ATAQUES CIBERNÉTICOS EM SISTEMAS GOVERNAMENTAIS DURANTE A PANDEMIA DO COVID-19 NOS ANOS 2020 E 2021

CYBER ATTACKS ON GOVERNMENT SYSTEMS DURING COVID-19 PANDEMIC IN 2020 AND 2021

Matheus Rangel Haddad
Fatec São Caetano do Sul - Antonio Russo
matheus.haddad@fatec.sp.gov.br

João Célio Mendes Filho
Fatec São Caetano do Sul - Antonio Russo
joao.mendes18@fatec.sp.gov.br

Estefânia Angelico Pianoski Arata
Fatec São Caetano do Sul - Antonio Russo
estefania.arata@fatec.sp.gov.br

Resumo

Este artigo tem como objetivo, analisar ataques cibernéticos a sistemas governamentais que ocorreram entre os anos de 2020 e 2021, durante o período da pandemia do *covid*-19, fazendo com que novas formas de trabalho fossem pensadas durante o *lockdown*, qual foi adotado por vários países. O teletrabalho foi uma das novas formas adotadas, em que um colaborador acessa os sistemas de sua organização, que são necessários para o cumprimento do seu papel dentro do negócio, a partir de sua casa ou de onde achar mais adequado, permitindo que não precise estar fisicamente no ambiente de trabalho. Por meio de estudos de caso sobre os ataques cibernéticos que ocorreram a alguns sistemas governamentais brasileiros, durante os anos de 2020 e 2021, foi feito um descritivo contendo os sistemas, as entidades responsáveis ou envolvidas, as possíveis vulnerabilidades exploradas que viabilizaram o ataque, as consequências desses ataques, tão como a apresentação de algumas boas práticas que podem vir a mitigar, ou até mesmo evitar que certos tipos de ataques cibernéticos ocorram.

Palavras-chave: ataques cibernéticos, sistemas governamentais, segurança da informação.

Abstract

This article aims to analyze cyber-attacks on government systems that occurred between 2020 and 2021, during the period of the covid-19 pandemic. The pandemic allowed us to think of new ways of working during the lockdown, adopted by several countries. Home office has been one of the new ways in which an employee is able to access the organization systems, fundamental for his in-company business, doing it from home or wherever is most appropriate. This allows him not to be physically in the work environment. Through case studies on cyberattacks that occurred in some systems of the Brazilian government, during the years 2020 and 2021, a description has been made containing the systems, the entities responsible and/or involved, the possible exploited vulnerabilities that made the attack possible, the consequences of these attacks, as well as the presentation of some good practices that can mitigate, or even prevent the occurrence of certain types of cyber-attacks.

Keywords: cyber-attacks, government systems, information security.

1. INTRODUÇÃO

A segurança da informação vem ganhando mais importância a cada dia que passa, e com a facilidade que a tecnologia permite a comunicação com diferentes entidades, é incontável o número de informações circulando pela rede todos os dias, inclusive dados pessoais sensíveis. Com a Organização Mundial da Saúde decretando em março de 2020 uma pandemia, muitos trabalhadores foram conduzidos para o teletrabalho, aumentando bruscamente a quantidade de informações que trafegam na rede, o que contribuiu para maiores possibilidades de atacantes realizarem ataques bem-sucedidos. Um dos maiores centralizadores de dados, o governo, que acaba por custodiar os dados de todos os cidadãos não ficou de fora como possível alvo desses agressores.

2. REFERENCIAL TEÓRICO

São considerados dados pessoais sensíveis, segundo a Lei Geral de Proteção de Dados (LGPD):

> "[...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018, Inciso II, Art. 5º da Lei Geral de Proteção de Dados Pessoais - LGPD).”

Muitos destes dados são custodiados por sistemas governamentais, já em 2019 a quantidade de empresas controladas pela União foi de 206 estatais (Governo Federal, 2020), sem contar empresas controladas pelo Governo dos Estados e pelas Secretárias Municipais das Prefeituras.

