XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

JOSÉ QUERINO TAVARES NETO

MÁRCIA HAYDÉE PORTO DE CARVALHO

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: José Querino Tavares Neto; Márcia Haydée Porto de Carvalho – Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-566-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Direitos Sociais, Constituição e Democracia na América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governança. 3. Novas tecnologias. XI Encontro Internacional do CONPEDI Chile - Santiago (2: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O Grupo envolveu pesquisadores de diferentes partes do país sobre uma temática rica e complexa, cujos temas mostraram-se ao final interligados.

Primeiramente a mestranda Gilmara de Jesus Azevedo Martins e a Professora Márcia Haydée Porto de Carvalho apresentaram dois artigos: 1) Liberdade de Expressão e Discurso Digital na Era Digital, no qual apresentaram o resultado de pesquisa sobre projetos de lei em tramitação no Congresso Nacional, envolvendo a temática; e 2) A Proteção da Privacidade frente à Liberdade de Expressão na Sociedade Tecnológica, trazendo a preocupação com a tutela da privacidade, através da fixação de limites à liberdade de expressão.

Em seguida, a mestranda Quitéria Maria de Souza Rocha tratou do Acesso à Justiça e as Inovações Tecnológicas Pós-Pandemia como Corolário da Efetivação do Princípio da Dignidade da Pessoa Humana, quando expressou ser essa uma questão bastante problemática dado o aumento geométrico das demandas sem que o sistema judicial esteja preparado para resolvê-la.

Depois, a mestranda Priscila Machado Martins abordou o assunto Decisões guiadas no Capitalismo de Vigilante, afirmando que há uma interferência digital na privacidade, mitigado pela autodeterminação da pessoa humana.

Logo passou-se a palavra para a mestranda Isabela Moreira Nascimento Domingues que apresentou seu artigo intitulado El Uso de las Tics para La Participación Ciudadana y el Control de la Corrupción en la Administración Pública Brasileña, falando sobre a importância das tecnologias de informação para se prevenir e combater a corrupção nos órgãos públicos.

A Professora Maria Cristina Zainagui e o mestrando Diego Vinícios Soares Bonetti expuseram a seguir o artigo Liberdade de Expressão e Direitos da Personalidade na Sociedade de Informação, quando também defenderam a necessidade de imposição de restrições à liberdade de expressão, desta feita para assegurar direitos de personalidade na sociedade tecnológica atual, marcada pela ampliação crescente da informação.

O mestrando Paulo Eduardo Alves da Silva apresentou dois artigos: 1) Limites e Possibilidades das Ferramentas de Inteligência Artificial pelo Poder Judiciário e 2) Proteção de Dados no Brasil e na Califórnia. Ao tratar do primeiro, asseverou que é premente o uso pelo judiciário não apenas de programas de separação de ações e recursos, mas de outras ferramentas e programas de softwear para agilizar e tornar mais efetivas suas decisões. No segundo momento, fez uma exposição comparativa do direito à proteção de dados na legislação do Estado norte-americano da Califórnia e do Brasil.

Com a palavra dada as mestrandas Fernanda Nunes Coelho Lana e Souza e Ana Maria Lima Maciel Marque Gontijo, estas ao tratarem sobre o tema Dilema do Conflito de Interesse no Âmbito da Governança Corporativa, esclareceram que há sim objetivos contrapostos no âmbito da governança das empresas e que precisam ser atacados para o bem dos envolvidos.

Os mestrandos Emerson Wendt e Renata Almeida da Costa abordaram o Medo e a Internet: Risco e Insegurança pela falta de Privacidade. Para os autores, vive-se uma constante falta de segurança pelo fato de a cada momento sermos obrigados a disponibilizar dados pessoais para navegadores e outras empresas na internet.

O mestrando Daniel Cezar discorreu acerca do seu artigo O uso da Tecnologia para o Cometimento de Crimes, assinalando que o aumento das sanções penais não é uma medida para enfrentar esse tipo de criminalidade, mas a exigência de medidas preventivas por parte dos particulares e empresas privadas.

Logo adiante, falaram os mestrandos Roberta Catarina Giácomo e Daniel Barile da Silveira sobre Os Deveres Jurídicos do Empresário, abordando a gestão de riscos no âmbito da responsabilidade penal pelo produto e o complience como mecanismo de proteção do consumidor, o qual, para os autores se encontra em situação de vulnerabilidade.

Finalmente, a mestranda Carla Liguori abordou Tecnologia e Direito Fundamental à Proteção de Dados, enfrentando a regulação desse direito previsto na Constituição por lei infraconstitucional já alterada inclusive por medida provisória.

Na realidade, o GT, teve discussões que se processaram numa emergência e urgência de superação dos velhos paradigmas centrados nas formas herméticas do conhecimento por perspectivas mais dialogais e multidisciplinares, sobretudo, pela insuficiência dos instrumentos das novas tecnologias que ultrapassam a fronteira da subestimação do conhecimento, mas, sobretudo, uma inclusão parceira das novas governanças e novas tecnologias no campo do direito como instrumento emancipatório.

