Submetido em 12.12.2017. Aprovado em 10.06.2018

Uso da Tecnologia na Solução de Crimes Virtuais e Boa Práticas de Segurança da Informação

Nickollas Barros Pinheiro
Rogério Oliveira da Silva

Resumo

A proposta deste artigo é mostrar ao leitor a evolução da tecnologia e sua aplicação na segurança pública de modo que auxilie e agilize os processos de investigação de crimes. Este artigo também tem o objetivo de orientar e alertar sobre os perigos e cuidados que se deve ter ao utilizar algum dispositivo como smartphone ou computador, principalmente se estiver conectado à internet. Outro objetivo deste artigo é abordar tópicos relevantes sobre segurança da informação, fazendo com que o leitor reflita sobre o assunto e avalie suas atitudes relacionadas à rede mundial de computadores.
Palavras-Chave: Crimes Virtuais; Segurança da Informação; Tecnologia.

Abstract

The purpose of this article is to show the reader about the evolution of technology and its application to public safety in a way that assists and expedites crime investigation processes. This article also aims to guide and alert you about the dangers and precautions you should take when using any device such as smartphone or computer, especially if you are connected to the internet. Another objective of this article is to address relevant topics on information security, causing the reader to reflect on the subject and assess their attitudes related to the global computer network.
Keywords: Virtual Crimes; Information security; Technology.

Introdução

Nos últimos anos, a internet adquiriu grande popularidade devido à sua expansão e alta velocidade de transferência de informações. Por outro lado, de acordo com a revista Exame, segundo um relatório do IBGE, em 2005 apenas cerca de 13,6% das residências do Brasil possuíam conexão com a internet, já em 2014, a pesquisa foi realizada novamente, e foi constatado que houve um salto para

54,9%. Da mesma maneira, a internet ainda não é tão acessível assim globalmente falando; em uma matéria divulgada no site da ONU, em um relatório realizado pela União Internacional de Telecomunicações (UIT) em 2016, apenas cerca de 50% da população mundial possui acesso à rede mundial de computadores. Essa taxa mediana se dá pelo motivo da grande desigualdade que ainda há no acesso à internet. Na mesma matéria divulgada pela ONU, há um relatório chamado “ICT Facts & Figures 2016” que confirma essa informação; em países desenvolvidos, a média de residências com acesso à internet sobe para 81%.

Por outro lado, apesar da acessibilidade, têm se observado uma crescente no aumento da taxa de crimes virtuais. O motivo é que, apesar da grande aceitação e adesão da tecnologia por parte do público, a segurança da informação e boas práticas de uso são frequentemente deixadas de lado. Técnicas de phishing para roubo de dados de usuários, ataques em massa às grandes empresas de tecnologia, bancos e outras instituições governamentais são destaques nos jornais quando o assunto é o cibercrime.

Todos os dias, muito dinheiro é gasto e muito esforço é concentrado para evitar esses contratempos. De acordo com uma matéria publicada no site da revista Exame, uma das carreiras de maior necessidade atualmente é voltada para a Segurança da Informação. Isso sem falar dos esforços voltados para a proteção de dados do governo nos órgãos de segurança e tecnologia, e nas perícias de crimes virtuais realizadas pelas polícias de cada país. Este artigo tem o objetivo de mostrar o uso da tecnologia para investigar, solucionar e prevenir crimes virtuais.

Boas Práticas de Segurança da Informação

Levando em consideração o assunto deste artigo, vale ressaltar como o usuário deve se precaver e evitar os mais variados tipos de ataques; portanto, entende-se por boas práticas de segurança da informação, um conjunto de atitudes de prevenção por parte do usuário, que irão evitar ou ao menos dificultar o sucesso das ações de pessoas mal intencionadas. Essas recomendações que serão

abordadas neste artigo valem tanto para o ambiente de trabalho quanto para qualquer outro ambiente, principalmente em casa.

Senhas

As senhas geralmente são o principal meio de autenticação, o seja, o meio mais usado para confirmar se quem está realizando um login é realmente o proprietário da conta. Com a grande quantidade de contas na internet (como por exemplo, e-mail, perfis de redes sociais) lembrar de várias senhas diferentes é uma tarefa cada vez mais difícil. É bastante comum encontrar usuários que usam a mesma senha em todas as contas, ou que utilizam nomes e números familiares como senha. Esse tipo de atitude facilita muito um tipo de ataque de força bruta por exemplo, visto que nesse caso, é utilizado um tipo de software que testa várias combinações de caracteres, sejam eles letras, números ou caracteres especiais até encontrar a senha correta. Para evitar isso, torna-se necessário escolher senhas que não possuam nomes e números familiares e que de preferência possuam pelo menos um caractere maiúsculo e um especial.

