ZOOMBOMBING: Vulnerabilidades na plataforma Zoom Meetings
ZOOMBOMBING: Vulnerabilities in the Zoom Meetings platform

THIAGO MIRANDA DE PAULA*
TIAGO BITTENCOURT NAZARÉ**

RESUMO

Desde o final de 2019, o mundo vive uma situação atípica. Por motivo do distanciamento social causado pela pandemia de COVID-19, muitas empresas foram levadas a implantar o regime *home office* ou aderir um revezamento de seus funcionários entre casa e empresa. Com isso, aplicativos de colaboração e reuniões online começaram a conquistar o público, que necessitavam estar trabalhando juntos, mas separados. Logo, as pessoas estão correndo um risco diferente da exposição ao novo agente do coronavírus, que é a exposição à vulnerabilidades presentes nas aplicações e ataques de cibercriminosos na rede durante esse período, que são facilmente exploradas através da utilização de *softwares* de videoconferências, de ambientes remotos e conexões V*PN's* (*Virtual Private Network*) por exemplo. Com isso, este trabalho busca expor as vulnerabilidades de uma dessas ferramentas que estão sendo atualmente bastante utilizadas: o *Zoom Meetings*. Nela são encontradas vulnerabilidades que se tornam preocupantes principalmente pelo início da vigência da Lei Geral de Proteção de Dados. Como consequência, um fenômeno denominado *Zoombombing*, começou a ocorrer frequentemente entre os usuários da plataforma, onde reuniões são invadidas por motivos de brincadeiras ou utilizando das falhas da aplicação para difundir discursos de ódio e assédio. Visto isso, as várias vulnerabilidades presentes na lista de Vulnerabilidades e Exposições Comuns (CVE) foram apresentadas, além de citados alguns cuidados para contornar essas falhas de segurança e trabalhar de forma mais segura.

Palavras-chave: Zoom, Home Office, Vulnerabilidade.

ABSTRACT

Since the end of 2019, the world has been experiencing an atypical situation. Due to the social distance caused by the COVID-19 pandemic, many companies were led to implement the home office or to join a rotation of their employees between home and company. As a result, collaboration apps and online meetings began to win over audiences, who needed to be working together, but separately. Therefore, people are taking a different risk of exposure to the new coronavirus agent, which is exposure to vulnerabilities present in applications and cybercriminal attacks on the network during this period, which are easily exploited through the use of videoconferencing software, from remote environments. and VPN connections for example. With this, this article seeks to expose the vulnerabilities of one of these tools that are currently being used a lot: Zoom Meetings. It contains vulnerabilities that become of concern mainly due to the beginning of the LGPD. As a consequence, a phenomenon called Zoombobing, began to occur frequently among users of the platform, where meetings are invaded for reasons of play or using the application's flaws to spread hate and harassment speeches. In view of this, the various vulnerabilities present in the list of Common

Vulnerabilities and Exposures (CVE) were presented, in addition to mentioning some precautions to circumvent these security flaws and work more safely.

Keywords: Zoom, Home Office, Vulnerability.

_____

* Rede de Ensino Doctum – Unidade Cataguases – thiagomirandadepaula@gmail.com – Graduando em Sistemas de Informação.

** Professor da Rede Doctum - Unidade Cataguases – prof.tiago.nazare@doctum.edu.br – Mestre em Gestão de Sistemas de Engenharia

1. Introdução

As pessoas vivem uma situação atípica desde o final de 2019, devido ao novo agente do coronavírus, doença provocada pelo *SARS-CoV-2* que ficou conhecida como *COVID-19* e, rapidamente, tornou-se um problema de saúde pública mundial, fazendo com que milhões de pessoas ficassem em isolamento social. Com isso, as empresas e instituições de ensino do país e do mundo foram levadas a se reinventar para funcionar com o máximo de qualidade possível para não perder o ritmo de seus serviços.

Assim, as empresas começaram a implantar o regime *home office* em todo mundo em razão das medidas de distanciamento social para seus colaboradores, e as instituições de ensino, a aderirem a educação à distância, evitando ao máximo a exposição de seus professores e alunos à doença. Assim, fez-se necessária a adoção de ferramentas e metodologias com o propósito de reunir as pessoas de forma *online* com o máximo de engajamento e resultado, para que profissionais e alunos não tivessem esse período prejudicado pela pandemia.

Devido a esta situação, uma solução foi a utilização de ferramentas que possibilitassem a realização de reuniões/aulas *online*. Assim aplicativos de videoconferências ganharam ou reconquistaram sua popularidade na quarentena.

Um desses aplicativos foi o *Zoom Meetings*, chegando a 300 milhões de participantes diários em sua plataforma.

Esse sistema se tornou fundamental por suas funcionalidades já existentes, assim, grandes corporações começaram a utilizar em seu dia a dia dentro da instituição. Visto a alta utilização e *feedbacks* dos clientes, a maioria dos aplicativos

de teleconferências começaram a se atualizar de acordo com a necessidade de seu público-alvo, tornando-se ainda mais funcionais.

Porém com a utilização dessas ferramentas para contornar o isolamento, as pessoas estão correndo um risco diferente da exposição ao *COVID-19*, que é a exposição a vulnerabilidades presentes nas aplicações e ataques cibercriminosos na rede, que são facilmente exploradas através da utilização de *softwares* de videoconferências, de ambientes remotos e conexões VPN's por exemplo.

Um desses aplicativos de videoconferências é o *Zoom Meetings*, que possui funcionalidades gratuitas e pagas para seus usuários usufruírem de acordo com seu propósito e teve um crescimento de 10 milhões para 300 milhões de participantes diários em abril de 2020 chamando a atenção de novos usuários e de cibercriminosos.

O presente trabalho se justifica pelo crescimento da utilização da ferramenta no momento atual, onde a maioria das pessoas foram forçadas a permanecer em casa e a maioria das empresas e instituições não estavam prontas para o novo cenário, foi onde começaram a aparecer comprometimentos de informações sigilosas de diversas pessoas e empresas, teleconferências sendo invadidas para distribuição de *malwares* e vazamentos de dados de mais de 500 mil usuários, podendo comprometer as empresas à penalização da nova Lei Geral de Proteção de Dados (LGPD) que entrou em vigor no dia 18 de setembro de 2020.

O objetivo geral desse artigo, é expor vulnerabilidades presentes na plataforma *Zoom Meetings,* que conta com falhas onde sua grande maioria, só foram descobertas após a alta de sua utilização no período pandêmico e devido ao seu funcionamento simplificado que expõe os usuários, como falhas de programação e deficiências na criptografia que protege a comunicação entre os usuários.