O USO DA TECNOLOGIA PARA O COMETIMENTO DE CRIMES: ANÁLISE DO MALWARE RANSOMWARE

USING TECHNOLOGY TO COMMIT CRIMES: MALWARE RANSOMWARE ANALYSIS

Daniel Cesar
Caio Sperandeo De Macedo
Ricardo Libel Waldman

Resumo

Analisar no contexto da Sociedade da Informação, o emprego das tecnologias digitais que causaram fortes mudanças na sociedade contemporânea. Referendar que as ferramentas da tecnologia da informação também se tornaram instrumentos para viabilizar novas formas de práticas delitivas, dentre elas a utilização de ransomware para cometer o crime de extorsão. Esse artigo busca, através de análise documental, entender o artificio do ransomware, bem como possíveis formas de prevenção para incidentes de segurança, analisando ainda tais práticas na perspectiva da legislação nacional.

Palavras-chave: Sociedade da informação, Segurança da informação, Crimes digitais, Ransomware, Engenharia social

Abstract/Resumen/Résumé

Analyze in the context of the Information Society, the use of digital technologies that caused strong changes in contemporary society. To endorse that information technology tools have also become instruments to enable new forms of criminal practices, including the use of ransomware to commit the crime of extortion. This article seeks, through document analysis, to understand the artifice of ransomware, as well as possible ways of preventing security incidents, analyzing such practices from the perspective of national legislation.

Keywords/Palabras-claves/Mots-clés: Information society, Information security, Digital crimes, Ransomware, Social engineering

Introdução

O uso da tecnologia da informação transformou e transforma a forma como a sociedade se relaciona. Mudou a forma como interagimos, deu voz às pessoas que no passado não conseguiam colocar seu ponto de vista, sendo possível receber informações vindas de todo o planeta em quantidade e velocidade absurdas.

No processo de transformação digital, cada vez mais produtos e serviços estão acessíveis na palma da mão. Empresas vendem seus produtos ao redor do mundo, possuem diferentes sistemas integrando diferentes áreas da empresa e gravam diferentes informações em seus bancos de dados.

No mundo das pessoas físicas isso também ocorre, os celulares possuem diferentes aplicativos, com os quais podemos fazer praticamente tudo. Fotos, documentos, outros arquivos estão no formato ou linguagem digital e se estiverem armazenados em serviços de nuvem, como as disponibilizadas por Google, Microsoft, Apple, por exemplo, podem ser acessados de qualquer lugar com conexão à internet.

Isso demonstra o quanto a tecnologia da informação está ligada ao dia a dia e a dependência que a sociedade tem dessas ferramentas. Como dizem[1], os dados são o 'novo petróleo'; o que também motiva a prática e aprimoramento de atividades criminosas por meio da mesma tecnologia da informação. Crimes como estelionato e extorsão são facilitados pela tecnologia, podendo alcançar mais pessoas e, a depender da vítima, com alto retorno financeiro, sendo muitas vezes difícil chegar a quem comete o crime.

Trata-se de um desafio para a nossa Sociedade da Informação. No presente artigo abordaremos especificamente a prática do crime de extorsão previsto no artigo 158 do Código Penal brasileiro através do uso de *ransomware*, uma estratégia de criptografia dos dados, na qual o agente solicita resgate em bitcoin para retirar a criptografia dos dados.

O presente estudo faz uso da metodologia dedutiva, com amparo na doutrina e em livros e artigos que guardam relação com o tema ora desenvolvido e subdividisse na abordagem da sociedade da informação, os crimes que são cometidos no contexto digital, atendo-se de forma mais aprofundada no *ransomware* e finalizando com uma visão dos esforços legislativos.

[1] Época Negócios. "Dados são o novo petróleo", diz CEO da Mastercard – exceto por um pequeno detalhe. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html Acesso em: 03 set. 2022.

1. A Sociedade nos dias de hoje

Nessa sociedade em que a informação é o elemento central, os dados possuem preponderância gigantesca e integram o núcleo do desenvolvimento da economia nos nossos dias. A informação é o que foram a terra, as máquinas a vapor e a eletricidade nas sociedades de outrora (BIONI, 2021, p. 4-5).

Esta transformação foi possível graças à tecnologia da informação que permitiu com que as distâncias fossem reduzidas, sendo possível saber o que se passa, comprar, vender em qualquer lugar do mundo onde se tenha um computador ou celular e internet. Castells (2020) cunhou o termo sociedade em rede que exprime muito bem essa nova realidade.

Fazendo referência à rede de computador, Castells traça um paralelo com nossa sociedade, com a flexibilização, a interação, a troca constante.

