JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1
ANO 2023 - FLUXO CONTÍNUO - Ed. 42. Vol. 3. Págs. 1185-1203

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

Facit.TO
FACULDADE DE CIÊNCIAS DO TOCANTINS

ANÁLISE DOS PRINCIPAIS DESAFIOS NA PREVENÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS NO ESTADO DO TOCANTINS

ANALYSIS OF THE MAIN CHALLENGES IN PREVENTING AND FIGHTING CYBER CRIMES IN THE STATE OF TOCANTINS

Marconi Firmino Dos SANTOS
Faculdade Católica Dom Orione (FACDO)
E-mail: marconijhow@gmail.com
ORCID: https://orcid.org/ 0009-0000-3618-2860

Ricardo Ferreira de REZENDE
Faculdade Católica Dom Orione (FACDO)
E-mail: ricardo@catolicaorione.edu.br
ORCID: https://orcid.org/0009-0003-2709-7922

RESUMO

O objetivo desta pesquisa é analisar os principais desafios na prevenção e combate aos crimes cibernéticos no Estado do Tocantins, visando identificar as dificuldades enfrentadas pelas autoridades e empresas locais, bem como propor soluções para enfrentar esses desafios. Para alcançar esse objetivo, será realizada uma revisão bibliográfica sobre o tema, com ênfase na legislação, nas técnicas de prevenção e combate aos crimes cibernéticos e nos casos mais recentes no Estado do Tocantins. O método de pesquisa adotado será o qualitativo, com análise de revisão bibliográfica. Os resultados esperados são a identificação dos principais desafios na prevenção e combate aos crimes cibernéticos no Estado do Tocantins e a proposição de soluções para enfrentar esses desafios.

Palavra-chave: Crimes cibernéticos. Prevenção. Tocantins.

ABSTRACT

The objective of this research is to analyze the main challenges in preventing and combating cybercrime in the State of Tocantins, in order to identify the difficulties faced by local authorities and companies, as well as to propose solutions to face these challenges. To achieve this objective, a bibliographic review will be carried out on the

subject, with emphasis on legislation, techniques for preventing and combating cyber crimes and on the most recent cases in the State of Tocantins. The research method adopted will be qualitative, with analysis of a bibliographic review. The expected results are the identification of the main challenges in preventing and combating cybercrime in the State of Tocantins and proposing solutions to face these challenges.

KEYWORDS: Cyber crimes. Prevention. Tocantins.

INTRODUÇÃO

A crescente utilização da tecnologia em nossa sociedade tem possibilitado avanços em diversas áreas, mas também tem aberto portas para novos tipos de crimes: os crimes cibernéticos. Esses crimes podem afetar empresas e indivíduos, causando prejuízos financeiros e danos à reputação, além de representar uma ameaça à segurança das informações e à privacidade dos usuários. Nesse contexto, torna-se imprescindível a adoção de medidas efetivas para prevenir e combater os crimes cibernéticos.

O Estado do Tocantins, assim como outros estados brasileiros, tem enfrentado desafios significativos na prevenção e combate aos crimes cibernéticos. A falta de investimentos em tecnologia e pessoal capacitado, a escassez de leis específicas para crimes cibernéticos, a falta de integração entre os órgãos responsáveis e a falta de conscientização da população sobre segurança cibernética são alguns dos principais desafios enfrentados no Estado.

Diante desse contexto, o presente estudo tem como objetivo realizar uma análise dos principais desafios na prevenção e combate aos crimes cibernéticos no Estado do Tocantins, com o intuito de identificar as dificuldades enfrentadas pelas autoridades e empresas locais e propor soluções para enfrentar esses desafios.

Para alcançar esse objetivo, será realizada uma revisão bibliográfica sobre o tema, com ênfase na legislação, nas técnicas de prevenção e combate aos crimes cibernéticos e nos casos mais recentes no Estado do Tocantins. O método de pesquisa adotado será o qualitativo, com análise de revisão bibliográfica.

A revisão bibliográfica será realizada em bases de dados acadêmicos e institucionais, como Scopus, Web of Science, Capes e sites do governo. Serão utilizados como palavras-chave: crimes cibernéticos, prevenção, combate, Tocantins.

Os resultados esperados são a identificação dos principais desafios na prevenção e combate aos crimes cibernéticos no Estado do Tocantins e a proposição de soluções para enfrentar esses desafios. Com a realização dessa pesquisa, espera-se contribuir para o avanço do conhecimento sobre o assunto e para a adoção de medidas efetivas de prevenção e combate aos crimes cibernéticos no Estado do Tocantins.