Com a advinda da pandemia e a solicitação de quarentena, as empresas tiveram de fechar as portas, afetando também empresas governamentais com sistemas imprescindíveis para a população. Além do teletrabalho, sistemas antes presenciais passaram a ser *online* e digitais. Um dos serviços implementado durante a fase da pandemia foi o Poupatempo Digital, anunciado pelo Governo de São Paulo, oferecendo mais de 60 serviços *online* (Borges; Bitar, 2020), o Poupatempo é responsável pela emissão de documentos e outros serviços no estado de São Paulo. Outro sistema desenvolvido foi o CPF Digital, pela Secretaria da Receita Federal, disponibilizando o cartão do CPF em formato digital através de um aplicativo (Martello, 2020). Algumas Prefeituras também realizaram o cadastro para vacinação contra o novo coronavírus em formato digital, como ocorreu na Prefeitura de Uberlândia (2021), com o cadastramento realizado diretamente no Portal da Prefeitura.

2.1. Crescimento de Ataques Cibernéticos Durante a Pandemia

No ano de 2020 foram registrados 8,5 bilhões de tentativas de ataques cibernéticos no Brasil, de acordo com a Fortinet (2022), e em 2021 foi registrado um aumento de mais 950% chegando a 88,5 bilhões de tentativas de ataques cibernéticos.

Segundo dados divulgados pela Sonicwall (2022), o Brasil saiu da nona posição de países que mais sofrem com ataques de *ransomware* e passou a ocupar o quarto lugar, em 2020 foram 3.800.000 ataques, já em 2021 esse número ultrapassou os 33 milhões. O ataque de *ransomware* tem crescido no mundo todo, em dados também divulgados pela Sonicwall (2022), os ataques de *ransomware* tiveram um aumento global de 105% em 2021 com relação a 2020 e mais que 300% que em 2019.

Toda essa mudança acabou levando muitas pessoas a um ambiente perigoso que elas não estão acostumadas onde muitos *hackers* poderiam se aproveitar da falta de conhecimento de suas vítimas na hora de cometer algum crime. Os funcionários não estão acostumados com essa forma nova de trabalho, e podem estar colocando a organização em risco mesmo que sem intenção, o que os torna o elo mais fraco, e a presa mais fácil (Cardoso, 2020, p. 4).

2.2. Como Funciona um Ataque Cibernético

A instalação de programas ilícitos, mudanças não autorizadas das configurações do sistema, criação de novas vulnerabilidades permitem que *hackers* infiltrem em sistemas e *sites* com os mais diversos objetivos (Barbosa *et al.*, 2021, p. 7). Ataques cibernéticos vão de tentativas a concretização do objetivo de roubar, danificar, modificar ou destruir informações, esses ataques podem deixar o acesso à informação indisponível, ou quebrar sua confidencialidade e sua integridade.

Levando em conta o anonimato *hackers* ou *crackers* precisam conhecer o sistema no qual eles pretendem invadir, sendo experts no assunto, praticam seus delitos pela *internet* (Wanderley *et al.*, 2022, p, 172). Dessa forma, pode-se dizer que a primeira coisa que um invasor normalmente faz é estudar o seu alvo, isto é feito através de um *scan* de portas, engenharia social ou *phishing*. Com o *scan* das portas o atacante pode descobrir quais são as portas que estão abertas, quais são os sistemas e serviços que estão instalados naquele servidor e com a engenharia social e o *phishing*, ele pode conseguir dados de usuários daquela rede, até mesmo credenciais de acesso.