> O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e o seu uso, (CASTELLS, 2020, p. 88)

Com o crescente uso da tecnologia os hábitos mudaram, os velhos arquivos de papel se transformaram em sistemas que guardam as informações em bancos de dados, as compras online cresceram muito, principalmente em decorrência da pandemia de COVID-19. A própria forma de trabalho também mudou, o home office foi a forma utilizada para muitas empresas continuarem funcionando e hoje podemos trabalhar para um empregador do outro lado do planeta, do conforto de casa, sem deslocamentos. Tudo isso sustentado pela tecnologia da informação, por sistemas, redes, uma infraestrutura que dá sustentação a todos esses movimentos que observamos no nosso dia a dia e que avança a cada lançamento de novos produtos, novas tecnologias.

Essa mudança tecnológica também trouxe novas formas para o cometimento de crimes. Alguns que até então eram praticados apenas no mundo físico, passaram ao digital, empregando técnicas para enganar a vítima, conseguir informações, acesso e assim furtar, extorquir, dentre outros.

2. Crimes e sua faceta digital

Os crimes acompanham o ser humano durante toda a sua história. A doutrina define crime sob um aspecto formal (comportamento positivo ou negativo, proibido em lei, sob ameaça de pena), material (violação de um bem penalmente protegido, contrariando valores ou interesses do corpo social, exigindo sua proibição) e analítico (fato típico e antijurídico). (JOPPERT, 2006, p. 97-98; BITENCOURT, 2012, p. 269-271).

Dessa forma, em síntese, é crime o que a lei descreve através de um tipo penal pré-existente que descreva determinada conduta como criminosa, alvo da preocupação e proteção pela sociedade e que culmina em uma pena.

No contexto digital, os crimes também passaram a fazer parte do dia a dia da sociedade da informação.

> O crime digital é modalidade de delito perpetrado por intermédio de meio eletrônico digital, ou que afete o objeto tutelado e protegido pelo Direito Penal, o qual pode consistir em aparelho digital físico (hardware), suporte lógico (software) ou dados armazenados por sistemas de tecnologia de informação. (PACHECO, 2011)

O crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciaram diretamente no direito penal (DAMÁSIO e MILAGRE apud ARAUJO, 2021, p. 497). Temos condutas nesse contexto informático que são crimes já previstos no Código Penal brasileiro, mas onde o uso da tecnologia tornou a perpetração e o impacto muito diferente do que se tinha até então.

Porém, existem crimes que só foram possíveis com a tecnologia, como a tipificação que foi incluída pela Lei nº 9.983/2000 que realizou mudanças no Código Penal adicionando os artigos 313-A e 313-B conforme descrito abaixo.

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:"
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente" (BRASIL, 2000).

Aqui as práticas envolvem sistemas de informação, onde o crime está na inserção de informações incorretas ou a atualização ou exclusão indevida de informações corretas de forma a conseguir vantagem. Altera-se assim informações em bancos de dados da Administração Pública a fim de se aferir ganhos indevidos. Já o artigo 313-B foca na alteração sem autorização de programa. Basicamente o artigo 313-A foca nos dados e o artigo 313-B foca no código do programa que é alterado sem a devida autorização para que este programa trate os dados de forma diversa ao esperado.

Outro exemplo é a Lei nº 12.737/2012 que ficou conhecida como lei Carolina Dickmann, atriz que teve seus dados copiados sem autorização pelo técnico que prestava manutenção em seu computador e acabou incentivando o Congresso Nacional a tipificar criminalmente delitos informáticos. Essa lei descreve como crime a prática de invasão de dispositivo informático. Na atualização do Código Penal que a Lei nº 12.737/2012 ocasionou, temos a seguinte redação para o artigo 154-A caput.

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012)

Não importa o meio que seja utilizado para efetuar a invasão, isso é, a entrada no dispositivo, sendo a ação com finalidade não autorizada pelo titular configurar-se-á o crime.

Incorre ainda no crime de invasão de dispositivo, conforme Artigo 154-A §1º do Código Penal brasileiro, quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador (BRASIL, 2012). Dessa forma, se uma pessoa ou grupo de pessoas desenvolverem um programa ou dispositivo eletrônico que através de seu uso supere, por exemplo, as defesas presentes no computador, ou quebre uma criptografia, esses também incorrerão no crime de invasão de dispositivo.

A Lei nº 12.737/2012 também inseriu no artigo 266[2] do Código Penal a inclusão da prática de interrupção de serviço telemático ou de informação de utilidade pública, ou ainda

[2] Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
Pena - detenção, de um a três anos, e multa.
§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

impedir ou dificultar o restabelecimento deste serviço, ampliando assim as práticas constantes no artigo 266 que até então previa a interrupção dos serviços telefônico, telegráfico e radiotelegráfico. Dessa forma, retirar do ar de forma intencional uma aplicativo de utilidade pública ou atuar para que não se reestabeleça tal serviço incorrerá no crime previsto no artigo 266 CP.

