ANBIMA Debate Cybersecurity

7 de junho de 2016
Local: São Paulo, com transmissão pela internet

Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais

APRESENTAÇÃO

A proteção de ativos digitais é o grande desafio das corporações, sejam elas de quaisquer áreas de negócios. O número de ataques a redes de dados é crescente e eles alcançam desde empresas de cartão de crédito até registros de dados médicos. Assim, como a motivação dos cibercriminosos é diversa, também são variadas as formas de ataque. Não há receita de segurança ou plano de proteção de prateleira. O desafio está justamente no equilíbrio entre as variáveis de cada negócio.

Para debater o tema, especialistas em segurança da informação participaram, em 7 de junho de 2016, da primeira edição da ANBIMA Debate, série de eventos exclusivos para associados criada para discutir temas de interesse do mercado.

O evento, realizado em São Paulo e transmitido pela internet, contou com 150 participantes, dentre profissionais de bancos, gestoras de recursos e distribuidoras. O público pôde assistir às apresentações e interagir com os debatedores enviando perguntas e sugestões.

Este relatório consolida os principais pontos da mesa-redonda.

Participantes:
Marcelo Amaral, head of security office and business continuity do BTG Pactual;
Nelson Novaes, chief information security officer do Itaú-Unibanco;
Paulo Martins, consultor independente.

Moderação:
Paulo Veloso, da HP Enterprise.

Conceito

É fácil lembrar apenas de tecnologia quando se fala em cybersecurity, mas o conceito é bem mais amplo. Envolve um conjunto de tecnologias, processos, pessoas e práticas destinado a proteger redes, computadores, programas, aplicação e/ou dados de ataques ou danos provenientes de acessos não autorizados.

A importância da cybersecurity cresce à medida que o mundo se torna cada vez mais digital, cenário no qual instituições de todos os setores da sociedade coletam, processam, armazenam e transmitem bilhões de informações confidenciais por meio de redes de comunicações.

A segurança dessas informações se apoia em três pilares:

usuários **aplicações** **dados**

A forma como essas partes se comunicam é o ponto de partida para qualquer plano de proteção a ativos digitais.

Parece simples, mas a atividade de proteger arquivos digitais se torna cada vez mais complexa devido às novas tecnologias que mudam diariamente nossos modelos de negócios. Tecnologias como armazenamento em nuvem ou internet das coisas trazem novas dimensões e paradigmas para a segurança da informação.

Assim como mudaram a forma de fazer negócio, essas tecnologias também obrigaram as empresas a reverem suas estratégias de segurança. Hoje os ativos de uma empresa não ficam confinados entre seus muros. Existem movimentos como o Bring Your Own Device, por exemplo, que permite aos funcionários trabalharem com seus próprios dispositivos. Também há um movimento de migração das operações para plataformas de nuvem. Assim, cybersecurity exige muito mais do que a preocupação com a plataforma x ou y. O desafio é a interação entre todas essas tecnologias. O mundo no qual tudo está aprisionado a uma infraestrutura única não existe mais.

"Não tem limites para a fraude e ela não é só financeira."
– Paulo Veloso, sobre a dimensão atual dos ataques cibernéticos

Números superlativos

Os números de ciberataques dão uma dimensão da grandiosidade do problema. Apenas em 2015 foram identificados mais de 898 milhões de registros comprometidos em mais de 4,8 mil ataques bem-sucedidos. Para as empresas, não se trata mais de considerar "se" elas serão atacadas, mas "quando" serão atacadas. Para especialistas, é só uma questão de tempo até que alguma quadrilha digital se interesse por sua empresa. E quando esse momento chegar é preciso estar preparado.

O setor financeiro é um dos que mais sofrem com os cibercrimes, pois seu modelo de negócio é baseado em dados financeiros e pessoais de milhões de pessoas, ou seja, informações de alto valor para criminosos digitais.

"Cybersecurity é mais do que só proteção a dados. É preciso considerar também a interação com as áreas de negócios."
– Paulo Veloso, sobre o impacto das novas tecnologias

Quem são os criminosos digitais?

Os criminosos digitais são inimigos que não têm rosto ou perfil. Eles se diferem em motivações, objetivos e estrutura. E por isso é tão difícil impedi-los de comprometer propriedades intelectuais, dados pessoais e/ou credenciais de acesso.

As organizações criminosas digitais são bastante sofisticadas. Elas têm uma estrutura muito parecida com as de uma empresa tradicional; têm recursos humanos, área de desenvolvimento de produtos, áreas de finanças e de vendas, além, é claro, de corpo jurídico. Essas quadrilhas conhecem bem as legislações internacionais, assim se instalam em lugares estratégicos nos quais elas possam tirar proveito das leis e dos modelos de extradição, por exemplo.