A partir do estudo de seu alvo, o atacante usa as informações que adquiriu a fim de encontrar vulnerabilidades para invadir o sistema. Quando um *hacker* mal-intencionado consegue invadir o sistema seu próximo passo é conseguir mais acesso, privilégios de *super user*, também chamado de acesso *root*, ou acesso a administradores de bancos de dados, ou acesso de administradores de redes, uma vez que consiga, o estrago causado é alto. Com este acesso privilegiado o atacante pode excluir ou alterar informações do banco de dados, vazá-las ou sequestrá-las, por exemplo. Há também a possibilidade de escalar o ataque, efetuar diversos ataques em cadeia sendo que o objetivo de um ataque é conseguir acesso ou preparar o ambiente para o próximo.

2.3. Caso Polícia Federal e Polícia Rodoviária Federal

Souza (2021) informou que no dia 10 de dezembro de 2021 foram derrubados os sistemas da Polícia Federal e da Polícia Rodoviária Federal. O ataque ocorreu no mesmo dia em que outros sistemas foram invadidos, são eles, Ministério da Saúde, o *site* da escola virtual, *sites* da Agência Nacional de Transportes Terrestres (ANTT) e outros ligados ao ministério da economia. A suspeita seria que um ou mais servidores com acesso privilegiado aos sistemas invadidos teriam contribuído para o ataque. O ataque poderia ser classificado como do tipo *ransomware*, um tipo de ataque que sequestra os dados e posteriormente é feito um pedido de resgate, mas nesse caso não houve um pedido de resgate.

Segundo Souza (2021), além do tempo de indisponibilidade, foram apagados dados de agentes com dívida ativa com a União, e possivelmente de condutores cadastrados nos bancos de dados das corporações. No dia 21 de dezembro de 2021, 11 dias após o ataque, foi restabelecido o Sistema Eletrônico de Informações (SEI), o sistema é utilizando pela Polícia Federal (PF) e pela Polícia Rodoviária Federal (PRF), como ferramenta de gestão dos processos eletrônicos. Com esse sistema indisponível, o trabalho de policiais em todo o país foi prejudicado, principalmente os que atuam na área investigativa e com levantamento de informações. O ataque contra a PRF levou a perda maior, em que quase 100 mil documentos que estavam no sistema eletrônico foram excluídos (Souza, 2021).

2.4. Caso Ministério da Saúde

Ainda em 10 de dezembro de 2022, ocorreu um ataque ao sistema do Ministério da Saúde (MS), no *site* havia uma mensagem dizendo que haviam sido copiados e excluídos 50 terabytes de dados do sistema. Também ficou indisponível o sistema do conecteSUS, que

provia a verificação da autenticidade do certificado de vacinação contra o novo vírus da *covid* (Folha de São Paulo, 2021).

O Ministério da Saúde confirmou que quem atacou os sistemas da pasta conseguiu acesso usando credenciais do banco de dados, com isso os atacantes conseguiram entrar no sistema e excluir dados sobre vacinas e registros de casos de óbitos relacionados a pandemia (Daros; Naìsa, 2022). O ataque feito seria classificado como do tipo *ransomware*, mas, ao que parece na verdade foi um sequestro de *Domain Name System* (DNS) que redirecionava o tráfico para um outro *site*, onde esse *site* apontava as coisas como se fosse um ataque de *ransomware* (Brito, 2021).

Dos danos causados por esse ataque, doses de vacinas aplicadas contra a *covid*-19, assim como o comprovante de vacinação dos usuários não constavam no sistema do conecteSUS. As divergências ocorrem em dados de pelo menos três estados, sendo mais de 1,5 milhão de doses que não constam no aplicativo em divergências de usuários do Distrito Federal e de São Paulo, o estado de Santa Catarina também possui a diferença de doses, mas, não foi quantificado (Folha de São Paulo, 2021).

