FACULDADE DE TECNOLOGIA DE SÃO PAULO – FATEC-SP

THIAGO SOUZA COSTA

ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO DIANTE DAS MUDANÇAS CAUSADAS PELA PANDEMIA

SÃO PAULO

2022

FACULDADE DE TECNOLOGIA DE SÃO PAULO – FATEC-SP

THIAGO SOUZA COSTA

ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO DIANTE DAS MUDANÇAS CAUSADAS PELA PANDEMIA

Trabalho de Conclusão do Curso Análise e Desenvolvimento de Sistemas, apresentado a FATEC-SP, como exigência parcial para aprovação para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas

Orientador: Professor Edson Ceroni.

SÃO PAULO

2022

FACULDADE DE TECNOLOGIA DE SÃO PAULO – SP

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

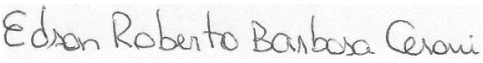
Parecer do Professor Orientador Edson Roberto Barbosa Ceroni
A pesquisa elaborada atende aos requisitos do trabalho de graduação composto por pesquisa bibliográfica e estudo de caso com análise de resultados.

Conceito/Nota Final: 9,0 (nove)

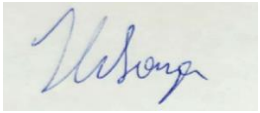
Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientador: Professor Edson Ceroni

SÃO PAULO, 27 de Junho de 2022.



_____
Assinatura do Orientador



_____
Assinatura do aluno

DEDICATÓRIA

Dedico este trabalho à minha família, amigos e professores pelo apoio que recebi durante esta jornada.

Resumo

COSTA, Thiago Souza. Estratégias de segurança da informação diante das mudanças causadas pela pandemia. 2022. Monografia (TCC) – Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de São Paulo, São Paulo. 2022.

Como todos sabem, a pandemia global sem precedentes que começou há dois anos trouxe diversas mudanças drásticas na forma que vivemos, na forma que saímos na rua, nos encontramos com amigos e parentes e trabalhamos. Devido a esse evento, muitas ideias, processos e negócios precisaram ser repensados, e um exemplo pertinente é a jornada de trabalho em casa (home office), seja parcialmente ou totalmente.

Esse conceito foi adotado por inúmeras empresas no Brasil e no mundo, mas ainda sim traz diversos questionamentos. Como evitar que dados pessoais e empresariais fiquem mais vulneráveis devido a essa mudança? Com a saúde mental fragilizada devido ao isolamento social, como impedir que essas pessoas sejam mais suscetíveis a cair em golpes na internet ou no telefone, e tenham seus dados violados? Esses são alguns exemplos de pontos críticos relacionados à segurança da informação que foram afetados pela pandemia e serão analisados neste documento.

Abstract

COSTA, Thiago Souza. Information Security Strategies in the face of the changes caused by the pandemic. 2022. Monography (TCC) – System Analysis and Development, Faculdade de Tecnologia de São Paulo, São Paulo. 2022.

As you all know, the unprecedented global pandemic, which started two years ago, brought many drastic changes to our way of living, the way we go outside, meet friends and relatives and the way we work. Due to this event, a lot of ideas, processes and business needed to be rethought, and a relevant example is the home office journey, partial or full period.

This concept was adopted by many companies in Brazil and around the world, but still brings forward many questions. How to avoid personal and business data from becoming more vulnerable due to this change? Since mental health is fragile because of social distancing, how to stop people from being susceptible to fall into frauds from internet or cellphone, and having their data violated? These are some examples of critical points related to information security which were affected by the pandemic and will be analyzed in this document.

Lista de Imagens

Lista de siglas e termos

ASP – *Active Server Pages*

ANPD – Autoridade Nacional de Proteção de Dados

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

CNI – Confederação Nacional da Indústria

Cracker – criminoso que invade um sistema de forma illegal

DBMS – *Data Base Management System*

DDOS – *Distributed Denial of Service*

DOS – *Denial of Service*

FSB – Empresa de comunicação do Brasil

HTML – *Hypertext Markup Language*

HTTP - *Hypertext Transfer Protocol*

HTTPS - *Hypertext Transfer Protocol Secure*

Infostealer – ladrão de informações, em inglês

IP – *Internet Protocol*

PHP – *Hypertext Preprocessor*

PDF – *Portable Document Format*

Scan – escanear, em inglês

SQL – *Structured Query Language*

Worms – notificações de atividades maliciosas na rede

Sumário

1. Introdução

1.1. Questão e Contexto atual

Como todos sabem, a pandemia global sem precedentes que começou há dois anos trouxe diversas mudanças drásticas na forma que vivemos, na forma que saímos na rua, nos encontramos com amigos e parentes e trabalhamos. Devido a esse evento, muitas ideias, processos e negócios precisaram ser repensados, e um exemplo pertinente é a jornada de trabalho em casa (home office), seja parcialmente ou totalmente.

Esse conceito foi adotado por inúmeras empresas no Brasil e no mundo, mas ainda sim traz diversos questionamentos. Como evitar que dados pessoais e empresariais fiquem mais vulneráveis devido a essa mudança? Com a saúde mental fragilizada devido ao isolamento social, como impedir que essas pessoas sejam mais suscetíveis a cair em golpes na internet ou no telefone, e tenham seus dados violados? Esses são alguns exemplos de pontos críticos relacionados à segurança da informação que foram afetados pela pandemia.

Um estudo realizado pela Ernst & Young (EY), uma empresa multinacional de serviços profissionais, apontou que oito a cada dez líderes sofreram algum impacto em suas operações em decorrência da pandemia de Covid-19, como com o aumento da incidência de ameaças cibernéticas, principalmente de *phishing*, *malware*, *ransomware* e ataques de negação de serviço [(1)]. Sendo assim, percebe-se que se os métodos empresariais passaram por uma adaptação, os métodos de crimes cibernéticos também se adaptaram, ao encontrar novas vulnerabilidades que surgiram, provando a importância de uma melhoria na segurança da informação, em um momento tão caótico como vivemos hoje.

No quesito de adaptação de empreendimentos, é inevitável que com a falta dos serviços e atendimentos presenciais, restaurantes, bares e comércios que conseguiram se manter abertos foram obrigados a inovar seu negócio. Portanto, softwares, sistemas e sites para suportar essa nova demanda de atendimento virtual ou via delivery foram algumas das alternativas mais usadas. Uma pesquisa realizada pelo Instituto FSB Pesquisa para a Confederação Nacional da Indústria (CNI) com amostra representativa de empresas grandes e médias do setor, mostrou que 93% das indústrias do país implementaram pelo menos um serviço de tecnologia e transformação digital dentro das suas rotinas [(2)], e continuou, afirmando que essas indústrias pretendem manter estes serviços para o próximo ano. Mais um ponto onde a cibersegurança deve ser considerada de extrema importância, para não haver transtornos entre essas empresas que ingressaram no mundo digital recentemente, que acabam sendo as mais vulneráveis em alguns casos.

1.2. Motivação

Levando em conta que atualmente, praticamente todas as informações do mundo estão conectadas digitalmente, e se integram cada vez mais, desde um pedido de comida via aplicativo a uma transação bancária importante. Sendo assim, pessoas e empresas são cada vez mais exigentes e receosas quanto à privacidade de seus dados. Portanto, o impacto de um acontecimento como a pandemia é algo que deve ser levado a sério, pois traz um panorama diferente em tudo que fazemos no nosso cotidiano.

Além das estatísticas recentes expostas logo acima, uma pesquisa realizada pela MZ, empresa de soluções de relações com investidores, com dados coletados pelo sistema de busca do site da Comissão de Valores imobiliários aponta que, no Brasil, os ataques cibernéticos aumentaram em 220% no primeiro semestre de 2021, quando comparado ao mesmo período do ano passado [(3)]. Portanto, percebemos que a cada dia surgem mais formas de violação de tais dados, e grande parte da população não está preparada para lidar e se prevenir desses ataques, e muitas pessoas não tiveram opção e se conectaram repentinamente neste universo tecnológico que existe, e a falta de conhecimento sobre o assunto as torna alvos mais vulneráveis ainda. Ainda mais que, em alguns casos, a tecnologia evolui mais rápido do que a capacidade dos seres humanos de se adaptar a esses avanços e usufruir deles de forma segura.

Para ter uma melhor base e estatísticas atualizadas sobre as ameaças tecnológicas existentes e a frequência com que elas aparecem, o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) faz estudos anuais sobre os números de incidentes reportados, que incluem qualquer tentativa de ataque, violação ou fraude de sistemas ou dispositivos.

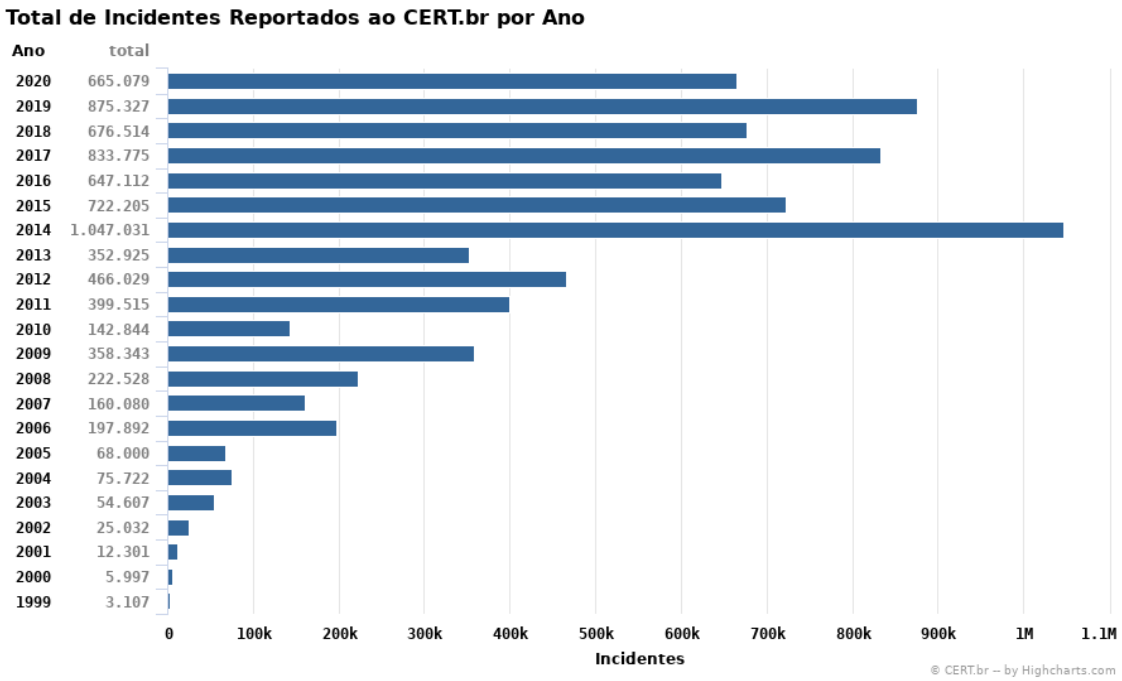


Figura 1 - Total de incidentes reportados em 2020. Fonte: www.cert.br

Nota-se no gráfico acima que apesar de ocorrer uma diminuição no número de incidentes de 2019 para 2020, ainda é um número alto e preocupante. No CERT não foram disponibilizadas estatísticas referentes a 2021 e 2022, devido a pandemia de COVID-19 que ainda ocorre.