Dentre os objetivos específicos estão a exposição de vulnerabilidades do *Zoom Meetings* com base nas Vulnerabilidades e Exposições Comuns (CVE), exposição de acontecimentos envolvendo a plataforma e quais, caso lançadas, as correções da plataforma para contorna-las e, pois, com maior uso de tecnologia, tem-se também maior risco de enfrentar ameaças cibernéticas.

1. Zoom Meetings: pandemia, vulnerabilidades e cuidados

1.1. Pandemia COVID-19

A Universidade Federal de Santa Maria (2020), descreve a *COVID-19* (termo em inglês que significa *Corona Virus Disease* 2019) como uma doença causada pelo novo agente do coronavírus, denominado *SARS-CoV-2*, que apresenta um espectro clínico variando de infecções assintomáticas a quadros graves. De acordo com a Organização Mundial de Saúde (OMS), a maioria (cerca de 80%) dos pacientes com *COVID-19* podem ser assintomáticos ou oligossintomáticos (poucos sintomas), e aproximadamente 20% dos casos detectados vão requerer atendimento hospitalar por apresentarem dificuldade respiratória, dos quais aproximadamente 5% podem necessitar de suporte ventilatório.

A doença se disseminou a partir do final do ano de 2019, com primeiros casos registrados na China com inicialmente 800 pessoas infectadas e 259 mortes, mas houve casos também no Japão, Tailândia, Coreia do Sul, França e Estados Unidos, todos associados a pessoas que haviam viajado para a China no período. Espalhando-se rapidamente, atingiu todos os continentes nos primeiros meses de 2020. No dia 11 de março, a *COVID-19* foi caracterizada como uma pandemia pela OMS.

Dessa forma, os países tiveram de suspender todas as atividades não essenciais, alguns líderes aderiram a *lockdowns* para evitar maior contágio da doença, e nesse período, foram colocadas em prática diversas restrições de viagens, proibição de eventos, circulação de carros e meios de transportes, e houve ordem de fechamento temporário de serviços como fábricas, empresas, escolas, bares e academias. Apenas hospitais, mercados, farmácias e outros serviços vitais, como de segurança pública, permaneceriam abertos adotando todas as medidas de segurança para a não propagação da doença.

Esse isolamento social se arrastou durante todo ano, com várias medidas de segurança sendo adotadas para que o funcionamento das atividades retornasse, os serviços começaram a ser liberados com inúmeras regras de funcionamento que devem ser seguidas. Assim, os locais trabalham com restrições de horários, regras de distanciamento, agendamento, obrigatoriedade de uso de máscaras e higienização com álcool em gel para funcionários e clientes.

1.2. Sistema de Teleconferências

Considerando-se que o prefixo "tele" significa "a distância", vê-se que qualquer forma de conferência entre duas ou mais pessoas, feitas a distância, independentemente da tecnologia utilizada e dos recursos oferecidos, possa ser categorizada como sendo uma "teleconferência". (VARGAS, 2002)

Essa comunicação é feita em tempo real e existem vários sistemas interpessoais de videoconferência que possibilitam isso. Além da transmissão simultânea de áudio e vídeo, esses sistemas oferecem ainda recursos de cooperação entre os usuários, com *chats*, compartilhamento de informações e de materiais de trabalho ou estudo.

Segundo SANTOS (1998), o uso da videoconferência apresenta uma série de vantagens:

- Economia de tempo, evitando o deslocamento físico para um local especial;
- Economia de recursos, com a redução dos gastos com viagens;
- Mais um recurso de pesquisa, já que a reunião pode ser gravada e disponibilizada posteriormente;

Além destes aspectos, os *softwares* que apoiam a realização da videoconferência, em sua maioria, permitem também, através da utilização de ferramentas de compartilhamento de documentos:

- Visualização e alteração pelos integrantes do diálogo em tempo real;
- Compartilhamento de aplicações;
- *Chats* durante a videoconferência;
- Compartilhamento de informações (transferência de arquivos);

Deslocar toda a equipe já não faz mais tanto sentido para a maioria dos negócios e as videoconferências são uma forma prática e simples de conectar-se, mesmo à distância, com as pessoas que trabalham numa equipe. Entretanto, se as reuniões não forem planejadas e conduzidas da melhor forma, elas podem representar uma grande dor de cabeça.

LAIS SCHULZ (2020), aborda que um dos critérios mais importantes para ter reuniões *online* sem interferências e limitações é, sem dúvidas, saber escolher o aplicativo de videoconferência a ser utilizado. Afinal, sem uma ferramenta de boa qualidade e utilidade, as reuniões podem não ser produtivas.

“A transformação digital tem facilitado cada vez mais a forma de se trabalhar remotamente. Sem barreiras físicas, hoje é possível contratar pessoas e fechar acordos sem nem mesmo um aperto de mão. ” (SCHULZ, 2020)

Com isso, a videoconferência como uma ótima alternativa às interações via *e-mail* ou outros canais de comunicação escrita. Com uma chamada *online* de vídeo, você pode ver como as pessoas do outro lado se expressam e entender exatamente o que elas querem dizer.

1.3. Ferramentas Colaborativas, reuniões e home office

Segundo ROMULO MARTINS (2015), em um mundo conectado, empresas que conseguem superar as limitações geográficas e temporais certamente se mostrarão mais competitivas do que as suas concorrentes. “O termo colaborativo tem se mostrado cada vez mais presente nas discussões, tendências e no *mindset* global, seja por meio da economia, da educação ou do trabalho. ” (MARTINS, 2015).

Uma ferramenta, *software* ou aplicativo colaborativo tem como principal finalidade, possibilitar o compartilhamento de arquivos de trabalho entre duas – ou mais – pessoas que desenvolvem uma tarefa em comum, dessa forma, SKIP ELLIS havia definido *software* colaborativo como algo que se trata de um sistema baseado em computador, que busca auxiliar um grupo de pessoas envolvidas em tarefas ou objetivos comuns, e que provê interface para um ambiente compartilhado.

Além de permitir que você possa se conectar de forma mais pessoal com colegas que não estão no mesmo lugar que você, interagir com essas pessoas e ter uma facilidade no compartilhamento de arquivos em que toda a equipe precisa editar e/ou revisar, essas ferramentas também trazem alguns outros benefícios, como por exemplo:

- **Alinhamento de expectativas**: Alinhando e trabalhando as metas com sua equipe de forma que todos presentes na reunião possam tirar dúvidas e saber exatamente o ponto no qual precisam chegar e o que é necessário ser feito.

