

Listen to Podcasts: <http://www.imperva.com/resources/podcasts.asp>

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit <http://www.imperva.com>, check out our blog at <http://blog.imperva.com>, follow us on Twitter at <http://www.twitter.com/imperva>, or send us an e-mail at blog@imperva.com.

Luiz Eduardo: Bemvindos ao podcast sobre segurança da Imperva. Meu nome é Luiz Eduardo Dos Santos, Engenheiro de Segurança Senior da Imperva para a América Latina, e, estou aqui hoje em nome de Brian Contos, Chief Security Strategist da Imperva.

Conosco hoje, no primeiro episódio do podcast que não é feito na língua inglesa, temos Rafael Koike da Telsinc.

A Telsinc é um parceiro da Imperva e atua no mercado desde 1994, oferecendo soluções de tecnologia avançada e prestação de serviços profissionais. A Telsinc é reconhecida como uma empresa ágil, experiente e inovadora na utilização e operação de alta tecnologia.

O Koike está na Telsinc desde 2006, quando foi contratado para desenvolver a área de negócios de segurança, trabalhando com soluções desde o perímetro até o end-point.

Ele tem mais de 10 anos de experiência no mercado de redes e segurança, tendo trabalhado antes na divisão de business services da Siemens.

Possui as certificações CISSP e CISM na área de governança e gestão, além das certificações técnicas CCSE da Check Point e CCNP da Cisco.

Contribuiu para um crescimento médio anual de 33% na unidade de segurança da Telsinc e prevêem um faturamento estimado de 11 milhões de reais para 2010 em produtos de segurança.

Oi Koike tudo bom?

Rafael Koike: Tudo bom, Luiz.

Luiz Eduardo: Preparado aí para uma série de perguntas importantes sobre o mercado de segurança de aplicação e bancos de dados?

Rafael Koike: Claro, com certeza. Vamos lá.

Luiz Eduardo: Então está bom. Importante, este é o primeiro podcast da Imperva que não é feito em inglês. Temos que fazer bonito o negócio

Rafael Koike: Me sinto honrado.

Luiz Eduardo: é isso aí. Então, para começar, me fala um pouco do papel da empresa, da Telsinc, no mercado de segurança da informação.

Rafael Koike: Bom, a Telsinc, ela, surgiu no mercado, principalmente na venda de soluções de infraestrutura de redes. Então, um dos grandes parceiros da Telsinc é a Cisco, e a Telsinc se profissionalizou/ se especializou nessa área de switching e roteamento.

Só que no decorrer do tempo a empresa foi crescendo, desenvolvendo aí os seus serviços e a sua oferta de soluções e com isso foi fundamental expandir essa oferta de infraestrutura para a parte de segurança de informação também. Então, de uns 5 anos para cá, a Telsinc vem aumentando o número de parcerias com empresas de segurança para complementar o seu portfolio de soluções. A Telsinc vem crescendo bastante no mercado de segurança, oferecendo não só produtos, mas também serviços.

Luiz Eduardo: E, falando de soluções para o mercado, qual é a sua opinião, de um modo geral, sobre segurança de dados no mercado brasileiro, hoje.

Rafael Koike: Bom, essa demanda é uma coisa que vem crescendo cada vez mais no Brasil. Eu vejo que inicialmente as empresas, os nossos clientes, começaram buscando ferramentas de DLP (Data Loss Prevention), para controlar o que vazava de informação nas estações de trabalho dos seus usuários. O grande desafio hoje no Brasil, é em relação a maturidade de segurança da informação nas empresas. Muitas das empresas ainda não tem uma política de segurança da informação bem definida. Se você não tem uma política de segurança da informação bem definida, você não consegue classificar essa informação corretamente. Ou seja, se eu não sei aquilo que é importante para a minha empresa, como é que quando eu crio uma informação, eu consigo definir se ela é confidencial, se ela é uma informação pública. Então acho que esse é um primeiro passo que as empresas no Brasil estão enfrentando. E com isso, você tendo uma dificuldade para definir qual é uma informação confidencial, qual informação pode estar sendo divulgada publicamente. Fica difícil eu implementar uma ferramenta de Data Loss Prevention. No entanto, muitas empresas brasileiras tem que ficar em conformidade com algumas normas, como Sarbanes-Oxley, PCI agora, então o Brasil está chegando agora a onda da PCI. Muitas das empresas que lidam com cartão de crédito tem que estar em conformidade com essa norma. Isso força essas empresas a buscar a criação de políticas de segurança, a buscar um desenvolvimento da área de segurança da informação para criar regras de classificação da informação. Começar a rotular as informações que são criadas, e com isso, essas empresas começam a buscar ferramentas que vão auxiliar nessa classificação da informação, nesse controle do acesso à informação. Então agora está chegando o momento que as empresas já tem uma estrutura de segurança definida, e com isso começam a buscar ferramentas para ajudar a controlar, auditar e bloquear o acesso a determinadas informações. Eu acho que, quem está puxando principalmente este desenvolvimento é o mercado financeiro. E eles vão estar levando junto com eles aí todo a vertical de retail, toda a cadeia de empresas que lidam com informações de cartão de crédito e com o decorrer do tempo as outras empresas, os outros mercados também vão começar a buscar esse tipo de maturidade, não é?