Outro levantamento neste feito pela CERT neste mesmo contexto aponta que 59,85% dos incidentes reportados são referentes à *Scan*, ou seja, varreduras feitas em redes de computadores para identificar a atividade dos computadores e do serviço disponibilizado por eles, geralmente utilizado para identificar potenciais alvos; e 20,15% vêm de Worms, que são notificações de atividades maliciosas e a propagação automática de códigos maliciosos em uma rede. O ataque de negação de serviço (DoS) ainda ocupa uma posição relevante no estudo, sendo 10,25% dos casos.

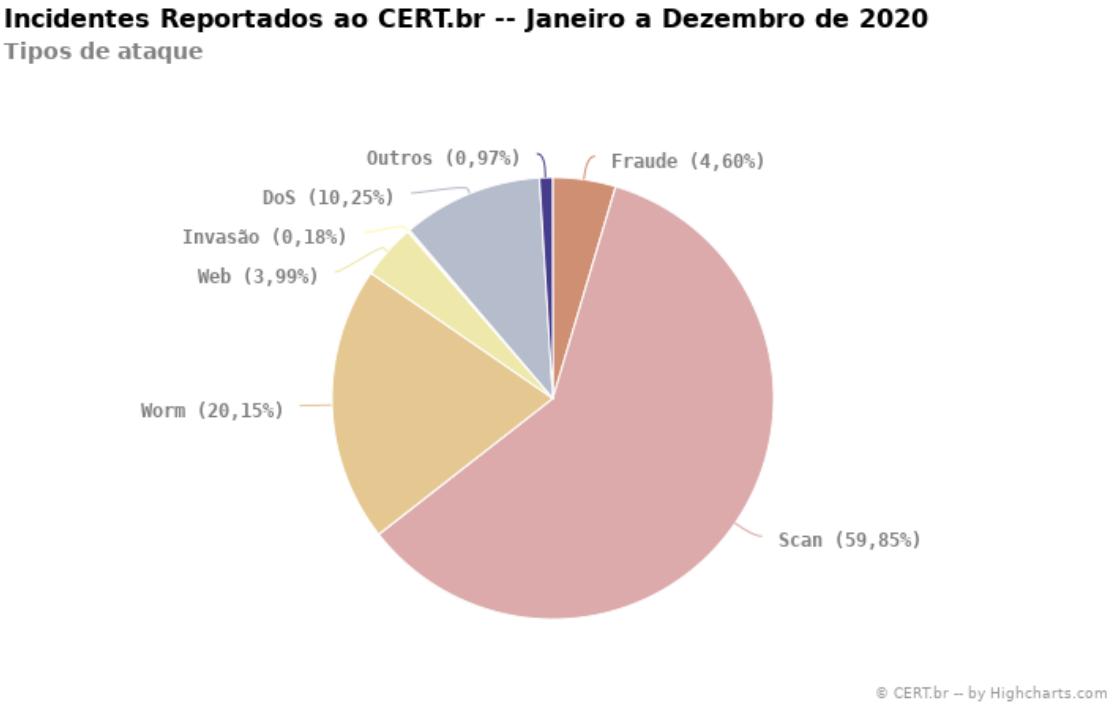


Figura 2 - Tipos de ataques reportados em 2020. Fonte: www.cert.br

1.3. Objetivo

Expor e analisar ameaças tecnológicas mais frequentes e estudar medidas a serem tomadas para melhorar a segurança de dados pessoais e empresariais, devido às mudanças de paradigma durante a pandemia da COVID-19, para prevenir crimes cibernéticos e violação de informações sensíveis, reduzindo possíveis impactos a curto e longo prazo no mundo digital.

1.4. Metodologia

1.4.1. Abordagem

A abordagem utilizada nesta pesquisa sobre segurança da informação se diversifica entre revisão bibliográfica e pesquisa documental para expor conceitos e os estudos mais recentes referentes ao assunto, e após a análise e interpretação dos dados obtidos, será possível utilizá-los como argumento em um estudo de caso a ser feito.

2. Conceitos Fundamentais

Este tópico tem como objetivo apresentar conceitos gerais sobre tecnologia e segurança da informação, para auxiliar na compreensão do contexto que envolve o tema desta monografia e no entendimento da ideia proposta.

2.1. Dado

É a menor forma de abstração de uma informação, mas que não possui significado sem um contexto para interpretá-lo. Segundo o dicionário Michaelis, pode significar “Aquilo que está disponível para estudo ou análise”, ou também “elemento que serve de base à solução de um problema”.

No contexto tecnológico, pode ser definido como “registros, fatos brutos coletados que não possuem qualquer significado ou contexto”. Sendo assim, para que lhe seja atribuído um significado, este dado deve ser interpretado, e então chegamos ao conceito seguinte.

2.2. Informação

É o dado interpretado, ou seja, a adição de um contexto ou significado a este dado. Para definir melhor, segundo o dicionário Michaelis, “reunião dos conhecimentos ou dados sobre um certo tema por meio de pesquisa ou instrução”. Portanto, nome, idade, peso de uma pessoa, são exemplos de informações sobre ela.

Com a globalização acelerada, e como tudo está interconectado atualmente, o valor da informação aumenta drasticamente. No contexto tecnológico, informação significa “reunião dos dados que, colocados num computador, são processados, dando resultados para um determinado projeto”. Informação, quando em posse de determinadas pessoas ou entidades possui um poder imenso, trazendo conhecimento a outros, seja este vindo de dados públicos ou privados, por meios legais ou ilegais. Podemos notar isso ao assistir telejornais, sobre a guerra na Ucrânia, pois quando algum evento importante ocorre, cada país quer passar essa informação de forma que consiga alguma vantagem, e os receptores são forçados a escolher o lado no qual vão acreditar.

2.3. Rede

O termo genérico define um conjunto de entidades interligados entre si, que permite circular elementos materiais ou imateriais entre estas entidades, de acordo com regras pré-definidas. Na área de tecnologia é o conjunto de computadores e/ou dispositivos interconectados que trocam informações na forma de dados numéricos.

É uma das principais portas de entrada para qualquer tipo de ataque cibernético. Quando acessamos a rede de internet, devemos tomar muito cuidado, pois assim como existe muitas informações úteis a serem encontradas, também existem coisas ruins e pessoas que desejam prejudicar a outras, roubando e sequestrando dados, ou fazendo ofertas enganosas.

3. Segurança da informação e principais conceitos

A segurança da informação é um conceito essencial no cotidiano, principalmente com os avanços tecnológicos e a facilidade do acesso à informação, o fato de conseguirmos realizar nossas atividades diárias, como compras e transferências bancárias, através de dispositivos que cabem na palma da mão. Também no quesito empresarial, as organizações dependem fortemente de um ambiente tecnológico e computacional para terem sucesso em seus negócios, e que mantém seus dados e aplicações de forma remota, com o sistema de armazenamento em nuvem, que está em um crescimento desenfreado conforme os anos passam. É o tema que cuida da defesa dos dados, e que garante que o acesso a estes dados será feito estritamente pelas entidades e indivíduos que possuem tal autorização.

O tema de segurança da informação tem cinco fundamentos principais: a confidencialidade, a irretratabilidade, a integridade, a disponibilidade e a autenticidade, os quais seguem a norma ABNT NBR ISO/IEC 27000.

Confidencialidade: envolve a proteção dos dados dos usuários contra acessos sem permissão, para preservar sua privacidade, de forma que apenas os usuários legítimos e outras pessoas autorizadas possam acessar estes dados. Também envolvendo dados empresariais, este requisito pode ser cumprido através de múltiplas autenticações e implementação de níveis de acesso.

Irretratabilidade: é a capacidade de provar que o usuário executou uma ação, como alterar um dado ou arquivo. Também conhecida como não repúdio, este fundamento possui forte relação com autenticidade e integridade.

Integridade: deve-se evitar que qualquer dado seja modificado indevidamente, e para isso, os sistemas devem ter uma estrutura sem brechas nem falhas de segurança que possam expor os arquivos a qualquer risco. Os softwares também devem manter sua integridade, para que funcionem normalmente e estejam sempre disponíveis ao usuário.

Disponibilidade: as informações devem estar disponíveis a serem acessadas a qualquer instante por aqueles que possuem a devida autorização

Autenticidade: se refere a legitimidade e autenticidade dos dados, onde nenhuma alteração, acesso ou realocação destes pode comprometê-la. E no caso de alteração, apenas pessoas autorizadas e que possuem um determinado nível de acesso podem realizá-las.

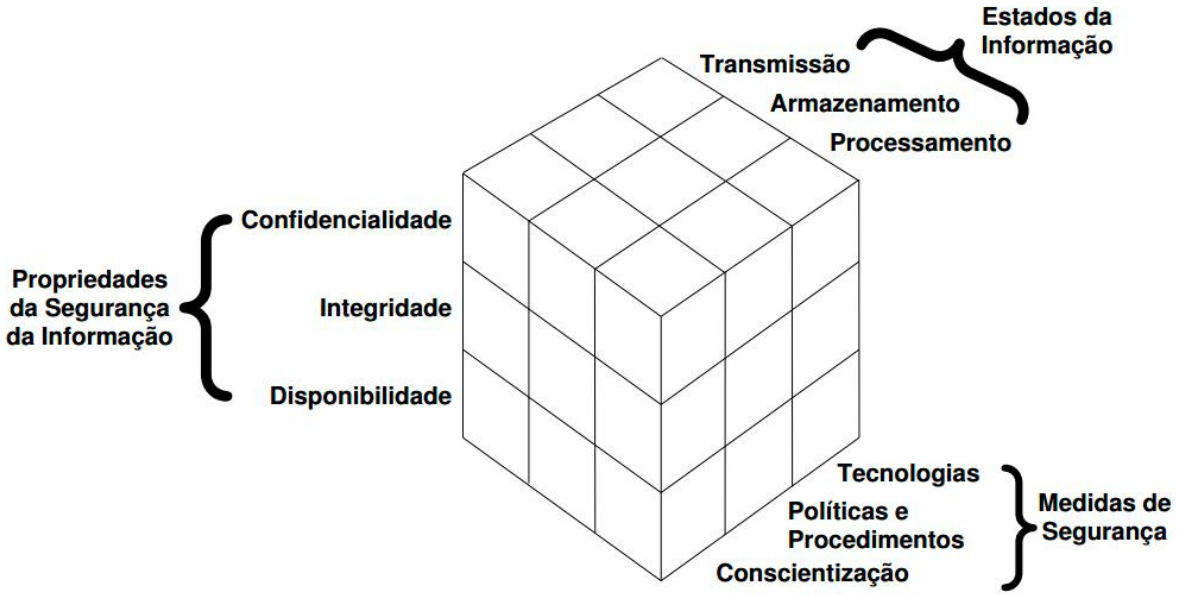


Figura 3 – Exemplo estrutural com os princípios da tecnologia da informação. Fonte: lumiun.com

Em complemento, existem alguns termos específicos, muitas vezes adaptados de outros idiomas, relacionados à segurança da informação que serão abordados neste trabalho. Portanto, sua compreensão é de igual importância para auxiliar ainda mais na assimilação dos fatos aqui descritos.