A Rede Nacional de Dados em Saúde (RNDS) reúne as informações registradas por estados e municípios, de vacinação, ficou sem suas informações, o que resultou em problemas para instituições que fazem o monitoramento da pandemia da *covid*. Uma das afetadas foi a Fundação Oswaldo Cruz (Fiocruz), passando não divulgar novos boletins do InfoGripe, por certo período, responsável por avaliar o cenário dos casos de Síndrome Respiratória Aguda Grave (SRAG), entre elas, a da *covid* e da *influenza*. Também haviam desaparecido os dados do Sivep-Gripe, um sistema onde os municípios reportavam casos da gripe *influenza* e da *covid*. O Ministério da Saúde informou que o restabelecimento dos serviços estava previsto para o dia 14 de janeiro (Folha de São Paulo, 2021).

2.5. Como Funciona Um Ataque de Ransomware

Um ataque de *ransomware* é um sequestro, entretanto, ao invés de um indivíduo, os atacantes sequestram os dados da vítima. Os dados sequestrados na verdade são criptografados utilizando uma chave de criptografia privada e a criptografia não é revertida até que se pague um resgate (Richardson; North, 2017). A vítima vai de uma empresa pública, uma empresa privada ou até mesmo os dados de uma pessoa física.

Ficando impossibilitado de visualizar o conteúdo dos arquivos, ainda que normalmente tenha-se acesso ao local onde os dados estão armazenados, a vítima fica incapacitada de

realizar procedimentos do funcionamento da empresa. Além dos atacantes cobrarem pelo resgate, também se aproveitam da fragilidade dos dados confidenciais e ameaçam a divulgação. Em 2021 o Brasil ficou em quarto lugar no ranking de países que mais sofreram ataques de *ransomware* (Sonicwall, 2022).

2.6. Como Funciona um Sequestro de DNS

O DNS funciona como um tradutor de termos para acesso, um deles sendo a *Uniform Resource Locator* (URL), e.g. endereco.dominio.br. Ele associa essa informação para endereços *Internet Protocol* (IP) (Satam et al., 2015, p. 85), possibilitando-se acessar os mais diversos *sites*, sem necessariamente saber o endereço IP deles. Também é possível apontar um nome específico para um endereço IP de um servidor interno.

Quando um sequestro de DNS ocorre, também conhecido como DNS *hijacking* e DNS *spoofing*, o atacante sequestra o DNS da vítima e passa a redirecionar as solicitações de tradução do DNS da vítima, assim, o atacante passa a resolver todas, ou algumas em específicos para um endereço em seu domínio (Carvalho; Pelli, 2017, p. 100). Esse tipo de ataque tem como objeto fraudar *sites*, causar indisponibilidade de sistemas e serviços, ou até mesmo simular outros tipos de ataques, como o *ransomware*. e.g. um sequestro de DNS ocorre, o atacante passa a direcionar as solicitações do DNS para um servidor onde é simulado um ataque de *ransomware*, todavia, esse servidor pertence aos atacantes e os dados são todos simulados. O servidor real da vítima permanece intacto, apenas não sendo possível o acesso pela tradução incorreta do DNS.

3. METODOLOGIA

Por meio de pesquisas de casos de ataques cibernéticos que ocorreram durante o período da pandemia (2020 e 2021), e que envolvam sistemas governamentais brasileiros foi feita uma análise de como esses ataques se concretizaram, quais os fatores que contribuíram para realização desses ataques cibernéticos, as vulnerabilidades que podem ter sido exploradas, riscos e ameaças que o ataque ocasionou, se seria possível escalar e causar mais danos aos sistemas e quais medidas podem ser tomadas para prevenir que tal tipo de ataque seja executado.

4. RESULTADOS E DISCUSSÕES

Constata-se que, os atacantes se aproveitam das situações e das oportunidades, tendo isso em mente, as empresas e órgãos do governo devem ficar atentos a esses fenômenos a fim de se prevenir contra es ses criminosos. Estes não executam os ataques espontaneamente, têm todo o processo de estudar as suas vítimas e adquirir informações necessárias antes de pôr seu conhecimento em prática, eles se aproveitam das vulnerabilidades que encontram e conseguem causar muitos prejuízos as suas vítimas. Para manter um ambiente seguro é necessário habilitar apenas aquilo que é utilizado, portas abertas inutilizadas e serviços inutilizados podem servir como superfície para os atacantes colocarem suas mãos em informações importantes que podem comprometer todo o resto. Manter um *firewall* bem configurado e monitorar tentativas de acesso também podem ajudar a prevenir contra vários tipos de ataques.