- **Flexibilidade**: Os colaboradores ou alunos tem a oportunidade de estar presencialmente no local de trabalho ou estudo, ou de estarem em qualquer lugar do mundo, desde que com acesso à *Internet* para se manter *online* e acompanhar as atividades requisitadas.

- **Produtividade**: Encontros *online* ajudam os participantes a economizar um tempo que gastariam com deslocamento e/ou outras atividades desnecessárias envolvidas nas reuniões presenciais;

- **Redução de custos**: Custos de deslocamento são gerados em encontros presenciais, que muitas vezes nem mesmo são necessários, onde poderiam facilmente ser resolvidos de forma remota.

Conforme TATIANA VAZ (2017), existem três tipos arranjos para se trabalhar no tão falado *home office*, são eles:

- **Teletrabalho**: sendo funcionário de uma empresa
- ***Freelancer***: trabalhando em projetos avulsos de onde quiser.
- **Empresário de uma empresa *home based*:** onde se é empresário de uma empresa que tem sede em uma residência.

MARINA BRIK (2013) expõe que com a expansão das redes de comunicação e a popularização dos dispositivos portáteis como *laptops*, *smartphones* e *tablets*, este tipo de trabalho atravessou fronteiras e ganhou o mundo, permitindo que atividades sejam realizadas de qualquer lugar que possua *Internet* disponível.

1.4. Princípios da Segurança da Informação

Com base na ISO 27001(2005), a Segurança da Informação é um conjunto de medidas e procedimentos aplicados para proteger e preservar a Informação,

garantindo seus princípios básicos: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Abaixo destacamos o que garante cada um dos princípios da Segurança da Informação:

Confidencialidade: Garantia que somente pessoas com permissões corretas acessem determinadas informações.

Integridade: Garantia da integridade da informação, que deve ser mantida integra e inalterada.

Disponibilidade: A informação deve estar sempre disponível para acesso dos usuários que têm permissão.

Autenticidade: Garantia da informação ser enviada por fontes legitimas e seguras. Sem alterações ou interceptações ocasionadas por ataques.

Legalidade: Garantia de a informação estar de acordo com a legislação do país.

Esses princípios podem ser comprometidos com possíveis ameaças que são classificadas em Ameaças Físicas e Ameaças Lógicas.

“Ameaças Físicas incluem todo e qualquer processo de natureza física que comprometa os princípios da segurança da informação” (MORENO, 2019). São exemplos desse tipo de ameaça tragédias climáticas como alagamentos, raios, tempestades, desabamentos, etc.

“Ameaças Lógicas incluem todo e qualquer processo de natureza lógica que comprometa os princípios da segurança da informação” (MORENO, 2019). Nesse caso estamos tratando de vírus, ataques de força bruta, sequestro de dados, escuta de dados, etc.

1.5. Vulnerabilidades

O aumento no desenvolvimento de novas tecnologias vem sendo acompanhadas por um grande número de sistemas sendo atacados, visto isso para

que a maioria destes ataques possam ser bem-sucedidos é necessária a existência de alguma vulnerabilidade.

Segundo YURI DIÓGENES e DANIEL MAUSER (2013), diversas vulnerabilidades são encontradas e exploradas sem o consentimento do fabricante da existência da vulnerabilidade. Esse período entre a descoberta da vulnerabilidade e a disponibilidade da correção é o que diferencia uma vulnerabilidade comum de uma vulnerabilidade “Dia Zero”.

A expressão Vulnerabilidade *zero day* é um termo que indica o período da descoberta da vulnerabilidade e flexibilidade da reparação, podendo se apresentar de duas maneiras: a partir de severas falhas de segurança descobertas ou então através de ataques onde são exploradas a existência dessas falhas por grupos de *hackers*.

O termo Vulnerabilidade *zero day* não só indica situações como citadas, mas também a quanto tempo em que o desenvolvedor conhece a falha, como diz o próprio nome, zero dias.

As etapas que uma vulnerabilidade *Zero Day* percorre são as seguintes:

- O estudo de um sistema ou aplicação e a descoberta de uma falha;
- A criação do *Exploit* através de alguma linguagem de programação para explorar a falha e se aproveitar do Sistema de alguma forma, seja ele para fins monetários ou acesso à informação privilegiada;

Exploits são pedaços de *software*, dados ou sequências de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade, com objetivo de causar um comportamento acidental ou imprevisto a ocorrer no *software* ou *hardware* de um computador ou em algum eletrônico.

Segundo GEORGIA WEIDMAN (2014), Antes de começarem a ser lançados *Exploits,* é preciso fazer um pouco mais de pesquisa e de análise. Quando uma vulnerabilidade é identificada, é procurado de forma ativa, problemas que levarão a um comprometimento na fase de exploração de falhas.

A partir desse momento, a pessoa que programou o *Exploit* para se aproveitar da vulnerabilidade do sistema define se ele será público ou privado. Se for público, rapidamente a fabricante terá ciência da vulnerabilidade para lançar atualizações para o sistema, porém, se for mantido como privado, dificilmente a fabricante terá ciência da forma que a exploração está sendo feita. Sendo assim, se o *Exploit* for público, a fabricante lançará uma atualização com as correções, caso contrário a falha continuará no anonimato até que alguém descubra.

Apesar de parecer sem solução, uma Vulnerabilidade *Zero Day* pode ser prevenida através de um Intrusion Prevention System (IPS) podendo adicionar uma assinatura com as características do ataque. Além disso, o IPS funciona de uma forma inteligente e imediata ao bloquear a rede caso tenha alguma tentativa de invasão, evitando que o atacante consiga chegar no seu alvo.

