



UNICARIOCA

CURSO DE CIÊNCIAS DA COMPUTAÇÃO

JOSELINA OLÍMPIO RAMOS

SEGURANÇA DA INFORMAÇÃO

A ERA DIGITAL E A VULNERABILIDADE DOS DADOS NA REDE

Rio de Janeiro / RJ

2022

JOSELINA OLÍMPIO RAMOS

SEGURANÇA DA INFORMAÇÃO

A ERA DIGITAL E A VULNERABILIDADE DOS DADOS NA REDE

Trabalho de Conclusão de Curso apresentado à banca examinadora do programa de graduação em Ciências da Computação do Centro Universitário Unicarioca, como exigência parcial para a obtenção do diploma de bacharel em Ciências da Computação.

Orientador: Prof. Marcelo Perantoni

Rio de Janeiro / RJ

2022

SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado à banca examinadora do programa de graduação em Ciências da Computação do Centro Universitário Unicarioca, como exigência parcial para a obtenção do diploma de bacharel em Ciências da Computação.

Professor Marcelo Perantoni.

Orientador.

Prof^a Daisy Cristine Albuquerque da Silva, M.Sc

Professora Convidada

.

Professor André Luiz Avelino Sobral M.

Coordenador do Curso

Rio de Janeiro, 06 de JUNHO de 2022.

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem a autorização da universidade, do (a) autor e do orientador.

Dedico esse trabalho a Deus, aos meus mentores espirituais, porque ao longo desses 04 anos e meio não só me guiaram, por vezes me carregaram no colo, a minha santa mãezinha (*Im memoriam*), que muito lutou para que eu pudesse estudar, às minhas irmãs, ao meu amor e alguns amigos por todo incentivo ao longo dessa jornada.

#gratidão

AGRADECIMENTOS

E lá vem textão...

Deus obrigado pelo fôlego da vida.

Por ter me permitido vir na família Ramos. A minha mãe Luzia (*Im memoriam*) todo meu amor;

As minhas irmãs, hoje falta uma, por isso o dia não está completo, obrigada irmã Neves (*Im memoriam*) por tudo, inclusive por ter me acompanhado a av2 quando minha perna me traiu, a você, meu abraço bem forte.

Da mesma forma agradeço as demais irmãs: Sonia, Rosa, Nilzete, pela ajuda nos trabalhos, pelas orações, vocês foram meu ar.

Obrigado aos meus sobrinhos em especial Rodrigo por ter se colocado a minha disposição, o sendo meu motorista me conduzindo a unicarioca, quando andar virou um algoritmo complicado.

Obrigado a minha sobrinha Christye Ramos pela ajuda nos trabalhos de estatística e mais que isso, por ter feito um trabalho forte de fisioterapia, me restabelecendo em 05 sessões, quando meu ortopedista Dr. TISSIANO quis me parar por 03 meses devido a ruptura do tendão de Aquiles,

naquele momento só tive uma certeza, se eu parar, não conseguirei retornar, contrariando as ordens médicas, segui capenga;

foi um período complicado, tive um baixo desempenho, no período seguinte não foi diferente, devido as mais de 80 fisioterapias, trabalho e faculdade meu semestre também não foi produtivo, com isso perdi o FIÉS, e agora???

Segurei nas mãos de DEUS e fui...

No sexto e sétimo período fui aluna prata e ouro, fui representar minha instituição no ENADE, ali mais uma vez eu vi que minha luta era interna comigo mesma.

gratidão ao meu parceiro Aroldo pela paciência.

Gratidão aos meus amigos em especial a Vanderléia Dantas e a Andréa Serrano, por ter trabalho todos os sábados durante três meses seguidos, para que eu pudesse fazer o curso de extensão em me aperfeiçoar, Gratidão as amigas irmãs Leila Borges e Marcia Soeiro, por cada palavra de incentivo.

