
FACULDADE BAIANA DE DIREITO
PÓS-GRADUAÇÃO EM DIREITO DIGITAL

**MARCUS MALTA NASCIMENTO**

# PRIVACIDADE DE DADOS E SEGURANÇA DA INFORMAÇÃO: Abordagem sobre vulnerabilidades, teste de invasão e Hacker Ético.

Salvador
2022

**MARCUS MALTA NASCIMENTO**

# PRIVACIDADE DE DADOS E SEGURANÇA DA INFORMAÇÃO: Abordagem sobre vulnerabilidades, teste de invasão e Hacker Ético.

Trabalho de conclusão de curso apresentado à Pós-Graduação em Direito Digital, Faculdade Baiana de Direito, como requisito para obtenção do título de Pós-Graduado em Direito Digital.

Salvador
2022

**MARCUS MALTA NASCIMENTO**

# PRIVACIDADE DE DADOS E SEGURANÇA DA INFORMAÇÃO: Abordagem sobre vulnerabilidades, teste de invasão e Hacker Ético.

Artigo aprovado como requisito para obtenção do grau de Especialista em Direito Digital, Faculdade Baiana de Direito, pelo seguinte avaliador:

Nome:

Titulação e instituição:

Salvador, ___/___/2022

## RESUMO

O presente trabalho trata da exigência de adoção de medidas de segurança pelos responsáveis pelo tratamento de dados, nos termos do art. 44 da lei 13.709/2018, especialmente com relação à segurança da informação nas redes de computadores. Para isso, traça um panorama geral sobre os riscos globais digitais, elenca os principais tipos de ocorrências relatadas até o ano de 2021, assim como apresenta elementos básicos sobre as atividades de um PenTest.


Palavras-chave: Teste de Invasão, Hacker, Proteção de Dados. LGPD. Cibersegurança, Vulnerabilidade.


## ABSTRACT

The present work deals with the requirement to adopt security measures by those responsible for data processing, under the terms of art. 44 of Law 13,709/2018, especially with regard to information security on computer networks. For this, it outlines an overview of global digital risks, lists the main types of occurrences reported up to the year 2021, as well as presents basic elements about the activities of a PenTest.


Keywords: Penetration Test, Hacker, Data Protection. LGPD. Cyber Security, Vulnerability.

# 1 - INTRODUÇÃO:

## 1.1 - Lei Geral de Proteção de Dados (lei 13.709/2018) e os Riscos Globais de Cibersegurança.

Passados quase 05 anos desde a publicação da Lei Geral de Proteção de Dados - LGPD (lei 13.709 de 14 de agosto de 2018), quando então o tema ganhou notoriedade nas discussões jurídicas e corporativas. Nesse tempo, percebe-se um forte incremento na percepção geral sobre o tratamento de dados pessoais por entes públicos e privados.

Tanto a Administração Pública como a iniciativa privada vêm desenvolvendo métodos, modelos, políticas e ferramentas no sentido de formatar *frameworks* para avaliação e implementação das regras de privacidade impostas por lei.

Um exemplo importante dessa iniciativa é o site https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados, mantido pelo Governo Federal, no qual são disponibilizados *templates*, guias e ferramentas que podem ser acessados pelos demais entes federados e órgãos públicos para serem utilizados de forma livre a gratuita. Apesar de se tratar de material endereçado essencialmente ao setor público, muito pode ser aproveitado para os demais setores.

Pois bem, dentre vários aspectos tratados pela LGPD, um deles tem destaque junto aos analistas de privacidade, juristas, técnicos de tecnologia da informação e ao público em geral. Cuida-se da Segurança da Informação, especialmente da segurança da informação no ciberespaço.

É cada vez mais comum notícias sobre invasões de sites, servidores, redes internas de empresas e entes públicos para a prática de atos ilícitos. Estes atos vão desde um simples “vandalismo virtual”, passando por ataques de negação de serviços (DoS), coleta e divulgação de dados, encriptação de arquivos com pedido de resgate (*ransomware*), ataques de *phishing*, *man-in-the-middle*, sites falsos, enfim, existe uma variedade de formas de ataques e riscos nas redes de computadores que podem comprometer a continuidade e perpetuidade dos negócios e, sobretudo, a segurança de dados pessoais. Os ataques cibernéticos se tornam cada dia mais profissionais, elaborados e organizados, causando prejuízos bilionários e muitos transtornos aos usuários.

No Relatório de Riscos Globais 2022 elaborado pelo Fórum Econômico Mundial, dentre as percepções de riscos globais estão as Dependências Digitais e Vulnerabilidades Cibernéticas, destacando que:

> "*No contexto da dependência generalizada de sistemas digitais cada vez mais complexos, as ameaças cibernéticas crescentes estão ultrapassando a capacidade das sociedades de prevenir-las e gerenciá-las com eficácia. Por exemplo, a digitalização de cadeias de suprimentos físicas cria novas vulnerabilidades porque essas cadeias de suprimentos dependem de provedores de tecnologia e outros terceiros, que também estão expostos a ameaças semelhantes e potencialmente contagiosas. 6 Em dezembro de 2021, apenas uma semana após a descoberta de uma falha crítica de segurança em uma biblioteca de software amplamente utilizada (Log4j), mais de 100 tentativas de explorar a vulnerabilidade foram detectadas a cada minuto, ilustrando como a codificação de acesso livre pode espalhar amplamente as vulnerabilidades. 7 O software de monitoramento e gerenciamento de tecnologia da informação (TI) também ilustra o potencial de exposição contagiosa, que pode romper as defesas das cadeias de suprimentos críticas de segurança cibernética, como mostrado pelo ataque Solar Winds Orion que ocorreu no final de 2020. 8 Embora uma instituição estatal com recursos altamente sofisticados provavelmente tenha apresentado esse ataque, outras organizações criminosas certamente tentarão replicar essa abordagem. 9 Ao mesmo tempo, vulnerabilidades mais antigas persistem com muitas organizações ainda confiando em sistemas ou tecnologias desatualizadas.*
>
> *A atividade maliciosa está se proliferando, em parte por causa das vulnerabilidades crescentes, mas também porque há poucas barreiras de entrada para participantes do setor de ransomware e pouco risco de extradição, processo ou*

> *sanção.10 O malware aumentou 358% em 2020, enquanto o ransomware aumentou 435%,11 com um aumento de quatro vezes no valor total da criptomoeda recebida por endereços de ransomware (veja a Figura 4.1).12 O "Ransomware como serviço" permite que até criminosos não técnicos executem ataques, uma tendência que pode se intensificar com o advento do malware com inteligência artificial (IA).13 Na verdade, grupos de mercenários cibernéticos com fins lucrativos estão prontos para fornecer acesso a ferramentas sofisticadas de invasão cibernética para facilitar esses ataques. Além disso, as criptomoedas também permitiram que os cibercriminosos coletassem pagamentos com um risco modesto de detecção ou devolução monetária.*" (https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities#chapter-3-digital-dependencies-and-cyber-vulnerabilities. Pesquisado em 25.04.2022).