De acordo com a ISO 27000, a portaria de Sistemas de Gestão de Segurança da Informação, as vulnerabilidades são “fraquezas de um ativo que poderia ser potencialmente explorado por uma ou mais ameaças”. Assim, é visto que existem vários tipos de vulnerabilidades que podem ser aproveitadas por um atacante, são elas:

Format String: onde um atacante consegue controlar a maneira que o programa é executado através de funções da família *printf*() e *syslog*();

Symbolic Link: que é um *link* que aponta para outro arquivo e atua como o arquivo apontado, a exploração, geralmente, ocorre em programas que não checam se o arquivo que devem abrir é ou não um *link*;

Injections: que acontecem, na maioria das vezes, devido a não validação de dados de entrada passados ao programa;

Race Condition: ocorre se um recurso que será utilizado por outro processo for intencionalmente modificado, sendo comum esse tipo de vulnerabilidade ser explorada em arquivos temporários;

Buffer Overflow: ocorre quando mais dados do que o suportado tentam ser armazenados, sendo atualmente a vulnerabilidade mais explorada em um *software*;

***Stack Smash*:** Objetiva modificar o endereço de retorno, faz com que este aponte para um código executável que deve ser inserido pelo atacante;

Outro ataque que pode ser facilmente aplicado é o ***Brute Force***, traduzido literalmente para “força bruta”, é um tipo de ataque onde força-se a entrada em algum sistema, site, servidor, aplicativo, etc. A técnica utilizada se dá através de sucessivas tentativas de acertar uma combinação de senha (uma chave), e assim conseguir acesso às informações e dados que deseja. A vulnerabilidade se dá quando não há um número máximo de tentativas para acesso, onde o usuário é bloqueado após determinado número de tentativas, e o padrão da senha não é considerado seguro.

De acordo com os resultados obtidos em uma revisão sistemática das ferramentas e técnicas mais utilizadas hoje para a detecção de vulnerabilidades, os seguintes tópicos podem ser estabelecidos:

- **Caixa-preta**: É uma técnica baseada na descoberta de vulnerabilidades em aplicativos da *web*, testando o aplicativo do ponto de vista do invasor (SREENIVASA & KUMAN, 2012).
- **Caixa branca**: está no lado do servidor. Neste tipo de abordagem, temos acesso a informações relevantes da organização (SREENIVASA & KUMAN, 2012).
- **Análise de código estático (auditoria de código fonte):** é um método em que o programa não precisa ser executado, ele realiza uma análise de código-fonte direto para determinar lacunas de segurança (SREENIVASA & KUMAN, 2012).
- **Análise dinâmica de código**: comunica-se com a aplicação *web* por meio de *front-end* do aplicativo, a fim de identificar vulnerabilidades de segurança potencial e pontos fracos na arquitetura do aplicativo da *web*(SREENIVASA & KUMAN, 2012).
- **Testes de penetração:** Consiste na simulação de um ataque pelo invasores mal-intencionados (que não têm um meio autorizado de acesso sistemas da organização) e usuários internos mal-intencionados (que têm alguns níveis de acesso autorizado). O processo envolve uma análise ativa do sistema procurando por possíveis vulnerabilidades que podem resultar de configuração do sistema pobre ou inadequada, falha de *hardware* ou *software*, conhecido e desconhecido, ou falhas operacionais em andamento ou contramedidas técnicas (THOMPSON, 2005).

- **Testes passivos:** os testes passivos são projetados para análise do tráfego de telecomunicações. Permite detectar falhas e defeitos de segurança examinando pacotes capturados (*livetrafficor* arquivos de *log*) (MAMMAR, AVALLI, & JIMENEZ, 2011).
- **Testes ativos:** Usa um agendador de *threads* atribuídos aleatoriamente para verificar se os avisos comunicados por uma análise programas preditivos são erros reais (XIAO-SONG ZHANG, 2008).
- **Teste *fuzz* (testes caixa preta):** Consiste em estimular o sistema em teste, usando dados aleatórios ou mutados desejados, a fim de detectar comportamentos indesejados, como violação de confidencialidade (XIAO-SONG ZHANG, 2008).

Temos a chamada CVE, ou *Commom Vulnerabilities and Exposures* (Vulnerabilidades e Exposições Comuns), uma iniciativa colaborativa de diversas organizações de tecnologia e segurança que criam listas de nomes padronizados para vulnerabilidades e outras exposições de segurança.

O objetivo é padronizar as vulnerabilidades e riscos conhecidas, facilitando a procura, o acesso e o compartilhamento de dados entre diversos indivíduos e empresas. Mais do que uma lista, a CVE é uma espécie de dicionário gratuito e público, sobre as vulnerabilidades encontradas no mundo virtual. Essa ferramenta é mantida através de representantes de organizações de segurança, instituições acadêmicas, governos e diversos especialistas.

As entradas CVE são usadas em vários produtos e serviços de segurança cibernética, incluindo o *National Vulnerability Database* (NVD). O NVD - banco de dados nacional de vulnerabilidades, é um banco sincronizado com o CVE. Ou seja, a lista CVE alimenta o NVD, que por sua vez, baseia-se nessas informações para aprimorar cada entrada e dá referências de correção, pontuação, classificação de impacto e mais recursos de pesquisa.

É importante saber que cada CVE tem seu formato que inclui três chaves básicas de informação, a sigla CVE, o ano, que representa quando que o *ID* do CVE foi atribuído ou o ano em que a vulnerabilidade se tornou pública e o número da sua sequência de *ID*, resultando em entradas como “CVE-1999-0067”, “CVE-2014-12345”, “CVE-2016-7654321”, entre muitas outras.

O *ID* da CVE, a sua parte numérica, são usados para manter o padrão das vulnerabilidades e fazer ligações com outros repositórios que também utilizam *IDs* de CVE. Nela deve incluir também uma breve descrição da vulnerabilidade ou da exposição para segurança e referências que podem ser importantes para aquela falha. As descrições das entradas são, normalmente, escritas por autoridades de numeração, *Numbering Authorities* (CNAs), pela equipe CVE ou por indivíduos que solicitem um *ID*.

Elas são utilizadas para fornecer os detalhes relevantes que ajudem os usuários a encontrar a vulnerabilidade ou distinguir aquelas semelhantes. As descrições, geralmente e na sua forma ideal, incluem detalhes como o nome do produto e do fornecedor afetado, versões afetadas, tipo de vulnerabilidade, impacto, entre outros.

1.6. Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) é a lei nº 13.709, aprovada em Agosto de 2018 e com vigência a partir de Agosto de 2020, criando um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja confusão, a lei traz logo de cara o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como as sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação.

Algumas definições estabelecidas pela LGPD são:

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal sensível:** 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;

- **Dado anonimizado:** dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

A Lei Geral de Proteção de Dados (LGPD) representa um avanço na segurança de dados pessoais ao definir uma padronização elevada para a proteção das informações relacionadas à pessoa física. A aprovação dessa lei resulta em transformações no âmbito organizacional e na maneira com que as empresas tratam os dados pessoais ao apresentar as diretrizes sobre a conduta correta para tal tratamento, resultando na necessidade de revisão dos processos de administração e segurança das informações.

