Titulo: Congresso nacional de segurança cibernética
Veículo: Revista Infra Outsouncing & Workplace
Página: 70 e 71
Tiragem: 10000
Seção: ***
Data: 01/05/2015
Centimetragem: 102950
Valor: R$ 15.895,48

SEGURANÇA CIBERNÉTICA | por Léa Lobo

Divulgação

CONGRESSO NACIONAL DE SEGURANÇA CIBERNÉTICA

■ Especialistas nacionais e internacionais debateram fragilidades e riscos para empresas e usuários da internet

Ataques cibernéticos fazem parte do dia a dia, causando transtornos e prejuízos a empresas e usuários que trocam informações e documentos na internet. Dados divulgados na imprensa informam que o crime cibernético é o terceiro que mais causa prejuízos ao mundo, depois de narcotráfico e falsificação de marcas e de propriedade intelectual. Para disseminar a importância da pauta, o Departamento de Segurança (Deseg) da Federação das Indústrias do Estado de São Paulo (Fiesp) e do Centro das Indústrias do Estado de São Paulo (Ciesp) promoveram no último 31/03 o Congresso Nacional de Segurança Cibernética.

Durante o congresso, o Deseg também lançou a "Cartilha de Boas Práticas", desenvolvida pelo Grupo de Trabalho em Segurança Cibernética da Fiesp para orientar empresas sobre segurança na utilização da internet e redes sociais e armazenamento de dados, dentre outros procedimentos na rede.

Com uma grade de 30 palestrantes na programação, estavam presentes Especialistas como Gabi Siboni, chefe do Programa de Militares e Assuntos Estratégicos e do Programa de Segurança Cibernética do Instituto de Estudos de Segurança Nacional de Israel e o inglês John Red, CEO da empresa que desenvolveu um software testado nos Jogos Olímpicos de Londres , em 2012, que monitora e alerta usuários de redes sociais sobre picos no volume de dados, enquanto identifica a localização geográfica do comentário. Raphael Mandarino Junior, Ex-diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC); João Rufino de Sales, CEO da IP Consultores; e o Diretor do Deseg, Rony Vainzof, também contribuíram no painel de abertura.

"Precisamos de segurança, ética e responsabilidade para ajudar a proteger a indústria e alavancar negócios no ambiente digital. Queremos uma internet que garanta nossos direitos fundamentais, que seja neutra e livre, e não um ambiente usado para fraudes e condutas ilícitas", disse Vainzof. Ele lembrou que é comprovado que a grande maioria dos ataques cibernéticos vem através do e-mail e apresentou uma síntese da pesquisa "Segurança Cibernética" elaborada pelo Deseg, incluindo pequenas, média e grandes indústrias e identificaram que o nível de maturidade é pequeno e que precisa ser melhorado. Confira alguns resultados:

- 23,5% das empresas não sabem quantos ataques ocorreram no último ano;
- 19,5% das grandes empresas não monitoraram os ataques no último ano;
- 59% dos ataques cibernéticos tiveram alvos financeiros no último ano, sendo que em sua maioria são em pequenas e médias empresas;

- 46,2% dos ataques visando a informações sigilosas tiveram como alvo grandes empresas;
- 47,1% das empresas não monitoram os e-mails dos seus colaboradores;
- 70,8% das empresas não utilizam computação em nuvem.

No painel, os integrantes deixam claro que a capacitação e a orientação das pessoas quanto ao tema são de fundamental importância, pois os ataques são maciços e sem precedentes. Diariamente as pessoas recebem e-mails maliciosos e fraudulentos que objetivam danificar e capturar informações em seus diversos tipos de computadores e gadgets. Muitos não sabem que um bilhão de dados pessoais foram roubados no mundo, sendo os de propriedade intelectual, os mais importantes deles. A maioria dos ataques vem de diversas localidades do mundo. Hoje, consegue-se rastrear, mas nem sempre, embora haja colaboração e confiança entre alguns países. Nem sempre é possível punir o criminoso, pois às vezes ele é de um determinado país, o roubo aconteceu em outra localidade e a legislação de cada unidade geográfica tem suas regras.

Siboni alertou o fato de que todos os dias há milhares de criminosos tentando invadir e capturar a informação e é preciso uma cooperação internacional para desenvolver um trabalho a fim de ajustar todo o conhecimento sobre os crimes cibernéticos dos países em conjunto. "A internet é o condutor e as pessoas estão cometendo erros, não de propósito, mas facilitam os acessos para o crime com a abertura de e-mails fraudulentos, por falta de informação sobre estes ataques cibernéticos", resumiu o palestrante de Israel.

Sales falou sobre a legislação que trata o tema: "O castelo da segurança muitas vezes é tirado do castelo da privacidade", e essa é mais uma das barreiras que os especialistas precisam trabalhar de forma diferenciada.

Mandarino lembrou que no Brasil, o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014) regula o uso da internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. Mas também possui suas vulnerabilidades e há casos em que protege inclusive os hackers. "É preciso criar medo na comunidade criminal, entretanto falta uma visão e ferramentas do Estado para tudo isso", reforça o Ex-diretor do DSIC.

É importante reforçar que a motivação para os ataques cibernéticos é o dinheiro, e se sua empresa e colaboradores querem se proteger, é melhor ficarem atentos para não facilitar que informações privilegiadas fiquem à disposição em notebooks e gadgets itinerantes, que ficam abertos em redes sociais de profissionais que, muitas vezes, desconhecem a malícia criminosa, entre tantos outros cuidados. Capacitar e orientar são deveres de todos! A conclusão do painel é de que essa ainda não é uma guerra perdida entre "moços e bandidos cibernéticos", mas é preciso pensar no longo prazo, capacitando, orientando e trabalhando em conjunto com a comunidade mundial para criar meios para conseguir uma comunicação segura no presente e no futuro para a internet. ■

CARTILHA DE ORIENTAÇÃO CONTRA FRAUDES E ATAQUES CIBERNÉTICOS

O Deseg da Fiesp lançou no dia do congresso uma cartilha com orientações a empresas para evitar fraudes e ataques cibernéticos. A cartilha orienta sobre como proteger dados, documentos e finanças manipuladas virtualmente, incluindo a implantação de regulamento e termos de uso dos sistemas, classificação e perfis de usuários, utilização de e-mails corporativos, uso de mídias sociais, cuidados ao disponibilizar instrumentos eletrônicos – como notebook, tablets e telefones – e uso da internet. Citados no caderno, dados da Kaspersky Lab, empresa especializada em produtos de proteção cibernética, informam que no Brasil, durante a Copa do Mundo e no segundo semestre de 2014, foram registradas 87,5 mil tentativas de infecção de vírus com objetivo de fraude financeira e mais de 365 mil com foco em dispositivos móveis. Segundo Vainzof, ameaças cibernéticas representam hoje um dos maiores problemas enfrentados por empresas que utilizam a internet para a comunicação com a cadeia de interesses do negócio e mantém expostas as informações. "Além da rapidez do trabalho, é importante avaliar os riscos, mudar os hábitos na rede e investir em ferramentas que garantam mais proteção às informações", explicou Vainzof.

Faça o download da cartilha no site da Fiesp, link: http://bit.ly/1IQ0UnR