3.1. Lei Geral de Proteção de Dados (LGPD)

A LGPD, de número 13.709/2018, tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade dos indivíduos, e aborda a questão do tratamento de dados pessoais, estejam eles em meio físico ou digital, de pessoa física ou jurídica, de direito público ou privado.

Neste contexto, o tratamento pode ser realizado por dois agentes, o controlador e o operador. Existe também a figura do encarregado, indicado pelo controlador, que atua como o meio de comunicação entre o controlador, o operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No âmbito legal, tratamento de dados refere-se a qualquer atividade que utilize algum dado pessoal na sua execução, como coleta, produção, recepção, classificação, acesso, reprodução, distribuição e processamento. Durante o compartilhamento destes dados, a entidade ou órgão coletor deve informar com clareza qual o dado compartilhado e quem terá acesso a ele, enquanto o órgão que solicita acesso ao dado deve justificar o pedido, baseando-se em políticas públicas determinadas, descrevendo o motivo e qual a finalidade do uso destes dados.

Além disso, a lei cria uma estrutura legal que garante direitos aos titulares de dados pessoais, estes devendo ser cumpridos durante toda a extensão do processo de tratamento de dados, e prevê um conjunto de ferramentas, que tem como objetivo aumentar a transparência do processo, divulgar boas práticas na Administração Pública da lei e meios de proteger dados pessoais.

3.2. Acesso

Em um contexto geral é o “ato de ingressar, transitar ou consultar uma informação, podendo ser aplicada uma eventual restrição a este ato”, que define a confidencialidade da informação. No contexto tecnológico é a possibilidade da recepção ou transmissão de dados por meio de dispositivos computacionais.

Como exemplo, para estabelecer uma conexão com a internet, através do computador ou de algum outro dispositivo, é necessário que exista um provedor de internet conectado ao dispositivo, seja via cabo ou sem fio; um navegador que possua suporte a este tipo de rede e ao sistema operacional do dispositivo; entre outros requisitos. Sem o cumprimento destes requisitos, que podem variar em número, o acesso à rede não será estabelecido.

3.3. Ameaça

Em um contexto geral, ameaça, segundo Peltier (2010) [5], é um evento indesejável que pode danificar um ativo, causando impactos no negócio e nos resultados. Também a divide entre três grupos básicos: ameaças naturais, eventos da natureza como enchentes e furacões; ameaças humanas, que são originárias ou facilitadas por um agente humano, como eventos de fraude, erros ou vírus; e ameaças ambientais, que podem advir de ação do tempo ou poluição.

No ambiente de segurança de informação, ameaça pode ser descrito como qualquer fator capaz de causar danos à integridade, confidencialidade, autenticidade ou disponibilidade de dados ou informações de uma pessoa ou instituição. Alguns exemplos a ser citados e que serão explicados a seguir são: falha humana ou na política de segurança de informação da organização, ferramentas como malwares, *ransomwares* e *spywares.*

3.4. Ameaça Persistente Avançada (APT)

É um evento onde se utiliza técnicas avançadas de invasão de forma ininterrupta para acessar um sistema e permanecer nele por um período prolongado, quanto mais longo este período, maior o potencial de danos a serem causados.

A APT é uma categoria de ameaça que pode ser letal devido a sua natureza direcionada e eficácia. Esses tipos de ataques geralmente são realizados por grupos de hackers com bons recursos ou patrocinados por grandes instituições [26].

3.5. Banco de dados

Os dados que utilizamos no dia a dia, documentos, informações bancárias e outros tipos de informações e dados estão armazenados em diversos lugares, e não só na memória do ser humano ou em um caderno pessoal. E estes lugares podem ser chamados de bancos de dados.

Um banco de dados é uma coleção organizada de informações - ou dados - estruturadas, normalmente armazenadas eletronicamente em um sistema de computador, que é geralmente controlado por um sistema de gerenciamento de banco de dados (DBMS). Assim, os dados e o DBMS, juntamente com os aplicativos associados a eles, são chamados de sistema de banco de dados, geralmente abreviados para apenas banco de dados [10].

Os dados armazenados nos principais bancos de dados utilizados atualmente são estruturados em um sistema de linhas e colunas, que são alocados dentro de tabelas para facilitar a consulta, gerenciamento, modificação e controle destes dados. Além disso, a maioria utiliza a linguagem de consulta estruturada (SQL) como base para qualquer operação necessária.

3.6. Certificado Digital

O certificado digital é um recurso criado por meio da Medida Provisória de número 2.200-2 em Agosto de 2001, que vem se popularizando bastante com a digitalização de informações e procedimentos, onde legitima-se o acesso do usuário à uma certa página na internet, à arquivos ou até autentica um documento importante.

Sobre seu funcionamento, o arquivo com informações e dados provenientes de um órgão específico, empresa ou pessoa física, que agrega uma chave pública e uma privada é denominado Certificado Digital. Neste processo existe um órgão fiscalizador, a Autoridade Certificadora (AC), que autentica a chave pública com uma organização, emite o PGP (“Privacidade muito boa”, em inglês) e a assinatura eletrônica a ser validada pela empresa emissora. Este certificado garante que as informações transferidas, trafegadas e informadas de forma online são verídicas e confiáveis. Os usuários com este certificado possuem uma chave pública pessoal e intransferível, que permite o envio e recebimento de informações sem que terceiros interfiram ou visualizem as mesmas [11].

O funcionamento deste recurso se baseia na troca destas chaves simétricas entre a entidade e o órgão fiscalizador, que analisa as informações expostas e realiza a criptografia delas.

3.7. Criptografia

A criptografia é um recurso fundamental em segurança da informação e tecnologia, mas não necessariamente restrito a estas áreas, já que praticamente qualquer dado, informação ou texto pode ser criptografado. A ideia consiste em cifrar o dado desejado, com base em uma chave criptográfica, podendo ser composta de símbolos, cálculos ou anagramas, e assim transformando-o em um código que se torna incompreensível para quem não tem autorização ou não possui a chave de decriptação. É um método amplo e relativamente simples de proteger informações utilizado por diversas empresas e usuários, que podem incluir dados de pagamento ou até dados pessoais. Os softwares de criptografia utilizam algoritmos complexos para encriptar os dados, de modo que só possam ser desvendados com um grande esforço de processamento.

3.8. Firewall

A tradução literal do inglês é “parede de fogo”, e isto nos permite pensar na ideia de um meio que previne a entrada de qualquer dado nocivo no sistema. Segundo a Cisco [27], firewall é um dispositivo de segurança de rede que monitora o tráfego de dados e informações na rede e pode permitir ou bloquear tráfegos específicos de acordo com um conjunto pré-estabelecido de regras de segurança.

Existem diversos tipos de firewall disponíveis atualmente, alguns deles são o firewall de proxy, onde é associada uma passagem entre duas redes para uma determinada aplicação, o que pode afetar um pouco a taxa de transferência; firewall com inspeção de estado, o mais comum hoje em dia, que bloqueia ou permite acesso por meio do protocolo, da porta de acesso na rede e do protocolo, monitorando toda a atividade do início ao fim da conexão; e o firewall de gerenciamento unificado de ameaças (UTM), que utiliza funções de um firewall de inspeção de estado junto com os recursos de proteção antivírus.

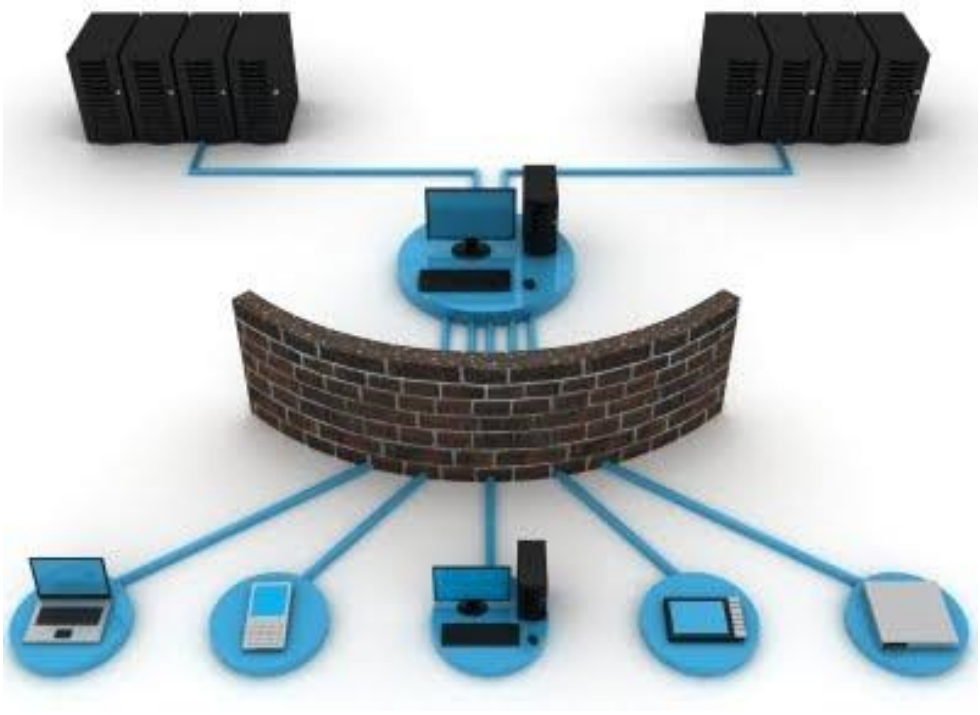


Figura 4 - Exemplo de estrutura de um firewall. Fonte: www.sites.google.com/site/genivaldosuporte/firewall-em-uma-rede

3.9. Log

A tradução direta do inglês, como já citado anteriormente, no contexto de tecnologia é “registro”. Para que um sistema, dispositivo ou aplicação possa funcionar adequadamente e ter uma maior facilidade na resolução de erros, é necessário que exista um recurso que registre as ações, mensagens e modificações realizadas por usuários ou administradores, e recurso é o log. Pode ser gravado em arquivo de texto, banco de dados, da forma mais conveniente de acordo com a necessidade. Além de ajudar na solução de problemas, também pode auxiliar também no rastreamento de vulnerabilidades, alterações indevidas no código do programa ou modificações na estrutura de dados do sistema.

