanto eles não se corrigirem.

Então, eu havia acabado de comprar um ingresso em Janeiro e escolhi imprimir. Okay, sou levado para a página de impressão do ingresso e recebo uma URL contendo um "id" com apenas números e já tendo quase certeza do que isso significava:

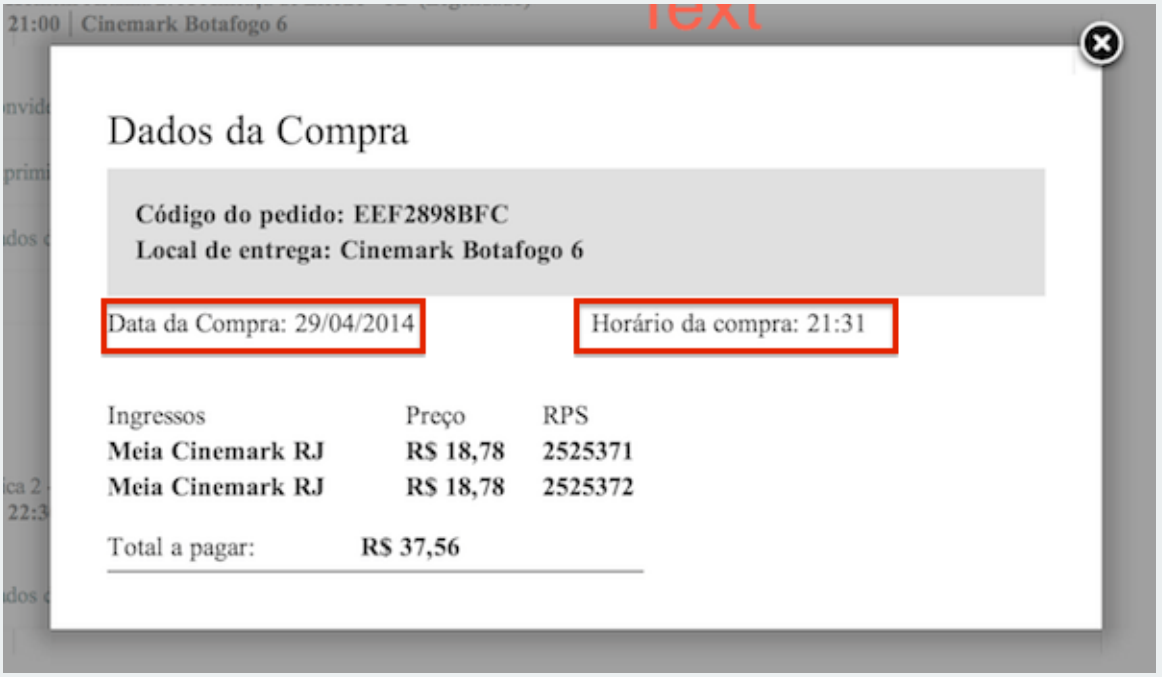
//o ingresso mostrado não é o de Janeiro e, sim, um recente (semana passada)

//escondi a URL completa por não ser necessário ficar tão explícito, apesar de continuar existindo por lá