Em resposta às perguntas formuladas pela Global Risks Perception Survey (GRPS), os entrevistados apontam a falha de segurança cibernética entre os 05 principais riscos no leste da Ásia, no Pacífico e na Europa. já Austrália, Grã-Bretanha, Irlanda e Nova Zelândia chegam a classifica o risco cibernético o número um.

No mesmo sentido, países altamente digitalizados como Israel, Japão, Taiwan (China), Cingapura e Emirados Árabes Unidos, os quais apontaram o problema entre os 05 mais preocupantes.

Por outro lado, o mundo enfrenta uma escassez de profissionais de TI especializados em Segurança da Informação - uma lacuna de aproximadamente 3 milhões de profissionais - o que agrava a situação, podendo impactar até mesmo no crescimento econômico global.

Nesse contexto, o mesmo relatório aponta que:

> "*O impacto de ataques cibernéticos disruptivos pode ser financeiramente devastador para empresas que não investem em proteções para sua infraestrutura digital, principalmente em um cenário em que os governos começam a proibir pagamentos de resgate ou penalizar práticas inadequadas de segurança*

> *cibernética. 51 Além disso, à medida que as preocupações ambientais, sociais e de governança (ESG) entram cada vez mais em foco (consulte o Capítulo 2), as empresas que não conseguem demonstrar uma governança corporativa forte em torno da segurança cibernética – como implementar sistemas robustos e protocolos de supervisão de processos e praticar responsabilidade e transparência no caso de uma violação - pode sofrer danos à reputação aos olhos dos investidores focados em ESG.*
>
> *As empresas também operam em um mundo em que 95% dos problemas de segurança cibernética podem ser atribuídos a erro humano, 52 e onde as ameaças internas (intencionais ou acidentais) representam 43% de todas as violações."*

Segue um gráfico representativo dos principais riscos globais apontados pelo Fórum Mundial para os próximos anos, demonstrando a posição da segurança da informação (entre outros) em janelas de tempo diferentes, lembrando que se trata de uma representação da percepção atual, o que pode ser alterada nos próximos anos de acordo com a evolução de cada tema.


**1.2 - Art. 44 da LGPD e a segurança da informação.**

Nos termos da lei 13.709/2018, tanto o controlador quanto o operador de dados deverão apresentar parâmetros adequados de segurança, sob pena de responderem por eventuais incidentes decorrentes de sua negligência. Conforme a Lei Geral de Proteção de Dados - LGPD:

> *"Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as*

> *circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.*
>
> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
>
> *§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.*
>
> *§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.*
>
> *Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.*
>
> *Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.* (grifos não originais).

Os trechos da lei em destaque não deixam dúvida sobre a obrigação de todos os envolvidos no tratamento de dados com a implementação e manutenção de

medidas para garantir a segurança da informação. Não há falar em privacidade de dados sem que se estabeleçam tais medidas, podendo abranger desde organização administrativa, até implantação de políticas de segurança, gestão de ativos, controle de acesso, criptografia, segurança física e do ambiente, controle das comunicações e do desenvolvimento de projetos entre outras. Enfim, serão necessárias abordagens físicas, lógicas e administrativas com o intuito de cumprir com as exigências legais.

Verifica-se então que responsáveis por tratamento de dados nas redes de computadores deverão incluir a cibersegurança no processo de adequação às exigências da LGDP, necessitando para isso de apoio de pessoal especializado na área.

Mas, afinal, o que seria cibersegurança? Segundo a enciclopédia digital Wikipédia, "*segurança de computadores ou cibersegurança é a proteção de sistemas de computador contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que fornecem*." (https://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_computadores. Acesso em 03.05.2022)

Parecida também é a definição da empresa especializada em segurança da informação Kaspersky, a qual apresenta o seguinte conceito: "*Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas*." (https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. visitada em 27.04.2022).

Ocorre que mesmo sendo a Cibersegurança uma área especializada do gênero "Tecnologia da Informação (TI)", ela também possui áreas distintas de atuação subespecializadas, a exemplo das áreas de Segurança e Análise de Redes, Pesquisa de Vulnerabilidades, Perícia Forense, Desenvolvimento, Segurança Defensiva e Ofensiva, Pentest entre outras.

Com efeito, o presente artigo tem por objetivo esclarecer um pouco sobre o mundo da segurança da informação nas redes de computadores, com especial ênfase na apresentação das atuais principais vulnerabilidades, teste de invasão (conhecido também como Pentest - Penetration Testing) e Hacker Ético.

## 2 - PRINCIPAIS AMEAÇAS ENFRENTADAS:

A Open Web Application Security Project - OWASP é uma fundação sem fins lucrativos que trabalha, de um modo geral, para melhorar a segurança na rede mundial de computadores (internet). Possui atuação global com dezenas de milhares de membros por todo o mundo. Fundada em dezembro de 2001, se dedica a pesquisa e divulgação de estudos na área de segurança na web, permitindo que organizações desenvolvam, adquiram, operem e mantenham aplicativos confiáveis. Em seu site (https://owasp.org) oferece seus projetos, ferramentas e documentos gratuita a qualquer interessado.

Pois bem, um dos projetos da OWASP é a divulgação de um *ranking* das maiores ameaças encontradas na internet. Cuida-se do relatório denominado “OWASP Top 10”, cuja mais atual versão data do ano de 2021 (https://owasp.org/www-project-top-ten/). Este documento dá uma ideia dos principais problemas enfrentados na gestão da segurança cibernética, assim como oferece sugestões de como evitá-los ou corrigi-los.