3.10. Navegador (browser)

O navegador é o programa de determinado dispositivo ou sistema que viabiliza o acesso do usuário à rede de internet, que processa diversas linguagens, como HTML e ASP. A palavra em inglês browser vem do verbo *browse,* que significa “buscar, procurar”, e para acessar o site desejado, é necessário digitar o endereço virtual ou o link correspondente, se digitado corretamente a requisição de acesso é enviada, e é feita uma busca por este endereço. Após processada, o navegador do usuário recebe como resposta a página do site.

3.11. Vulnerabilidade

Em um contexto geral, vulnerabilidade, segundo o dicionário Michaelis, significa “algo frágil, que pode ser ferido ou danificado”. Já no contexto de segurança de informação, pode ser acrescentado nesta definição a ideia de que é algo do qual pode se obter vantagem, pois de acordo com a ISO 27000, de um conjunto de padrões e certificações voltada para a segurança da informação e proteção de dados, a vulnerabilidade é “uma fraqueza de um ativo que poderia ser potencialmente explorada por ameaças”. Complementando, ativos nesta área são recursos como softwares, hardwares ou sistemas que uma empresa possui, e o dano potencial que esta vulnerabilidade pode sofrer é chamado de risco. Alguns dos exemplos de vulnerabilidades são falhas na estrutura em si, como redes mal configuradas, aplicações com riscos à segurança expostos, e o principal deles: o fator humano.

3.12. Website

Um website, ou apenas site, é o conjunto de páginas web acessíveis online, que possuem uma determinada finalidade, sendo identificado por um URL único, que geralmente leva à página inicial do site.

Cada uma dessas páginas é escrita em código de programação, onde por meio de links (textos ou imagens clicáveis) o usuário é redirecionado para as outras páginas que o site possui. Além disso, o usuário pode utilizar motores de busca, como o Google, para encontrar a página que deseja com maior facilidade.

Após diversos avanços tecnológicos, existem recursos que permitem que um único servidor contenha ou hospede vários sites, diminuindo o custo do serviço de manter as páginas operacionais.

4. Principais ameaças

Neste tópico, elencamos as ameaças mais utilizadas por cibercriminosos nos dias de hoje para invadir sistemas e roubar dados sensíveis, explicando sua definição e informando exemplos com casos reais.

4.1. *Backdoor*

Em um sistema computacional ou software, *backdoor* (porta dos fundos, em inglês) é geralmente uma porta de acesso não listada, que é mais vulnerável por ser um meio de acessar informações rapidamente, sem enfrentar a maior parte das defesas do sistema.

O *backdoor* é um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada. Para esse fim, os códigos maliciosos podem explorar falhas críticas não documentadas existentes em programas instalados, falhas em softwares desatualizados ou no firewall, para abrir portas do roteador.

Um exemplo famoso de falha *backdoor* é o NetBus, que foi utilizado por diversos *crackers* (indivíduos que violam um sistema de segurança de forma ilegal) na década de 90. Outros exemplos conhecidos são o Bifrost, o c99Shell e o RST. Para evitar estas ameaças, deve-se manter os sistemas atualizados e o firewall ativo [28].

4.2. Cavalo de Troia (*trojan*)

Baseado no evento histórico da Grécia Antiga, onde foi utilizado um cavalo de madeira como um falso presente para Troia, pois possuía soldados escondidos dentro dele que, quando levado para dentro dos muros da cidade, foram os protagonistas da queda da cidade durante a Guerra de Troia. O conceito na área de tecnologia é o mesmo, onde oculta-se um programa malicioso dentro de um arquivo ou mensagem que aparenta normal e legítimo.

Os exemplos mais conhecidos são: o Cavalo de Troia de porta dos fundos, onde o arquivo camuflado cria uma porta dos fundos para acessar o sistema e roubar dados sensíveis do usuário; o Cavalo de Troia *downloader*, onde é feito o download de conteúdos maliciosos em adição ao conteúdo desejado pelo usuário, também como partes de malware; o cavalo de Troia *infostealer* (ladrão de dados, em inglês), cujo objetivo é roubar dados e informações do dispositivo infectado; e o cavalo de DDoS, que executa ataques de negação de serviço distribuído (tradução de DDoS, que em inglês significa *Distributed Denial of Service*), para derrubar a rede após sobrecarrega-la [23].

Em 2021, um cavalo de Troia direcionado a bancos conhecido como Mekotio, reapareceu e está infectando diversos dispositivos. Segundo o site de notícias de segurança CISO Advisor, pesquisadores da Check Point Research (CPR), divisão de inteligência em ameaças da Check Point Software, bloquearam mais de 100 ataques com esta ferramenta direcionados à países da América Latina, em apenas algumas

semanas. Os pesquisadores acreditam que grupos de cibercriminosos do Brasil e da Espanha tenham colaborado entre si para iniciar esta sequência de ataques [22].

O Mekotio, desenvolvido especificamente para sistemas Windows, utiliza táticas como e-mails falsos, que possuem aparência legítima. Quando o dispositivo é infectado, o cavalo de Troia fica oculto e inativo, aguardando o momento em que o usuário realiza um login em contas bancárias, e roubam seus dados.

4.3. Código malicioso

A definição de código malicioso, segundo Kaspersky [18], é um código ou *script* da web nocivo que tem como objetivo criar vulnerabilidades no sistema, gerando *backdoors*, violações de segurança, roubo de dados e informações, além de outros danos potenciais a sistemas de arquivos e computadores.

Por ser diferente de malware, os softwares antivírus geralmente utilizados não conseguem detectar nem bloquear esta ameaça. É um programa que se executa automaticamente e pode assumir diversas formas como plug-ins, controles ActiveX e aplicativos legítimos conhecidos, mas baixados de fontes não-confiáveis. O código permite que o criminoso cibernético consiga acesso remoto ao sistema sem permissão, podendo acessar dados sensíveis, senhas e até sequestrar dados.

4.4. Força bruta

Como o próprio nome já diz, a ideia é tentar diversas vezes violar uma senha ou sistema, utilizando padrões comuns, como data de nascimento, nome de parentes ou animais de estimação. Pode ser utilizado também para descobrir a chave usada para criptografar algum dado, e assim como citado no conceito de criptografia, dependendo da complexidade este processo pode levar de alguns segundos até anos.

Existem estratégias simples que auxiliam no combate a este tipo de ataque. Alguns hackers utilizam de dicionários para facilitar a busca, associando os caracteres especiais e números às palavras, utilizando senhas anteriormente vazadas na rede, ou dicionários especiais. Também existem ferramentas automatizadas que ajudam neste ataque, como Medusa e Brutus.

4.5. Injeção SQL

A definição mais simples é a manipulação e inserção de um código malicioso em SQL, linguagem utilizada em consulta de bancos de dados, para atacar websites ou aplicações e ter acesso a dados restritos dos usuários e modificar as principais funções do sistema.

Mesmo que estes ataques não sejam difíceis de evitar, são considerados uma grande ameaça que já prejudicou diversas empresas e meios de comunicação. Estima-se que mais da metade de todos os ciberataques dos dias atuais ocorreram

por meio de técnicas de injeção SQL. Um exemplo é o caso que ocorreu em 2008, onde dois hackers russos atacaram a Heartland Payment Systems, fornecedora de soluções que processam pagamentos, utilizando injeção SQL. Os dois criminosos conseguiram acesso a mais de 150 milhões de dados de cartões de crédito, o que causou um prejuízo ao negócio de mais de 300 milhões de dólares [24].

4.6. *Keylogger*

Se dividirmos a palavra e traduzirmos separadamente, *key* significa “tecla” e *log* significa “um registro de ações”, podemos dizer que este programa tem como objetivo gravar as informações digitadas pelo usuário em um teclado de computador. Ele se enquadra na categoria de *spyware*, onde o hacker consegue visualizar informações restritas como senhas, dados bancários ou informações pessoais. É comumente utilizado em ataques de *phishing*, um exemplo básico sendo um link solicitando para que o usuário altere a senha de sua conta, e para que isso seja realizado ele precisa digitar a senha anterior, que é capturada pelo *keylogger*.

Apesar de ser muito utilizado por criminosos cibernéticos, o *keylogger* é um recurso que também possui finalidades legítimas. Como para empresas que desejam monitorar atividades dos funcionários, ou para escritores de livros e artigos, onde caso haja uma queda de energia, o *keylogger* registra o conteúdo digitado e este pode ser recuperado posteriormente, evitando a perda de dados.

Um caso deste tipo de ataque ocorrido em 2022, foi de uma campanha que misturou arquivos em formato PDF com outros do sistema Office da Microsoft, que assim, confunde os usuários e os induz a instalação de um vírus keylogger. As mensagens, distribuídas em massa pelos criminosos, são recebidas por email. Apesar de ser um método de propagação de malwares diferente do usual, as empresas de segurança já estavam monitorando-o, para prevenir a disseminação de links maliciosos. Além disso, na campanha identificada pela HP, porém, o método aparece vinculado a um arquivo em formato do Word, com uma caixa de diálogo que aparece automaticamente no momento da execução do PDF e ainda acompanha uma mensagem afirmando que os dados foram verificados, como mais uma maneira de induzir o usuário a aceitar [25].

O que também chamou a atenção de especialistas foi o quanto a brecha utilizada pelos criminosos é antiga, que foi descoberta e solucionada em 2017. Além disso, a lentidão na atualização do Windows na época fez com que os hackers abusassem ainda mais dessa vulnerabilidade, demonstrando a importância de manter o sistema operacional dos dispositivos sempre atualizado, e o cuidado com os diversos e-mails enganosos que podemos encontrar em nosso cotidiano.

4.7. Malware

Conhecido também como software malicioso, é um conceito que descreve programas que ao entrar em um dispositivo, podem causar sérios prejuízos invadindo, danificando ou até incapacitando sistemas, redes, aparelhos móveis. Podem se esconder dentro de aplicações que aparentam ser legítimas, mesmo que sejam baixadas de uma loja ou site seguro.