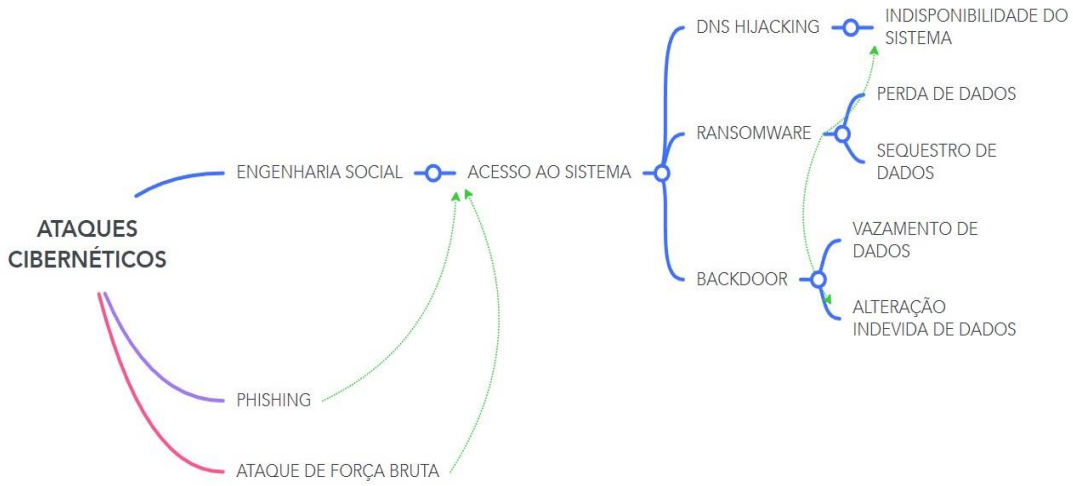
Um fator crucial que fez com que os ataques aumentassem durante o período de trabalho remoto é que as vítimas não conhecem as boas práticas de segurança, não foram treinadas para lidar com essa situação, colocando-os e os atacantes como ameaças. Manter uma política de segurança atualizada, com regras para controle de acesso, e treinamento para os usuários, são itens essenciais que devem ser levados em consideração antes de conceder o acesso. Funcionários precisam ser orientados sobre quais tipos de ataques vem aumentando, e devem ser capacitados para poder cumprir seu papel sem colocar a organização em risco. São boas práticas não baixar nada de *sites* desconhecidos, abrir *e-mail* de origem desconhecida, e não confiar suas credenciais a ninguém.

Profissionais com conhecimento técnico dentro da empresa, seja ela pública ou privada, podem criar documentos, seções dentro da política de segurança, ou dar palestras para os funcionários a respeito disso. Empresas, principalmente órgãos governamentais, precisam estar preparados para lidar com ataques de indisponibilidade, em especial o *ransomware*, uma vez que informações podem ser perdidas e dados podem ser vazados. *Softwares* e sistemas devem ser atualizados periodicamente, já que versões antigas não possuem as últimas correções de *bugs* e vulnerabilidades, o que serve como superfície para *hackers* mal-intencionados. Agir em conformidade com normas de órgãos reconhecidos como a *International Organization for Standardization* (ISO), que disponibiliza a ISO 27002 abordando sobre as boas práticas de segurança da informação, a ISO 27005 que trata a gestão de risco na segurança da informação, são outros pontos chave que vão ajudar na prevenção.

