

Foi com a provocação do título que teve início na terça-feira, 7, o ANBIMA Debate: Cybersecurity. A frase é de Paulo Veloso, especialista em segurança da informação da HP Enterprise, que moderou a discussão que foi acompanhada por mais de 130 pessoas.

O evento é o primeiro de uma série de encontros exclusivos para profissionais das instituições associadas, que discutirá assuntos de interesse do mercado do ponto de vista dos negócios. Para a estreia, convidamos Marcelo Amaral, head of security office and business continuity do BTG Pactual; Nelson Novaes, chief information security officer do Itaú-Unibanco; e Paulo Martins, consultor independente.

Paulo Veloso abriu o evento contextualizado cibersegurança e apresentando alguns casos de ataques no mercado financeiro. Segundo ele, segurança cibernética é um conjunto de tecnologias, processos e práticas destinado a proteger as redes, computadores, programas e dados de ataques, danos ou acessos não autorizados. “No ano passado, foram registrados mais de 898 milhões de registros comprometidos”, disse ele. “E a fraude não é local, ela é global e cada vez mais especializada”.

Saiba mais

[Apresentação - Paulo Veloso](#)

[Baixe a apresentação dos palestrantes](#)

[Assista à íntegra do evento](#)

[Inscreva-se em nosso canal no YouTube e assista aos vídeos de nossos eventos](#)

Um dos pontos do debate foram os desafios de segurança trazidos pela digitalização dos serviços. Para Marcelo Amaral, o cenário atual gera novas possibilidades de ataque e o potencial de dano é ampliado. “O nosso grande desafio é desvendar como oferecer novos canais digitais dando simplicidade para o negócio sem prejudicar a usabilidade para o cliente”, explicou. “Precisamos ter áreas de segurança da informação e gestão de risco que sejam pró-business e a favor do usuário e, ao mesmo tempo, sem incorrer mais risco”.

Os especialistas elencaram os tipos de ataque mais comuns e problemáticos para as empresas. Segundo eles, os mais comuns são os ataques de denial of service, que derrubam serviços e os deixam indisponíveis; phishing, que é a tentativa de adquirir dados pessoais enganando usuários; ransomware, sequestro de sistemas de informação e devolução mediante o pagamento de resgate; e APT, sigla para ameaça persistente avançada.

“O APT é um ataque mais avançado que utiliza um conjunto de técnicas que vai desde engenharias sociais à contratação de artefatos que dão a garantia de passar todos os seus controles”, explica Nelson Novaes. “Grandes bancos de todo o mundo já foram comprometidos por esse tipo de ataque porque não existe uma forma infalível de evitá-lo”.

Segundo Paulo Martins, um dos pontos básicos da segurança contra esses ataques é implantar a segurança máxima possível, monitorar e saber reagir. “Essas invasões geram comportamentos anormais nas redes e temos diversas tecnologias – como analytics e inteligência artificial – que podem detectar esses padrões considerando, inclusive, as peculiaridades de cada dia”, explica o consultor.

Um dos desafios levantados durante o evento também foi o atrito entre a velocidade necessária para lançamento de novos produtos e serviços e a necessidade de tempo para garantir a segurança plena dos mesmos. Para Nelson Novaes, a equipe de segurança precisa tomar decisões rápidas e estar sempre alinhada com a estratégia de negócio. “Para diminuir este atrito é preciso inserir a área de segurança desde a fase de concepção de um projeto para garantir que todos os caminhos de segurança sejam contemplados”, explicou.

Os especialistas discutiram ainda criptografia, fintechs, ataques internos, entre outros temas. A

Íntegra do ANBIMA Debate: Cybersecurity está disponível em nosso canal do YouTube.

Fonte: [ANBIMA](#), em 09.06.2016.