Gratidão ao amigo de turma Sérgio Felipe, quando na pandemia minha irmã partiu, segurou na minha mão e me ajudou a concluir aquele semestre tenebroso.

Gratidão aos professores da unicarioca principalmente ao Marcelo Perantoni por ter aceitado ser meu orientador, pela calma ao me direcionar ao fim desse trabalho.

Foram 04 anos e meio de muitas incertezas, eu sempre soube que o caminho não estava pronto, ele se faria com o meu andar, nunca pensei em desistir, por vezes achei que não conseguiria.

Espero fazer a diferença na segurança da informação, com amor me dediquei a esse curso, com esse mesmo amor vou trabalhar duro para colocar a tecnologia principalmente a Segurança da informação no patamar mais alto que puder, mas nunca acima do Homem.

Porque a máquina executar, mas quem cria é o Homem.

“Epígrafe...

Se cheguei até aqui, foi porque me apoiei no ombro dos gigantes.

Isaac Newton.

RESUMO

Um dos fatores mais importantes para uma empresa atualmente é a informação, pois a mesma é valiosa, tanto para o planejamento estratégico de uma empresa como para as tomadas de decisões. Em todos os casos, a obtenção de informação e seu correto uso é de suma importância para a empresa se manter no mercado em tempos tão competitivos. O presente trabalho discorrerá sobre a Segurança da Informação e como a mesma pode auxiliar as empresas na identificação de tais atos. Esse estudo se centrará em três pilares: Em primeiro se abordará as noções de engenharia social e segurança da informação além de tratar também da dimensão da informação nos dias de hoje para as companhias e indivíduos. Em segundo lugar, serão apresentados aspectos específicos do ser humano e sua vulnerabilidade, as aptidões do engenheiro social com suas principais artimanhas e alguns processos relevantes como treinamento e capacitação de funcionários. E por último, serão apresentadas sugestões de como se prevenir para não se tornar vítima do engenheiro social. O trabalho foi desenvolvido usando a revisão de literatura como metodologia, além de um estudo de caso em uma empresa. Como resultado...

Palavras-Chave: Engenharia Social; Segurança, Informação, corporativismo.

ABSTRACT

One of the most important factors for a company today is information, as it is valuable, both for the strategic planning of a company and for decision making. In all cases, obtaining information and its correct use is of paramount importance for the company to remain in the market at such competitive times. This work will discuss information security and how it can assist companies in identifying such acts. This study will focus on three pillars: First, the basics of social engineering and information security will be addressed, as well as addressing the size of information today for companies and individuals. Secondly, specific aspects of the human being and their vulnerability, the social engineer's skills with their main tricks and some relevant processes such as training and training of employees will be presented. And finally, suggestions will be presented on how to prevent yourself from becoming a victim of the social engineer. The work was developed using literature review as methodology, in addition to a case study in a company. As a result, ...

Keywords: Social Engineering; Security, information, corporatism.

SUMÁRIO

1. INTRODUÇÃO	10
2. SEGURANÇA DA INFORMAÇÃO E O RISCO DE DADOS NA REDE	11
2.1 Conceito de Informação.....	14
2.2 Covid 19 (Pandemia) X Aumento de Uso das Redes e Ataques Cibernéticos	15
2.3 Engenharia Social – Hackers	16
3. A VULNERABILIDADE DO ELEMENTO HUMANO	18
4. ALGUNS TIPOS DE ATAQUES	21
5. COMO PREVENIR AS VULNERABILIDADES DE UMA REDE	22
5.1. Como proteger a rede.....	24
6. OS PILARES DA SEGURANÇA DA INFORMAÇÃO	24
6.1 Propriedades de Segurança	25
6.2 Inventário Digital.....	28
6.3 LGPD Os principais pontos dessa lei são:.....	30
7. CRIPTOGRAFIA	32
8. INTELIGÊNCIA ARTIFICIAL e a SEGURANÇA DA INFORMAÇÃO.....	39
9. IA EM 2022 - TENDÊNCIA, RISCOS E BENEFÍCIOS	40
9.1 O Fenômeno chamado 5G	42
10. OWASP TOP TEN	43
11. ESTUDO DE CASO e ANÁLISE DOS RESULTADOS	46
12. CONSIDERAÇÕES FINAIS.	47
13. BIBLIOGRAFIAS:	47