Luiz Eduardo: maturidade, era isso que eu ia falar, parece que o mercado de segurança da informação no Brasil, chegou em um ponto que está realmente maduro.

Rafael Koike: e também até porque , eu acho que o mercado em si, estava talvez aguardando o surgimento de ferramentas que auxiliassem eles nesse processo. Então, o mercado começou a desenvolver ferramentas para auxiliar no processo de DLP, auxiliar em um processo de segurança de dados, e com isso você começa a impulsionar os clientes/empresas para utilizar essas ferramentas, e para elas usarem essas ferramentas elas precisam ter uma maturidade nos seus processos e isso gera um ciclo.

Eu acho que as coisas estão se desenvolvendo juntas.

Luiz Eduardo: e me diz uma coisa, na sua opinião, porque a segurança de aplicações web e bancos de dados são importantes para empresas e órgãos governamentais no Brasil.

Sem falar do apagão da semana passada.

Rafael Koike: Bom, eu ia mencionar esse caso...

Luiz Eduardo: menciona de leve então

Rafael Koike: porque?

Luiz Eduardo: então menciona então

Rafael Koike: com a evolução dos ataques de hackers, e com a evolução das soluções de segurança que as empresas e o governo vem implementando. Os hackers, ou melhor dizendo, os crackers. Usando o jargão correto. Eles vem saindo dos ataques voltados a infraestrutura de rede e passam a se utilizar de brechas nas aplicações e nos bancos de dados para fazer suas invasões.

Outra coisa também muito importante, é que os objetivos dos hackers nos primórdios eram os de status. Ou seja, fazer um defacement em uma página era mais importante do que se ganhar dinheiro. Porque o cracker queria ter a notoriedade.

Hoje os ataques para as empresas, são voltados com fins financeiros. Ou seja, eu prefiro invadir uma aplicação de um sistema e coletar informações que depois eu possa ter lucratividade com elas, eu posso vende-las para alguém, eu posso utilizar para comprar um produto, do que ter status. Eu prefiro entrar em uma aplicação e me manter escondido, me manter atrás da aplicação.

Luiz Eduardo: e poder usar isso depois, poder se aproveitar mais desse exploit

Antes era por fun and profit, agora é mais profit do que por fun.

Rafael Koike: isso. Então, o que acontece, os hackers não vão mais atacar a minha infraestrutura de redes para tentar derrubá-la.

Eles vão tentar atacar minha aplicação para se esconder atrás dela. Então, segurança de bancos de dados, e segurança de aplicações web, eu acho que é o foco hoje para você conseguir se proteger do tipo de ameaça que os hackers e os crackers tentam entrar na sua rede. Então, a gente está saindo do ambiente de firewall e ips, que já está consolidado, e que é muito mais difícil de você tentar burlar. Do que aplicação e banco de dados, que hoje, as empresas ainda estão começando a olhar para esse lado do prisma. Ou seja, eu tenho uma aplicação web que eu não penso em segurança nativamente dela, eu tenho um banco de dados em que eu não penso nativamente numa segurança desse banco.

Muitas vezes, uma aplicação web, tem seu usuário e senha de banco de dados, gravada ou programada dentro de sua própria linguagem. Ou seja, eu tenho uma variável username e password, hardcoded dentro do meu .php, dentro do meu .asp. Então não existe uma segurança razoável nisso, eu tenho um único usuário e senha para acessar o meu banco de dados o que para mim é um ponto de falhas. E que no futuro isso tenho certeza que isso vai evoluir.

Luiz Eduardo: Claro. Do mesmo jeito que os ataques saíram da camada de redes, e subiram na camada OSI e hoje estão em aplicações. E vai saber aonde estão. E nem vamos falar do problema de fraude interna e essas outras coisas que de repente você vai mencionar depois.

Como você estava falando de normativas antes, pergunto para você, no mercado brasileiro, qual é o papel de normativas como PCI, SOX, etc...