E-mail

Outra técnica bastante usada até hoje, mas que possui grande eficiência é o uso de ataques via e-mail. Muitos usuários ainda não entendem o sentido da palavra “spam”, ou mesmo nem sequer ouviram falar algo sobre. Nesse cenário é bastante comum que pessoas mal intencionadas utilizem também alguma técnica de engenharia social - tentar se passar por um familiar ou chefe do alvo por exemplo - para obter informações sobre sigilosas sobre alguma empresa ou alguém. Essa é apenas uma das formas de se obter sucesso nessas ações, mas, para usar engenharia social, nem mesmo é preciso de um computador. Quando um e-mail suspeito for encontrado, é recomendado excluir imediatamente. Muitas vezes esses e-mails contêm imagens com promoções chamativas, links e mensagens apelativas ao emocional que fazem com que o usuário não perceba e acabe caindo na armadilha. De acordo com o Relatório da Segurança Digital no Brasil, realizado pelo DFNDR Lab, no terceiro semestre de 2017, houve um aumento de ataques por meio

de links maliciosos na internet para 44%. Em outras palavras, houve um salto de 45,72 milhões para 65,78 milhões de ataques à usuários.

Aplicativos e Softwares Não-Confiáveis

Recentemente a própria Google passou por uma situação complicada em sua plataforma de aplicativos para dispositivos móveis, a Google Play. Vários aplicativos da plataforma foram banidos e removidos por serem considerados maliciosos. Esses aplicativos infectados passaram pelo algoritmo de avaliação da empresa e em seguida publicados. A solução proposta após a descoberta e exclusão foi a criação do Google Play Protect, um recurso de segurança que verifica em tempo real se um aplicativo móvel é malicioso ou não.

Além do Android, todo sistema operacional é vulnerável a ataques. Levando isso em consideração, é necessário cuidado redobrado durante o download e instalação de algum software novo, seja em algum dispositivo móvel, Windows, Mac, ou qualquer outro sistema operacional. Caso seja necessário baixar e instalar um novo software, é importante que o usuário sempre baixe de fontes confiáveis, principalmente pelo próprio site do desenvolvedor ou empresa responsável. É muito difícil atualmente encontrar algo de qualidade que foi desenvolvido apenas pela boa vontade de alguém. Torrents e pirataria em geral à primeira vista são de graça, mas, o usuário quase nunca sabe o preço disso. Essas são portas facilmente abertas à uma pessoa mal intencionada. Vazamento de fotos íntimas, números de cartão e senhas ficam completamente vulneráveis se alguém estiver espionando seu computador, portanto, todo cuidado deve ser redobrado.

Tecnologia e Investigações Criminais

Em agosto de 2013, foi divulgada uma matéria no Canal Tech onde o FBI em uma operação conseguiu prender o dono de um site de pedofilia, e em seguida, foi solicitada pela polícia e concedida por um juiz uma permissão para que o próprio FBI durante duas semanas se passasse pelo criminoso preso, com o objetivo de atrair e prender o maior número de criminosos. Em outras palavras, o FBI prendeu o dono do site, e se passou pelo mesmo, continuando as postagens e interagindo com as pessoas que acessaram o site, de modo que a audiência não percebesse o

ocorrido. Resultado: quando descoberto, o site possuía mais de 5.600 usuários, e cerca de 24 mil mensagens. Além disso, foram encontradas cerca de 10 mil imagens de crianças nuas e de estupro ou abuso de menores.

Recentemente, nas investigações da operação Lava Jato aqui no Brasil, grandes esforços da Polícia Federal têm sido concentrados em perícias principalmente de dados. Escutas telefônicas, documentos, imagens e todo tipo de dado tornou-se o principal alvo de investigações, pois, por se tratar de um grande esquema de corrupção, tudo acontece às escondidas; e é aí que a tecnologia entra. Nesta operação, tem sido empregado um dispositivo que pode recuperar até mesmo dados apagados.

Outro caso interessante divulgado pelo site Olhar Digital, relata que a tecnologia de reconhecimento facial é empregada pela polícia de Gales do Sul, no Reino Unido, para localizar e prender suspeitos de crimes. A polícia teve sucesso, e pelo resultado das investigações, a mesma tecnologia já vem sendo empregada em outros casos, de forma a auxiliar e agilizar os processos. A tecnologia empregada é a mesma utilizada em aeroportos para agilizar o processo de aferição de passaportes. Para aperfeiçoá-la e aumentar as imagens dos bancos de dados, grandes eventos tornaram-se um prato cheio para a polícia, pois são lugares de grande concentração de pessoas, tornando possível um grande acúmulo de informação de uma só vez para comparação com bancos de dados da polícia. As polícias militar e civil do Brasil utilizam uma tecnologia parecida; um óculos com uma microcâmera que realiza o reconhecimento facial em tempo real, também em grandes eventos. A tecnologia vem de Israel, e auxilia o trabalho de reconhecimento de suspeitos em locais de grande concentração de pessoas, outro caso onde a tecnologia é empregada de forma a beneficiar as investigações.