Existem diversas formas e versões de malware utilizadas atualmente por criminosos, as principais são: os vírus de computador, que são malwares que se fixam a um programa que quando executado sem atenção pelo usuário, se replica, atacando outros programas e diversas partes do sistema, da mesma forma que os vírus que atacam seres humanos ou animais; o *ransomware*, que bloqueia o acesso ao dispositivo ou criptografa os arquivos do sistema, exigindo um pagamento de resgate para a devolução seja feita, tática muito utilizada pelos criminosos cibernéticos, já que a existência de criptomoedas possibilita um pagamento alto e uma grande dificuldade em rastreá-lo; e o *spyware*, que observa informações e dados do usuário sem autorização, permitindo a realização de fraudes com estas informações ou até a venda delas no mercado negro [(12)].

4.8. Malvertising

Abreviação da expressão que em português significa “propaganda maliciosa”, são os anúncios que carregam conteúdo nocivo, apesar de não serem considerados uma ameaça séria há alguns anos, as vítimas deste tipo de ataque vêm aumentando rapidamente.

A infecção por *malvertising* ocorre quando o usuário clica na propaganda ou realiza ações que redirecionam para sites maliciosos, que permite que malwares e vírus entrem no sistema ou algum software suspeito seja instalado. Em alguns casos, estas propagandas apenas instalam cookies de rastreamento, mas após a aprovação da GDPR, a equivalente europeia da Lei Geral de Proteção de Dados (LGPD), esta também se tornou uma prática ilegal [(13)].

4.9. Negação de serviço (DOS)

Ataques DOS (*Denial of Service*, em inglês), ou ataque de negação de serviço, tem como objetivo sobrecarregar um computador ou servidor, de forma que seus recursos fiquem indisponíveis para o acesso do usuário.

O método consiste no envio de múltiplos pacotes de dados para o dispositivo alvo, até que ocorra a sobrecarga, fazendo com que o sistema fique sem resposta para outras requisições. Os principais alvos deste tipo de ataque são os servidores web, mas não se caracteriza como invasão, visto que o hacker apenas desabilita o sistema para qualquer pessoa que tente acessá-lo, mas os invasores utilizam deste método para chantagear as empresas, requerendo determinada quantia em dinheiro para que o servidor volte a funcionar.

No ataque DOS, apenas uma máquina é utilizada para enviar os pacotes e causar a sobrecarga. Porém, existe uma variação onde um computador gerencia outros computadores, chamados de zumbis, a fazerem a mesma coisa. Esta variação é denominada ataque distribuído de negação de serviço, também conhecido pela sigla DDoS (*Distributed Denial of Service*, em inglês), e possui um potencial de impacto muito maior que pode afetar até os servidores mais potentes de sites conhecidos [14]. Abaixo temos uma imagem que demonstra a estrutura do ataque DDoS:

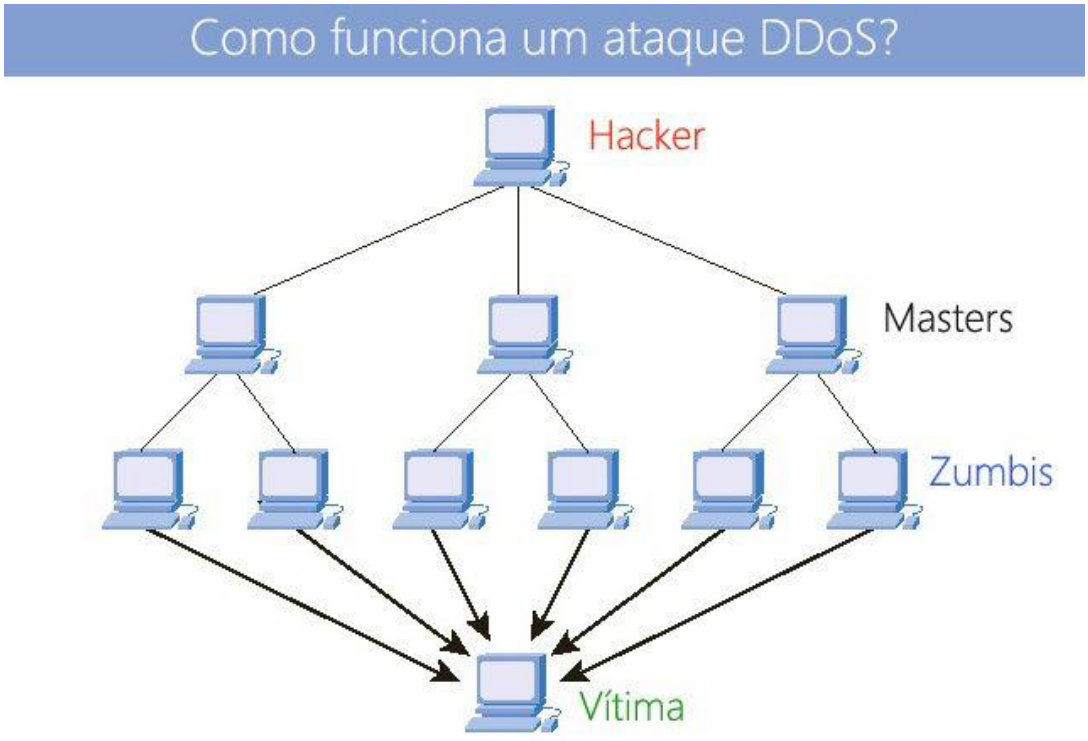


Figura 5. Estrutura de um ataque de DDoS (Imagem: Canaltech)

4.10. *Phishing*

Advindo de uma variação da palavra em inglês *fishing*, que significa “pescar”, *phishing*, é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito [15].

Existem diversas maneiras de utilizar este ataque, e diversos meios de comunicação para realizá-lo, como e-mails, aplicativos de mensagem, SMS, o que acaba aumentando cada vez mais o número de vítimas, sendo elas pessoas comuns ou grandes organizações. O usuário recebe uma mensagem ou e-mail, com um texto que aparenta ser de fonte confiável, com conteúdo persuasivo que induz a vítima a realizar ações, e estas ações envolvem o fornecimento de informações sensíveis como dados pessoais e bancários, ou o requerimento de um login com usuário e senha. Caso forneçam esses dados, os criminosos utilizam para roubar identidades ou apenas vendê-las no mercado negro.

Além disso, existe uma variação deste tipo de invasão, chamada *spear phishing.* A ideia é a mesma, mas o ataque é mais direcionado a um indivíduo, organização ou empresa específicos. Ambos os ataques utilizam táticas para chamar a atenção das vítimas, ou então engenharia social para criar mensagens personalizadas, que tem maior garantia de atrair a pessoa e induzi-la ao erro de seguir as instruções da mensagem [16].

4.11. Spoofing

Traduzido para português como “falsificação”, este método pode ser considerado uma variação do *phishing*, pois utilizam métodos enganosos e tentam ludibriar as vítimas para tirar vantagem delas. É um termo amplo para o tipo de comportamento em que um criminoso virtual se disfarça como um usuário ou dispositivo confiável para que você faça algo que beneficie o hacker e prejudique você [17].

Existem diversos meios utilizados por este ataque, entre os mais utilizados temos o *spoofing* de e-mail, onde são solicitadas informações pessoas ou dados de transações financeiras por meio de e-mails aparentemente confiáveis. Estes e-mails também podem conter cavalos de Troia ou malwares no seu conteúdo ou nos anexos, que são projetados para infectar toda uma rede.

Há também o *spoofing* de endereço IP (identificador de uma rede), que não se concentra em um usuário, como no *spoofing* de e-mail, mas sim em toda uma rede. Neste caso, o hacker tenta obter acesso ao sistema, enviando mensagens por meio de um endereço IP falso, fazendo que pareça ser de fonte confiável. Caso consiga o acesso, rouba informações pessoais ou sensíveis de usuários desta rede.

5. Métodos de Prevenção e defesa

Existem diversas formas de evitar que esses dados fiquem mais protegidos, tanto para pessoas comuns quanto para empresas, mas nem todas são acessíveis para quem precisa. Em alguns casos, pequenas e médias empresas apontam dificuldade para investir em cibersegurança, por questões de custo, que é um ponto a ser considerado. Entretanto, existem outras formas de tornar os processos mais seguros sem necessidade de aumentar muito os gastos. Segundo Roberto Rebouças, gerente executivo da Kaspersky no Brasil, deve ser avaliada a alternativa de automatizar processos de rotina e a escolha correta de tecnologias, reduzindo custos sem afetar a infraestrutura geral da empresa. Além disso, aumentar o foco em projetos que possam garantir a sobrevivência ou até o crescimento do negócio [(4)].

Por outro lado, mesmo com a Lei Geral de Proteção de Dados (LGPD) homologada neste ano, ainda existem muitas brechas a serem preenchidas, e incentivos do governo e de empresas maiores para dar maior suporte aos negócios com dificuldade em melhorar a segurança. Em um teor mais técnico, existem diversos métodos que se popularizaram muito durante a pandemia, divididos entre os âmbitos empresarial e pessoal, mas o nível de eficácia depende de cada necessidade. De tal modo, grande parte destas estratégias estão interligadas e não estão restritas a um ambiente específico, podendo ser eficiente e eficaz tanto para pessoas quando para grandes companhias.

5.1. Comportamento individual

Como já diziam e ainda dizem os filósofos, sociólogos e pensadores: para mudar algo, devemos começar mudando nós mesmos. Esta ideia comportamental também se aplica em segurança da informação, pois o fator humano está presente na totalidade das situações de vulnerabilidade. Existem diversos meios para prevenir e combater as ameaças citadas acima, dentre elas, algumas atitudes simples são: verificar a fonte de qualquer dado ou informação ao acessá-lo e antes de divulgá-lo para outros, utilizar senhas complexas e difíceis de decifrar, sem dados pessoais como data de aniversário ou nome do animal doméstico; não abrir links suspeitos, sejam eles enviados por parentes ou terceiros; não compartilhar contas de acesso a sites ou aplicações com outras pessoas, principalmente aquelas que contém dados como informações pessoais, contas bancárias ou cartões de crédito. Além disso, existem diversos recursos que melhoram a segurança dos dados, sendo eficiente também para usuários comuns.

5.1.1. Antivírus e Firewalls

Atualmente, a maioria dos novos computadores e dispositivos como smartphones já vem com um sistema antivírus e proteção de firewall por padrão. Entretanto, este serviço pode não ser muito eficiente ou não atender às necessidades do usuário. Para isso, existem inúmeras aplicações antivírus, gratuitas ou com assinatura, que podem ser baixadas e instaladas no dispositivo, algumas focam em um tipo específico de malware, outras em verificar constantemente os arquivos do computador para defender contra ameaças internas. Porém, deve-se tomar cuidado, pois também existem ferramentas de proteção ilegítimas ou que não possuem fonte confiável, e estas podem danificar ainda mais o computador e corromper os dados existentes nele. Há também casos em que os programas oferecem a instalação de outros serviços em conjunto com o desejado, então a atenção deve ser redobrada.