Vejamos quais são essas ameaças (na ordem de importância) trazidas relatório OWASP Top 10 do ano de 2021. Advirta-se que a enumeração abaixo obedece a ordem da maior ocorrência para a menor e que será apresentado uma descrição simplificada sem que se pretenda (e nem poderia) esgotar o assunto ou todas as definições envolvidas. Como dito, o objetivo é tomar ciência das ocorrências e ter uma noção geral sobre elas.

## 2.1 - Ameaças em espécie (TOP 10 da OWASP):

1- Controle de acesso quebrado:

Acontece quando um usuário comum tem acesso à informações as quais ele não deveria em razão da criticidade do dado. No caso, há uma falha com as definições de acesso, poderes e atribuições de cada usuário ao sistema e com o nível hierárquico atribuído a cada um.

Os níveis de acesso devem ser definidos nas políticas de segurança de cada entidade, descrevendo qual nível de informações ou nível de gerenciamento do sistema cada usuário poderá dispor. Por exemplo, um usuário comum não deve ter

permissões de administrador do sistema ou livre acesso a um banco de dados com dados sensíveis.

Falhas desse tipo possibilitam que um funcionário possa agir fora de suas atribuições funcionais, levando à divulgação, modificação ou destruição de informações não autorizadas, alterações dos sistemas de informática, alteração dos parâmetros de segurança na navegação na internet, afastando pré - configurações, entre outros.

2 – Falhas criptográficas:

Inicialmente, vale entender que criptografia é um conjunto de princípios e técnicas empregadas para cifrar a escrita ao ponto de torná-la ininteligível para os que não tenham acesso aos códigos de reversão.

Assim, a criptografia é utilizada para que, caso uma mensagem (ou um banco de dados) seja interceptada ou acessada por terceiro, este não conseguirá ler os dados, uma vez que eles apareceram em uma linguagem completamente desconexa, impossível de ser compreendida. Isso significa que o atacante terá os dados em mãos, mas não poderá fazer nada com eles, já que não se pode extrair a informação ali contida.

Nesse sentido, a falha de criptografia significa exatamente a insuficiência da técnica utilizada ou mesmo a ausência total de qualquer técnica. No caso da insuficiência, é possível que técnicas de criptografia mais simples e já conhecidas sejam desfeitas com certa facilidade com o uso de programas dedicados a isso.

Quanto mais sensível o dado a ser protegido, como senhas, números de cartão de crédito, registros de saúde, informações pessoais e segredos comerciais, maior será a necessidade do uso de técnicas mais avançadas e frequentemente revisadas.

3 – Injeção:

Acontecem quando um atacante envia dados para um interpretador simulando uma consulta ou comando legítimos, mas que na verdade escondem tentativas de execução de comandos não permitidos ou exposição de dados não autorizados. Ou seja, a falha acontece quando uma solicitação maliciosa feita pelo usuário é interpretada como comandos ou parâmetros reais pelo aplicativo, fazendo com que o servidor/banco de dados responda algo que não deveria.

Como exemplo, poderíamos citar um campo de pesquisa de situação cadastral junto a um órgão público (banco de dados), utilizando linguagem SQL. Aqui, normalmente, o usuário/atacante colocaria no campo de pesquisa valores válidos como número de CPF, RG ou NIT, mas, ao invés disso, ele digita uma linha de comando para listar todos os arquivos do diretório/pasta e o sistema executa aquela linha de comando e entregando a informação solicitada.

Isso acontece porque o sistema não foi devidamente preparado para filtrar e rejeitar esse tipo de solicitação e acaba validando o comando. A depender da gravidade da falha, esses comandos específicos, podem permitir que o atacante consiga senhas de usuários com privilégios e execute o login no sistema com autorizações de administrador, podendo baixar arquivos, apagá-los ou criptografá-los, causando graves prejuízos à vítima.

4 – Design inseguro:

Esta é uma nova categoria introduzida pela OWASP no ano de 2021. Tem por base o princípio do Secure by Design. Significa que a segurança da aplicação deve ser observada desde a concepção do projeto, fazendo com que cada etapa de seu desenvolvimento seja testada e construída para evitar vulnerabilidades.

O design seguro deve ser incorporado à metodologia do desenvolvimento, com avaliações frequentes das ameaças, certificando-se de que o código foi concebido e testado contra ataques conhecidos.

Nesse sentido, a participação de especialistas em cibersegurança já nas etapas iniciais pode evitar grandes prejuízos futuros com a correção de defeitos de forma antecipada, de modo que as mudanças a serem implementadas não serão tão custosas de serem feitas como no caso se aguardar a finalização do projeto para tanto.

Vale registrar que um design seguro não isenta o projeto de eventual vulnerabilidade. O objetivo do primeiro é criar uma estrutura que diminua os riscos do segundo ocorrer e, caso ocorra, o problema seja corrigido com o menor custo.

5 – Configuração incorreta de segurança:

Esta categoria trata de falhas nas configurações de segurança de dispositivos e softwares. É mais comum do que se pensa, isso porque muitos usuários não alteram

as configurações de segurança que vêm por padrão nas aplicações. Essas configurações podem ser suficientes para garantir o mínimo de segurança com usabilidade, mas a depender da atividade desenvolvida, em certos casos é necessário introduzir camadas extras de segurança.

Por vezes, medidas simples como alterar a senha e usuário padrão, configurar o firewall ou um serviço proxy são negligenciadas e acabam permitindo que atacantes se utilizem dessas falhas para controlar os dispositivos alheios.

Um outro exemplo de configuração incorreta de segurança são os ataques de Entidades Externas de XML (XML External Entity - XXE), a qual constituía uma categoria própria no rol anterior do ano de 2017.

Trata-se de uma vulnerabilidade própria de sistemas que utilizam linguagem XML (E**x**tensible **M**arkup **L**anguage), linguagem está muito comum em softwares emissores de documentos fiscais mais antigos (geralmente sistemas legados). Atualmente, essa tecnologia vem sendo substituída por outras linguagens como a JSON ou REST.

Em resumo, o XML é usado para definir padrões e formatação de um documento de forma que diversos sistemas serão capazes de visualizá-los, mesmo se tratando de sistemas diferentes. É como se fossem instruções para que qualquer sistema entendesse como aquele documento deve ser montado exposto ao usuário.