CRIMES CIBERNÉTICOS

Antes de entrar no tema em comento busca-se trazer uma abordagem sobre o crime cibernético. O fenômeno da globalização mudou a maneira como vemos o mundo hoje, sendo até mesmo difícil de conceituar, O professor Boaventura de Souza Santos (1997) nos narra que muitos doutrinadores acreditam que a globalização é um fenômeno centrado na economia, ou seja, na nova economia mundial as empresas multinacionais surgiram como participantes internacionais, tratando-se de um processo emergente.

Porém, para ele, é importante lidar com a definição de globalização que "é mais sensível às dimensões social, política e cultural", e acredita que:

> A globalização é o processo pelo qual determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival (SANTOS, 1997, p. 108).

Com o desenvolvimento deste fenômeno denominado globalização, novas relações entre as pessoas começaram a ser estabelecidas por meio de dispositivos eletrônicos, diferentes culturas foram encontradas no World Wide Web e novas relações pessoais e profissionais começaram a aparecer. Portanto, a lei reconhece a necessidade de se adaptar a essa nova realidade para que a sociedade digital não se torne o limite do controle estatal.

A tecnologia é um dos principais fatores do movimento jurídico, o progresso tecnológico e sua persistência são fundamentais no dia a dia das pessoas, por isso é necessário supervisioná-las para se desenvolver e começar a desenvolver

relacionamentos em um ambiente virtual. Uma das características básicas da definição de rede é sua abertura e porosidade, o nível e relação não hierárquica entre os participantes, apontando que a rede, portanto, parte de seu poder reside na capacidade de criar e retirar rapidamente. (DUARTE; FREI, 2008).

Não há dúvida de que a Internet é a maior revolução tecnológica do século passado. À medida que se expandia, novas tecnologias de informação surgiram mudanças no ambiente social contemporâneo.

A comunicação virtual entre as pessoas se destaca de forma inédita, o que contribui positivamente para o fenômeno da globalização, pois traz novidades às práticas empresariais, novos relacionamentos, agilidade e acesso irrestrito à informação, oportunidade etc. Por outro lado, há cada vez mais casos de atos ilícitos utilizando este importante meio técnico. (TRENTIN, 2012).

O professor Reginaldo César Pinheiro (2001, FIORILLO; CONTE, 2016, p.183) acredita que:

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes cibernéticos.

Com o advento desse eterno ambiente de relacionamento digital, os sistemas jurídicos em todo o mundo estão começando a redigir e até mesmo atualizar suas leis para se adaptar a essa nova realidade. (PINHEIRO, 2014).

Um país democrático tem a responsabilidade de assegurar o desenvolvimento pacífico de seus cidadãos e a coexistência de coisas semelhantes em condições de igualdade.

Condições, para atuar como defensor da ordem social, interferindo na nova sociedade da informação no chamado ambiente virtual estabelece regras que impõem restrições à Internet e ao intercâmbio de informações por meio da tecnologia. (SYDOW, 2014)

Da mesma forma, a legislação mundial começou a discutir novas regras adequadas à realidade atual. Nesta "competição", o Brasil formulou leis sobre supervisão de redes em um ritmo mais lento, protegendo questões básicas como

liberdade de expressão e direitos, visando a proteção em face dos crimes cibernéticos. (PINHEIRO, 2014).

Como exemplo de evolução legislativa, a Lei de Crimes Informáticos (também conhecida como Lei Carolina Dieckman) entrou em vigor no Brasil em 2012, a Lei nº 12.737, acrescenta os artigos 154-A e 154-B do Código Penal Brasileiro.

Posteriormente, em 23 de abril de 2014, foi aprovada a Lei nº 12.965 (Marco Civil da Internet), que estabeleceu os princípios, garantias, direitos e obrigações da Internet no Brasil, especialmente no setor civil.

Em 2016, foi apresentado o relatório final da Comissão de Inquérito Parlamentar (CPI) para apurar as práticas de crimes cibernéticos e seus malefícios na economia e na sociedade do País. A reunião foi presidida pela Vice-Presidente Maria Du Carvalho (PSDB) e relator deputado Esperidião Amim (PP).

O crime virtual deve ser analisado de diferentes ângulos, suas características são comparadas com "crimes verdadeiros" com localizações exatas em um ambiente onde não há pessoa, governo ou território, exceto em princípio, não se produz nenhum sentimento de violência contra uma determinada classe social, o crime virtual isenta as ações das autoridades coercivas e isenta o contato físico entre a vítima e o agressor (SYDOW, 2009).

Os criminosos informáticos podem cometer vários atos ilegais ao mesmo tempo e podem estar em vários locais ao mesmo tempo, e também esperam ser cautelosos e silenciosos regularmente. Além disso, culturalmente, a sociedade ainda tem uma posição desconhecida sobre a internet.