1. INTRODUÇÃO

Nos dias atuais, o conhecimento e a informação são muito importantes para as empresas. Através das informações armazenadas em seus bancos de dados, as empresas podem otimizar o seu planejamento estratégico, tanto para as tomadas de decisões, como para se manter mais competitivas no mercado.

Valendo-se de tais informações, entretanto, alguns indivíduos conhecidos como Engenheiros Sociais, com intenções inescrupulosas, atuam com o intuito de prejudicar usuários quer pelo uso de chantagens, venda de informação sigilosa a concorrentes ou até mesmo por diversão.

Algumas empresas ficam vulneráveis, pois, a revelação de importantes informações sobre o seu negócio pode ameaçar a sua produtividade, confiabilidade e resultados. Será que uma melhor capacitação dos colaboradores que lidam com o trânsito de informações dentro de uma empresa evitaria o risco da ação de engenheiros sociais?

O objetivo deste trabalho é auxiliar os indivíduos na compreensão da ação do engenheiro social, tomando ações pontuais para evitar a sua atuação. Assim, o trabalho se estruturará por conceituar a Engenharia Social; abordar o elemento humano e sua vulnerabilidade, trazendo a importância do treinamento e capacitação; analisar os tipos mais comuns de fraudes e apresentar orientações específicas para evitar tornar-se vítima de tais ações.

Diante de tais aspectos, torna-se relevante em primeiro lugar conceituar a engenharia social e todos os recursos que esta tem usado para roubar informações. Outro fator é que o elemento humano é essencial para a proteção de informações, pois quanto mais avançados estiverem a tecnologia e os dispositivos de segurança, mais os invasores abusarão do elemento humano, buscando encontrar a sua vulnerabilidade.

Assim se faz cada vez mais necessários os investimentos em capacitação e treinamento, mas para tanto, precisa-se conhecer de forma mais plena possível as fraudes mais comuns utilizadas.

Geralmente, este assunto não é tratado como deveria pelas empresas o argumento de que estão se equipando com melhor tecnologia e se sentem protegidas pelos seus sistemas de *firewalls*, *anti-malwares*, sistemas de detecção de intrusão

(IDS), meios de autenticação cada vez mais eficazes, *tokens*, *smart cards*, biometria, dentre outros.

Entende-se que tais tecnologias são muito importantes, mas infelizmente, não há como se sentir totalmente protegido, pois o conhecimento do engenheiro social tem se tornado cada vez mais amplo, tornando assim necessário que haja constante inovação.

A ausência de conhecimento dos indivíduos em relação às técnicas de engenharia social é fator determinante no sucesso da ação do engenheiro social. Assim, a empresa deve prestar treinamento a todos os seus funcionários, tanto aos que estão ingressando como aos que já estão há um tempo em sua função.

2. SEGURANÇA DA INFORMAÇÃO E O RISCO DE DADOS NA REDE

A segurança da informação é uma área delicada dentro de uma empresa, pois está relacionada com a proteção de dados que são de extrema relevância para os processos da organização. O acesso de tais informações para pessoas indevidas ou não autorizadas pode causar um verdadeiro rombo e ser uma ameaça a prosperidade da empresa (SANTOS, 2018).

A referência da segurança da informação está relacionada à preservação de uma quantidade de informações, voltadas para resguardar o seu valor tanto para uma pessoa ou empresa. São básicos os gêneros da segurança da informação e suas características são a confidencialidade, integridade, disponibilidade e autenticidade, uma vez que não estão seguras e restritas a sistemas computacionais, indicações eletrônicas ou sistemas de armazenamento (SCHWARTAU, 2010).