Os firewalls podem ser configuráveis de acordo com a necessidade, para restringirem um maior grupo de dados e monitorar com mais rigor o tráfego de informações através das regras de portas de rede do computador, ou então ser menos restrito e mais permissivo quanto ao fluxo de dados. Também pode ser configurado para permitir que um segundo dispositivo tenha acesso aos dados deste primeiro, caso estejam conectados a uma mesma rede, seja local ou remota.

5.1.2. Cópias de segurança

Também chamado de backup, é a ação de fazer cópias de segurança de um arquivo, aplicação, dados ou até um sistema inteiro, e realocar essas cópias em um ou mais dispositivos de armazenamentos diferentes, caso o dispositivo principal falhe. Armazenamento de backups em nuvem, sistemas de armazenamento virtual, é uma ideia bastante popular atualmente, além de ser mais segura, seu volume varia de acordo com a necessidade, e possui menor custo do que investir em diversos dispositivos físicos diferentes. Utilizar este recurso ajuda na proteção contra ataques que sequestram dados (*ransomwares*) ou ataques de negação de serviço (DoS), que ocorrem com mais frequência contra empresas. No caso deste último, pode ser contornado caso o sistema possua um servidor secundário, que entra em ação quando o principal, pare de funcionar corretamente, evitando assim o prejuízo e a perda de dados.

5.2. Entidades e organizações

5.2.1. VPN

Virtual Private Network (VPN), que significa “Rede Privada Virtual” é um recurso que permite que o usuário estabeleça uma conexão de rede privada, mesmo utilizando redes públicas. Seu funcionamento consiste no ocultamento do endereço IP do usuário, e assim faz com que a rede que o usuário se conectou, ao invés de redirecioná-lo utilizando seu próprio IP, o faz por meio de um servidor remoto específico, executado por um *host* (hospedador) de VPN. Entretanto, quando o usuário utiliza a internet, os dados buscados são fornecidos pela VPN em si, e seu provedor de internet não consegue visualizar os websites que o usuário visitou, nem os dados recebidos e enviados.

Utilizar uma VPN traz diversos benefícios, já que camufla seu tráfego de dados e protege contra acessos externos através da criptografia. Este recurso pode ser utilizado tanto por usuários comuns quanto por empresas, e para estas se tornou essencial, devido ao crescimento do trabalho remoto durante a pandemia. Por meio da VPN, funcionários conseguem acessar os sistemas internos e trabalhar remotamente, sem o risco de comprometer a integridade dos arquivos e programas que acessa.

5.2.2. Políticas de segurança e treinamento

Além dos cuidados diários necessários ao acessar dados e arquivos em um computador ou outro dispositivo conectado à internet, as grandes empresas estabelecem um conjunto de políticas e normas que devem ser seguidas, para que não ocorram violações de privacidade nem vazamento de informações através do fator humano da empresa, os funcionários. Mas não basta apenas estabelecer estas políticas de segurança, elas também devem ser difundidas nos ambientes da empresa, conscientizando propriamente os colaboradores e indicando o procedimento correto em qualquer operação a ser executada, seja dentro do ambiente da empresa (tanto fisicamente quanto virtualmente) ou fora dela.

Existem inúmeros métodos e políticas diferentes atualmente, que se adaptam de acordo com a necessidade da empresa e seus valores. Um exemplo é o modelo Confiança Zero (*Zero Trust*), estratégia proposta pelo analista John Kindervag.

Possui como estratégia a ideia de “nunca confiar, sempre verificar”, que indica como não podemos confiar cegamente nos outros, nem dar acessos sem que o usuário seja propriamente autorizado. Mesmo que o usuário já tenha acessado o sistema diversas vezes anteriormente, o processo de verificação não pode ser evitado [19]. O *Zero Trust* também pode ser expandido para o ambiente físico da empresa, com credenciais de acesso para entrar no complexo e para circular entre os prédios dentro dele, onde estas credenciais que identificam os colaboradores são geralmente crachás, porém a segurança é ainda maior em algumas empresas, ao utilizar a biometria como meio de acesso.

O processo do sistema de Confiança Zero também pode implementar análise, filtragem e registro para monitorar o comportamento do usuário, que caso realize alguma ação que indique um possível comprometimento, ele passa a ser identificado como uma possível ameaça. Um exemplo, Marcus na Acme Co. normalmente faz login em Columbus, Ohio, nos Estados Unidos, mas hoje ele está tentando acessar a intranet da Acme em Berlim, Alemanha. Este tipo de comportamento entra no padrão de ações suspeitas e força o usuário a confirmar sua identidade mais uma vez [19].

Complementando, esta estratégia é geralmente utilizada em conjunto com as VPNs, para permitir o acesso remoto dos funcionários, onde a rede do local de trabalho é isolada e só pode ser acessada a partir de uma autenticação de um ou mais fatores.

5.2.3. Computação em nuvem

Computação em nuvem, ou *cloud computing,* em inglês, é a ideia de executar aplicações, mover sistemas e arquivos para servidores em uma nuvem virtual, como o próprio Google Drive ou outros serviços de nuvem voltados para empresas, por exemplo a AWS. Traz vantagens como maior segurança, dada a grande dificuldade de violação destes servidores; e em caso de perda de dados, que podem ser recuperados caso este recurso seja utilizado em conjunto com as cópias de segurança [20].

Outros benefícios que são mais aproveitados pelas companhias que utilizam esta tecnologia são o menor custo, pois evita a necessidade de despesas com servidores físicos, melhor gerenciamento dos recursos necessários, sem precisar redirecioná-los para absorver picos de atividades em certos sistemas; maior agilidade em implementação de serviços e maior gama de tecnologias disponíveis para uso.

Segundo a AWS, divisão de serviços de tecnologia em nuvem da Amazon, existem três principais métodos de computação em nuvem, são eles:

Infraestrutura como um serviço: também pode ser abreviada como IaaS, e tem como objetivo manter os principais componentes de tecnologia em nuvem e usualmente, permite o acesso a recursos de rede e armazenamento de dados. Focado em melhorar o controle e gerenciamento dos recursos de TI na empresa

Plataforma como um serviço: tira a preocupação da própria empresa ter que gerenciar sua infraestrutura, como softwares e sistemas operacionais, contratação de recursos e manutenção de programas, e assim permite maior concentração em implantações e gerenciamento destas aplicações.

Software como um serviço: um produto completo, totalmente gerenciado pelo provedor. Quando utilizam este modelo, as pessoas geralmente se referem às aplicações de usuário final, além de não haver necessidade de planejar como o serviço será mantido ou sobre a gestão da infraestrutura, apenas em como o software será usado [20].

5.2.4. Controle de acesso

Este recurso, mais utilizado por grandes corporações e empresas de tecnologia, define níveis de permissão para acessar um tipo de arquivo ou sistema, impedindo que um funcionário mal-intencionado faça alterações indevidas; e na classificação da sensibilidade de documentos, desde uma tabela simples com dados simbólicos, até o plano de expansão dos negócios da empresa, com muitos dados secretos. Com isso, é possível monitorar documentos ou arquivos via email, principalmente quando enviado para endereços externos, além de reforçar a hierarquia da empresa.

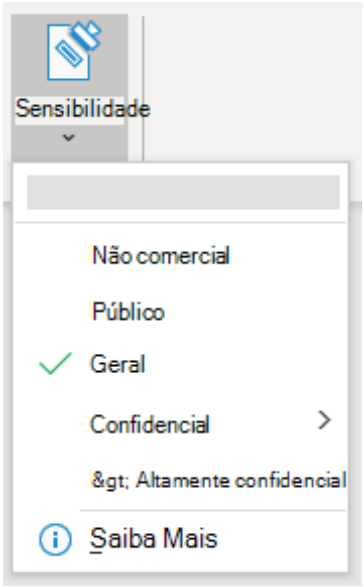


Figura 6 - Aplicando rótulos de confidencialidade nos arquivos e e-mails. Fonte: https://support.microsoft.com/

6. Estudo de caso

6.1. Caso CPFs - Receita Federal

A Receita Federal do Brasil (RFB), também chamada de Secretaria Especial da Receita Federal do Brasil, é um órgão único, responsável pela administração dos tributos devidos, tanto de pessoas físicas como pessoas jurídicas, e é subordinado ao Ministério da economia. Possui valores como o respeito ao cidadão, a integridade, profissionalismo e transparência. Além disso, o órgão é conhecido por realizar altos investimentos em tecnologia, sendo um dos primeiros a digitalizar completamente seus sistemas.

O Cadastro de Pessoa Física (CPF), segundo a própria RFB, é um banco de dados gerenciado pelo órgão, que armazena informações cadastrais de contribuintes obrigados à inscrição no CPF, ou que se inscreveram voluntariamente. É um documento com 11 dígitos numéricos que identifica e valida a cidadania de um indivíduo, além de permitir a realização de transações financeiras, compras online ou até empréstimos.

Em janeiro de 2021, houve um megavazamento de dados no Brasil, que expôs informações pessoais de 223 milhões de números de CPF, que foram postos à venda por criminosos cibernéticos no mercado negro. Foram dois vazamentos, onde um deles continha dados dos veículos e algumas informações de cada número de CPF atingido, e estes circulam livremente na internet, estando até disponíveis para download. O segundo vazamento, mais abrangente, é de difícil acesso e contém informações como dados de escolaridade, benefícios do INSS (Instituto Nacional do Seguro Social) e outros programas sociais (por exemplo o Bolsa Família), renda e pontuação de crédito do detentor do CPF.

Os criminosos pretendem vender o conjunto de dados obtidos neste vazamento, mas oferecendo apenas trechos dele. E para comprovar a autenticidade destes dados, publicaram alguns arquivos com mil amostras de cada informação

Dado que a população brasileira estar estimada em 214 milhões de pessoas, aparenta ser impossível existir um número de CPF maior que o do número de pessoas no país. Isto ocorre pelo fato de que os dados também incluem documentos de pessoas já falecidas.

A Autoridade Nacional de Proteção de Dados (ANPD), criada em agosto de 2020, um mês antes da Lei Geral de Proteção de Dados entrar em vigor, solicitou em fevereiro que a Polícia Federal abrisse uma investigação sobre o ocorrido. Entretanto, no período que ocorreu o vazamento, a agência ainda não estava em funcionamento, e a aplicação das medidas da LGPD não foram feitas. Após quase 3 meses de investigação, a Polícia Federal prendeu hackers suspeitos de colocar as informações à venda.