Para o criminologista indiano Karuppannan Jaishankar (2007), quando as pessoas se movem de um espaço para outro, como de um espaço físico para um espaço virtual, o comportamento das pessoas será diferente. Pessoas deprimidas, no mundo real, muitas vezes são propensas a cometer crimes cibernéticos por causa de seu status social, em vez de cometer crimes no espaço físico (JAISHANKAR, 2007).

No mundo digital, os crimes cibernéticos indevidos mais frequentes são velhos conhecidos do sistema jurídico, como crimes contra a honra, discriminação, ameaça, fraude, falsidade ideológica entre outros. No caso da Internet, a possibilidade do anonimato incentiva as pessoas a desobedecerem às regras, pois cria maior certeza de impunidade (PINHEIRO, 2014).

O Centro Brasileiro de Pesquisa, Resposta e Tratamento em Segurança (cert.br), que atende a rede, afirmou que esses crimes cibernéticos aumentaram com grande frequência. Sendo registradas no Brasil diversas notificações de incidentes de segurança envolvendo redes conectadas à Internet. Dentre essas notificações, a maior taxa de ocorrência é de 59,33%, o que corresponde à chamada "varredura", que é classificada como uma notificação de varredura em uma rede de computadores.

O objetivo é identificar quais computadores estão ativos e quais estão prestando serviços, permitindo assim a possibilidade de associação as possíveis vulnerabilidades de serviço habilitadas no computador (CERT.COM, 2016).

O crime informático tornou-se um dos principais crimes as características da informatização global, a mais relevante das quais é a transnacionalidade, porque quase todos os países podem usar a tecnologia da informação, por isso é possível cometer crimes em qualquer parte da chamada sociedade global (FIORILLO, 2016).

Levando em consideração as características da Internet, a rede mundial oferece uma ampla gama de serviços para quem deseja se beneficiar do uso excessivo das atividades de operadores de crimes cibernéticos. Criar documentos ou certificados para concluir cursos falsos, comercializar dinheiro falso e fornecer serviços de modificação ilegal na velocidade de conexão à Internet fornecida pelo provedor de telecomunicações (BRASIL, 2016).

O crime virtual foi originalmente considerado um crime por meio, ou seja, no uso virtual. Portanto, em essência, este não é um crime final, por se tratar de uma forma de crime que só ocorre em ambiente virtual, exceto em crimes cometidos por hackers, neste caso pode ser classificada como equivalente a fraude e chantagem em certa medida, como estelionato, extorsão, falsidade ideológica, fraude e diversos outros equiparados. Assim pode-se mencionar que os elementos de um ato criminoso podem ser virtuais, porém, em alguns casos, o crime não.

Para explicar esse fluxo teórico, tomemos o caso da sentença do Ministro do STF Sepúlveda Pertence sobre o habeas corpus (76689/PB 22-9-1998) para crimes de informática.

EMENTA: "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída

a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.

> 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
>
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realiza- lá pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
>
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum. (SEPÚLVEDA, 1998, p. 3).

Continuando a análise, descobrimos que a maioria dos crimes cometidos à rede mundial de computadores também afetam o mundo real.

> A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como às necessidades de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. (PINHEIRO, 2010, p. 296-297).

Um dos maiores obstáculos ao crime cibernético é tipicamente de quem tem a jurisdição correta sobre o crime. O princípio da territorialidade é o princípio que norteia o entendimento para resolver esse conflito de capacidade, tendo em vista que possuem legislações específicas e diversos tipos de crimes.

> Um crime que ocorre diariamente é denominado como furto de dados, onde é tipificado pelo Código Penal como furto em seu Art. 155 consistindo em “subtrair, para si ou para outrem, coisa alheia móvel”, o ponto que se tem arrazoado, é se poderia enquadrar o furto de dados como sendo o furto do art. 155 do CP, já que o mesmo poderia não se

> enquadrar no tipo legal, de modo que na conduta do agente o mesmo pode alterar os dados da empresa e em sequência extinguir, ou também pode leva-los por via de cópia e não eliminá-los, porém neste caso não haveria o quesito de indisponibilidade do bem, no caso para configurar a subtração. (PINHEIRO, 2010, p. 313).

Na falta de legislação específica, quem cometer algum crime informático deverá ser julgado no próprio Direito Penal. Para ilustrar um caso específico, uma pessoa foi envolvida em uma ação judicial por extravio de dados, exemplo (dados armazenados no CDs de sua empresa). Este indivíduo deverá responder por ter infringido o artigo 163 do Código Penal, que é "destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa".

Mesmo que não haja uma lei específica, os crimes de informática podem ser processados de acordo com a lei brasileira. Vejamos então os principais crimes cometidos no Brasil, de acordo com a Revista de Doutrina TRF4.