O ataque acontece quando é enviado um arquivo XML com algum código malicioso dentre as informações contidas no documento. Quando o processador do XML então passa a ler as informações ali contidas, ele vai registrando as informações conforme as linhas de comando do documento aparecem. Ocorre que em um dado ponto, o código inserido é lido e simplesmente executado sem qualquer filtro, como se fosse uma informação válida. Tal código pode ser um comando de conexão com outra máquina, uma ordem de backup e envio dos arquivos, encriptação de banco de dados, entre outros.

Enfim, é preciso que o software esteja preparado para identificar códigos maliciosos inseridos dentro do XML e isolá-los.

6 – Componentes Vulneráveis e Desatualizados:

Aqui estão incluídas as mais diversas condutas que empresas e usuários em geral poderiam manter para mitigar os riscos de ataques cibernéticos. É certo que muitas delas são preocupações comuns apenas para usuários qualificados, passando

um pouco longe das pessoas com conhecimento comum na operação de computadores, já que os ajustes necessários por vezes demandam conhecimentos específicos.

Dentre essas ações podemos citar a necessidade de conhecer os componentes que orbitam o sistema principal tais como o gerenciador do banco de dados, sistema operacional, aplicativos, os APIs (Interface de Programação de Aplicações/Application Programming Interface) utilizados, entre outros e se tais componentes possuem suporte e atualização adequados.

Verificação regular/periódica de vulnerabilidades, assim como acompanhamento de novas descobertas em boletins informativos e comunidades dedicadas ao tema, correção e atualização dos sistemas, todas são medidas a serem implementadas na rotina dos usuários.

7 – Falhas de Identificação e Autenticação.

São ataques relacionados com a autenticação de usuários no sistema e níveis de permissão de acesso. Tem origem, muitas das vezes, na má configuração do sistema, e permite que um invasor quebre senhas, chaves, tokens e assuma o usuário de uma outrem.

Existem várias formas de quebra da identidade, dentre elas destacam-se os ataques de força bruta, no qual são testadas milhares (ou até milhões) de senhas até que se encontre a combinação exata, ataques de engenharia social, phishing, escuta de portas, entre outros. Cada uma dessas modalidades tem o objetivo de descobrir as senhas e logins utilizando os mais diversos métodos.

Interessa registrar que existem programas dedicados à tarefa de quebra de senha, seja pelo método de tentativa e erro, seja com o uso de listas desses dados vazadas na internet. Nesse contexto, o atacante não tentará utilizá-las manualmente site por site. Isso levaria uma vida inteira. Mas para um computador, testar milhares de senhas e logins é uma questão de poucos segundos.

Para diminuir os riscos de quebra de autenticação é aconselhável a adoção de senha fortes, com o uso de números, letras e caracteres especiais, somado ainda a autenticação de dois fatores e a não repetição da senha em diversos serviços.

8 - Falhas de integridade de software e dados:

Esta é uma falha bastante interessante. Nela o problema não está no software em si, mas sim nas fontes de dados que alimentam suas funcionalidades. Acontece quando se utiliza, por exemplo, bibliotecas, módulos, repertórios de conteúdo não confiáveis. Nesse caso, através desse canal, um código malicioso pode ser injetado e comprometer o sistema.

Um outro exemplo pode surgir de uma atualização automática baixada sem a devida verificação de integridade, alterando o aplicativo que era anteriormente confiável. Invasores podem modificar não seu sistema individualmente, mas assim fazer alterações junto ao repertório (inseguro) onde as atualizações são buscadas de forma a ampliar exponencialmente seu ataque para todos os que baixarem a atualização.

Verificação das assinaturas digitais e uso de ferramentas de checagem de segurança dessas fontes de dados são medidas que podem minimizar os riscos desse tipo de ataque.

9 – Falhas de registro e monitoramento de segurança:

Este é um item voltado para sistemas um pouco mais robustos. Sendo realista, dificilmente um usuário comum vai conseguir manter uma estrutura de registro de monitoramento de sua rede, especialmente em se tratando de uma rede LAN (Local Area Network).

Como o nome sugere, cuida-se do registro dos acessos realizados na rede e demais atividades realizadas por cada usuário. A manutenção desse tipo de registro é de grande importância no caso de instauração de uma investigação de um ataque.

Tão importante quanto o registro dos acessos é também o monitoramento das ações dentro da rede. Nesse caso, no monitoramento existe um acompanhamento constante do fluxo de dados, o que permite que atividades suspeitas, fora de um perfil previamente configurado, sejam imediatamente detectadas e sinalizadas para tomada de medidas preventivas e de resposta.

Além disso, vale registrar que manter sistemas de registro e monitoramento eficazes, apesar de não garantir totalmente a segurança dos dados, deve ser levado

em consideração na hipótese de apuração de responsabilidade civil do controlador ou operador de dados, nos termos dos arts. 43 e seguintes da lei 13.709/2018.

10 – Falsificação de solicitação do lado do servidor (Server-Side Request Forgery – SSRF).

Nesse tipo de falha, temos um cenário em que existe um servidor web hospedando um site público de uma empresa, sendo os demais sistemas internos (também conectados à internet), protegidos por um firewall. No caso, este firewall está configurado para impedir requisições oriundas de usuários externos, não permitindo que informações contidas dentro da rede interna sejam acessadas por terceiros. Por exemplo, somente o site comercial da empresa estaria liberado para livre visitação, enquanto outros serviços (intranet, banco de dados, servidores internos) estaria inacessível por conta do firewall.

Assim, encontrando a falha de SSRF neste site público, o atacante passa a forçá-lo a fazer requisições aos servidores internos. Dessa forma, considerando que a solicitação parte de um servidor da própria empresa, tal solicitação não fica barrada pelas regras de segurança, já que na de configuração feita no firewall não está prevista o impedimento de requisições oriunda do próprio site da empresa.

Em resumo, o atacante passa a controlar/utilizar um servidor com acesso autorizado para fazer sua exploração como se fosse legítima, driblando a segurança do firewall.

Por fim, registre-se que o SSRF tanto pode ser utilizado para exploração de servidores internos de uma rede (como no exemplo aqui mencionado) como para outros serviços na internet que usuários comuns normalmente não teria acesso.

## 3 - HACKING ÉTICO E OS TESTES DE INVASÃO:

### 3.1 - Introdução:

Apesar de todo o desenvolvimento da internet e da popularização de seus principais elementos, a figura do Hacker ainda causa muita confusão no imaginário dos usuários em geral. Quase que diariamente são noticiados casos de

vazamentos de dados, violação de sistemas, desvio de valores, indisponibilidade de serviços, entre outros, associadas a “ataques hackers”.