Rafael Koike: Acho que cada vez mais tem um papel mais importante, porque muitas das empresas brasileiras tem seus papéis negociados lá fora. Nos Estados Unidos, por exemplo. Então, estar em conformidade com uma norma como a Sarbanes-Oxley, é quase que obrigatório para uma empresa que quer vender para um mercado como o americano. Em todo esse mercado globalizado, é quase indispensável para uma empresa que quer crescer, que quer aumentar o seu volume de vendas e que quer vender para o mundo todo, estar em conformidade com normas. E fora isso, muitas das empresas que não precisam vender lá fora, também querem estar em conformidade com normas internacionais para mostrar a seriedade da empresa, para mostrar a seriedade do que ela fatura, dos seus números contábeis. Então também acaba sendo um diferencial para uma empresa nacional, mesmo que não vá vender/ negociar seus papéis lá fora. Ela está em conformidade, muitas vezes, com normas internacionais.

Luiz Eduardo: Exato. Isso vem muito de encontro com o que você tinha comentado antes. A evolução do mercado, digamos assim. A níveis de soluções e etc. Hoje é um pouco mais do que proteger, já foi a época que colocar um firewall, configurá-lo propriamente e, ter certeza que a rede estava segura... já passamos dessa fase. Estamos hoje em uma fase, como profissionais de segurança, temos que provar, por políticas internas ou então até por uma questão de compliance, provar que o firewall está realmente protegendo do jeito que deveria proteger.

Rafael Koike: Eu acho que o mercado todo mudou o objetivo do que era TI de 10 anos atrás para o que é TI hoje. Há 10 anos atrás, você tinha a necessidade de se conectar a internet para consultar uma página, de um site, para navegar por questões recreativas. Hoje, estar conectado na internet é ganhar dinheiro. Ou seja, você tem rentabilidade em ter a sua empresa divulgada na internet, você tem rentabilidade quando você otimiza o seu processo de pagamento e recebimento online. Enviando transações através da internet para o seu banco, efetuando o pagamento da sua folha de funcionários. Então, hoje o papel da internet, o papel da TI, é muito mais forte e tem muito mais o cunho financeiro do que há 10 anos ou 5 anos atrás. Quando o impacto de se ter uma rede fora do ar, não é tão grande quanto hoje. A nossa informação está digitalizada, ela está em bancos de dados, aplicações e está virada para a web, ela tem esse acesso web. A gente tem um tempo de transação muito menor do que há 10 anos atrás, há 5 anos atrás. Então, é fundamental, hoje você dar essa segurança, não só porque a sua infraestrutura vai sair para a internet para navegação. Mas, porque se você para o seu ambiente, hoje, de aplicações, você perde dinheiro com isso. Com certeza, é fundamental, ter segurança hoje. E, juntando essa questão de se perder dinheiro, com normas/ conformidades. A área de segurança da informação hoje, ela se justifica através desses requisitos, aquilo que há 10 anos atrás, investimento em infraestrutura de segurança, era um custo para a empresa, ou seja, não tinha justificativa, você não conseguia justificar altos investimentos. Hoje isso se auto-justifica, só pela questão de conformidade com normas e pelo prejuízo financeiro que você consegue fazer através de uma análise de risco. Então hoje, a área de segurança de informação, a área de segurança da aplicação ela se justifica por si só.

Luiz Eduardo: o famoso Retorno de Investimento (RoI), muito discutido pelo mundo.

Rafael Koike: Pois é. Coisa que antes você não encarava a área de segurança como Retorno de Investimento, mas sim, como um custo. Hoje você tem isso de maneira palpável, você consegue mostrar isso com a+b para a seus clientes, para a sua área diretiva.

Luiz Eduardo: Certo. Legal, agora a pergunta mais difícil. Dos assuntos do mundo de segurança, quais tiram o seu sono, tirando o apagão, que só ajuda a gente dormir um pouco mais e perder a hora no dia seguinte.

Rafael Koike: A questão de você ter que estar em conformidade, é uma questão que a gente sempre fica pensando. A questão também do SaaS e Cloud Computing, é uma coisa que também tira o sono, porque é uma quebra de paradigma que estamos começando a enfrentar. O Cloud Computing tirando a informação do seu ambiente e mandando ela para a nuvem. Isso vem sendo muito discutido entre os meus colegas da segurança da informação. Como eu garanto que essa informação continua íntegra e confidencial. Em termos de governo, como o governo pode passar a sua informação que está hoje dentro do seu ambiente, do seu domínio físico para um ambiente externo e garantir que isso não vai cair em mãos erradas, como outros países, ou, concorrentes políticos. Isso é um grande desafio hoje.

Luiz Eduardo: Coisas que em termos tecnológicos, talvez ninguém tenha pensado. Vai saber se os seus dados estão lá “dormindo” do lado dos dados do seu arqui-inimigo.

Rafael Koike: Pois é, eu fico imaginando, por exemplo os Estados Unidos, que presam muito para a questão de segurança nacional. Será que em algum momento o governo vai aderir ao Cloud Computing? Como que isso vai acontecer? Como vamos garantir que isso vai funcionar? Acho que esse é um grande desafio hoje, o Cloud, para o governo e para as empresas. Quer dizer, algumas empresas também vem se questionando se elas devem ir para o Cloud, de que maneira isso vai acontecer. Isso é um grande desafio.