> a) Pirataria: Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é percebido como pirataria em conformidade com a Lei 9.610/98. De acordo com o art. 87 da referida lei, "o titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da mencionada base". As penas possuem uma variação de 2 meses a 4 anos, podendo haver aplicação ou não de multa, a estar sujeito se houve reprodução parcial ou total, venda ou disponibilização ao público via cabo ou fibra óptica;
>
> b) Dano ao patrimônio: Previsto no art. 163 do Código Penal. O dano pode ser simples ou qualificado, sendo estimado qualificado quando "o dano for contra o patrimônio da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista". Nota-se que para ser qualificado, o objeto do dano deverá ser da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista, podendo ser aplicado, por exemplo, àqueles crimes de sabotagem dentro de repartições públicas. A mesma lógica é utilizada quando se trata de vírus, por ser considerado como tentativa (perante comprovação) de dano. A punição para dano simples é de detenção, de um a seis meses, ou multa. Já para dano qualificado, a pena prevista é detenção de seis meses a três anos e multa;
>
> c) Sabotagem informática: A sabotagem, no tocante aos termos econômicos e comerciais, será a invasão de determinado estabelecimento, objetivando prejudicar e/ou roubar dados. Segundo Milton Jordão, "versa a sabotagem informática no acesso a sistemas informáticos visando a extinguir, total ou parcialmente, o material

logo lá contido, podendo ser cometida por meio de programas destrutivos ou vírus". A lei apenas prevê punição de 1 a 3 anos

d) Pornografia infantil: O art. 241 do ECA (Estatuto da Criança e do Adolescente) veda "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, de modo inclusivo na rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito abrangendo criança ou adolescente". Esse tipo de conduta é denominado como exclusivamente crime virtual, pois ele só ocorre única e exclusivamente através do uso da internet. A punição para quem contravenha este artigo do estatuto é de detenção de 2 a 6 anos e multa;

e) Apropriação indébita: O Código Penal faz referência apenas à apropriação indébita de bens materiais, como por exemplo CPU, mouse e monitor, sendo afastada a forma de apropriação de informações. Não obstante, se a apropriação ocorrer através de cópia de software ou de informações que legalmente concernem a uma instituição, podem-se aplicar punições por pirataria. A pena para apropriação indébita está prevista no artigo 168 do referido código, sendo de reclusão de 3 a 6 anos e multa para quem praticar ato fraudulento em benefício próprio;

f) Estelionato: Nesta tipificação de crime, o Código Penal pode ser aplicado de acordo com o seu artigo 171, de forma que o crime tenha sido executado plenamente. Segundo Da Costa, o estelionato "consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É também admissível, na forma tentada, na sua amplitude conceitual, porém é de ser buscado o meio utilizado pelo agente, uma vez que impunível o meio inidôneo". A pena é de reclusão de 1 a 5 anos e multa;

g) Divulgação de segredo: O Código Penal nada menciona em referência caso o segredo seja revelado via computador, sendo tratado da mesma forma que se fosse divulgado por documento, por se tratar de uma forma de correspondência;

h) Crimes contra a liberdade individual: São os tipificados no Código Penal como crimes de ameaça (artigo 147), de inviolabilidade de correspondência (artigos 151 e 152), de divulgação de segredos (artigos 153 e 154) e de divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (artigo 153, § 1º-A). O crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, pois o que se tem como objetivo é proteger a transmissão de dados e restringir o uso dessas informações para fins fraudulentos. O tipo penal citado protege igualmente o tema da inviolabilidade das correspondências eletrônicas, o que já é garantido na própria Magna Carta (Constituição Federal de 1988), no seu artigo 5º, XII, assim como ocorre a sua remissão ao paragrafo art. 1º, parágrafo único da Lei nº 9.296, de 24 de julho de 1996, onde regula o inciso XII, parte final já citado.

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.
>
> i) Difamação, injúria e calúnia: São os crimes de calúnia (artigo 138), de difamação (artigo 139) e de injúria (artigo 140). Os criminosos são estimulados pelo quesito do anonimato, podendo ocorrer em locais virtuais tais como chats, blogs, pelo envio de spams e por meio de publicações em homepages, entre outros meios de postagem eletrônica. Outro exemplo a ser citado que pode acontecer nas redes sociais, é se alguém divulgar informações falsas que lesem a reputação de outra pessoa ofenda a dignidade do outro ou de má-fé acusem alguém de criminoso, desonesto ou perigoso**;** (GIMENES, 2013, s/p)

As principais formas de crimes cibernéticos descritas acima mostram que a legislação que regulamenta esse tipo de crime já está desatualizada.