Órgãos governamentais tem posse de muitas informações sigilosas e pessoais, de todos os cidadãos, essas informações precisam estar protegidas contra quebra de integridade e confidencialidade. Caso informações como número de vacinados, controle de doenças, multas, procurados pela polícia, resultados e evidencias de crimes fossem excluídos ou alterados, sem um *backup* dessas informações, criminosos poderiam sair impunes, ter pena reduzida, pessoas inocentes poderiam acabar sendo acusadas de crimes que não cometeram, dinheiro poderia ser mal investido entre outros fatores negativos a sociedade. Uma vez que a informação foi alterada, há a possibilidade de fazer uma verba onde naturalmente iria à prevenção de uma doença fosse direcionada para outro setor, por exemplo, por isso a segurança da informação nesses órgãos precisa ser de ponta.

A figura 1 a seguir apresenta um mapa mental que ilustra as etapas para alguns dos ataques cibernéticos comentados no presente artigo, dividindo-os de acordo com suas características e métodos.

Figura 1 – Mapa Mental de Ataque Cibernético.



Fonte: Autores

A engenharia social é uma técnica quais os atacantes manipulam usuários para obter informações e/ou acesso a sistemas, explorando a confiança e/ou descuido humano, utilizando-se de técnicas psicológicas. O *phishing* envolve o envio de mensagens fraudulentas, normalmente e-mails que parecem ser de fontes confiáveis para enganar as vítimas e induzi-las a fornecer informações. O ataque de força bruta é uma técnica que atacantes utilizam para adivinhar as credenciais de acesso por meio de tentativa e erro.

Independente do método utilizado o objeto é obter acesso ao sistema, uma vez com acesso ao sistema o atacante irá escalar o ataque, executando outros ataques na sequência,

tendo em vista o sistema já comprometido. A partir daí o atacante pode optar por passos mais silenciosos dando sequência com um ataque do tipo *backdoor*, vazando e alterando dados de forma quase imperceptível, podendo a vítima demorar a descobrir que foi lesada. Optando por algo mais estrondoso como o *ransomware*, rapidamente a vítima descobre que foi lesada, nesse caso, além dos dados serem alterados e correr risco de vazamento, pode haver também a perda total dos dados, além da indisponibilidade do sistema pelo fato dos dados estarem criptografados.

5. CONSIDERAÇÕES ADICIONAIS

Ataques cibernéticos representam um risco sério para qualquer organização, em principais organizações governamentais. Cada tipo de ataque possui métodos e objetivos específicos, a defesa contra esses ataques exige um conjunto de boas práticas, políticas de segurança rigorosas e conscientização dos usuários sobre técnicas de engenharia social e *phishing*.

Diante do cenário exposto, pode-se dizer que nem todo incidente de segurança representa um ataque-cibernético, o erro humano pode ocorrer e informações podem ser perdidas ou alteradas no processo, e ambientes podem ficar indisponíveis. Devemos lembrar também que muitos equipamentos precisam ser distribuídos para funcionários poderem trabalhar remotamente, e questões burocráticas podem atrasar a chegada de equipamentos essenciais. Outros órgãos governamentais foram afetados durante a pandemia, nos anos de 2020 e 2021, quais não foram detalhados no presente artigo.

Referências

BARBOSA, Juliana Souza; SILVA, Danihanne Borges; OLIVEIRA, Daniela Cabral de; JESUS, Dilça Cabral de; MIRANDA, Wesley Flávio de. **A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional.** *Research, Society and Development*, v. 10, n. 10, p. e383101018557, 2021. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/12557. Acesso em: 15 ago. 2022.

BORGES, Beatriz e BITAR, Renata. ***Governo de SP lança Poupatempo digital para emissão online de documentos e seguro-desemprego*** (2020) Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/05/06/governo-de-sp-lanca-poupatempodigital-para-emissao-online-de-documentos-e-seguro-desemprego.ghtml Acesso em 31 de agosto, 2022.