Nas práticas mais atualizadas e utilizadas em crimes digitais, temos o p*hishing*, que ocorre quando um agente criminoso (*phisher*) cria uma réplica praticamente perfeita de um site, normalmente de uma instituição financeira que possibilita acesso à conta corrente por internet (*homebanking*), e, com esta réplica, tenta enganar o usuário a inserir nela seus dados pessoais, tais como senhas, logins, números de conta, entre outros (PACHECO, 2011). Esta prática pode ser utilizada para disseminação do *ransomware*, enganando o usuário que baixa o programa, infectando-se.

O criminoso faz uso de e-mails com títulos chamativos, identidade visual muito próxima à da empresa real, tentando fazer com que o usuário abra o link e coloque suas informações, tais como conta, senha, permitindo que seja possível utilizá-las em compras que serão debitadas da conta do usuário que caiu na fraude. Tal atividade pode ser enquadrada como estelionato (artigo 171 CP quer versa em seu caput, "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento") ou furto mediante a fraude (artigo 155, § 4º, II CP que traz a furto realizado com abuso de confiança, ou mediante fraude, escalada ou destreza), (BRASIL, 1940).

Uma outra técnica adotada pelos criminosos é a utilização de *malwares*. *Malwares* são códigos maliciosos que, quando instalados na máquina, podem desviar, impedir ou comprometer a utilização usual do dispositivo, desviar as informações da máquina ou ganhar acesso autorizado aos recursos do sistema, entre outros comportamentos abusivos (PACHECO, 2011).

São exemplos de malwares o *spyware*, *adware*, *ransomware*, *trojans* e *worms.* Nesse artigo, vamos nos deter a um *malware* que vem aparecendo constantemente na mídia e causando transtornos a diferentes empresas, o *ransomware*, mas para dar uma visão geral dos demais, faremos uma suscinta explicação de cada um dos tipos de *malware* conforme Pacheco (2011).

- ***Spyware***: coleta informações do usuário sem que esse saiba que isso está acontecendo. Pode coletar o que é digitado, o que é visitado, comprado, atuando como um espião;
- ***Adware***: o código tem como finalidade mostrar propagandas no computador infectado e com isso gerar renda para quem desenvolveu. A remuneração sendo feita por acesso, o programa automaticamente acessando, gera esse retorno financeiro, não a vítima, mas quem desenvolveu o adware;
- ***Trojans*****:** também conhecido como Cavalo de Tróia. Aparentemente um programa benigno, normal, mas que uma vez executado abre uma brecha para controle remoto, transmissão de dados dentre outras atividades;
- ***Worms***: se propaga pela internet, via dispositivos de armazenamento móvel, pela rede local. Sua finalidade é ficar se replicando.

Existem assim diferentes algoritmos que são utilizados para diferentes fins criminosos. Por algoritmo, entende-se aqui, como um conjunto de etapas que são executadas para que se alcance um determinado resultado, realize-se uma determinada tarefa (CORMEN, 2014, p. 1). Um algoritmo pode ser imaginado como uma sequência de linhas de código, repletos de complexos cálculos matemáticos (PELLIZZARI; BARRETO JUNIOR, 2019, p. 59). Nos casos citados acima, temos diferentes tipos, muitos deles não são novidades no mundo da computação, apenas se desenvolveram, porém, destacaremos um em específico e que vem causando grandes transtornos financeiros e para a imagem das empresas, o *ransoware*.

3. Ransomware: raio x sobre essa prática criminosa

Como visto, *ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário (Cert.br, online).

Nesse crime, temos um programa de computador que, uma vez instalado na máquina em rede, é capaz de criptografar os dados presentes em um banco de dados, tornando-os indecifráveis e impactando o funcionamento da empresa atacada com a parada de seus sistemas.

Tal prática pode ser enquadrada no crime de extorsão previsto no artigo 158 do Código Penal, descrito como “Constranger alguém, mediante violência ou grave ameaça, e com o

intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa". (BRASIL, 1940).

Quem pratica esse crime, deseja obter resgate, isso é, uma vantagem patrimonial ilícita, para liberar a chave que desencriptará os dados, tornando-os acessíveis novamente. Caso contrário, os dados ficam criptografados e inúteis, trazendo transtornos financeiros, danos à imagem da empresa, aos seus compromissos com clientes, parceiros e fornecedores.

O frigorifico JBS é um exemplo de empresa que sofreu ataque *ransomware*. A empresa pagou 11 milhões de dólares aos hackers responsáveis pelo ataque para reaver seus dados[3]. Um outro ataque ransomware ocorreu no final de 2020 no Superior Tribunal de Justiça (STJ), onde os dados de processos foram criptografados, impedindo o acesso a estes. As atividades no Tribunal foram suspensas enquanto buscava-se resolver o problema. No caso do STJ não houve o pagamento do resgate, sendo utilizado um backup para restaurar os dados que haviam sido perdidos pela criptografia[4].