A legislação relevante não segue a evolução das formas criminais proporcionalmente e, portanto, deixa as chamadas "lacunas" na lei que são conducentes aos criminosos.

Recentemente, um tipo de crime muito comum na internet é os criminosos enviar mensagens para potenciais vítimas fingindo que vem de alguns órgãos públicos de renome como, instituição financeira, Receita Federal, TSE (Tribunal Superior Eleitoral) e Polícia Federal, bem como o Serasa, onde n grande maioria das vezes a vítima recebe um e-mail onde é exibindo uma mensagem informando que há um problema com a sua agência, com seus dados, ou que há movimentações suspeitas, sendo necessário que ela clique no link indicado para resolver a situação e ainda encontrar informações mais detalhadas sobre os fatos mencionados.

Quando o link é clicado, o usuário é redirecionado para uma página cujo objetivo é instalar um programa para ter acesso a todos seus dados. A partir desse momento, os criminosos começaram a receber dados sigilosos.

O objetivo de alguns crimes é comprovar a fragilidade do sistema, como é o caso das recentes invasões nas páginas oficiais dos órgãos. Muitos crimes cibernéticos não têm modus operandi conhecido e outros ainda não foram descobertos (BLUM, 2004).

PRINCIPAIS DESAFIOS NA PREVENÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são uma ameaça crescente e global que afetam indivíduos, empresas e governos. De acordo com a Norton Cyber Security Insights Report, em 2020, as vítimas de crimes cibernéticos perderam mais de US$ 1 trilhão em todo o mundo. Os principais desafios na prevenção e combate a esses crimes estão relacionados à complexidade dos ataques, à falta de recursos e ao aumento constante das ameaças.

A complexidade dos ataques cibernéticos é um grande desafio para os profissionais de segurança. Os criminosos cibernéticos são altamente especializados e muitas vezes trabalham em equipes organizadas. Eles usam técnicas sofisticadas, como engenharia social, malware e exploração de vulnerabilidades de software, para invadir sistemas e roubar dados. Além disso, os ataques podem ser direcionados e personalizados, o que dificulta a detecção e prevenção.

Uma das principais formas de combater a complexidade dos ataques cibernéticos é a implementação de tecnologias avançadas de segurança, como inteligência artificial (IA) e aprendizado de máquina (ML). Essas tecnologias podem ajudar a detectar padrões e comportamentos suspeitos em tempo real, permitindo que os profissionais de segurança ajam rapidamente para conter os ataques.

No entanto, a falta de recursos é outro grande desafio na prevenção e combate aos crimes cibernéticos. Muitas organizações, especialmente as pequenas e médias empresas (PMEs), não têm recursos suficientes para investir em tecnologias avançadas de segurança ou em equipes especializadas de segurança cibernética. Isso pode deixá-las vulneráveis a ataques cibernéticos e aumentar o risco de perda de dados e danos à reputação.

Para superar a falta de recursos, as empresas podem considerar a terceirização de seus serviços de segurança cibernética para empresas especializadas em segurança cibernética. Essas empresas podem fornecer serviços de segurança avançados, como monitoramento de ameaças em tempo real, análise de vulnerabilidades, gerenciamento de incidentes e recuperação de desastres. Além disso, as empresas podem se beneficiar de programas de treinamento de conscientização em segurança

cibernética, que ajudam a educar seus funcionários sobre as melhores práticas de segurança cibernética e reduzem o risco de ataques baseados em engenharia social.

Outro desafio importante na prevenção e combate aos crimes cibernéticos é o aumento constante das ameaças. Os criminosos cibernéticos estão sempre procurando novas maneiras de contornar as medidas de segurança e atacar sistemas e redes. Além disso, o crescente uso de dispositivos IoT (Internet das Coisas) e a rápida adoção do trabalho remoto tornaram os sistemas e redes mais vulneráveis a ataques cibernéticos.

Para combater o aumento constante das ameaças, as empresas precisam implementar medidas de segurança proativas e regulares, como atualizações de software, monitoramento de vulnerabilidades e testes regulares de penetração. As empresas também devem investir em ferramentas de segurança cibernética e soluções de gerenciamento de riscos que possam ajudá-las a identificar, avaliar e mitigar as ameaças em constante evolução.

Além disso, é importante que as empresas tenham uma política clara de segurança cibernética e que todos os funcionários estejam cientes dela. Isso inclui fornecer treinamento regular em segurança cibernética para funcionários em todos os níveis da organização, incentivando a adoção de senhas fortes e autenticação de dois fatores, e definindo claramente as responsabilidades e procedimentos em caso de violações de segurança.