Ética, Segurança dos dados, Legislação

Até então, foram abordadas grandes vantagens da aplicação da tecnologia no assunto que este artigo aborda; mas a questão é a seguinte: a internet, a era digital e suas tecnologias não possuímos uma regulamentação. Em caso de uma invasão a um banco de dados desse porte contendo várias informações desse tipo,

seria invasão de privacidade? Levando em consideração que apesar de conterem dados de criminosos e suspeitos, também haveriam dados de pessoas inocentes. E se caso esse banco de dados fosse invadido por uma pessoa com más intenções e informações fossem adulteradas? Podemos concluir que uma pessoa inocente poderia ser julgada e receber uma pena injusta.

Outro ponto a ser destacado, ainda falando da era digital, seria: Com o avanço da tecnologia, muitas coisas novas surgem a cada minuto. Inteligência artificial e carros autônomos talvez seriam os assuntos mais comentados atualmente. E se caso um carro autônomo atropelasse uma pessoa? Quem deveria ser responsabilizado?

Invasões e crimes virtuais muitas vezes não recebem um julgamento correto por parte da justiça pela falta de discussão e conhecimento dos assuntos relativos à segurança, tecnologia e ética. Outro setor da tecnologia que tem grande destaque da mídia atualmente, e que tem recebido grandes investimentos das indústrias de tecnologia é a internet das coisas. Assistentes virtuais como a Siri, Alexa, Cortana e Assistente da Google não estão mais localizadas apenas nos smartphones. Já existem dispositivos físicos para uso residencial como o Google Home ou a Alexa da Amazon, que trazem grande conforto para os usuários, mas que por muitas vezes falham no quesito segurança.

Por fim, pode-se perceber que, a tecnologia avança, mas algumas questões a serem discutidas muitas vezes são negligenciadas. Se a atitude do ser humano não for a de se precaver e estar preparado sempre possuindo o controle de tudo, talvez a tecnologia tome esse lugar e iremos viver em um mundo controlado pelas máquinas, e não por nós.

Conclusão

Do que foi dito até o momento, pode-se concluir que, a segurança é talvez um dos assuntos mais importantes, e torna-se necessária a aplicação das boas práticas em nosso cotidiano, começando mesmo a partir de casa.

O conhecimento e a capacidade de raciocínio da raça humana é sem dúvida uma benção que nos foi concedida. Sem essa base, a humanidade como um

conjunto não teria evoluído tanto e alcançado o que possuímos até hoje. Sabemos que a ciência e a tecnologia aliadas uma à outra, nos trazem conhecimento, verdades sobre nosso universo e o conforto que precisamos. Seguindo essa linha de raciocínio, elas devem ser sempre usadas em nosso favor, para o bem. Infelizmente, há pessoas que a usam para tirar proveito próprio, e por isso, devemos sempre seguir as boas práticas de segurança, evitando que sejamos alvos de crimes e situações ilegais, principalmente na internet. Lembrando, a segurança começa a partir da conscientização de cada um.

Referências

SANTOS, Barbara. “Apesar de expansão, acesso à internet no Brasil ainda é baixo”, 2016. Disponível em:<https://exame.abril.com.br/brasil/apesar-de-expansao-acesso-a-internet-no-brasil-ainda-e-baixo />. Acesso em: 19/10/2017.

ONU. “UIT: 3,7 bilhões de pessoas ainda não têm acesso à Internet no mundo”, 2016. Disponível em: <https://nacoesunidas.org/uit-37-bilhoes-de-pessoas-ainda-nao-tem-acesso-a-internet-no-mundo />. Acesso em: 19/10/2017.

PATI, Camila. “Os 7 profissionais mais disputados (agora) na área de TI”, 2016. Disponível em:<https://exame.abril.com.br/carreira/os-7-profissionais-mais-disputados-na-area-de-ti />. Acesso em: 19/10/2017.

IDGNOW. “Ciberataques crescem 44% no Brasil, segundo pesquisa”, 2017. Disponível em: <http://idgnow.com.br/internet/2017/10/19/ciberataques-crescem-44-no-brasil-segundo-pesquisa/>. Acesso em: 20/10/2017.

CANALTECH. “FBI compartilhou pornografia infantil para prender pedófilos”, 2013. Disponível em: <https://canaltech.com.br/internet/FBI-compartilhou-pornografia-infantil-para-prender-pedofilos/>. Acesso em: 20/10/2017.

OLIVEIRA, Déborah. “Polícia Federal usa tecnologia que extrai até informações apagadas em operação Lava Jato”, 2015. Disponível em: <https://itforum365.com.br/tecnologias/produtos-e-servicos/policia-federal-usa-tecnologia-que-extrai-ate-informacoes-apagadas-em-operacao-lava-jato>. Acesso em: 20/10/2017.

SUMARES, Gustavo. “Polícia usa reconhecimento facial para encontrar e prender suspeito”, 2017. Disponível em <https://olhardigital.com.br/fique_seguro/noticia/policia-usa-reconhecimento-facial-para-encontrar-e-prender-suspeito/68881>. Acesso em: 20/10/2017.

IG. “Polícia usa tecnologia para combater o crime”, 2011. Disponível em: <http://ultimosegundo.ig.com.br/brasil/sp/policia-usa-tecnologia-para-combater-o-crime/n1597095324505.html>. Acesso em: 20/10/2017.