Na verdade, os hackers são pessoas que conhecem o funcionamento de redes de computadores, de hardwares e de softwares e que se utilizam desses conhecimentos no melhoramento dos sistemas de informática. Ao contrário do que o senso comum pensa, a atuação do Hacker é benéfica à sociedade.

De outro lado, temos a figura dos “Crakes”. Estes sim são indivíduos violadores das regras. Usam o conhecimento para “quebrar” sistemas de segurança, causando prejuízo a terceiros.

Percebe-se então que as figuras dos Hackers e Crakers são comumente confundidas, acabando por prevalecer o primeiro termo de forma genérica.

Ainda sobre o universo dos hackers, estes podem ser classificados em como White Hat (chapéu branco) associado ao hacker do bem, ou hacker ético, atuante na área de segurança da informação; o Black Hat (chapéu preto), que seria um “hacker” do mal (na verdade um cracker como dito acima) que usa seus conhecimentos para locupletar-se de forma ilícita; e ainda o Grey Hat, que seria um meio termo entre os dois primeiros, ou seja, sua motivação inicial seria lícita (por exemplo busca de vulnerabilidades), mas que pode se tornar ilegal a medida que sua expectativa não é correspondida (por exemplo, não pagamento de recompensa pela vulnerabilidade reportada ao fornecedor do serviço, quando então ele passa a explorar a descoberta, prejudicando o serviço).

## 3.2 - Teste de Invasão.

Conforme dito na introdução, o art. 46 da Lei 13.709/2018 exige que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e, neste contexto, o Teste de Invasão surge como uma das ferramentas úteis a implementação de tais medidas.

O termo “Teste de Invasão” também pode ser encontrado como PenTest, Penetration Testing, Hacking Ético, Teste de Segurança Ofensiva, Red Teaming entre outros. Pode ser definido como “*uma tentativa legal e autorizada de localizar e explorar sistemas de computadores de forma bem-sucedida com o intuito de tornar*

*esses sistemas mais seguros*.” (ENGEBRETSON, Patrick: Introdução ao Hacking e aos Testes de Invasão: Facilitando o hacking ético e os testes de invasão. São Paulo. Ed. Novatec, 2014, p. 23).

Ou, em outras palavras:

> “*Testes de invasão ou pentesting (não confundir com testes de caneta esferográfica ou de canetas-tinteiro) envolvem a simulação de ataques reais para avaliar os riscos associados a potenciais brechas de segurança. Em um teste de invasão (em oposição a uma avaliação de vulnerabilidades), os pentesters não só identificam vulnerabilidades que poderiam ser usadas pelos invasores, mas também exploram essas vulnerabilidades, sempre que possível, para avaliar o que os invasores poderiam obter após uma exploração bem-sucedida das falhas.”* (WEIDMAN, Georgia. Testes de Invasão: Uma introdução prática ao hacking, ed. Novatec Editora Ltda, 2014, p. 30).

Trata-se de um instrumento relativamente novo, o qual, até algum tempo atrás, não possuía padrões definidos para sua realização. Hoje, diversas entidades se dedicam a formulação de documentos visando a implementação de metodologias, procedimentos, técnicas, relatórios que ajudam os profissionais da área no registro de toda a investigação até a entrega dos resultados.

Um dos principais *standart* é o Penetration Testing Execution Standard (PTES), formulado por uma comunidade de profissionais da área com o objetivo de orientar a realização de tais testes e a apresentação dos resultados. É possível citar também o NIST 800-115, um guia técnico para testes e avaliação de Segurança da Informação do Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, o Open Source Security Testing Methodology (OSSTMM) da OWASP, abrangendo uma metodologia para testes de segurança física, administrativa e técnica, sendo uma referência de suporte da ISO 27001, o OWASP Testing Guide, voltado para aplicações web, dentre outros.

O uso de um *framework* é importante porque não só conduz o profissional em uma linha de trabalho organizado e evolutivo, bem como possibilita que as entregas de cada fase sejam aproveitadas como base para a próxima, construindo a conclusão de forma lógica e fundamentada.

Outra interessante iniciativa da comunidade é, além da produção de conteúdo técnico, a criação de códigos de conduta para os profissionais do segmento, podendo ser citados o Certified Ethical Hacker - CEH da EC-Council ou o Certified Information Systems Security Professional (CISSP) da International Information System Security Certification Consortium - ISC2.

Os profissionais da área podem ser certificados por suas habilidades por meio de provas aplicadas, em geral, em inglês e que exigem níveis gradativos de conhecimento conforme se avança na trilha da certificação. Registre-se ainda que, na área da Tecnologia da Informação, as certificações têm grande relevância no reconhecimento e contratação de profissionais.

Para a condução de um teste de invasão várias ferramentas foram desenvolvidas, em especial para Sistemas Operacionais baseados no Linux. Comumente, são programas de código aberto (open source) e gratuitos.

Com o objetivo de facilitar o trabalho, algumas distribuições Linux foram criadas especialmente para isso, como é o caso do Kali Linux e do Parrot OS. Ambos são distribuições Linux baseadas no Debian e que reúnem diversas ferramentas para ataques e testes, passando desde a coleta de informações, até engenharia social, análise de redes, quebradores de senhas, analisadores de vulnerabilidades etc.