Para que os dados pessoais possam ser coletados e tratados, é necessário que o titular, a pessoa com direitos sobre eles e sobre a qual os dados se referem, consinta explicitamente a sua utilização. Este consentimento deve ser fornecido apenas após o titular ter sido devidamente informados sobre os termos de uso, as extensões da autorização e a necessidade da aquisição de tais dados. Para essa regra, aplica-se exceções nas situações em que o uso das informações for indispensável para cumprir alguma obrigação legal ou executar políticas públicas previstas em lei.

A lei também fornece ao cidadão o controle sobre os seus dados e uma série de garantias, entre as quais, o direito de requerer a exclusão dos seus dados e de cancelar o consentimento. Assim, a LGPD fornece ao indivíduo o controle sobre suas informações e a capacidade de punir os responsáveis por danos devido ao uso indevido e nocivo dos dados.

Para assegurar o cumprimento da LGPD foi criada a instituição denominada Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar a segurança dos dados pessoais por parte das pessoas jurídicas, podendo solicitar relatórios de privacidade às empresas para verificar se a conduta condiz com o estabelecido pela lei. Além disso, terá como tarefa a regulamentação e orientação preventiva sobre como realizar a aplicação da Lei Geral de Proteção de Dados. A autoridade nacional disponibilizará alertas e orientações às organizações antes de aplicar as penalidades, que serão definidas conforme a gravidade da falha.

Além da ANPD, a lei também conta com os agentes de tratamento de dados, sendo eles: agente controlador, responsável pelas decisões sobre o tratamento; agente operador, que executa o tratamento conforme definido pelo controlador; e agente encarregado, cuja função é a interação com os cidadãos e a autoridade nacional, o qual poderá não existir dependendo do porte organizacional.

Por último, há a administração de riscos e falhas, que representa a necessidade de definir medidas preventivas de segurança, adotar boas certificações do mercado, realizar auditorias, elaborar planos de contingência, e apresentar resoluções ágeis perante incidentes. Dessa forma, no caso de vazamento de dados, a empresa deverá imediatamente informar a ANPD e os titulares afetados.

2. Metodologia

Essa pesquisa foi realizada de modo exploratório, utilizando a ferramenta *Zoom Meetings* como foco para expor as vulnerabilidades da aplicação e abordar alguns dos riscos que estão presentes ao aderir ambientes de colaboração com o mesmo propósito.

Com isso, foram levantados alguns aplicativos de colaboração que estão sendo os mais utilizados nesse período, onde empresas e instituições buscam aderir a *softwares* de colaboração para lidar com o distanciamento social, assim foi realizada a escolha da plataforma do *Zoom Meetings* para foco desta pesquisa, após a escolha da ferramenta, foi realizado o levantamento das vulnerabilidades presentes. Com isso, foram levantadas as CVE's presentes na plataforma para abordagem.

Assim, foi realizado o refinamento das melhores prevenções dessas vulnerabilidades, evitar que sejam alvos de ataques maliciosos e conscientizar os usuários de forma efetiva para menor exposição aos riscos que o *home office* traz neste período de pandemia, onde contamos com uma quantidade alta de pessoas sendo expostas na rede, na qual sua maioria não possuem preparo com essa nova forma de trabalho, e acabam sendo alvos de cibercriminosos a espera de um deslize para aplicar seus conhecimentos de forma mal-intencionada.

Como preocupação, tem-se a nova Lei Geral de Proteção de Dados, onde as empresas serão penalizadas caso dados de seus funcionários ou clientes sejam expostos.

2.1 Objeto de estudo

A *Zoom Video Communications* é uma empresa americana de serviços de conferência remota sediada em San Jose, Califórnia. Ela fornece um serviço de conferência remota "*Zoom Meetings*" que combina videoconferência, reuniões *online*, bate-papo e colaboração móvel.

Assim, essa pesquisa é feita em cima da ferramenta *Zoom Meetings*, sistema de videoconferência baseada em nuvem, que pode ser utilizada para se encontrar virtualmente com outras pessoas, seja por vídeo ou apenas por chamada

de áudio. Além disso ele permite que as sessões sejam gravadas e salvas para serem reproduzidas após o evento.

A plataforma está disponível em *Android* e *IOS*, e é possível acessar via navegador ou instalado no computador. O *Zoom Meetings* oferece a opção de uma conta gratuita, a qual você pode criar facilmente apenas registrando um endereço de *e-mail* e uma senha. Com essa conta você pode realizar chamadas com até 100 participantes, com um limite de 40 minutos por vídeo chamada com mais de 2 pessoas. Passados esses 40 minutos, a chamada é finalizada.

É possível realizar chamadas com até 100 participantes, com um limite de 40 minutos por vídeo chamada com mais de 2 pessoas. Passados esses 40 minutos, a chamada é finalizada. Os usuários contam com acesso a vários recursos interessantes como: compartilhar a tela do seu dispositivo com os demais participantes, comunicar-se por *chat* de bate-papo, usar um quadro branco para fazer anotações, enviar arquivos como fotos ou documentos e gravar a vídeo chamada.

O *Zoom Meetings* disponibiliza três tipos de planos pagos, indicados para empresas de diferentes tamanhos. Cada plano estabelece um valor mensal por anfitrião. Dessa maneira, os planos pagos devem ser escolhidos de acordo ao número de anfitriões que sua empresa deseja ter. São eles: Plano profissional, plano coorporativo e plano empresarial.

3. Resultados e discussões

Objetivo - Dentre os objetivos específicos estão a exposição das vulnerabilidades do *Zoom Meetings* com base nas Vulnerabilidades e Exposições Comuns (CVE), exposição de acontecimentos envolvendo a plataforma e quais, caso lançadas, as correções da plataforma para contorna-las, pois, com maior uso de tecnologia, tem-se também maior risco de enfrentar ameaças cibernéticas.

É fato que a pandemia provocou uma reviravolta nas empresas, para lidar com o distanciamento, cerca de 3 a cada 4 empresas adotaram o trabalho remoto ou o uso de horários flexíveis no período de pandemia.

O fato de a ferramenta *Zoom Meetings* passar a ser tão utilizada hoje para fins profissionais tornou-a um alvo justamente pelos possíveis dados que seus datacenters armazenam sobre seus usuários.