De acordo com Peixoto (2006), a segurança da informação está relacionada com a proteção dos ativos da informação, evitando que haja acessos realizado de modo indevido e sem autorização. Em alguns casos, se faz necessário inclusive que se criem mecanismos que evitem as modificações não autorizadas, evitando a disponibilização das informações

A máxima se aplica a todas as perspectivas de sustentar as informações e dados. A segurança informática ou segurança de computadores está privada e relacionada com o de segurança da informação, abrangendo não apenas a segurança dos dados/informação, mas também a dos sistemas em SI (SANTOS, 2018).

Portanto a informação necessita ser protegida adequadamente para o âmbito organizacional:

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005, p.2).

A caracterização da segurança da informação está na referência do resguardo às informações de uma determinada pessoa ou corporação, isto é, empregar tanto as informações corporativas quanto as informações pessoais. Compreende-se por informação todo e qualquer continência ou dado que tenha valor para a pessoa ou organização. Ela pode estar resguardada para uso restrito ou evidenciada ao público para consulta ou obtenção (RUSSEL, 2013).

As atribuições estabelecidas das métricas para delineação do nível de segurança existente e, assim serem concebidas as bases para análise da melhoria ou o agravar da situação de segurança existente. A segurança de uma especificada informação pode ser prejudicada por fatores computacionais e de uso de quem pode usufruir a mesma, pelo espaço ou infraestrutura que a cerca ou por indivíduos ostensivos que tem objetivo de roubar, solapar ou comedir tal informação (SCHWARTAU, 2010).

De acordo com uma pesquisa quantitativa realizada por Bannwart, (2011), 53% das empresas no Brasil, mostram que os funcionários que trabalham diretamente com a manipulação de dados estão insatisfeitos com os mecanismos criados para dar à segurança da informação. Além disso, a pesquisa apontou também que 40% dos entrevistados já foram vítimas de algum tipo de invasão ou de roubo de informação.

A segurança da informação é formada por confidencialidade, integridade, disponibilidade, não repúdio e autenticidade. Confidencialidade é a garantia de que as informações chegarão ao destino proposto, integridade é a garantia de que a informação não sofrerá modificações, disponibilidade é a possibilidade de que tal informação estará disponível ao seu destino, seguindo os critérios anteriores e não

repúdio e autenticidade têm a ver com a responsabilidade final, garantindo a identidade e integridade de quem emitiu a informação. (PEIXOTO, 2006).

De acordo com Santos (2018), o sucesso de um negócio está justamente em armazenar informações e dados que lhe darão vantagens competitivas, levando a obtenção de resultados financeiros positivos. Assim, a proteção de tais informações é de suma importância, passando a ser inclusive considerado com um ativo da organização.

Os principais princípios da segurança da informação são:

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação pode ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. [...] a função da segurança da informação é viabilizar os negócios [...] (ABNT, 2005, p.2).

Recomenda-se então que cada indivíduo resguarde a segurança de seu computador ou dispositivo eletrônico com respeito a senhas e dados pessoais que facilitariam o acesso a contas em banco e cartões.

É explicado pelo Comitê Gestor da Internet no Brasil:

Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de e-mails; armazenamento de dados, sejam eles pessoais ou comerciais, etc. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2006, p. 1).

Segundo o Comitê Gestor da Internet No Brasil (2006), o engenheiro social buscará usar computadores de outras pessoas para atuar de forma inescrupulosa, disseminando lixo eletrônico nos e-mails, buscando danificar os equipamentos de várias pessoas por meio de vírus. Assim, com tal tecnologia é possível obter informações sigilosas de cunho geralmente financeiro.