De acordo com a investigação, Marcos Roberto Correia da Silva, conhecido como "Vandathegod", foi o responsável por divulgar informações de 223 milhões de brasileiros. Na casa do segundo criminoso, Yuri Batista Novaes, a Polícia Federal apreendeu 4 terabytes de dados. Além disso, Marcos já foi denunciado por outras

invasões, como a invasão ao sistema do Senado Federal, ocorrida em agosto do ano anterior.

Ainda não foi descoberta a origem do vazamento. Existe a possibilidade em que os criminosos cruzaram informações de diversas fontes e de vazamentos anteriores, principalmente de órgãos do governo, para consolidar este pacote massivo de dados. Alguns dos dados tem referência a determinadas empresas, mas não se pode garantir que foram destas empresas que os dados foram roubados [21].

Apesar do caso ser inconclusivo quanto à fonte do vazamento ou os métodos utilizados pelos criminosos, estas informações estão armazenadas em bancos de dados do governo federal. Já foram reportados diversos incidentes do tipo anteriormente, como o caso de vazamento de senhas em novembro de 2021, e o comércio ilegal de informações cadastradas em programas governamentais como o Sistema Único de Saúde (SUS) e da Receita Federal denunciado em dezembro de 2021 [33]. Como a quantidade de casos vêm aumentando consideravelmente, fica a dúvida sobre o motivo deste aumento e se algo está sendo feito para combatê-lo.

Segundo um estudo realizado pela Axur, uma empresa de monitoramento e combate a riscos digitais na internet, foram identificados 465,5 milhões de dados vazados no segundo trimestre de 2021, principalmente de órgãos governamentais, mas também com presença de empresas privadas, com uma queda de 87,6% em comparação ao primeiro trimestre, mas com um aumento alarmante no vazamento de credenciais do governo, com aumento de 236,75% [34].

Deste conjunto de dados, o mais relevante foi o número de CPFs vazados foi o mais relevante, sendo 82,9% do total, com aumento de 89% em comparação ao trimestre anterior, com grande influência do megavazamento citado acima.

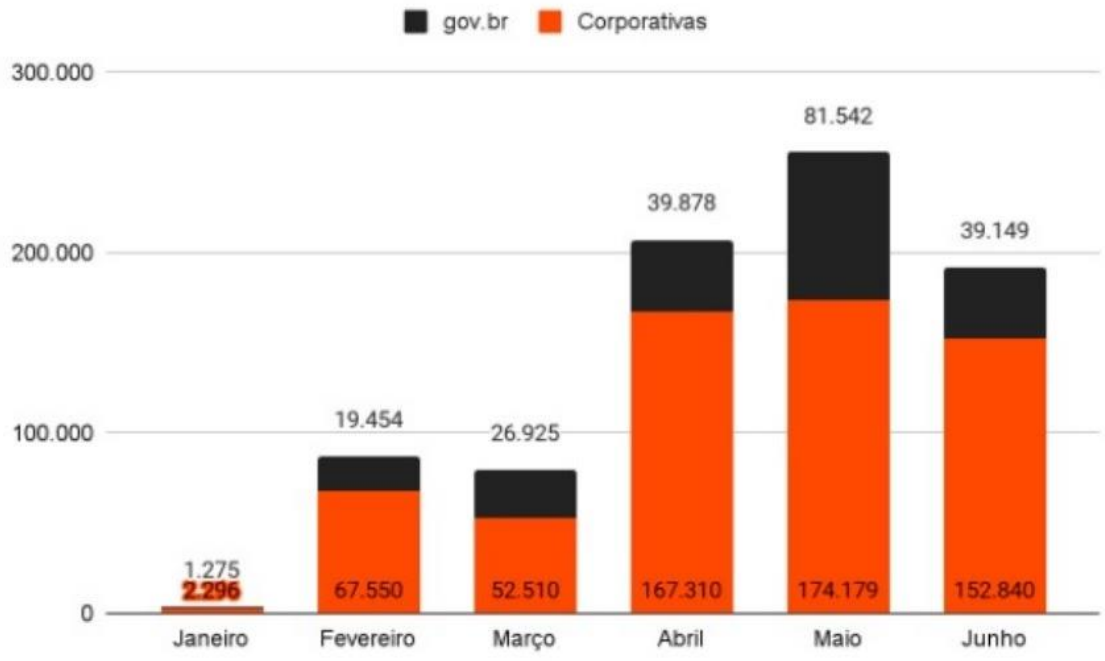


Figura 7 - dados sobre o vazamento de dados de janeiro a junho de 2021 - fonte: https://www.cisoadvisor.com.br/vazamento-de-dados-do-governo-cresce-237-no-2o-trimestre/

O total de credenciais expostas de empresas privadas e governamentais também sofreu aumento: entre abril e junho, a Axur levantou 181,5 milhões de casos, crescimento de 220% em relação ao trimestre anterior, e o principal responsável por este aumento é o vazamento de credenciais do governo, que foi de 47.654 no primeiro trimestre para 160.478 no segundo trimestre. O CEO da Axur, Fábio Ramos, indica que o aumento de casos de vazamentos não indica que os sistemas foram comprometidos, e comenta: “[...] há vários motivos para uma credencial ser vazada. Por exemplo, um ponto de atenção para a população é o uso do e-mail de trabalho para cadastros em sites com interesses pessoais.” (34).

Isto comprova uma negligência das autoridades governamentais para investir em melhorias de segurança e aprimoramento de seus sistemas, e acabam por tornar vazamentos como estes desastres anunciados.

Fabio Ramos, alguns meses antes, também afirmou que o principal erro do governo brasileiro ocorre na manutenção da segurança digital dos serviços que presta, principalmente ao comparar com o modo que é feito em empresas privadas, e diz que os principais motivos são o baixo investimento e os problemas burocráticos, onde um processo de licitação é tão longo e demorado que, quando homologado, a solução que era proposta nele já está obsoleta (32).

Sites governamentais são constantemente alvos de ciberataques devido à possibilidade de acesso a um amplo banco de dados, monetização rápida dos dados roubados, e o baixo investimento em segurança e infraestrutura cibernética do governo. Segundo Fabio Assolini, analista sênior de segurança da Kaspersky, os sites do governo não são necessariamente mais visados, mas chamam maior atenção por realizarem tratamento de dados públicos (32).

As principais vulnerabilidades de sistemas e sites, segundo a lista gerada pela Open Web Application Security Project, são: quebra de autenticação, onde o hacker consegue acessar o perfil de usuário utilizando senhas óbvias, que não são recomendadas pela maioria das empresas, justamente pela baixa segurança; exposição de dados sensíveis, quando o criminoso usa uma brecha na aplicação para acessar informações pessoais dos usuários; e configurações incorretas, com bancos de dados na nuvem sem camadas de proteção necessárias (32).

Sendo assim, os fatos apresentados nos levam a crer que levará um tempo considerável até que o governo tome as medidas necessárias para melhorar a segurança de seus sistemas e dos dados armazenados neles, pois há burocracia em excesso em praticamente qualquer processo, implementação ou mudança que necessita de aprovação, além dos desvios de dinheiro recorrentes em todos os setores, o que atrasa ainda mais esta melhoria e causa grande preocupação aos proprietários dos dados tratados nestes sistemas.

6.2. Caso Renner

A Lojas Renner, famosa marca de roupas no Brasil, sofreu um ataque de *ransomware* em seus sistemas em 19 de agosto de 2021. O *ransomware* tirou o sistema de lojas físicas da empresa do ar, além do site e do aplicativo de vendas online. Os criminosos exigiam o valor de 1 bilhão de dólares para liberar o sistema.

Um *ransomware* sequestra os dados de um sistema e os criptografam, impedindo o acesso a eles. E a partir disso, os criminosos solicitam algum tipo de resgate para que o sistema seja reestabelecido. A Renner retomou suas vendas online pelo site no dia 21 de agosto, e pelo aplicativo no dia 22, seguindo as orientações das autoridades e não realizando o pagamento do resgate aos criminosos [30].

Figura 8 - Tela do WannaCry, famoso ransomware que atingiu milhares de sistemas ao redor do mundo em 2017[30]

Segundo o site de notícias de segurança tecnológica CISO Advisor, o ataque utilizou um *ransomware* do tipo RansomEXX para a invasão, o mesmo utilizado anteriormente em ataques a outras grandes companhias como a Embraer e o STJ [30]. A JBS, uma das maiores empresas de processamento de carnes do mundo, também foi alvo deste tipo de ataque, e acabou pagando o resgate demandado pelos criminosos, atitude não-recomendada pelos especialistas em segurança cibernética.

Um relatório feito pela Check Point Research (CPR), empresa especializada em análises de segurança, afirma que as empresas que sofreram ataques de

ransomware tem gastos 7 vezes maiores em reparos do que o valor pago no resgate dos dados. Na pesquisa, foram analisados os custos adicionais, que geralmente não são contabilizados, causados durante e depois do ataque, e foi constatado que as perdas à longo prazo são muito mais significativas do que a maioria presume [35].

As análises também determinaram que os criminosos exigem um resgate que seja proporcional à receita anual da vítima, oscilando entre 0,7% e 5% deste valor. Além do mais, houve uma queda significativa na duração de um ataque de ransomware em 2021, de 15 dias para 9 dias [35].

No cenário do estudo realizado, os custos altos pagos por estas empresas incluem fatores como resposta e restauração dos sistemas e aplicações, trabalhos de rotina, gastos com advogados e com monitoramento. Sergey Shykevich, gerente do grupo de inteligência de ameaças da Check Point Software, comentou sobre o tema: “O principal aprendizado é que o resgate pago, que é o número com o qual a maioria das pesquisas lida, não é um número chave no ecossistema de *ransomware*. Tanto os cibercriminosos quanto as vítimas têm muitos outros aspectos financeiros e considerações em torno do ataque” [35].

Após o ataque, a Renner adotou uma metodologia de segurança em multicamadas, e o PROCON de São Paulo afirmou que a empresa também disseminou as ferramentas que são utilizadas neste processo [31].

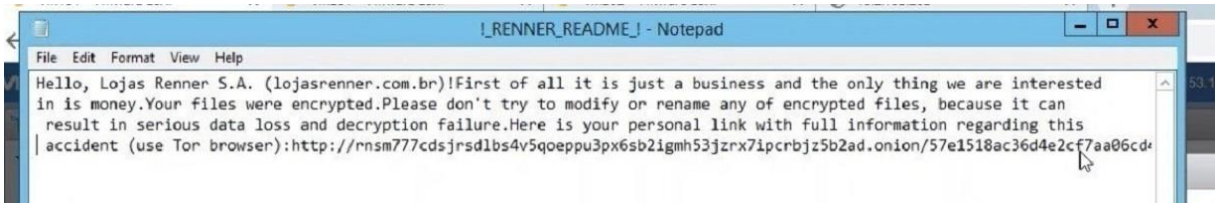


Figura 9 - Mensagem deixada pelos criminosos, solicitando o resgate pelos dados [30].