O problema em seu funcionamento é o fato de suas reuniões serem públicas (sem necessidade de nenhuma senha para acesso) por padrão, o que permite a entrada de pessoas aleatórias nas salas. Ao longo do tempo ocorreram casos de racismo, compartilhamento de links maliciosos nos *chats* e até mesmo imagens com conteúdo obsceno.

Tal vulnerabilidade ficou conhecida como "*zoombombing*" e mostra como de fato nem mesmo uma grande plataforma é capaz de conter abordagens maliciosas. Os trabalhadores remotos tornam-se grandes alvos da Engenharia Social no distanciamento de seus escritórios, mas uma empresa com uma cultura de conscientização não deve temer isso.

Com isso, a seguir, estão listadas as Vulnerabilidades e Exposições Comuns da ferramenta:

CVE-2020-9767: Segundo CVE-2020-9767 é uma vulnerabilidade relacionada ao carregamento da Biblioteca de *link* dinâmico (& # 8220; DLL & # 8221;) no Serviço de Compartilhamento de *Zoom* permitiria que um invasor que tivesse acesso local a uma máquina na qual o serviço estivesse em execução com privilégios elevados elevasse seus privilégios de sistema como bem através do uso de uma DLL maliciosa. O *Zoom* tratou desse problema, que se aplica apenas a usuários do Windows, na versão 5.0.4 do cliente.

CVE-2020-6110: Segundo CVE-2020-6110 é uma vulnerabilidade de travessia de caminho parcial explorável na maneira como o *Zoom Client* versão 4.6.10 processa mensagens incluindo trechos de código compartilhados. Uma mensagem de bate-papo especialmente criada pode causar um plantio binário arbitrário que pode ser usado de forma abusiva para obter a execução de código arbitrário. Um invasor precisa enviar uma mensagem especialmente criada a um usuário ou grupo alvo para acionar esta vulnerabilidade. Para o efeito mais severo, é necessária a interação do usuário alvo.

CVE-2020-6109: Segundo CVE-2020-6109 é uma vulnerabilidade de travessia de caminho explorável no cliente *Zoom*, a versão 4.6.10 processa mensagens incluindo *GIFs* animados. Uma mensagem de bate-papo especialmente criada pode causar a gravação de um arquivo arbitrário, que pode ser potencialmente usado para obter a execução de código arbitrário. Um invasor precisa enviar uma mensagem especialmente criada a um usuário ou grupo alvo para explorar esta vulnerabilidade.

CVE-2020-11876: Segundo CVE-2020-11876 * *DISPUTED* * airhost.exe no *Zoom Client for Meetings* 4.6.11 usa 3423423432325249 como o vetor de inicialização (IV) para criptografia AES-256 CBC. NOTA: o fornecedor afirma que este IV é usado apenas em códigos inacessíveis.

CVE-2020-11876: Segundo CVE-2020-11876 * *DISPUTED* * airhost.exe no *Zoom Client for Meetings* 4.6.11 usa o *hash* SHA-256 de 0123425234234fsdfsdr3242 para a inicialização de um contexto OpenSSL EVP AES-256 CBC. NOTA: o fornecedor afirma que está inicialização ocorre apenas em código inacessível.

CVE-2020-11500: Segundo CVE-2020-11500 o *Zoom Client for Meetings* até 4.6.9 usa o modo ECB do AES para criptografia de vídeo e áudio. Em uma reunião, todos os participantes usam uma única chave de 128 *bits*.

CVE-2020-11470: Segundo CVE-2020-11470 o *Zoom Client for Meetings* até 4.6.8 no macOS tem o direito *disable-library-validation*, que permite que um processo local (com os privilégios do usuário) obtenha acesso não solicitado ao microfone e à câmera carregando uma biblioteca criada e, assim, herdando o microfone e a câmera do *Zoom Client* Acesso.

CVE-2020-11469: Segundo CVE-2020-11469 o *Zoom Client for Meetings* até 4.6.8 em cópias do macOS *runwithroot* para um diretório temporário gravável pelo usuário durante a instalação, que permite que um processo local (com os privilégios do usuário) obtenha acesso root substituindo *runwithroot*.

CVE-2020-11443: Segundo CVE-2020-11443 o instalador do *Zoom IT* para *Windows* (*ZoomInstallerFull.msi*) anterior à versão 4.6.10 exclui os arquivos

localizados em% *APPDATA*% \ Zoom antes de instalar uma versão atualizada do cliente. Os usuários padrão podem gravar neste diretório e podem gravar *links* para outros diretórios na máquina. Como o instalador é executado com privilégios de SISTEMA e segue esses *links*, um usuário pode fazer com que o instalador exclua arquivos que, de outra forma, não poderiam ser excluídos pelo usuário.

CVE-2019-18822: Segundo CVE-2019-18822 uma vulnerabilidade de escalonamento de privilégios no *ZOOM Call Recording* 6.3.1 permite que sua conta de usuário (ou seja, a conta sob a qual o programa é executado - por padrão, a conta *callrec*) eleve privilégios de *root* abusando de *callrec-rs @ .service*. O *callrec-rs @ .service* inicia o binário / opt / callrec / bin / rs com privilégios de *root*, e este binário é propriedade de *callrec*. Ele pode ser substituído por um cavalo de Tróia.

CVE-2019-16273: Segundo CVE-2019-16273 dispositivos DTEN D5 e D7 anteriores a 1.3.4 permitem acesso *root shell* não autenticado por meio do *Android Debug Bridge* (adb), levando à execução arbitrária de códigos e à administração do sistema. Além disso, oferece uma capacidade oculta de capturar dados da tela do *Zoom Client* no *Windows*, executando comandos no sistema operacional *Android*.

CVE-2019-13567: Segundo CVE-2019-13567 o cliente *Zoom* anterior a 4.4.53932.0709 no *macOS* permite a execução remota de código, uma vulnerabilidade diferente do CVE-2019-13450. Se o *daemon ZoomOpener* (também conhecido como servidor da *web* oculto) estiver em execução, mas o cliente *Zoom* não estiver instalado ou não puder ser aberto, um invasor pode executar o código remotamente com um URL de inicialização criado com códigos maliciosos. NOTA: O *ZoomOpener* é removido pela ferramenta de remoção de *malware* da *Apple* (MRT) se essa ferramenta estiver ativada e tiver o MRTConfigData de 10/07/2019.