A principal função da segurança da informação é a preservação da confidencialidade, uma vez que a empresa desenvolveu ao longo dos anos, técnicas

e recursos para atuar e produzir. Além disso, há muitos dados referentes a clientes, fornecedores e investidores que precisa ser protegido. Assim, se faz relevante que a empresa invista na proteção desses dados, para que possa salvaguardar os seus interesses.

2.1 Conceito de Informação

A informação significa uma evolução de ideias que resulta na compulsão e organização de dados, de forma que representa uma conversão no conhecimento do sistema que recebe. Por meio da informação pode-se realizar planejamento futuros ou as devidas tomadas de decisão (SANTOS, 2018).

Enquanto conceito ela representa variadas significações, no uso do dia a dia ao técnico. De uma forma universal, o conceito de informação tem como propósito: restrição, comunicação, instrução, dados, forma, controle, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento (ALLEN, 2006).

Observa-se com o código de prática para a gestão da segurança da informação que diz:

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS-ABNT, 2005, p.2)

Para uma organização a informação é um patrimônio que sempre está em constante risco, pois ela representa a ideia competitiva do negócio, sendo reconhecida como um ativo crítico para o desenvolvimento da operação e saúde da empresa, por isso seu valor é de extrema importância e precisa ser protegida (SANTOS, 2004).

“A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa.” (PEIXOTO, 2006, p. 37).

2.2 Covid 19 (Pandemia) X Aumento de Uso das Redes e Ataques Cibernéticos

É importante destacar que, devido à covid-19, houve aumento no uso de recursos computacionais. O futuro chegou antes do que prevíamos. Porém, percebemos que apesar das diferenças sociais aprendemos de certa forma a conviver com o novo. A Internet das Coisas, que vem sendo falada há algum tempo, já é uma realidade. Utilizamos recursos computacionais para agendamento e até consultas médicas, realizamos compras, acessamos aplicativos de bancos, estudamos, entre tantos outros serviços que utilizamos de forma online. Além disso pessoas passaram a trabalhar remotamente. É indiscutível que com o crescimento e popularização da tecnologia, os ataques cibernéticos também cresceram consideravelmente.

A Figura 1 mostra o crescimento do uso de internet para compras e serviços e dos ataques de engenhheiros sociais. <https://olhardigital.com.br/2020/08/21/noticias/pandemia-impulsiona-aumento-de-compras-online-no-pais/>