Outras mudanças importantes feitas pela empresa para evitar este tipo de situação foram a coleta de dados cadastrais de clientes através de criptografia com padrão internacional, e permitem que o usuário, de acordo com os termos da LGPD, solicite a atualização ou exclusão de informações pessoais do sistema [31].

Portanto, a ameaça de ataques por *ransomware* deve ser levada a sério, pois pode causar diversos danos à estrutura da empresa e altos prejuízos financeiros. A prevenção é a principal arma das empresas para combater este sequestro de dados, com a melhoria das políticas de segurança, evitando brechas causadas pelo mau uso das contas de acesso dos funcionários, e um planejamento detalhado de um método de resposta. Também é eficaz que a empresa tenha uma estratégia recuperação de desastres, contra este tipo de ataque e diversos outros que afete completamente os sistemas, que inclua em seus processos a realização de backup de arquivos de acesso e outros dados regularmente, assim como a implementação de um servidor reserva contendo os serviços e aplicações essenciais da empresa, sem conexão com o principal, para que possa ser ativado caso ocorra algum problema sistêmico.

7. Conclusão

A partir dos dados estatísticos analisados e dos casos estudados ao longo deste documento, pode-se observar que existem diversas ameaças tecnológicas “invisíveis” que requerem muita atenção, pois inicialmente parecem inofensivas, camufladas dentro de mensagens persuasivas e ofertas fora do senso comum, mas podem trazer diversos danos para as empresas e para os usuários comuns. O período de pandemia no qual ainda vivemos causou um impacto muito grande em tudo que fazemos, e na forma que fazemos. Fomos forçados pela situação a criar hábitos completamente novos, e no caso de empresas, adaptar seu negócio de forma que consiga continuar operando durante este período de adversidades.

Diante de um mundo tão interconectado, onde tempo é dinheiro e informações são muito valiosas, caso as pessoas e empresas não tomem medidas para proteger seus dados, seja por não achar necessário ou por algum outro motivo, sérios problemas poderão surgir, e podem se generalizar.

8. Trabalhos Futuros

Assim como a tecnologia avança com velocidade, onde diariamente surgem inovações em ações e processos que não imaginávamos ser possível, as novas ameaças também surgem em paralelo. Sendo assim, cria-se a necessidade de repensar cada vez mais, para se adaptar às novas tecnologias e às novas ameaças que elas trazem. Assim como não é possível determinar os limites do que a tecnologia pode alcançar, existe também um mundo de possibilidades, para criar ferramentas mais seguras, metodologias de desenvolvimento de software mais rígidas, monitoramento mais detalhado de processos, estratégias de resposta e prevenção contra ataques virtuais. Em suma, é essencial que ocorra um bom aproveitamento das inovações para tornar as informações do mundo digital, os processos existentes e os que podem surgir mais seguros.

9. Referências

1. *COVID-19: How future investment in cybersecurity will be impacted. EY Global*, 2020. Disponível em: www.ey.com/en_gl/consulting/how-the-covid-19-pandemic-is-impacting-future-investment-in-security-and-privacy. Acesso em: 15 de novembro de 2021.

2. 93% das indústrias adotaram serviços de TI no cotidiano durante a pandemia. Exame, 2021. Disponível em: https://exame.com/bussola/93-das-industrias-adotaram-servicos-de-ti-no-cotidiano-durante-a-pandemia/. Acesso em: 15 de novembro de 2021.

3. Ataques cibernéticos aumentaram 220% no primeiro semestre de 2021. Segs, 2021. Disponível em: https://www.segs.com.br/seguros/318700-ataques-ciberneticos-aumentaram-220-no-primeiro-semestre-de-2021. Acesso em: 16 de novembro de 2021.

4. BRANCO, Dácio Castelo. 40% das pequenas e médias empresas têm dificuldade de investir em cibersegurança. Canaltech, 2021. Disponível em: https://canaltech.com.br/seguranca/40-das-pequenas-e-medias-empresas-tem-dificuldade-de-investir-em-ciberseguranca-199842/. Acesso em: 15 de novembro de 2021.

5. PELTIER, T. R. Information security risk analysis, 3.ed. Auerbach Publication, 2010. 331 p.

6. A Segurança da Informação: os princípios. NETEYE, 2021. Disponível em: https://neteye.co/a-seguranca-da-informacao-os-principios/. Acesso em: 11 de junho de 2022.

7. Os pilares de segurança de informação nas empresas. Netsupport, 2022. Disponível em: https://netsupport.com.br/pilares-seguranca-da-informacao/. Acesso em: 10 de junho de 2022.

8. HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002, Brasport, 24 de janeiro de 2018. 256 p.

9. FONTES, Edison. Segurança da informação: o usuário faz a diferença. São Paulo, Saraiva, 2006.

10. O que é um banco de dados? | Oracle Brasil. Oracle Brasil, 2022. Disponível em: https://www.oracle.com/br/database/what-is-database/. Acesso em: 13 de junho de 2022.

11. Certificado Digital – Segurança e Informática. InfoEscola, 2022. Disponível em: https://www.infoescola.com/informatica/certificado-digital/. Acesso em: 12 de junho de 2022.

12. O que é Malware?. Malwarebytes, 2022. Disponível em: https://pt.malwarebytes.com/malware/. Acesso em: 13 de junho de 2022.

13. Malvertising: como se proteger?. CLS Informática, 2019. Disponível em: https://clsinfo.com.br/noticias/malvertising-como-se-proteger. Acesso em: 13 de junho de 2022.

14. COSTA, Matheus Bigogno. O que é DoS e DDoS?. Canaltech, 2014. Disponível em: https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/. Acesso em: 12 de junho de 2022.

15. O que é *phishing*? Tipos e exemplos de phishing. Malwarebytes, 2022. Disponível em: https://br.malwarebytes.com/phishing/. Acesso em: 14 de junho de 2022.

16. O que é *spear phishing?* | Definição e riscos. Kaspersky, 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/spear-phishing. Acesso em: 9 de junho de 2022.

17. O que é *spoofing?* Ataques de *spoofing* de IP e e-mail. Kaspersy, 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/ip-and-email-spoofing. Acesso em: 10 de junho de 2022.

18. *Internet Security Definitions* | Kaspersky. Kaspersky, 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions. Acesso em: 10 de junho de 2022.

19. O que é *Zero Trust?* | Modelo de Segurança *Zero Trust.* Akamai, 2022. Disponível em: https://www.akamai.com/pt/our-thinking/zero-trust/zero-trust-security-model. Acesso em: 17 de junho de 2022.

20. O Que é *cloud computing* (Computação em nuvem)?. Amazon Web Services, 2022. Disponível em: https://aws.amazon.com/pt/what-is-cloud-computing/. Acesso em: 17 de junho de 2022.

21. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. G1, 2022. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 18 de junho de 2022.

22. Cavalo de Troia Mekotio retorna por meio de hackers brasileiros. CISO Advisor, 2022. Disponível em: https://www.cisoadvisor.com.br/cavalo-de-troia-mekotio-retorna-por-meio-hackers-brasileiros/. Acesso em: 15 de junho de 2022.

23. O que é um cavalo de Troia?. Norton, 2022. Disponível em: https://br.norton.com/internetsecurity-malware-what-is-a-trojan.html. Acesso em: 13 de junho de 2022.

24. O que é uma Injeção SQL? Os 5 principais tipos. SoftwareLab, 2022. Disponível em: https://softwarelab.org/pt/injecao-sql/. Acesso em: 12 de junho de 2022.

25. DEMARTINI, Felipe. Campanha mistura documentos em PDF e do Word para instalar vírus que rouba dados. Canaltech, 23 de maio de 2022. Disponível em: https://canaltech.com.br/seguranca/campanha-mistura-documentos-em-pdf-e-do-word-para-instalar-virus-que-rouba-dados-216915/ Acesso em: 16 de junho de 2022.

26. Ameaça Persistente Avançada (APT): Como proteger a sua empresa. VNX Partners, 2022. Disponível em: https://vnx.partners/ameaca-persistente-avancada-apt/. Acesso em: 11 de junho de 2022.

27. O que é um Firewall? | CISCO. Cisco, 2022. Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html. Acesso em: 10 de junho de 2022.

28. Backdoor (porta dos fundos). O que são?. PSafe, 2022. Disponível em: https://www.psafe.com/blog/backdoor/. Acesso: 13 de junho de 2022.

29. Lojas Renner sai do ar após infecção com *ransomware.* Tecmundo, 2021. Disponível em: https://www.tecmundo.com.br/seguranca/223412-lojas-renner-sai-ar-infeccao-ransomware.htm. Acesso em: 19 de junho de 2022.

30. Ransomware: entenda o caso que abalou a Renner e conheça os diferentes tipos de ciberataques. UPX, 25 de agosto de 2021. Disponível em: https://www.upx.com/post/ransomware-renner/. Acesso em: 18 de junho de 2022.

31. MARQUES, Ana. Renner explica impactos do ataque de ransomware a pedido do Procon-SP. Technoblog, 1 de outubro de 2021. Disponível em: https://tecnoblog.net/noticias/2021/10/01/renner-explica-impactos-do-ataque-de-ransomware-a-pedido-do-procon-sp/. Acesso em: 18 de junho de 2022.

32. Por que sites do governo são alvo de tantos vazamentos de dados pessoais?. Uol, 3 de dezembro de 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/03/27/falha-seguranca-sites-do-governo.htm. Acesso em: 26 de junho de 2022.

33. Criminosos vendem por R$ 200 acesso a dados completos de milhões de brasileiros. Folha de São Paulo, 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/12/criminosos-vendem-por-r-

200-acesso-a-dados-completos-de-milhoes-de-brasileiros.shtml?origin=folha. Acesso em: 26 de junho de 2022.

34. Vazamento de dados do governo cresce 237% no 2º trimestre. CISO Advisor, 8 de setembro de 2021. https://www.cisoadvisor.com.br/vazamento-de-dados-do-governo-cresce-237-no-2o-trimestre/. Acesso em: 26 de junho de 2022.

35. MANCUZO, Ronnie. Depois de pagar resgate de ransomware, empresas ainda têm que gastar 7 vezes mais em reparos. Olhar Digital, 1 de junho de 2022. Disponível em: https://olhardigital.com.br/2022/06/01/seguranca/depois-de-pagar-resgate-de-ransomware-empresas-ainda-tem-que-gastar-7-vezes-mais-em-reparos/. Acesso em: 26 de junho de 2022