"Já descobrimos organizações complexas com áreas especializadas em criar phishing para bancos brasileiros"
– Paulo Veloso, sobre a especialização dos cibercriminosos.

Quais são os principais desafios?

O principal problema para as empresas é a equação perversa entre os custos do ataque e da defesa. Quem ataca tem tudo muito barato e potencial lucrativo muito grande. Por outro lado, quem precisa se defender tem custo altíssimo para proteger seus sistemas.

Devido a essa facilidade, surgem diariamente diversos novos tipos de ameaça. O trabalho de atualização das defesas é constante e nem sempre simples. Os tipos mais comuns de ataques nas empresas são:

Denial of service: ataque que inviabiliza a utilização de sistemas e serviços, como tirar um site do ar ou impedir o uso de caixas eletrônicos, por exemplo;

Phishing: fraude que tenta roubar dados pessoais ao se fazer passar por uma instituição confiável;

Ransonware: sequestro de sistemas e informações, impedindo o acesso até que seja pago o "resgate";

APT: sigla para ameaça persistente avançada, que consiste em atacar uma rede a partir de um programa capaz de permanecer oculto dentro dos sistemas por longos períodos. Trata-se de um ataque extremamente sofisticado, idealizado para quebrar as diversas barreiras de segurança de um sistema sem ser identificado. O invasor acessa o ambiente digital e permanece lá dentro por muito tempo, coletando dados ou adormecido, até que a melhor oportunidade de roubo de informação apareça.

"O APT é um grande problema porque com tempo, motivação e dinheiro, o hacker consegue qualquer coisa."
– Marcelo Amaral, sobre as principais ameaças cibernéticas

Como se proteger?

Para que a segurança da informação seja bem feita, é necessário que as bases de todo o sistema sejam sólidas e consistentes. Na idealização dos projetos, é preciso pensar na simplificação dos processos, sem diminuir a importância deles; não os entender apenas como algo rotineiro, mas como algo essencial, e evoluir a partir daí. Só assim é possível tirar o máximo proveito das novas tecnologias.

Neste novo cenário, mais do que nunca, as empresas precisam investir muito em monitoramento para identificar comportamentos suspeitos; e estabelecer estratégias de reação. Os ataques são eminentes e a equipe de segurança precisa estar apta para detê-los assim que detectados.

"Não existe 100% de segurança. É preciso pensar no processo e saber como reagir aos ataques."

– Paulo Martins, sobre o panorama atual da segurança

"Ao trabalhar com segurança, é preciso extrapolar a área de conhecimento, estar atualizado e entender como as novidades impactam o negócio."

– Nelson Novaes, sobre o papel do profissional de segurança

As novas tecnologias também podem ser utilizadas para auxiliar na segurança da informação. Uma tendência em alta nos dias atuais é a proteção com foco no comportamento do usuário, por meio da qual os sistemas aprendem e reconhecem as formas como os clientes interagem com os serviços, evitando falsas autenticações. Com isso, a segurança entra no campo da inteligência artificial.