CVE-2019-13450: Segundo CVE-2019-13450 no *Zoom Client* através do 4.4.4 e *RingCentral* 7.0.136380.0312 no *macOS*, os invasores remotos podem forçar um usuário a ingressar em uma chamada de vídeo com a câmera de vídeo ativa. Isso ocorre porque qualquer site da *Web* pode interagir com o servidor da *Web* do *Zoom* na porta *localhost* 19421 ou 19424. NOTA: uma máquina permanece vulnerável se o Cliente *Zoom* foi instalado anteriormente e depois desinstalado. O bloqueio da exploração requer etapas adicionais, como a preferência ZDisableVideo

e / ou eliminação do servidor da *web*, exclusão do diretório ~ / .zoomus e criação de um arquivo simples ~ / .zoomus.

CVE-2018-20401: Segundo CVE-2018-20401 os dispositivos *Zoom* 5352 v5.5.8.6Y permitem que atacantes remotos descubram credenciais por meio de solicitações *Simple Network Management Protocol* (SNMP) iso.3.6.1.4.1.4491.2.4.1.1.6.1.1.0 e iso.3.6.1.4.1.4491.2.4.1.1.6.1.2.0

No final de março, especialistas descobriram que o *Zoom* era vulnerável a uma falha chamada "*UNC path injection*". Essa vulnerabilidade pode ser explorada para o roubo de senhas do *Windows*. Isso ocorre porque o cliente do *Zoom* converte caminhos UNC, abreviação para *Universal Naming Convention* (em português Convenção de Nomenclatura Uniforme), de rede do *Windows* em *hiperlinks* no *chat* da ferramenta, permitindo assim que invasores roubem credenciais de usuários do *Windows* ao clicarem nesse *link*.

Esse tipo de ataque pode ocorrer através de engenharia social, fazendo a vítima clicar nesse *link* para que o *Windows* tente gerar uma conexão remota ao site através do protocolo *Server Message Block* (SMB), que é um protocolo de compartilhamento de arquivos em rede que permite que os aplicativos de um computador leiam e gravem em arquivos e solicitem serviços dos programas do servidor em uma rede de computadores.

Tecnicamente, o cenário de ataque é baseado no *SMBRelay*, programa de computador que pode ser usado para realizar ataques *man-in-the-middle* (MITM) SMB em máquinas *Windows*. MITM em português, homem no meio, é um ataque cibernético em que o invasor retransmite secretamente e possivelmente altera as comunicações entre duas partes que acreditam estar se comunicando diretamente. Sendo assim, o nome de usuário NTLM (conjunto de protocolos de segurança da *Microsoft* que fornece autenticação, integridade e confidencialidade aos usuários) e a senha com *hash* serão automaticamente enviados para o servidor SMB remoto. Após isso, o invasor pode utilizar a ferramenta e responder no Sistema Operacional Kali Linux para capturar as credenciais.

Após a captura, o invasor pode utilizar ferramentas como *John the Ripper* ou *HashCat* que são capazes de transformar a *hash* da senha capturada na verdadeira

senha. Além disso, essa falha também pode ser utilizada para que o computador execute um comando programado pelo invasor, tornando as possibilidades infinitas.

Como correção, foi lançada a versão 4.6.19253.0401 do cliente da ferramenta, impedindo que todas URLs e caminhos UNC possam ser convertidos em *links* clicáveis no *chat* de grupo do *Zoom*. Apesar de a atualização ter sido lançada, cabe ao usuário atualizar a ferramenta para que não haja oportunidade da exploração em questão.

Outra vulnerabilidade foi descoberta com uma investigação do *New York Times*, que revelou que a ferramenta usava uma função de mineração de dados que coletava nomes de usuário e endereços de *e-mail* para vincular os participantes aos seus perfis do *LinkedIn*, mesmo que eles usassem um pseudônimo para permanecer anônimos. Além disso, segundo o jornal, a ferramenta permitia que os participantes da reunião acessassem os dados do perfil do *LinkedIn* sem que o *Zoom Meetings* solicitasse permissão para visitar as informações do perfil dos participantes ou mesmo lhes informasse que outros usuários estavam visitando sua conta na rede social. O Zoom *Meetings* revelou que já desativou esta função.

Uma questão citada no *site Motherboard* da *Vice,* revelou que o *Zoom Meetings* vazava endereços de *e-mail* e fotos de milhares de usuários, permitindo que desconhecidos pudessem entrar em contato através da ferramenta. O problema está na função “Diretório da empresa”, que adiciona automaticamente outras pessoas a uma lista de contatos que se registraram no *Zoom Meetings* com um *e-mail* que compartilha o mesmo domínio. No entanto, muitos usuários registrados com contas de *e-mail* pessoais perceberam que o programa os incluía em listas de contatos com outros usuários como se fossem parte da mesma empresa, expondo suas informações pessoais para outros usuários, como nomes, endereços de *e-mail* e fotos.

Durante a pandemia, ocorreu o fenômeno chamado *Zoombombing*, também conhecido como *Zoom raiding* é um fenômeno que ocorre a participação de algum participante indesejado em uma chamada de vídeo, durante uma reunião. Mesmo alguns desses incidentes terem sidos brincadeiras houve uma parte que estavam se utilizando disso para discursos de ódio e assédio.

Segundo uma análise do *The New York Times*, foram encontradas diversas contas no *Instagram*, *Twitter*, fóruns de mensagens ativos no *Reddit* além do *4Chan*, onde diversas pessoas se reuniram para organizar campanha de assédio utilizando o *Zoom Meetings* como ferramenta, compartilhando senhas de reuniões para semear o caos em reuniões públicas e privadas.

Um texto publicado no *Washington Post* em 3 de Abril revelou que milhares de gravações de chamadas feitas através do *Zoom Meetings* haviam sido armazenadas no domínio público. Além disso, devido à maneira de nomear os arquivos implementados pelo *Zoom Meetings*, foi possível encontrar vídeos, acessíveis a qualquer pessoa, em serviços de armazenamento como os oferecidos pela *Amazon*.

Embora o *Zoom Meetings* pretenda implementar criptografia de ponta a ponta em suas comunicações, parece que esse não é o caso. De acordo com o site *The Intercept*, o *Zoom Meetings* tem acesso a vídeos e áudios sem criptografia das reuniões realizadas por meio do aplicativo. A empresa esclareceu que o conteúdo das videoconferências (bate-papos, vídeos, áudios e telas compartilhadas) possui criptografia de ponta a ponta, mas se qualquer serviço, como gravação em nuvem, estiver ativado, o *Zoom Meetings* terá acesso às chaves de descriptografia que atualmente mantém na nuvem. Isso não deveria ocorrer, garantem alguns especialistas, já que em um verdadeiro sistema de criptografia de ponta a ponta, o provedor de serviços (neste caso, o *Zoom Meetings*) não deve poder acessar o conteúdo descriptografado das comunicações. Isso garantiria não apenas que o provedor não possa ler seus dados, mas também que um invasor não possa comprometer o aplicativo ou seus serviços em nuvem.