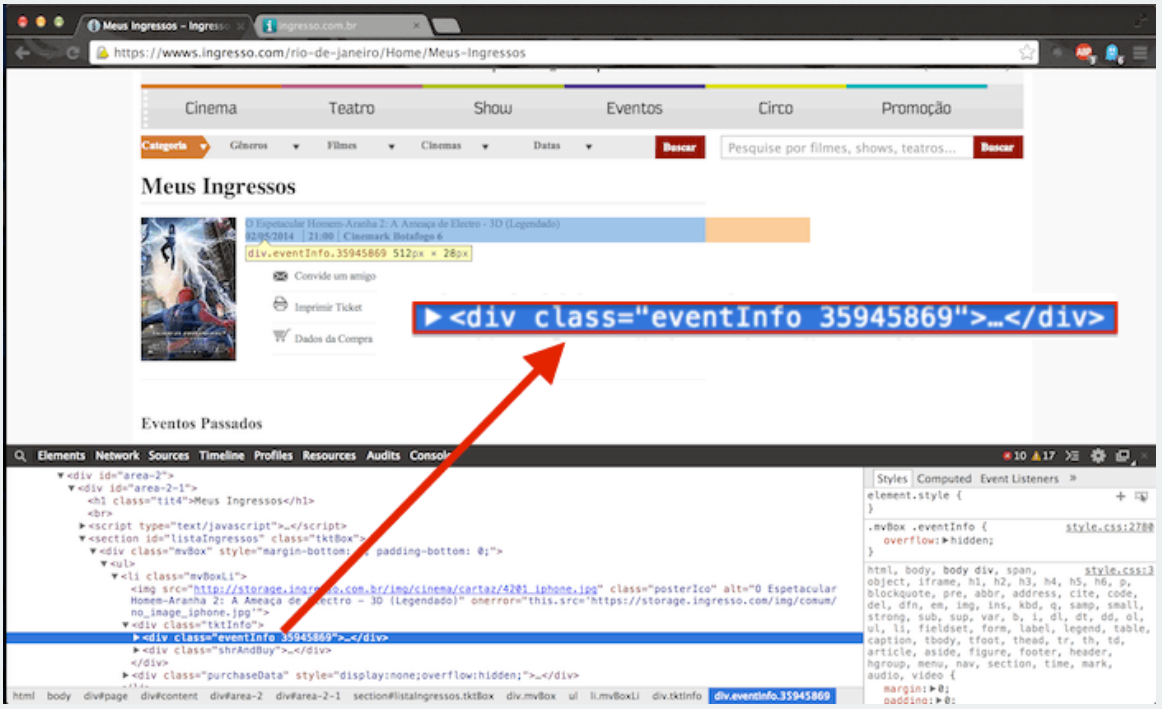


Lá estava o "id" do meu ingresso e não precisou muito para que eu o dividisse em quatro partes: 29042014 28557363 35945869 0931 -> A primeira e última partes são, respectivamente, o dia e a hora em que a compra do

ingresso foi efetuada:



Logo em seguida, achei o número que realmente importava: o terceiro. Ao alterar ele, infelizmente, tive um outro
ingresso diferente aberto contendo os dados de outra pessoa e pronto para uso. Mas, até então, eu estava com o segundo
e terceiro números ligados como um só ainda. E aqui está como descobri do que se tratava este
terceiro número:



Daí para frente, eu podia ignorar todos os outros números e usar apenas o "envetInfo" no "id" da URL para requisitar outros ingressos sem nenhuma
restrição. O "id" pôde, simplesmente, ficar assim: 00000000 00000000 35945869 0000 *(sem os espaços)*. De fato, eu pude arrancar ainda mais daí ao retirar os zeros equivalentes
ao horário da compra.

Agora, já era mais do que fácil de se aventurar por esse número em busca de outros ingressos. Qualquer programador sabe que é trivial criar um algoritmo
para iterar pelo número, requisitar as URL, checar e guardar as que contém um ingresso... entre outras diversas possibilidades de acordo com o interesse do programador.

Para colocar fim nesta segunda falha, aqui vai uma lista de algumas das informações de clientes abertas por este

meio:

- Nome completo;
- RG;
- CPF;
- Informações sobre a compra, como por exemplo: estudante, meia-itaú, etc...

Além do ingresso simplesmente estar lá para qualquer pessoa mal-intencionada usar - desde ingressos de cinema até ingressos de shows caros e disputados.

Um grave problema afetando o serviço principal do site apenas esperando para ser explorado.

Este tipo de post público torna a Ingresso.com mais insegura?

Não, não torna. O sistema deles já é inseguro e, com certeza, as falhas são postadas e comentadas em fóruns privados entre pessoas com todos os tipos de intenções. Se uma insegurança existe, ela existe e ponto final. Eu fiz o que não é obrigação de um cliente e tentei fazer com que a empresa prestasse atenção nesses problemas para que os corrigissem desde JANEIRO deste ano... E nada foi feito. Acredito que este tipo de post público, tendo em vista as tentativas de contato para correção das falhas,
se faz um dever e apenas ajuda às pessoas a saberem o tipo de risco que estão correndo ao negociar com o serviço web da Ingresso.com. E, sim, é possível que falhas

críticas
(e, mais uma vez, simples) de segurança no site já tenham sido exploradas por bandidos.

O que me leva ao tal "e-mail da Copa"...