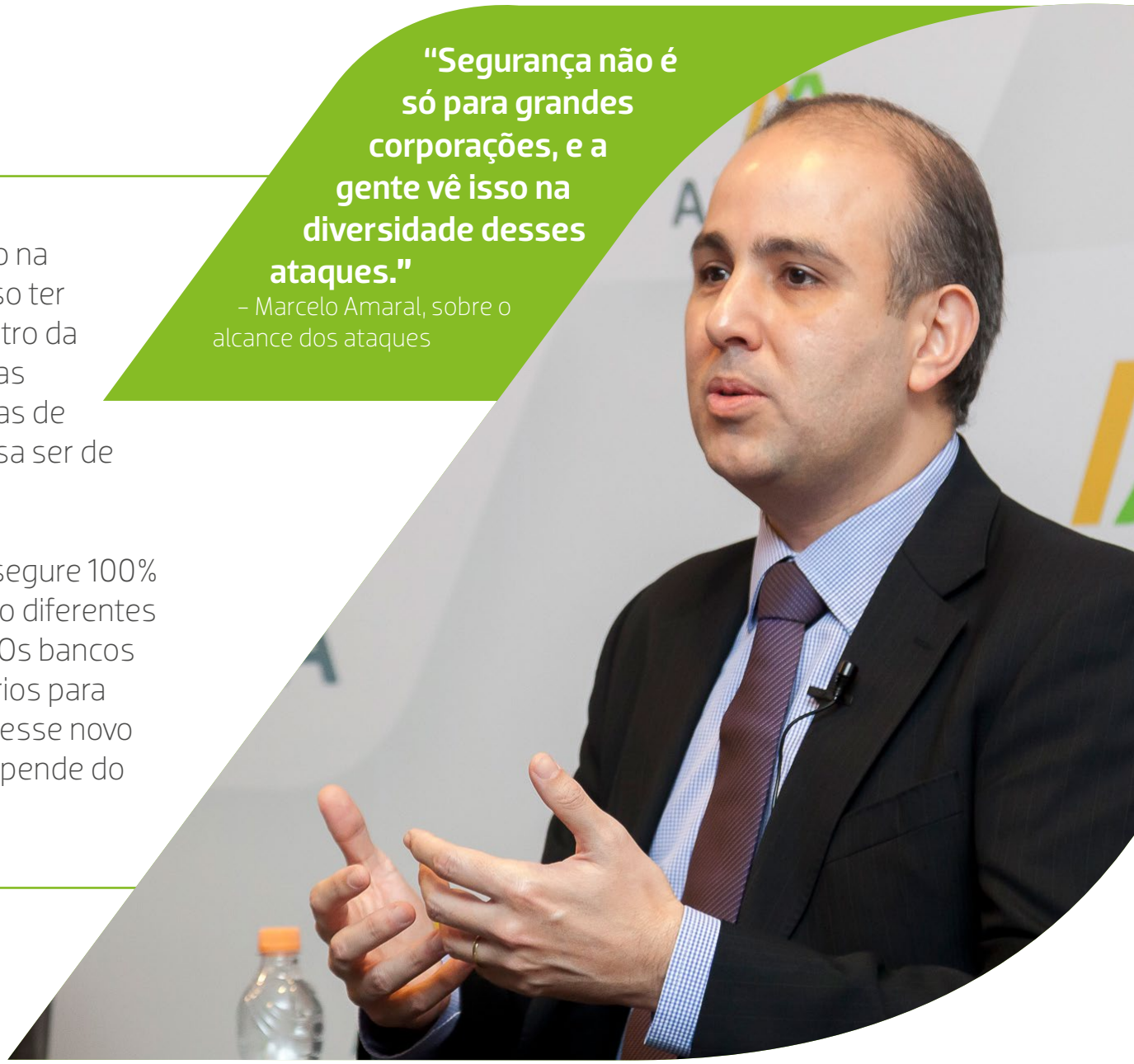
Mas nada disso será eficiente se a segurança da informação não estiver alinhada à estratégia de negócio da empresa. Para diminuir atritos com as áreas que têm poder de decisão, é necessário assegurar que o aspecto segurança esteja inserido desde a fase de concepção de um negócio. Isso significa que a equipe de tecnologia deve estar envolvida em todos os projetos desde o início. Só assim se pode garantir que o quesito segurança seja contemplado e que o produto seja lançado com todos os controles e as ações mitigatórias.

O ataque externo não é o único a ser considerado na segurança da informação nas empresas. É preciso ter consciência de que os ataques podem vir de dentro da empresa. Para isso, é necessário estabelecer boas políticas e deixar claro quais são as regras internas de segurança e as punições aplicáveis. A visão precisa ser de 360 graus, ou pode-se ser surpreendido.

Não existe um modelo pré-estabelecido que assegure 100% de segurança digital. Até porque as empresas são diferentes entre si e os modelos de negócios são diversos. Os bancos digitais, por exemplo, criaram mecanismos próprios para balancear os riscos e as vantagens resultantes desse novo tipo de serviço. A sustentabilidade do negócio depende do equilíbrio.

"Segurança não é só para grandes corporações, e a gente vê isso na diversidade desses ataques."

– Marcelo Amaral, sobre o alcance dos ataques



A novidade agora são as fintechs, empresas essencialmente tecnológicas que oferecem serviços financeiros. A atuação delas está ligada a um movimento disruptivo, que ainda precisa encontrar um modelo de proteção das informações. A experiência mostra que as disrupções tecnológicas passam por um ciclo de amadurecimento até que o modelo seja definido. A euforia inicial avança para um processo de "desilusão", durante o qual muitas empresas naufragam. As que sobrevivem passam por processos de experimentação até alcançarem o patamar de maturidade.

A questão é: como será a segurança da informação das fintechs que alcançarem a maturidade? Provavelmente não será a segurança como conhecemos hoje, mas deve continuar assegurando o equilíbrio entre o risco e o custo.

"Não nos iludamos. A forma de fazer segurança da informação no futuro não será a que temos hoje."
– Paulo Martins, sobre o futuro e a influência das fintechs

ANBIMA Debate Cybersecurity

Saiba mais

Assista ao vídeo completo do ANBIMA Debate: Cybersecurity realizado em 7 de junho de 2016

Acessar »

HP Cyber Risk Report 2016:

Acessar »

Apresentação: Cybersecurity (por Paulo Veloso):

Acessar »