BRITO, P. **Ataque sequestra DNS e congela serviços do Ministério da Saúde** (2021) Disponível em: https://www.cisoadvisor.com.br/ataque-sequestra-dns-e-congela-servicos-doministerio-da-saude/ Acesso em 27 de agosto, 2022.

CARDOSO, Nágila Magalhães. **A Pandemia do Cibercrime**. Revista Eletrônica Direito & TI, v. 1, n. 12, p. 8, (2020)

CARVALHO, H. e PELLI, E. ***Técnicas de reconhecimento de padrões para identificação de ataque de DNS.*** Revista Brasileira de Computação Aplicada, v. 9, n. 2, p. 99-110 (2017)

DAROS, Gabriel e NAÍSA, Letícia. **Hackers acessaram nuvem do Ministério da Saúde com senha; entenda o ataque.** (2022) Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/01/14/hackers-do-ministerio-da-saudeacessaram-sistema-com-senha-diz-secretario.htm Acesso em 5 de agosto, 2022.

FOLHA DE SÃO PAULO. **Ataque hacker tira do ar sites do Ministério da Saúde e do Conecte SUS** (2021) Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/12/sites-do-ministerio-da-saude-e-doconecte-sus-saem-do-ar-apos-suposto-ataque-hacker.shtml Acesso em 27 de abril, 2022.

FORTINET. **Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021** (2022) Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021 Acesso em 20 de agosto, 2022.

GOVERNO FEDERAL. *Total de empresas controladas direta e indiretamente pela União em 2019 foi de 206 estatais, 7 a menos que em 2018* (2020)

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 15 ago. 2018, Seção 1, p. 1.

MARTELLO, Alexandro. **Receita Federal lança 'CPF Digital', aplicativo que permite ter o documento no celular** (2020). Disponível em: https://g1.globo.com/economia/noticia/2020/05/14/receita-federal-lanca-cpf-digitalaplicativo-que-permite-ter-o-documento-no-celular.ghtml Acesso em 31 de agosto, 2022.

MORAIS, Cézar Henrique Junio Pontes de. **Ransomware: segurança da informação e prevenção.** (2021) Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1619 Acesso em 24 de agosto, 2022.

PREFEITURA DE UBERLÂNDIA. **Prefeitura abre cadastro da vacina contra Covid-19 para pessoas com deficiência permanente** (2021). Disponível em: https://www.uberlandia.mg.gov.br/2021/05/26/prefeitura-abre-cadastro-da-vacina-contracovid-19-para-pessoas-com-deficiencia-permanente Acesso em 31 de agosto, 2022.

RICHARDSON, Ronny e NORTH, Max M., **Ransomware: Evolution, Mitigation and Prevention** (2017). Faculty Publications. 4276. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276 Acesso em 5 de agosto, 2022.

SATAM, Patrik et al. ***Anomaly Behavior Analysis of DNS Protocol***. (2015)

SILVA, D. **Análise de métodos de detecção de ataques de Ransomware em dispositivos IOT em redes TCP/IP** (2020) Disponível em: https://repositorio.ifpe.edu.br/xmlui/handle/123456789/630 Acesso em 24 de agosto, 2022.

SONICWALL. Relatório De Ameaças Cibernéticas Da Sonicwall 2022. 2022. Disponível em: https://www.sonicwall.com/pt-br/2022-cyber-threat-report. Acesso em: 20 ago. 2022.

SOUZA, Renato. **Hackers apagaram quase 100 mil documentos do sistema da PRF.** (2021). Disponível em: https://noticias.r7.com/brasilia/hackers-apagaram-quase-100-mildocumentos-do-sistema-da-prf-21122021 Acesso em 5 de agosto, 2022.

WANDERLEY, Carlos Alberto Cardoso, et al. ***Crimes cibernéticos em tempos de pandemia: O isolamento social como propulsor da vulnerabilidade da população e do aumento dos casos***. (2022)