O Centro Canadense de Segurança Cibernética traz a seguinte definição do que é *ransomware* e seus tipos.

> Ransomware é um tipo de malware que, em última análise, nega o acesso de um usuário a arquivos ou sistemas até que uma quantia seja paga. O ransomware pode usar sua rede para se espalhar para todos os dispositivos conectados. Existem dois tipos proeminentes de ransomware:
>
> O crypto ransomware que remove o acesso aos seus arquivos, substituindo-os por dados criptografados.
>
> Locker ransomware bloqueia o acesso de login no seu dispositivo. (CANADIAN CENTRE FOR CYBER SECURITY, 2021) (tradução nossa)

Quanto à forma que esse *malware* chega, a infecção pode ser através de click em links ou baixando anexos colocados em sites não seguros, e-mails de *phishing* e aplicativos de mídia social. (CANADIAN CENTRE FOR CYBER SECURITY, 2021, online). Como explicado anteriormente o *pishing* faz com que o usuário acredite estar acessando o site real de uma

---

[3] Exame. **JBS pagou US$ 11 milhões em resgate a autores de ataque ransomware**. Disponível em: https://exame.com/tecnologia/jbs-pagou-us-11-milhoes-a-autores-de-ataque-de-ransomware/ Acessado em: 30 nov. 2021.

[4] Migalhas. **39 dias após o ataque cibernético ao STJ: reflexões e desafios**: Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios Acessado em 30 nov. 2021.

empresa e com isso execute o programa malicioso que irá se propagar na rede, realizando o algoritmo de sua programação.

No dia 21 de outubro de 2021 o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo brasileiro (CTIR) fez um alerta sobre um novo *ransomware*, indicando qual era, quais falhas eram exploradas e um roteiro de prevenção. Das práticas de prevenção explicitadas neste alerta, destacamos a adoção de campanhas de conscientização dos usuários quanto a prática de engenharia social[5].

No presente caso o grupo CTIR, vinculado ao Gabinete de Segurança Institucional da Presidência da República, trouxe a seguinte explicação.

> BlackMatter é um malware do tipo "Ransomware como Serviço" (RaaS) que normalmente faz uso de credenciais previamente comprometidas do Lightweight Directory Access Protocol (LDAP) e do protocolo Server Message Block (SMB) para enumerar recursos em um Active Directory (AD). Sua nova variante descobre todos os demais dispositivos da rede afetada e os criptografa à medida que são encontrados.

Traduzindo temos aqui o *malware* desenvolvido para se espalhar pela rede, criptografando todos os dispositivos que encontrar nesta rede atacada. Para isso ele faz uso de uma credencial (usuário e senha) comprometida e utiliza o protocolo de comunicação para realizar a "caminhada" pela rede.

Uma vez que a infecção aconteça, os usuários são informados do que ocorreu. O *Canadian Centre for Cyber Security* (2021, online) explica da seguinte forma essa comunicação entre o criminoso e as vítimas, estando tudo devidamente implementado no código do malware.

> Se o seu dispositivo estiver infectado com ransomware, você receberá um aviso de resgate na tela indicando que seus arquivos foram criptografados e estão inacessíveis até que o resgate seja pago. Os atores da ameaça muitas vezes ameaçam destruir seus dados permanentemente ou divulgá-los publicamente, se você não pagar o resgate no prazo solicitado. O pagamento é frequentemente solicitado na forma de moeda digital, como bitcoin, uma vez que a transferência seria difícil de rastrear. Cartões de crédito pré-pagos ou cartões-presente também podem ser solicitados (tradução nossa)

[5] Alerta 03/2021. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-03-2021 Acessado em: 30 nov. 2021.

O primeiro *ransomware* que se tem notícia foi utilizado em 1989, em uma época tão diferente dos dias atuais, a infecção ocorria via disquete e exigia-se o pagamento de 189 dólares americanos em uma conta no Panamá (MOHURLE; PATIL, 2017). Ao longo das décadas o processo foi evoluindo e o valor do resgate cresceu, como vimos o caso JBS envolveu o pagamento de 11 milhões de dólares e hoje a forma de propagação se dá pela Internet.

Em 2017, ocorreu um ataque *ransomware* que ficou famoso, ocorrendo em diferentes partes do mundo. O ataque do *ransomware WannaCry* afetou hospitais, companhias, universidades e organizações governamentais, atingindo 99 países, incluindo o Brasil, onde foi detectado em 15 estados, impactando o Ministério Público Federal, o Tribunal de Justiça de São Paulo e o Instituto Nacional do Seguro Social (INSS) (BRITTO; FREITAS, 2017; p. 2).