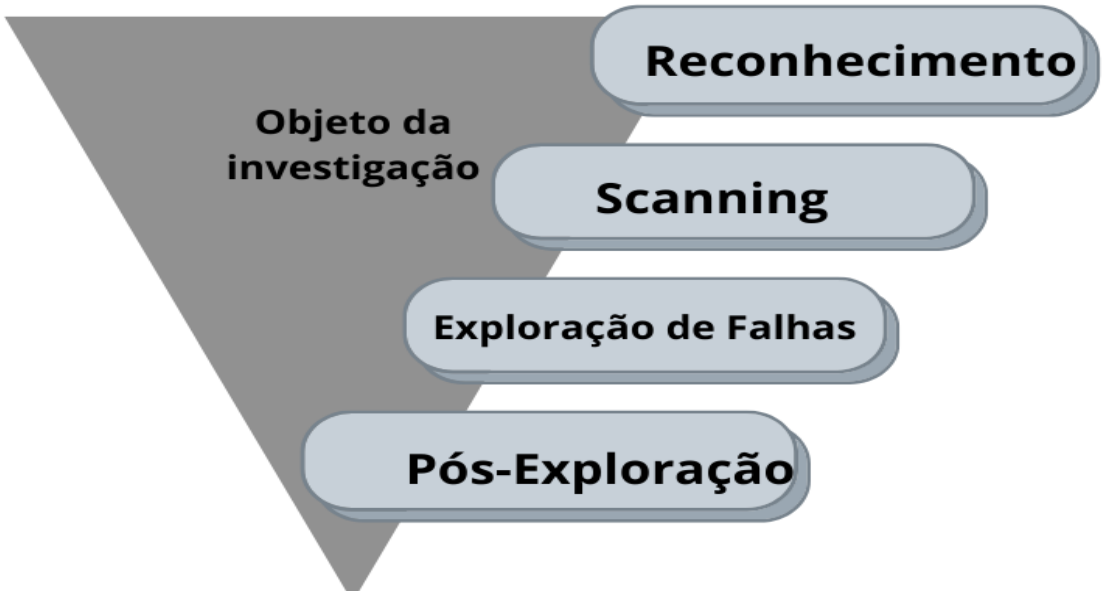
A vantagem dessas distribuições é que elas são especializadas em hacking, não sendo necessário que o operador instale cada aplicação. Uma vez instalado, as principais ferramentas estarão disponíveis, mas lembrando que novos recursos podem ser adicionados, bem como estes mesmo programas podem ser utilizados em outras distribuições Linux.

### **3.3 - Fases de um Pentest**.

Por se tratar de um breve articulado, será utilizada uma visão mais simplificada para examinar e descrever os principais pontos e características de um teste de invasão. Nos padrões citados acima, podem ser encontradas de quatro a sete diferentes fases de um Pentest, com diferença nas nomenclaturas, mas, independentemente da quantidade de divisões e nomes, todos eles abordam conteúdos semelhantes.

Tomaremos por base quatro fases, sendo elas: 1 - Reconhecimento (Information Gathering), 2- Scanning, 3 - Exploração de Falhas (Exploitation) e 3 - Pós-Exploração.

A figura de um triângulo invertido é bastante didática para a visualização do que acontece na prática:




Isso porque, no início do trabalho, por vezes, o campo de investigação é bastante amplo; todos os detalhes sobre o alvo são importantes. Vários são os exemplos na literatura onde detalhes aparentemente irrelevantes, ao final, resultaram em explorações bem-sucedidas. As mais diversas informações devem ser coletadas e armazenadas e, como dito, cada detalhe conta.

O volume de informações iniciais vai variar conforme seja a amplitude do objeto contratado. Testes conhecidos como Black Box, no qual o testador possui conhecimento mínimo sobre o objeto (por vezes somente o nome da empresa) pode revelar a necessidade de lidar e organizar grande quantidade de informações. Em outros casos, o teste pode ser restrito à apenas um aplicativo ou domínio, demandando menor quantidade de dados.

De uma forma ou de outra, a quantidade de dados a se lidar vai afunilando à medida que a investigação avança, passando do aspecto quantitativo para um mais qualitativo. Esse aspecto será melhor entendido com a apresentação de cada fase.

### 3.3.1 - Reconhecimento:

A fase de Reconhecimento (Information Gathering), muitas vezes, é negligenciada pelos pentesters iniciantes, os quais, ansiosos pelos resultados, desejam partir direto para a fase de exploração. Mas esta não é a melhor prática.

Aqui, um bom profissional de Pentest buscará por cada informação possível que poderá ajudá-lo na fase de exploração. Ele buscará informações sobre os funcionários, acessos físicos da empresa, rotinas de produção, sites e seus subdomínios, e-mails, servidores, hosts, logins e senhas, sistemas de segurança, sistemas operacionais, softwares e suas versões, firewalls, serviços, portas lógicas, redes sociais entre outros.

Nessa tarefa, um dos instrumentos mais utilizados é o Google Hacking, que nada mais é do que a utilização do buscador Google de forma direcionada, com o uso de filtros específicos. São informações obtidas por meio da OSINT (sigla para Open Source Intelligence ou Inteligência de Código Aberto), ou seja, em fontes abertas na internet, mas que contém um volume espantoso de informações sobre pessoas e empresas.

Mas também existem outras ferramentas úteis para coleta de informações, as quais vão variar a depender do objeto. Um exemplo interessante de ferramenta de busca que automatiza pesquisas na rede social Instagram é o OSINGRAN. Este é uma aplicação OSINT que oferece uma tela com diversas opções para análises de contas do Instagram de qualquer usuário por seu apelido.

É possível, por exemplo, obter o total de comentários das postagens do alvo, lista de seus seguidores, com e-mail e telefones, fotos postadas com metadados, lista de usuários marcados pelo alvo e que lhe marcaram, enfim, os mais variados tipos de informação disponível.

Outras ferramentas podem ser citadas nesta como o HTTrack, que permite que se faça uma cópia integral de um site de forma que o atacante possa analisá-lo offline e longe de monitoramento, o Whois que possui detalhes sobre determinado número IP (Internet Protocol), o The Harvester para encontrar e-mails de determinado domínio e listá-los, Netcraft para buscar por sites e seus subdomínios vinculados ao argumento passado, o MetaGooFil, usado para varrer a internet em busca de documentos pertencentes ao alvo e, uma vez encontrados, a ferramenta baixa e passa a fazer a leitura de metadados úteis, o Host usado para traduzir números de IP em nomes de hosts e vice versa, entre outros.

Como visto, existem muitas ferramentas que podem ser utilizadas para executar pesquisas de forma automatizada, retornando um volume grande de informações, as quais precisarão ser organizadas, filtradas e armazenadas, lembrando que é altamente recomendável que cada passo deva ser de logo documentado para efeito de apresentação de relatório final.

O Reconhecimento é tido por muitos especialistas como a fase mais importante das quatro. Quanto melhor for elaborada e documentada, maiores serão as chances de sucesso nas seguintes. Mas, como dito anteriormente, costuma ser uma parte menosprezada, seja porque é pouco compreendida sua importância, seja porque é uma parte menos "técnica" e empolgante.