Fui buscar saber do que se tratava o tal e-mail da Copa e descobri que foi um incidente em que falhas do site já foram exploradas e usadas em uma fraude por
e-mail contendo as informações dos clientes. Em meu último contato, eu liguei para a Assessoria de Imprensa da B2W que é responsável pela Ingresso.com
buscando esclarecimentos, fui razoavelmente bem atendido e fiquei de entrar em contato por e-mail com eles. Vejamos... O lugar que melhor
respondeu à solicitação, mesmo não tendo sido de forma ideal por não ser responsabilidade deles, foi um setor que nada tem a ver com esse tipo de assunto...
ponto positivo para quem me atendeu na Assessoria de Imprensa deles e ponto negativo para a estrutura
da Ingresso.com. Infelizmente, eu tive a certeza de que subiria este post antes de continuar o contato, passando o mesmo para eles por e-mail, após saber
com mais detalhes o que foi esse e-mail da Copa, aparentemente, no mês de Março deste ano. Aqui estão os links para quem quiser saber o que foi:

- Olhar Digital, Época Negócios;
- Busca sobre a fraude no "Reclame Aqui".

Considerações finais

Eu consigo apontar algumas soluções técnicas possíveis para os problemas apresentados, porém, acho que mais importante do que focar na parte técnica neste post é focar na parte humana. Logo, deixo algumas sinceras considerações:

Aos *developers*: Estude muito bem a área em que você está trabalhando, não trate segurança como algo trivial ou que qualquer um pode cuidar sem o devido conhecimento adquirido, não "invente moda" quando se trata de segurança da informação e esteja atualizado sobre as melhores práticas recomendadas para a sua linguagem e frameworks em uso. Mas, acima de tudo, seja humilde e admita até que ponto as suas *skills* chegam e se certifique de que as expectativas estão muito bem alinhadas. E, quando ocorrer um erro seja rápido em admitir e até mais rápido em solucioná-lo ou propor uma solução.

Aos clientes: Fique atento às possíveis falhas de segurança quando se trata de seus dados, especialmente, quando se trata do simples retorno de uma senha em puro "plain text". Reporte qualquer problema à empresa e verifique a forma com que a empresa lida com o ocorrido para decidir se você poderá continuar confiando nela. E, se quiser, fique à vontade para me mandar empresas com serviços web que tenham políticas de restrição de senha e/ou que tenha retornado a senha em "plain text" para você, especialmente se o serviço estiver entre os 500 com maior tráfego no Brasil

no Alexa.

A todos os membros de empresas: Dê a devida atenção à segurança da informação e não hesite em contratar uma boa consultoria na área, procure entender o contexto do negócio em que você está envolvido com o intuito de poder apontar possíveis problemas e evite-os, mas não tenha medo de problemas; Eles vão ocorrer e cabe aos membros de uma empresa solucionarem, aprenderem e saírem mais fortes do que antes de tais problemas. Amor pelo aprendizado, crescimento pessoal e pela geração de valor são essenciais.

Finalmente, termino este post com a esperança de que a empresa consiga corrigir os problemas e solucionar quaisquer danos causados de forma transparente e de que os clientes da Ingresso.com (e outros serviços web) saibam o que ocorre e ao risco que podem estar expostos devido a más práticas e mal gerenciamento de problemas encontrados por clientes.

Atualização (06/05/2014): *Parece que, apesar de não terem se pronunciado, a Ingresso.com já está trabalhando em corrigir as falhas, pois algo já mudou. Não sei quanto está sendo melhorado e nem creio que caiba a mim ficar cobrando nada com postagens, meu objetivo não é ficar viralizando em cima desta mesma tecla; O recado foi dado. Enfim, se estiverem trabalhando nas melhorias de segurança: Parabéns! E espero que se comuniquem melhor com seus vários clientes que se identificaram com este post.*

Atualização (07/05/2014): *A B2W Digital, responsável pela Ingresso.com, entrou em contato comigo e, por mais que eu não saiba como estão trabalhando por lá, tenho certeza que pessoas influentes dentro da empresa estão interessadas e correndo atrás das soluções. Eu não posso garantir os resultados dessas soluções pois isso cabe a eles, mas, como eu disse no post, problemas acontecem... e espero que solucionem tudo da melhor forma possível para todos.*

Atualização (12/05/2014): *Após repercussão deste post nas mídias sociais, alguns jornalistas se interessaram pelo assunto e escreveram sobre o caso deste post. Todo esse interesse pela parte de todos que compartilharam pelas mídias sociais só prova o quanto segurança importa e que existe a demanda dos usuários para que tenham os seus dados tratados de forma segura. Aqui vão os links:*

- *Revista INFO*
- *Canaltech*
- *EXAME*

Marco Agner

Hi, I'm @marcoagner. I'm a minimalist traveler who works from anywhere with a stable internet connection. I write about bitcoin, entrepreneurship and Information Security. Join me on Twitter, contact me or keep scrolling to read my posts.

http://marcoagner.com