Como formas de precaver e diminuir os impactos no caso da ocorrência são previstos alguns itens (MOHURLE; PATIL, 2017):

- Manter antivírus atualizado
- As mensagens de spam, remetentes desconhecidos, links de mensagens suspeitas não devem ser abertos
- Manter os softwares atualizados
- Manter um ponto de restauração do sistema atualizado
- Não deixar habilitada as opções de conexão sem fio quando não estiver utilizando
- Manter firewall ligado e configurado
- Desabilitar serviços de acesso remoto
- Ter cuidado ao acessar redes wifi públicas, desconhecidas
- Filtrar e-mails que contenham arquivos executáveis em anexo
- Manter backup em dia e em outro local, permitindo assim a recuperação dos dados a partir do backup, se necessário

Numa visão para corporação, o *Canadian Centre for Cyber Security* (2021, online) traz pontos que a empresa deve se atentar para evitar ou na ocorrência, conseguir dar os passos necessários dentro de uma crise. Tais passos passam pelo planejamento de resposta a incidentes que abordará a monitoração, detecção, resposta, designação de responsabilidades, plano de comunicação, dentre outros pontos.

Treinar as pessoas da organização para que elas não sejam vítimas das atividades maliciosas e simular o plano gerado são elementos importantes para a preparação e diminuição

da incidência de riscos e do tempo de retomada a normalidade pós um incidente. As simulações poderão trazer ensinamentos que alimentarão o plano e ajudarão a organização a estar mais bem preparada para a ocorrência de um caso real.

Por fim, o *Canadian Centre for Cyber Security* (2021, online) instrui ainda que a organização considere a contratação de um seguro cibernético visando assim amparar a organização na ocorrência de eventos de cybersegurança.

O planejamento é de suma importância, ter os controles e os responsáveis auxiliará a organização a saber como agir. Importante destacar o treinamento dos funcionários, a conscientização é imprescindível para diminuir a probabilidade de infecção.

Os costumes ou práticas corriqueiras das pessoas são considerados o elemento mais fraco dentro do mundo da Segurança da Informação.

> Atitudes comuns como escrever senhas em papéis avulsos, ceder a um pedido gentil de informações sobre dados estratégicos, conceder seu login a um amigo de trabalho, abrir endereços virtuais a partir do e-mail corporativo, entre outras, são exemplos que parecem inofensivas, mas representam falhas constantemente utilizadas por invasores. Para Silva Filho (2004), o ser humano apresenta algumas características que o torna vulnerável e suscetível a falhas como vontade de ser útil, a busca por novas amizades, a prorrogação de responsabilidades e persuasão. (FREIRE; SILVA; QUEIROZ; BATISTA, 2017, p. 150)

Dentro desse ponto faz-se importante abordar um tema que tem se mostrado o modus operandi dos criminosos para conseguir informações que podem abrir brechas para o cometimento dos crimes, a engenharia social.

A engenharia social compreende técnicas e práticas que são utilizadas para obtenção de informações importantes ou sigilosas de uma organização, se aproveitando das pessoas que possuem essas informações desejadas, que as passa por ingenuidade ou confiança (ELIAS, 2004 apud COELHO; RASMA; MORALES, 2013, p. 39).

> Estas técnicas eram o principal recurso utilizado pelo famoso hacker Kevin Mitnik, que utilizava do expediente psico social de ludibriar empregados, secretárias ou outros serventes, para que injetasse o código malicioso, ou conseguindo senhas privadas que muita das vezes são dados pessoais óbvios, de fácil dedução, como datas de aniversário. Ou, ainda, o emprego de expediente mais simples, como inserção de pendrive (dispositivo de armazenamento de dados) no computador da vítima em um momento de distração. (PACHECO, 2011)

Ligações telefônicas, mensagens via *chat* (*whatsapp*, por exemplo), também são instrumentos utilizados pelos criminosos para coletar informações ou fazer com que a vítima realize alguma atividade de interesse do criminoso.

Não resta dúvida que a educação digital se faz de suma importância para que esse elo mais fraco da cadeia de segurança digital torne-se mais forte, evitando cair em golpes, clicar em links duvidosos, passar informações sensíveis, isso tanto no contexto corporativo quanto pessoal, dado que a nossa vida na Sociedade da Informação se perfaz através do uso da tecnologia da informação no nosso dia a dia.

Mas, fechando a ação da extorsão, há o pedido da vantagem conforme artigo 158 do Código Penal que traz na descrição desse crime os atos de constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. Para esse crime a pena prevista é de reclusão, de quatro a dez anos, e multa.

Aquele que faz uso do *ransomware* criptografa os dados, ameaçando apagá-los ou liberá-los ao público visando ganhar uma vantagem financeira, o resgate. O intuito final é auferir esse ganho financeiro forçando a vítima a pagar-lhe para ter seus dados restaurados. A forma de pagamento solicitada na maioria das vezes é através de bitcoins, o que torna a descoberta de quem é o destinatário do dinheiro muito difícil de ocorrer.

