Publicado no Jornal i online
18/08/2021

OBSERVATÓRIO CONTRA A FRAUDE

Breves reflexões sobre fraudes digitais

É importante que as pessoas sejam informadas e com bastante frequência, uma vez que o autor da fraude conta sempre com o descuido do usuário

Aldo Andretta

Fraudes digitais sempre foram uma grande preocupação tanto para pessoas quanto para organizações. Nesta reflexão, falaremos um pouco dos impactos que elas causam, vamos trazer algumas pesquisas referenciais e a problemática quanto a regulamentação internacional do assunto.

A pandemia trouxe uma aceleração dos negócios digitais; muitos foram fortalecidos pela necessidade de confinamento da população e outros foram tirados do papel ou criados para essa nova realidade.

Consequentemente os lucros destes negócios digitais dispararam, mas por outro lado as fraudes também, pois os cibercriminosos aproveitaram as oportunidades de um maior volume de transações, falta de preparação das organizações com o tema, bem como as fragilidades das proteções cibernéticas, como a falta ou a desatualização de antivírus e firewalls, além de redes domésticas menos protegidas.

Para o cibercriminoso o crime na maioria das vezes compensa. Primeiramente, porque sempre dão o primeiro passo no aspecto tecnológico. Depois é que conseguem se esconder por de trás da tecnologia e de legislações enfraquecidas, como veremos adiante. Em muito tem avançado os órgãos de investigação para identificar estes criminosos, porém, ainda há muito que se fazer.

Tais cibercriminosos em sua grande maioria agem em conjunto. Segundo pesquisa denominada "*2021 Data Breach investigation Report*" realizada pela Verizon (https://www.verizon.com/business/en-gb/resources/reports/dbir/) podemos ver que em 85% dos casos analisados foram executados por organizações criminosas. Os dados ainda mostram que 70% dos crimes tiveram motivação financeira, o que de certo modo é evidente.

Isso explica o aumento de 10% para 30% do interesse de criminosos por dados como BIN de cartões de Crédito (primeiros números dos cartões, pois os fraudadores fazem um estudo de quais são mais fáceis de serem aprovados), número na integra dos cartões, número de identificação dos bancos e CVV (Card Verification Value, que são três números que estão atrás dos cartões). Ou seja, temos uma captura de informações de cartões, geralmente de pessoas físicas, que serão utilizados em e-commerces espalhados pelo mundo todo. Ou seja, fraudam a pessoa natural e a organização!

Os dados acima podem ser capturados simplesmente na internet. Inúmeros sites fornecem dados de cartões que podem ser validados por criminosos. Mas a pesquisa citada nos mostra que 35% destas violações ocorrem por intermédio da engenharia social. O principal caso que estas violações acontecem são relacionados ao Phising, que consiste na técnica de se passar por alguma organização confiável e coletar os dados do usuário, por intermédio de um e-mail, site ou aplicativo. E as pessoas caem, mostrando que falta um bocado de "educação tecnológica" para evitar este tipo de fraude.

Há um trabalho informativo, muito claro preciso, realizado pela Comissão de Mercado de Valores Mobiliários - CMVM, mostrando como o que é cada tipo de fraude, como os fraudadores agem e como as pessoas se protegem deste tipo de ameaça. (https://www.cmvm.pt/pt/EstatisticasEstudosEPublicacoes/Brochuras/Documents/11-Fraudes%20Digitais.pdf). É importante que as pessoas sejam informadas e com bastante frequência, uma vez que o fraudador sempre conta com o descuido do usuário.

Não podemos esquecer, também, dos malwares, que tem o objetivo de infectar sistemas, programas e aplicativos, com o único intuito de capturar os dados e transmiti-los a cibercriminosos. Mostrando a transnacionalidade deste tipo de crime, um malware denominado "Bizarro", de origem brasileira infectou bancos na América do Sul e Europa, sendo o mais recente um banco italiano

(https://epocanegocios.globo.com/Tecnologia/noticia/2021/05/novo-malware-brasileiro-afeta-sistema-bancario-na-italia.html).

Há outro tipo de ataque cibernético que vem crescendo demasiadamente e causa grande pavor nas organizações que é o ataque de Ransomware (nada mais é do que um malware), que consiste na criptografia de todas as informações de uma organização, sendo que para liberar a chave para decriptografar os arquivos é necessário pagar um alto valor, em bitcoins. Em Portugal, por exemplo, houve um aumento de 70% neste tipo de ataque em dois meses (https://www.tveuropa.pt/noticias/ataques-de-ransomware-aumentam-70-em-dois-meses-em-portugal/)

Segundo um dos estudos em que se baseou a notícia acima, o da empresa (https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/), os cibercriminosos, além de cobrar pela liberação da chave de criptografia, o que não é garantia de que aconteça após o pagamento, cometem uma double-extortion, pedindo quantia para que não divulguem os dados copiados da empresa. Também não há a menor garantia de que os dados foram copiados, quanto não serão divulgados. Porém, há criminosos que cometem uma triple-extortion, sendo que além das duas cobranças mencionadas, cobram dos titulares dos dados que eles não sejam divulgados.