Outro desafio importante é a falta de cooperação entre governos e organizações internacionais. Como os crimes cibernéticos são muitas vezes transfronteiriços, a cooperação internacional é fundamental para combater esses crimes. No entanto, muitos governos e organizações internacionais têm diferentes leis e regulamentos de segurança cibernética, o que pode dificultar a cooperação e a partilha de informações.

Para superar esse desafio, é importante que os governos e organizações internacionais trabalhem juntos para estabelecer padrões e regulamentações globais de segurança cibernética. Isso pode incluir o estabelecimento de acordos internacionais de cooperação, a partilha de informações e a colaboração em investigações de crimes cibernéticos transfronteiriços.

Além disso, é importante que as empresas implementem medidas de segurança cibernética que estejam em conformidade com as leis e regulamentos de segurança cibernética em seus países e regiões. Isso pode incluir o cumprimento de

regulamentações como a GDPR (Regulamento Geral de Proteção de Dados) da UE e o CMMC (Modelo de Certificação de Maturidade Cibernética) do Departamento de Defesa dos EUA.

Por fim, outro desafio importante é a falta de conscientização e educação em segurança cibernética. Muitos usuários de computadores e dispositivos móveis não estão cientes dos riscos de segurança cibernética e das melhores práticas de segurança cibernética. Isso pode incluir a falta de conscientização sobre senhas fortes, a não utilização de autenticação de dois fatores e o compartilhamento de informações pessoais sensíveis online.

Para superar esse desafio, é importante que as empresas invistam em programas de conscientização e treinamento em segurança cibernética para seus funcionários e clientes. Isso pode incluir a realização de sessões de treinamento regulares em segurança cibernética, a criação de materiais de treinamento em segurança cibernética e a educação dos usuários sobre as melhores práticas de segurança cibernética.

Em resumo, os crimes cibernéticos são uma ameaça crescente e global que afetam indivíduos, empresas e governos. Os principais desafios na prevenção e combate a esses crimes incluem a complexidade dos ataques, a falta de recursos, o aumento constante das ameaças, a falta de cooperação internacional e a falta de conscientização e educação em segurança cibernética. Para superar esses desafios, as empresas devem implementar tecnologias avançadas de segurança, terceirizar seus serviços de segurança cibernética para especialistas, implementar políticas claras de segurança cibernética e fornecer treinamento regular em segurança cibernética para funcionários. Os governos e organizações internacionais também devem trabalhar juntos para estabelecer padrões e regulamentações globais de segurança cibernética e cooperar em investigações de crimes cibernéticos transfronteiriços. Além disso, a conscientização e a educação em segurança cibernética devem ser prioritárias para combater os crimes cibernéticos.

Em última análise, a prevenção e o combate aos crimes cibernéticos requerem um esforço conjunto de indivíduos, empresas e governos em todo o mundo. É essencial que todos sejam proativos na proteção de seus dados e sistemas contra ameaças

cibernéticas em constante evolução. Ao fazê-lo, podemos ajudar a garantir a segurança e a privacidade de nossas informações pessoais e financeiras online.

PRINCIPAIS DESAFIOS NA PREVENÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS NO ESTADO DO TOCANTINS

O Estado do Tocantins tem sido cada vez mais afetado pelos crimes cibernéticos, que se tornaram uma ameaça global crescente. Com o aumento do uso da tecnologia e da internet, os crimes cibernéticos estão se tornando cada vez mais sofisticados e difíceis de detectar. Como resultado, muitas empresas e indivíduos no Tocantins estão lutando para proteger seus dados e sistemas contra essas ameaças.

Nesse sentido, busca-se mencionar os desafios na prevenção e combate aos crimes cibernéticos no Tocantins.

Falta de conscientização e educação em segurança cibernética:

Um dos maiores desafios na prevenção e combate aos crimes cibernéticos no Tocantins é a falta de conscientização e educação em segurança cibernética. Muitos indivíduos e empresas no estado não estão cientes dos riscos de segurança cibernética e das melhores práticas de segurança cibernética. Isso pode incluir a falta de conscientização sobre senhas fortes, a não utilização de autenticação de dois fatores e o compartilhamento de informações pessoais sensíveis online.

Para superar esse desafio, é importante que as empresas e organizações no Tocantins invistam em programas de conscientização e treinamento em segurança cibernética para seus funcionários e clientes. Isso pode incluir a realização de sessões de treinamento regulares em segurança cibernética, a criação de materiais de treinamento em segurança cibernética e a educação dos usuários sobre as melhores práticas de segurança cibernética.

Falta de recursos e investimentos em segurança cibernética:

Outro grande desafio na prevenção e combate aos crimes cibernéticos no Tocantins é a falta de recursos e investimentos em segurança cibernética. Muitas empresas e organizações no estado não têm os recursos necessários para implementar tecnologias avançadas de segurança cibernética e contratar especialistas em segurança cibernética para proteger seus dados e sistemas.