Trata-se de um crime de complexa resolução, com o mundo conectado que temos hoje, o criminoso pode estar em qualquer lugar no mundo, o uso de bitcoin dificulta o rastreamento do dinheiro pago em um resgate. A melhor forma de se combater é tomar todas as medidas técnicas para diminuir a probabilidade do dano, ter o backup sempre preparado, assim será possível resgatar os dados via backup, treinar as pessoas, no caso de corporações e envolver a polícia para que essa possa realizar as investigações.

4. Perspectivas de atuação legislativa e internacional frente a extorsão digital

O pagamento do resgate à extorsão proporcionada pelo *ransoware* acaba por incentivar o cometimento do crime, uma vez que com a prática alcançando seu objetivo, os criminosos podem engendrar novos ataques, incentivando o desenvolvimento de algoritmos ainda mais sofisticados, além do que o pagamento não é certeza da recuperação da base de dados e nem que a empresa não sofrerá novos ataques.

Para a empresa, o que resta é ter um plano de continuidade bem definido e funcional, com backups atualizados para conseguir superar o problema no menor tempo possível, além de sempre buscar a atualização de suas defesas e na educação de seus empregados. Em termos legislativos existe um projeto de lei de autoria do deputado federal Vitor Hugo que visa atualizar o Código Penal para prever a qualificadora de extorsão cibernética, atualizando o artigo 158 do Código Penal e prevendo a reclusão de 6 (seis) a 12 (doze) anos e multa para quem comete esse tipo de extorsão (BRASIL, 2021).

Na prática o projeto explicita extorsão cibernética, partindo de uma pena maior que a extorsão do caput do artigo 158 que hoje é de 4 anos, e aumentando também o máximo da pena base que é de 10 anos. Fora isso, aumento da pena, não há evolução significativa, dado que a prática hoje já é de extorsão.

Nos Estados Unidos, há um projeto de lei que propõe que as empresas que tenham pagado o resgate informe em até 48 horas esse pagamento, informando o valor, a forma pela qual o pagamento foi realizado e a entidade que solicitou o resgate. Prevê, ainda, que o Departamento de Segurança Interna publique informações do último ano, descaracterizando quem pagou, e que seja avaliado de que forma as criptomoedas facilitaram a prática do crime. Além disso, que o Departamento provenha recomendações para proteger sistemas informáticos e o aprimoramento da segurança destes (WARREN, 2021, online).

Conversas internacionais também vem ocorrendo e investigações internacionais estão buscando prender pessoas que participem de ações de *ransoware*. Prisões foram reportadas em novembro deste ano na Polônia, Romênia, Coréia do Sul e Kwait de pessoas que supostamente fazem parte do REvil, uma gangue de *ransoware* que atua desde 2019[6].

A União Europeia vem tramitando uma diretiva de cibersegurança que visa atualizar a diretiva de segurança de redes e de sistemas de informação na União Europeia de 2018, criando uma versão que aumenta a quantidade de entidades e setores que devem tomar medidas de segurança, simplificar as obrigações de comunicação, introduzir medidas mais rigorosas de supervisão e de requisitos de aplicação e harmonização das sanções. Tais medidas visam a aumentar o nível de cibersegurança na União Europeia (EUROPEAN PARLIAMENT, 2021, online).

[6] NBC News. Ransomware crackdown spreads in U.S., Europe and Asia. Disponível em: https://www.nbcnews.com/tech/security/ransomware-crackdown-spreads-us-europe-asia-rcna4829 Acesso em: 18 dez. 2021.

Além de medidas legais, são necessárias medidas técnicas e de cooperação entre os países para atuarem sobre os *ransomwares*. Medias de cibersegurança, que cobrem investimentos, políticas de segurança e fiscalização, são necessidades frente a uma evolução constante do aparato ferramental. Da mesma forma, as defesas devem ser evoluídas, com equipamentos, ferramentas e pessoas devidamente capacitadas, tanto nas empresas privadas, quanto no ambiente público, dado que invasões e indisponibilidades vem sendo verificadas no ambiente público, como no caso do aplicativo Conecta SUS[7].

Conclusão

A tecnologia da informação transformou-nos em uma sociedade na qual os dados impulsionam a nossa economia e o social, onde os dados são um ativo valioso, servindo de insumo para diferentes atividades.

Nesse contexto os crimes também evoluíram, os agentes utilizam as ferramentas da tecnologia da informação para o cometimento de crimes. Através dos meios tecnológicos, qualquer lugar pode ser alcançado, como vimos, a ocorrência do *WannaCry* alcançou 99 países ao redor do mundo.

Nesse processo de extorsão tivemos casos grandes que foram impactados, a multinacional JBS pagou 13 milhões de dólares de resgate para ter seus dados de volta, Superior Tribunal de Justiça ficou semanas com seu expediente suspenso, sendo restaurado através do uso dos backups. Em 2017 tivemos também o Ministério Público Federal, Tribunal de Justiça de São Paulo e o INSS também alvo de *ransomware*. Alguns de tantos outros casos que sofreram com essa extorsão via algoritmo.