O relatório da empresa Chainalysis (https://blog.chainalysis.com/reports/ransomware-update-may-2021) traz dados assustadores. Em 2020 foram pagos mais de US$400 milhões em bitcoins referentes a resgate de Ransomware. Já em 2021 o número está em US$80 milhões.

Recomenda-se fortemente que estes valores não sejam pagos, uma vez que além de não ter qualquer garantia de que os dados vão ser reestabelecidos, bem como não haverá vazamento de dados, inexiste. É aí que as empresas devem fortalecer seu compliance, pois assim como não há que se utilizar verbas indevidamente para subornar órgãos públicos, também não há que se negociar com cibercriminosos.

Entendo que este assunto é uma faca de dois gumes, pois de um lado não podemos pagar, mas pelo outro o negócio será inviabilizado, pela falta de seus sistemas informático. Existem seguros para riscos cibernéticos, mas minha singela opinião é que é só mais um incentivo para a pratica de cibercrimes. A preocupação é tamanha que alguns países, a exemplo dos Estados Unidos, projetam punir empresa que façam este tipo de pagamento.

Aqui por nossa terra, tivemos ataques não só a empresas, mas também a órgãos públicos. Em 2020 o Tribunal Superior de Justiça foi vítima deste tipo de crime (https://tecnoblog.net/381613/stj-e-vitima-de-ransomware-que-atacou-varias-empresas-nos-eua/) e mais recentemente o Tesouro Nacional também foi (está) sendo vítima de uma ataque de ransomware (https://www.uol.com.br/tilt/noticias/redacao/2021/08/16/tesouro-sofre-ataque-do-tipo-ransomware-o-que-e-isso.htm).

Os ataques de ransomware, talvez sejam as mais transnacionais que existem atualmente. Por exemplo, oataque desferido a empresa JBS nos Estados Unidos, partiu de um grupo Russo (https://www.bbc.com/portuguese/internacional-57344706), denominado REvil. Há outros grupos baseados no Irão, Coréia do Norte, Vietnã, China e Estados Unidos (https://blog.chainalysis.com/reports/ransomware-update-may-2021).

Isso traz um sério problema! Enquanto alguns países tentam inibir por intermédio de legislação e aparelhando os órgãos de investigação, outros não possuem a mesma transparência, pois não há qualquer tipo de cooperação para que estes cibercrimes sejam devidamente investigados. Lava-se as mãos!

Também, não há nenhum organismo internacional que regule o tema. Governos como dos Estados Unidos, Alemanha e Estônia foram atacados por grupos hackers. E aqui fica a pergunta: a quem interessa estes ataques?

Quanto as organizações, cabe a árdua tarefa de se preparar a cada dia com o intuito de não ser vítima de cibercriminosos. Muitas não estão preparadas para evitar o minimizar ataques de Ransomware, por exemplo. Um estudo da ITSecurity mostra que metade das empresas portuguesas não estão preparadas para enfrentar um ataque Ransomware. (https://www.itsecurity.pt/news/analysis/apenas-metade-das-organizacoes-estao-preparadas-para-se-defender-de-ransomware). No Brasil, somente 1/3 das empresas se protegem contra este tipo de ameaça (https://www.cnnbrasil.com.br/business/2021/07/26/pais-esta-na-mira-dos-hackers-mas-so-1-3-das-empresas-se-protege-contra-ataques). E não resta outra alternativa a não ser se preparar!

Quanto a nós, pessoas naturais, em algum momento seremos atacados por Ransomware. A medida que as proteções das organizações forem se fortalecendo os alvos mudaram. Atualmente, por exemplo, perder dados de smartphones causam um verdadeiro estrago na vida de uma

pessoa. O que vou dizer parece um pouco futurista e trágico, não querendo ser cavaleiro do apocalipse, mas por intermédio da tecnologia se controla praticamente tudo: carro que você pode ligar e desligar, regular temperatura de ar condicionado, sem estar dentro dele; casa totalmente automatizadas, que se pode ligar ar condicionado, abrir porta, regular eletroeletrônicos, tudo pelo smartphone. Imagine, por exemplo um carro parando no meio de uma rua ou rodovia, por um ataque cibernético. Já pensaram que alguém pode não entrar mais em casa?

Cabe nos prepararmos para evitarmos os ataques mais simples, em um primeiro momento, quer contratando uma simples ferramentas de antivírus, como não “cair em tentações” com ofertas mirabolantes, bem como não baixarmos arquivos e aplicativos gratuitos! Lembrando que não existe refeição grátis, pois quando se recebe algo gratuitamente, o produto é você!

Não podemos esquecer que a tecnologia avança e a cada dia que ela avança estamos mais vulneráveis a ataques de cibercriminosos. Então, estejamos sempre atentos!