Em resumo, há duas metas principais nessa fase. 1) reunir o maior volume possível de dados sobre o alvo e 2) criar uma lista de endereços IP ou de URLs (Uniform Resource Locators) passíveis de ataque.

### 3.3.2 - Scanning.

Após o passo descrito acima, o Pentester terá uma boa compreensão do alvo, das suas atividades, negócios, empregados etc. De posse disso, ele inicia o segundo passo, qual seja, o scanning.

O fato é que as redes internas de computadores das empresas, em sua grande maioria, estão conectadas à internet, mantendo constante tráfego de arquivos com os mais diversos usuários. O Scanning consiste no processo de identificar quais sistemas estão ativos na rede e quais serviços existem nesses sistemas.

A tarefa pode ser separada em quatro partes (lembrando que não se trata de um método rígido, mas sim de uma sugestão de trilha a ser seguida):

1 - Identificação dos sistemas ativos;

2 – Varredura dos sistemas ativos com uso do Nmap;

3 - Uso do NSE (Nmap Scripting Engine) para refinar as informações;

4 - Varrer o sistema em busca de vulnerabilidades:

Vejamos cada um deles:

Na **identificação dos sistemas ativos**, o atacante busca determinar quais sistemas-alvo estão ativos e são capazes de interagir com um computador externo.

Para isso utiliza-se o comando ping para enviar pacotes na rede e receber a resposta. Por meio dessas respostas é possível verificar o status dos hosts, já que

para cada pacote ping enviado, a resposta revelará se o sistema está ativo ou não e se houve algum erro na comunicação. O comando ping (Packet Internet Network Groper ou localizador de pacotes na rede de internet) utiliza o protocolo ICMP (Internet Control Message Protocol - Protocolo de Mensagens de Controle de Internet) para codificar tais erros.

Este procedimento exige cuidado do testador, uma vez que gera muitos falsos positivos ou falsos negativos quando o alvo possui defesa contra esse tipo de verificação, a exemplo de firewalls configurados para impedir o tráfego desses pacotes. Mas, de toda forma, os resultados devem ser anotados para uso posterior.

Já no segundo procedimento, **o scanning de portas usando o Nmap**, o objetivo é encontrar as portas e serviços que estão rodando no servidor.

A título de esclarecimento, portas são conexões que permitem que os computadores troquem informações. Cada porta possibilita um tipo de conexão com um software ou serviço diferente, sendo que cada host pode ter até 65.536 portas TCP, numeradas de 0 a 65535. A princípio, cada porta pode ser configurada para receber qualquer tipo de serviço, mas, por convenção, existem algumas que usualmente tem determinada função, tais como: porta 80 rodam serviços de HTTP, 443 rodam HTTPS, 25 serviços de e-mail (SMTP), 20 e 21 com FTP, entre outras.

O uso de portas diferentes para cada tipo de serviço permite uma melhor organização do tráfego de dados e a comunicação simultânea sem necessidade de espera.

Nesse contexto, o software Nmap faz esse tipo de varredura em um determinado endereço IP, retornando o resultado as portas e serviços ativos, podendo ainda identificar quais programas estão sendo utilizados, versões, entre outras informações.

Cada porta identificada e aberta pode ser um potencial ponto de entrada no sistema. Mais uma vez os dados devem ser organizados e armazenados.

O passo seguinte consiste na **aplicação do NSE (Nmap Scripting Engine)** para obter informações adicionais sobre aquilo que foi encontrado até o momento. O NSE é como uma evolução do Nmap, adicionando novos recursos à ferramenta clássica. Com o NSE é possível avançar na pesquisa incluindo já varredura de vulnerabilidades, localização de backdoors (portas não documentadas/escondidas), exploração de falhas, além da inclusão de detalhes do alvo.

Como se pode imaginar, essa etapa refina ainda mais as informações do alvo, afunilando o escopo e aprofundando no nível de detalhamento.

Por fim, inicia-se efetivamente a **fase de busca de vulnerabilidades**, que é o processo de localização e identificação de falhas e pontos fracos nas mais diversas estruturas que compõem o alvo.

Essas vulnerabilidades podem ser classificadas conforme sua criticidade, ou seja, existem vulnerabilidades que, se exploradas, não causarão grande comprometimento, assim como existirão outras que possibilitam ao atacante um controle total do alvo.

Essa busca por vulnerabilidades, em sua grande maioria, se inicia pelos dispositivos mais periféricos como roteadores, firewalls, servidores, enfim, aqueles que estão mais na fronteira de uma rede protegida. Dificilmente o ataque se dá diretamente ao centro do sistema. Uma das razões para isso é que a maioria das informações obtidas na primeira fase descrita (Reconhecimento) encontra informações sobre esses periféricos e não sobre os sistemas internos.

O procedimento de conquistar o controle sobre um periférico ou outro computador e, em seguida, utilizá-lo como ponte para um alvo mais interno é chamado de “pivoteamento” (pivoting).

Uma vez avançando sobre as camadas de proteção, o processo de scanning é reiniciado a fim de encontrar alvos adicionais, montando um mapa das redes internas antes escondidas atrás de firewalls.

### 3.3.3 - Exploração de falhas (exploitation).

A exploração de falhas é exatamente o que o título descreve. Nesta fase, o atacante já terá identificado detalhes da rede e suas vulnerabilidades e passará a explorá-las para obter controle dos sistemas, lembrando que nem toda falha resultará no comprometimento total do alvo. Como dito, umas são mais críticas do que outras.

Geralmente o objetivo da exploração é ter acesso ao nível de administrador, o que permite ao atacante realizar as mais diversas alterações no sistema. Por vezes, a ideia também pode ser transformar o computador dominado apenas em um instrumento para a realização de outros ataques.

Pois bem, softwares são lançados no mercado e a partir de então a comunidade hacker passa a estudá-los em busca de problemas de segurança. Uma vez identificados, esses problemas podem ser:

1 - Informados aos desenvolvedores para que corrijam a falha. Nessa hipótese, é bastante comum o pagamento de recompensas pelas empresas àqueles que encontram o problema e alertam aos interessados. Inclusive, atualmente vem se desenvolvendo muito o chamado mercado de “Bug Bounty”, que são programas, públicos ou privados, em que empresas submetem seus produtos digitais ao escrutínio da comunidade e, em contrapartida, pagam valores para quem comprovar e informar a existência de falhas de segurança. Os valores variam conforme a gravidade do problema.