No final de Março, os pesquisadores relataram um aumento no registro de domínios que usavam o termo *Zoom* como parte dos nomes de domínio, algo que provavelmente tem uma explicação na intenção dos cibercriminosos de criar sites que fazem passar pela plataforma para induzir os usuários a baixar executáveis maliciosos. Nesta semana, de acordo com a *Trend Micro,* cibercriminosos estão escondendo *malware* para minerar criptomoedas de instaladores legítimos do aplicativo. Além disso, o site *Bleeping Computer* informou que descobriu outros instaladores do *Zoom Meetings* em *sites* não oficiais sendo usados para distribuir um

trojan de acesso remoto (RAT) que permite ao invasor obter acesso total ao computador comprometido.

Embora o *Zoom Meetings* esteja aprimorando cada vez mais a segurança de seus aplicativos, alguns tipos de invasão ainda dependem principalmente de certas atitudes e configurações do próprio usuário.

Abaixo, estão relacionadas algumas dicas importantes para blindar as reuniões e evitar incidentes de *zoombombing*, seja na esfera pessoal, profissional ou educacional:

- Optar por uma senha forte e ative a autenticação de dois fatores (2FA), garantindo assim que ninguém entre em seu perfil por força bruta.
- É essencial tomar cuidado com os *links* de reuniões, evitando compartilhá-los em ambientes abertos como grupos de redes sociais.
- O *Zoom Meetings* possui uma funcionalidade de “Sala de Espera”, na qual um indivíduo só pode participar da conferência caso tenha sua entrada aprovada.
- Preferir usar a interface do programa para navegadores em prol da instalável, devido os vários aplicativos clientes do *Zoom Meetings* demonstraram uma variedade de falhas. Algumas versões permitem que *hackers* acessem a câmera e o microfone do dispositivo; outros permitem que sites adicionem usuários a chamadas sem consentimento.
- Cuidado com falsos instaladores do *Zoom Meetings* recheados com *malwares,* que de acordo o Cert (2017), *Malwares* ou *softwares* maliciosos, são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computado distribuídos por criminosos, caso necessário, optar por instaladores com o menor número de *gadgets* possível é a melhor saída.

4. Considerações Finais

A plataforma *Zoom Meetings*, possibilita a aproximação das pessoas nesse período de distanciamento social através de suas conferências com outras pessoas. Com opções de contas gratuitas ou pagas, os usuários contam com a possibilidade de realizar chamadas, fazer reuniões, *webinares* e trabalhar colaborativamente.

Porém com essa facilidade, vem também as vulnerabilidades expostas e descobertas após sua alta utilização pelas empresas e usuários atualmente.

Com essas novas formas de trabalho, será necessário um maior preparo dos profissionais das corporações para que consigam utilizar a ferramenta de forma útil e segura para a empresa, assim, é importante focar na capacitação dos funcionários existentes para manejo de tais ferramentas e cuidados com o compartilhamento de dados. Nas novas contratações, será um diferencial que os candidatos já tenham conhecimentos das ferramentas utilizadas nas empresas, e algum certificado de participação em palestras que abordem o tema da LGPD.

Assim, é preciso que a ferramenta lance as correções de suas vulnerabilidades já conhecidas e realize a rotinas de testes de segurança para melhor proteção de seus usuários, além de alterar métodos de entradas de usuários nas reuniões e suas regras de cadastro para deixar a ferramenta *compliance*.

Referências

«LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponivel em: www.planalto.gov.br . Acesso em 30 de agosto de 2020

BRIK, M. BRIK, A. "**Trabalho Portátil**: Produtividade, economia e qualidade de vida no *home office* das empresas". 1. ed. Curitiba: Ed. do autor, 2013. 188 p.

CERT.br. **Códigos maliciosos (Malware)** Disponível em: https://cartilha.cert.br/malware/.cartilha.cert.br . Acesso em 4 de dezembro de 2020

MAMMAR, A., CAVALLI, A., & JIMENEZ, W. (2011). **Using testing techniques for vulnerability detection in C programs**. Testing Software and …, 80–96. Disponível em: http://link.springer.com/chapter/10.1007/978-3-642-24580-0_7

MORENO, D. **Introdução ao Pentest**; Editora Novatec; 2 ed; 2019. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=FD-4DwAAQBAJ&oi=fnd&pg=PA18&dq=pentest&ots=cB3wdaH9XC&sig=UUaZiIwn7vm5UnjjSef_3PeCD5o#v=onepage&q=pentest&f=false . Acesso em: 22 de Junho 2020.

WEIDMAN, G., **Penetration Testing A Hands-On Introduction to Hacking;**Editora Novatec; 1 ed; 2014. Disponível em: https://books.google.com.br/books?id=T_LlAwAAQBAJ&printsec=frontcover&dq=Pentest+Georgia+W&hl=pt-BR&sa=X&ved=2ahUKEwinhaPgm-TtAhURK7kGHWGEC7UQ6AEwAHoECAIQAg#v=onepage&q=Pentest%20Georgia%20W&f=false

SREENIVASA, R., & KUMAN, N. (2012). **APPLICATION VULNERABILITY DETECTION USING DYNAMIC ANALYSIS**. International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849.

SANTOS, N. dos. **Educação à distância e as novas tecnologias de Informação e Aprendizagem**. Disponível em: http://www.engenheiro2001.org.br/programas/980201a2.htm. Acesso em: 25 de novembro de 2020.

VARGAS, M. R. M**, Educação a Distância e as Novas Tecnologias**: o uso da videoconferência em treinamentos organizacionais. Disponível em: http://seer.abed.net.br/index.php/RBAAD/article/download/107/11#:~:text=Considerando%2Dse%20que%20o%20prefixo,como%20sendo%20uma%20%22teleconfer%C3%AAncia%22. Acesso em 20´de novembro de 2020.

SCHULZ, L., **Os 6 melhores apps de videoconferência para 2020**. Disponível em: https://www.oberlo.com.br/blog/videoconferencia. Acesso em: 29 de Novembro de 2020.