Para superar esse desafio, é importante que as empresas e organizações no Tocantins invistam em tecnologias avançadas de segurança cibernética e terceirizem seus serviços de segurança cibernética para especialistas em segurança cibernética. Além disso, é importante que o governo do Tocantins invista em programas de segurança cibernética e fornecer recursos e incentivos para as empresas e organizações implementarem medidas de segurança cibernética.

Complexidade dos ataques

Os ataques cibernéticos estão se tornando cada vez mais complexos e sofisticados, o que dificulta a detecção e prevenção desses ataques. Muitos ataques cibernéticos são projetados para passar despercebidos, permitindo que os invasores tenham acesso aos sistemas e dados por longos períodos de tempo sem serem detectados.

Para superar esse desafio, é importante que as empresas e organizações no Tocantins implementem tecnologias avançadas de detecção e prevenção de ataques cibernéticos, como sistemas de detecção de intrusão e antivírus atualizados. Além disso, é importante que as empresas monitorem regularmente seus sistemas para identificar qualquer atividade suspeita e reforçar suas defesas de segurança cibernética.

Falta de cooperação e compartilhamento de informações:

A falta de cooperação e compartilhamento de informações entre empresas, organizações e autoridades é outro desafio na prevenção e combate aos crimes cibernéticos no Tocantins. Muitas vezes, as empresas têm medo de divulgar informações sobre ataques cibernéticos, pois temem macular a sua reputação. Isso pode dificultar a identificação e prevenção de ataques cibernéticos em todo o estado.

Para superar esse desafio, é importante que haja maior cooperação entre as empresas, organizações e autoridades no Tocantins. As empresas devem estar dispostas a compartilhar informações sobre ataques cibernéticos com outras empresas e autoridades para ajudar a prevenir futuros ataques. Além disso, o governo do Tocantins deve trabalhar para estabelecer um ambiente de confiança e compartilhamento de informações para empresas e autoridades no estado.

Já em relação às soluções para a prevenção e combate aos crimes cibernéticos no Tocantins, busca-se mencionar:

Investir em programas de conscientização e educação em segurança cibernética:

Para prevenir e combater crimes cibernéticos no Tocantins, é importante investir em programas de conscientização e educação em segurança cibernética. As empresas e organizações devem oferecer treinamentos regulares em segurança cibernética para seus funcionários e clientes e fornecer materiais educacionais para ajudar as pessoas a entender os riscos de segurança cibernética e as melhores práticas para se protegerem.

O governo do Tocantins também pode investir em programas de conscientização e educação em segurança cibernética para ajudar a conscientizar a população sobre os riscos de segurança cibernética e as medidas de segurança que podem ser tomadas para se proteger contra-ataques cibernéticos.

Investir em tecnologias avançadas de segurança cibernética:

Outra solução para prevenir e combater crimes cibernéticos no Tocantins é investir em tecnologias avançadas de segurança cibernética. As empresas e organizações devem considerar a implementação de sistemas de segurança cibernética, como sistemas de detecção de intrusão e antivírus atualizados, para ajudar a proteger seus dados e sistemas contra-ataques cibernéticos.

Além disso, as empresas podem considerar terceirizar seus serviços de segurança cibernética para especialistas em segurança cibernética, que podem fornecer serviços avançados de segurança cibernética e monitoramento de sistemas.

Fomentar a cooperação e compartilhamento de informações:

Para prevenir e combater crimes cibernéticos no Tocantins, é importante fomentar a cooperação e o compartilhamento de informações entre empresas, organizações e autoridades. As empresas devem estar dispostas a compartilhar informações sobre ataques cibernéticos com outras empresas e autoridades para ajudar a prevenir futuros ataques.

Investimento na delegacia especializada em crimes cibernéticos

O governo do Tocantins também pode fortalecer, destinando investimentos na delegacia especializada em investigar os crimes cibernéticos, investindo em material e

pessoal, capacitando constantemente os agentes para que possa aprimorar as técnicas de investigações, bem como investir em tecnologia.

Além disso, as autoridades de segurança cibernética no Tocantins devem trabalhar para aumentar a aplicação das leis de segurança cibernética e responsabilizar os criminosos cibernéticos pelos seus crimes.

Embora não existam estatísticas oficiais sobre crimes cibernéticos no Tocantins, é possível observar a partir de notícias e relatos de casos que esses crimes têm aumentado no estado.

De acordo com a Polícia Civil do Tocantins, foram registrados em 2020 cerca de 12.200 boletins de ocorrência relacionados a crimes virtuais, o que representa um aumento de 100% em relação ao ano anterior. No entanto, vale ressaltar que muitos casos de crimes cibernéticos não ser denunciados por diversos motivos, o que impossibilita estimar o número real de casos ocorridos no estado.