Luiz Eduardo: Então, agora como estamos no podcast da Imperva. Vamos falar sobre Imperva. Qual é as suas opiniões sobre o DAS, WAF, DAM e DBFW, falar um pouco sobre o que você acha de cada uma dessas soluções e como tudo isso junto trás benefícios ao mercado.

Rafael Koike: Imperva é uma empresa dedicada a segurança de aplicações e bancos de dados. Isso é um grande diferencial em relação à seus concorrentes. Até porque a Telsinc não tinha nenhum parceiro que oferecesse solução para atender essa demanda de mercado. Então, como a gente está saindo de um mercado consolidado, como o de infraestrutura de segurança, e começando a olhar para a segurança de bancos de dados. A Imperva tem um papel chave nesse mercado. Quanto ao DAS, é uma ferramenta que vai ajudar muito aumentar a segurança de bancos de dados, porque ela vai analisar o meu ambiente de rede, encontrando ali bancos de dados que eu ainda não tinha monitorado, que ainda não estava analisando. E vai monitorar esses bancos de dados e começar a saber se eu tenho a mesma informação em outros bancos, se eu tenho informações sensíveis nesses bancos. Vai ajudar a categorizar, ajudar a conseguir a encontrar aonde estão as informações sensíveis nos meus bancos de dados. O WAF, junto com o DAM e DBFW, formam uma solução que eu não encontro em nenhuma outra solução do mercado. Que é enxergar desde o endereço IP da estação que está lá na internet, o usuário que essa estação se logou no meu web application e, com que banco de dados ele está se conectando e qual consulta que ele está fazendo. Essa visão completa vai me gerar uma trilha de auditoria, que hoje eu não tenho como enxergar. Ou seja, sem esse tipo de solução, a minha análise forense para qualquer tipo de incidente é totalmente manual e passível de falhas. Se eu tiver uma ferramenta que me auxilia na automatização desse processo, olhando 24 horas/dia quem está acessando a minha aplicação web e o que está sendo acessado no meu banco de dados, eu acho que é um diferencial incomparável no mercado. E a Imperva está à frente dos seus concorrentes, junto com a Telsinc, para oferecer isso para os clientes. Estamos no início da onda, estamos no começo do mercado de segurança de aplicações e bancos de dados.

Luiz Eduardo: Ótimo. E, para finalizar, quais são as suas previsões pro mercado de segurança no Brasil, em um futuro próximo e talvez em um não tão próximo.

Rafael Koike: Eu entendo que o mercado brasileiro está começando a se globalizar, e, está muito mais antenado com o que acontece no mercado americano. Então aquilo que, normalmente, as tendências de mercado que aconteciam primeiro no mercado americano e se levava em torno de 5 anos para começar a maturar dentro do mercado brasileiro. Esse tempo, esse delay que existe entre o mercado americano e brasileiro, vai diminuir muito nos próximos anos. Ou seja, eu entendo que, a curto e médio prazo, as tendências que estão acontecendo no mercado americano vão vir para o Brasil de uma maneira muito mais rápida. E até porque, eu acho que olhando a aposta do mundo, de que o Brasil é o futuro, de que o Brasil é um país emergente que tem muito futuro. Acho que faz muito sentido isso que estou falando, de que cada vez mais o Brasil vai estar ao lado do mercado americano e os países de primeiro mundo.

Luiz Eduardo: é isso aí, Koike. Queria agradecer a sua presença no podcast da Imperva. E, não sei se você quer falar alguma coisa final aqui

Rafael Koike: Bom, eu queria agradecer muito em estar sendo esse brasileiro que está fazendo este primeiro podcast em português. Dizer para os ouvintes que vão estar ouvindo este podcast no Brasil e no mundo, saibam que o mercado brasileiro tem muito ainda para contribuir na evolução das ferramentas de soluções de segurança. E com certeza, eu acho que a Telsinc vai ser um grande parceiro para os clientes que estejam buscando ferramentas de segurança para banco de dados e aplicações web. Então, fica aí, a minha mensagem de agradecimento à Imperva, e a minha mensagem aos clientes ouvindo este podcast que estamos muito otimistas em relação à essa parceria com a Imperva. É isso aí.

Luiz Eduardo: Muito obrigado, Rafael.

Rafael Koike: Obrigado, Luiz.

Luiz Eduardo: Se você quiser saber mais sobre os assuntos discutidos neste podcast ou sobre a Imperva, pode nos visitar no nosso site na web <http://www.imperva.com>, ou o nosso blog <http://blog.imperva.com>, e também pode nos seguir no twitter twitter.com/imperva ou então, pode também nos enviar um email no blog@imperva.com



Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004