2 - Inseridos em repertórios de vulnerabilidades que podem ser acessados por qualquer interessado, formando um banco de dados de falhas dos mais diversos programas e versões, bem como o script/exploit que pode ser utilizado para exploração.
Sites como https://www.exploit-db.com/ ou https://nvd.nist.gov/vuln/search são exemplos disso. Neles é possível encontrar falhas já catalogadas e organizadas por tipo, data, autor, sistema etc. No sentido de padronizar os relatos, foi criado o sistema de CVE, ou *Commom Vulnerabilities and Exposures*, onde organizações de tecnologia e segurança atribuem um código para cada problema encontrado após analisá-los. A padronização da forma de armazenamento facilita a pesquisa e a divulgação do conhecimento.

3 - Utilizados diretamente pelo atacante para obter alguma vantagem do alvo. Neste caso, ele foi responsável pela descoberta e se vale disso para a exploração do sistema. É a chamada falha “Zero Day”, que é quando se trata de falha nova, não reportada e que ainda não possui uma correção.
Mas como se dá esse procedimento de exploração? Identificada a falha e obtido o correspondente exploit, este é enviado ao alvo. Um exploit é a conversão da falha encontrada em uma forma de controle. Ele contém um código malicioso; uma carga chamada de payload que, uma vez executada no alvo, acaba por ser interpretada pelo sistema como um comando válido, realizando aquilo que o atacante deseja.

Esses payloads podem alterar funcionalidades originais do sistema, fazer cópias de arquivos, apagar outros, conferir privilégios de administrador, adicionar usuários, abrir backdoors, desabilitar tarefas, revelar dados sigilosos e muito mais.

Esta etapa é bastante ampla. Existem diversas ferramentas a serem utilizadas e o atacante deve estar preparado para lidar com situações inesperadas, já que cada rede tem suas particularidades, com sistemas operacionais diferentes, rodando diferentes formas de proteção.

Esta última afirmação ajuda um pouco a responder o porquê o processo de Pentest não é completamente automatizado, bastando um simples click em um software que reunisse e desencadeasse cada etapa em sequência; porque simplesmente não se cria um comando para rodar os scanners e exploits de forma autônoma, esperar apenas os resultados e receber um relatório compilado.

O fato é que, por enquanto, nas explorações mais complexas e bem-sucedidas, o quebra-cabeça a ser montado para atingir um alvo ainda necessita, além do conhecimento técnico, da inventividade e criatividade da mente humana.

### 3.3.4 - Pós-exploração de falhas.

Na pós-exploração o atacante já conseguiu acesso ao alvo. Nesta fase são vasculhadas informações sobre o sistema invadido, arquivos interessantes, busca por elevação de nível de privilégio, pivoteamento, entre outros. A depender do objeto do contrato, a exploração pode avançar sobre áreas até então desconhecidas pelo atacante. O profissional contratado deverá apresentar “provas de conceito” que são justamente a demonstração da falha encontrada, da exploração feita dessa falha, bem como as implicações para a rede.

De forma simplificada, é possível incluir nesta etapa a confecção de relatórios dos processos e de seus resultados, a apresentação deles, bem como, se necessário, o treinamento das equipes sobre questões de cibersegurança.

Importa ressaltar que a correção das falhas encontradas nem sempre será de obrigação do Hacker responsável pelo teste. Comumente, isso é feito por desenvolvedores ou equipe interna e novamente checados após as correções.

## 4 - Conclusão.

Este breve artigo buscou trazer uma visão geral sobre a necessidade de adequação técnica exigida pelo art. 44 e seguintes da lei 13.709/2018 e temática da segurança cibernética, com foco nas principais ocorrências verificadas atualmente, assim como esclarecendo um pouco sobre em que consiste um processo de Teste de Penetração (Pentest), as figuras envolvidas, etapas, modo de realização.

Ainda são poucas as empresas que realizam esses tipos de testes, mas, à medida que cresce a importância da informação como ativo um coorporativo, juntamente com a própria necessidade (legal e comercial) de guarda e proteção dos dados, será cada vez mais comum a sua realização, se não permanente, ao menos periódica dessas avaliações. A falha na manutenção da segurança cibernética, em alguns casos, pode impactar na própria continuidade do negócio.

Vale sempre alertar que um teste de invasão bem conduzido não representa garantia de que nunca haverá problemas nessa área. Não há como garantir que redes acessíveis via internet estejam completamente imunes a violações.

O que se busca é a mitigação dos riscos e o contínuo aprimoramento dos processos. Nesse sentido, outras práticas devem ser somadas, a exemplo da implementação de políticas de segurança, treinamento de pessoal, manutenção das redes, fortalecimento da cultura corporativa de segurança, canais de denúncia, equipes preparadas para resposta imediata aos incidentes entre outras.

O Hacker Ético profissional deve ser inserido nesta realidade. Sua atividade deve sair do lugar “obscuro” e, muitas vezes, pouco compreendida para se tornar parte do processo produtivo, contribuindo para o desenvolvimento de um ambiente digital confiável, íntegro e disponível.

# REFERÊNCIAS

Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 05 fev. 2022.

https://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_computadores. Acesso em 27.04.2022.

https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Visitada em 27.04.2022.

https://owasp.org/www-project-top-ten/

CASELLI, Guilherme. Manual de Investigação Digital. São Paulo: Ed JusPodivm, 2021.

ENGEBRETSON, Patrick. Título original iIntrodução ao Hacking e aos Testes de Invasão: Facilitando o hacking ético e os testes de invasão. São Paulo: Ed. Novatec, 2014.

HINTZBERGE... [ET AL]; Tradução de Alan de Sá: Fundamentos de Segurança da Informação com base na ISSO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2018.

PINHEIRO, Patrícia Pack. Direito Digital, 7ª ed. São Paulo: Ed. Saraiva Educação, 2021.

SÊMOLA. Marco. Gestão da Segurança da Informação: uma visão executiva. 2ª ed. Rio de Janeiro: Elservier, 2014.

TANENBAUM, Andrew. Redes de Computadores. Andrew Tanenbaum, Nick Feamster, David Wetherall. 6ª ed. Porto Alegre: Bookman, 2021.

WEIDMAN, Georgia. Testes de Invasão: Uma introdução prática ao hacking: Ed. Novatec Editora Ltda, 2014.