Observar as questões técnicas, com software atualizados, bem configurados, backup atualizado e protegido são essenciais para que se diminua as chances de ser vítima e no caso de ser, poder voltar as atividades de forma mais rápida e sem pagamento do resgate solicitado.

[7] Veja. Governo informa que ConecteSUS só voltará a funcionar na semana que vem. Disponível em: https://veja.abril.com.br/saude/governo-informa-que-conectesus-so-volta-a-funcionar-na-semana-que-vem/ Acesso em: 18 dez. 2021.

O fator humano é o elo mais fraco dentro do ramo da segurança da informação, sendo assim, a educação digital (treinar as pessoas), pode ajudar que indivíduos não fiquem suscetíveis.

Ações de cooperação e de investimento em cibersegurança são imprescindíveis. A utilização de ferramentas e atualização dessas para acompanhar o desenvolvimento dos riscos, a atualização dos softwares utilizados nos computadores, configurações mais restritivas, uma maior educação digital, são elementos essenciais para se buscar uma diminuição das probabilidades e impactos dos riscos.

Referências

ARAUJO, Cláudio Rodrigues. ANÁLISE DA APLICAÇÃO DO DIREITO PENAL NOS CRIMES VIRTUAIS. **Pensar Acadêmico**. v. 19, n. 2, p. 494-511, maio - setembro, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2ª edição. Rio de Janeiro: Forense, 2021.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral 1**. 17ª edição. São Paulo: Editora Saraiva, 2012.

BRASIL. **Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acessado em: 01 set. 2022.

_____. **Lei 9.983 de 14 de julho de 2000**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9983.htm Acesso em: 01 set. 2022.

_____. **Lei 12.737 de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 01 set. 2022.

_____. Câmara dos Deputados. **Projeto de Lei 2.232/2021**. Altera o art. 158 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940
(Código Penal), para prever a qualificadora da extorsão cibernética. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2038974 Acesso em: 30 ago. 2022.

BRITTO, Gladstone Avelino; FREITAS, Maristella Barros. Ciberataques em massa e os limites do poder punitivo na tipificação de crimes informáticos. **Revista de Direito Penal, Processo Penal e Constituição**. v.3, n.2, jul-dez, 2017.

CASTELLS, Manuel. **A sociedade em rede**. 22ª edição. São Paulo: Paz e Terra, 2020.

CANADIAN CENTRE FOR CYBER SECURITY. **Ransomware: How to prevent and recover (ITSAP.00.099)**. Disponível em: https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099 Acessado em: 02 set. 2022.

CERT.BR. **Ransomware**. Disponível em: https://cartilha.cert.br/ransomware/ Acessado em: 02 set. 2022.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO. **Exatas & Engenharias**, v. 3, n. 05, mar. 2013.

CORMEN, Thomas. **Desmistificando Algoritmos**. Rio de Janeiro: Elsevier, 2014.

EUROPEAN PARLIAMENT. **The NIS2 Directive: A high common level of cybersecurity in the EU**. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 Acesso em: 02 set. 2022.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva; SILVA, Fernanda Viero da. Phishing e engenharia social: entre a criminalização e a utilização de meios sociais de proteção. **Revista Meritum**, Belo Horizonte, v. 15, n. 1, p. 147-165, jan-abr. 2020.

FREIRE, Rodolfo Francisco Paz; SILVA, Humberto Caetano Cardoso da; QUEIROZ, Ricardo Gomes de; BATISTA, Amélia Acácia de Miranda. O fator humano como uma vulnerabilidade em segurança da informação. **Revista Brasileira de Administração Científica**, v.8, n.3, p.146-157, 2017.

JOPPERT, Alexandre Couto. **Fundamentos do Direito Penal. Aplicação da Lei Penal, Teoria Geral do Crime, Concurso de Agentes**. Rio de Janeiro: Editora Lumen Juris, 2006.

MOHURLE, Savita; PATIL, Manisha. A brief study of Wannacry Threat: ransomware attack 2017. **International Journal of Advanced Research in Computer Science**. Vol. 8, n. 5, may-june 2017.

PACHECO, Wilfredo Enrique Pires. **Crimes Digitais: Responsabilização Penal de Hackers, Crackers e Engenheiros Sociais**. Edição Kindle, 2011.

PELLIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. Bolhas Sociais e seus Efeitos na Sociedade da Informação: Ditadura do Algoritmo e Entropia na Internet. **Revista de Direito, Governança e Novas Tecnologias**. Belém, v. 5, n. 2, p. 57 – 73, jul/dez, 2019.

WARREN, Elizabeth. **Warren & Ross Introduce Bill to Require Disclosures of Ransomware Payments**. Disponível em: https://www.warren.senate.gov/newsroom/press-releases/warren-and-ross-introduce-bill-to-require-disclosures-of-ransomware-payments Acesso em: 03 set. 2022.