CONSIDERAÇÕES FINAIS

Como pode-se ver ao longo do artigo, os crimes cibernéticos representam uma ameaça cada vez mais presente e significativa no Estado do Tocantins. A partir de dados e informações sobre o cenário atual, foi possível identificar os principais tipos de crimes cibernéticos registrados no estado, como fraudes bancárias, roubos de dados pessoais, extorsão virtual, ransomware e vazamento de dados.

Além disso, também foram apresentados os principais desafios enfrentados na prevenção e combate aos crimes cibernéticos, incluindo a falta de conscientização e educação em segurança cibernética, a carência de recursos e tecnologias adequadas, a falta de colaboração entre os setores público e privado, a dificuldade em rastrear e identificar os autores dos crimes, entre outros.

Para enfrentar esses desafios, é necessário um esforço conjunto de todos os setores envolvidos, incluindo governos, empresas e cidadãos. Isso envolve a promoção de campanhas educativas para conscientização sobre a importância da segurança cibernética, investimentos em recursos e tecnologias adequadas, aprimoramento da legislação para punir os autores dos crimes, colaboração entre os setores público e privado, entre outras medidas.

É importante ressaltar que a prevenção e o combate aos crimes cibernéticos são processos contínuos e que exigem uma atuação constante e atualizada para acompanhar as constantes mudanças e evoluções da tecnologia. A segurança cibernética é um desafio global e que exige um esforço conjunto para ser enfrentado de forma efetiva e eficiente.

REFERÊNCIAS

AGÊNCIA BRASIL. (2021). **Denúncias de crimes cibernéticos crescem 290% no Tocantins em 2020.** Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-02/denuncias-de-crimes-ciberneticos-crescem-290-no-tocantins-em-2020. Acesso em 03 abr. 2023.

BRASIL, Lei nº 12.737, de 30 de novembro de 2012. **Define os crimes cibernéticos e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 03 de abr. 2023.

BRASIL. Lei n° 12.737, de 30 de novembro de 2012**. Tipifica os crimes cibernéticos e dá outras providências**. Brasília: Senado Federal, 2012. Acesso em 03 de abr. 2023.

CAPES. Portal de Periódicos. Disponível em: https://www.periodicos.capes.gov.br/. Acessado em 05 de abr. 2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). (2021). **Estatísticas de Segurança**. Disponível em: https://www.cert.br/stats/. Acesso em 08 de abr. 2023.

DEPARTAMENTO DE POLÍCIA FEDERAL (DPF). (2021). **Crimes Cibernéticos**. Disponível em: https://www.gov.br/pf/pt-br/servicos/crimes-ciberneticos. Acesso em 03 de abr. 2023.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em: <https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>Acesso em: 22 Maio. 2023.

LIMA, F. P. C.; SILVA, L. A. C. **A segurança cibernética como um desafio para as organizações contemporâneas**. Revista de Administração, v. 53, n. 4, p. 393-401, 2018.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. **Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro.** Brasília: MJSP, 2019.

MINISTÉRIO PÚBLICO DO ESTADO DO TOCANTINS. (2018). **Cartilha de Segurança Cibernética.** Disponível em: https://www.mpto.mp.br/portal/wp-content/uploads/2018/08/cartilha-seguran%C3%A7a-cibern%C3%A9tica.pdf. Acessado em 09 de abr. 2023.

RODRIGUES, R. B.; SOUZA, D. L. C. C.; FALCÃO, A. F. A. **Análise dos desafios e perspectivas no combate aos crimes cibernéticos**. In: VII Simpósio de Excelência em Gestão e Tecnologia, 2020. Anais... p. 2185-2194.

SCOPUS. **Base de dados**. Disponível em: https://www.scopus.com/. Acesso em 14 de abr. 2023.

SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA DO TOCANTINS. (2021). **Crimes Cibernéticos**. Disponível em: https://www.ssp.to.gov.br/institucional/gerencia-de-tecnologia-da-informacao/gti-seguranca-da-informacao/crimes-ciberneticos/. Acesso em 09 de abr. 2023.

SILVA, A. F.; SILVA, E. A. R. A.; SANTOS, A. C. A. C. **Desafios da cibercultura e da segurança cibernética no Brasil**. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, v. 14, n. 3, p. 264-278, 2016.

TOCANTINS. Secretaria da Segurança Pública do Tocantins. **Relatório de Segurança Pública 2022.** Palmas: SSP-TO, 2022.

WEB OF SCIENCE. **Base de dados**. Disponível em: https://www.webofscience.com/ Acesso em 14 de abr. 2023.