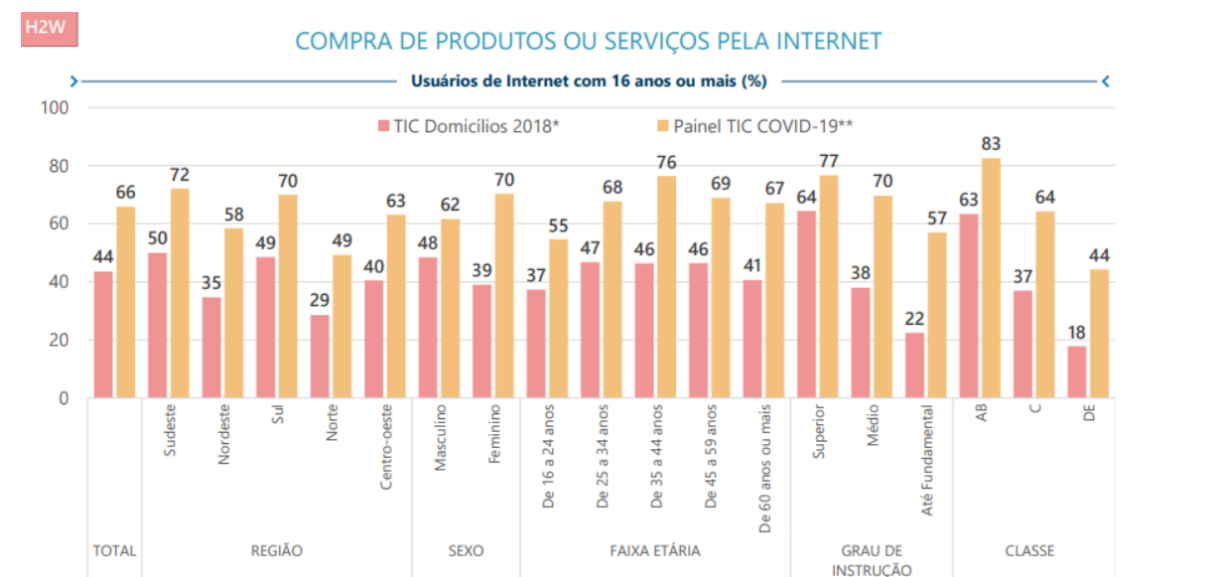
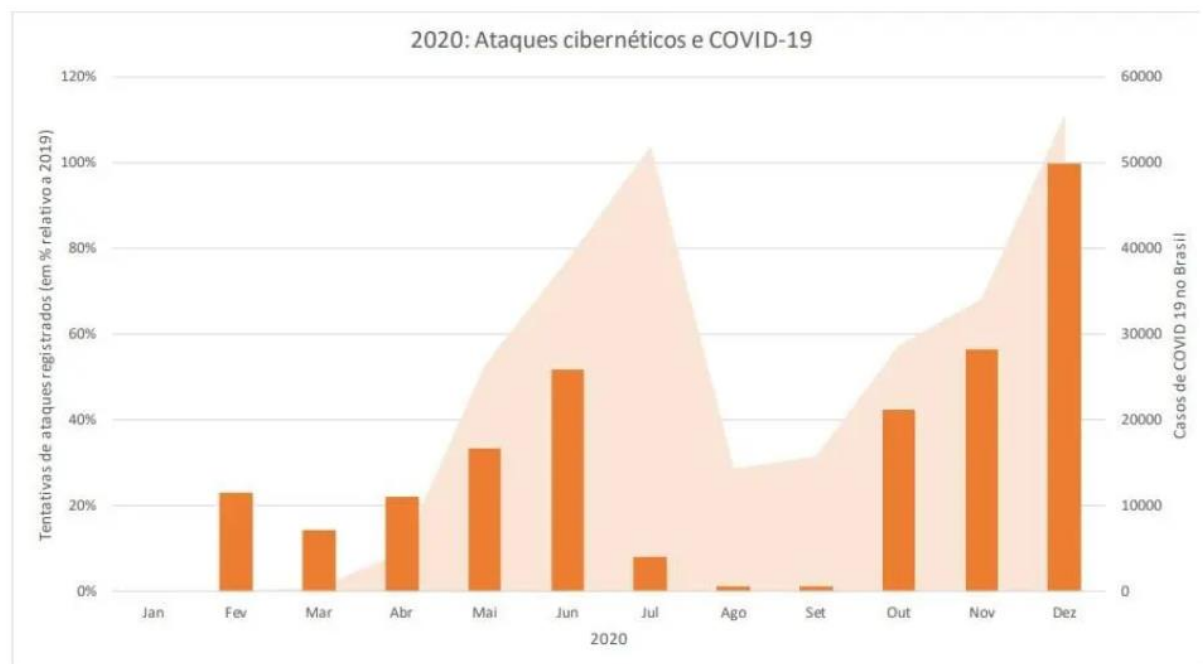


Figura 2 - Estudos mostram que os ataques cibernéticos no Brasil cresceram 860% na pandemia. figura extraída em 18/05/2022 do site <https://inforchannel.com.br/2021/03/03/ataques-ciberneticos-no-brasil-crescem-860-na-pandemia/>



2.3 Engenharia Social – Hackers

Engenheiros Sociais, no contexto da Segurança da Informação, são criminosos virtuais que induzem a usuários desavisados a enviarem dados confidenciais. Pode-se definir o termo Engenharia Social, por avaliar o sentido das suas palavras que a compõe: Engenharia, que está relacionado a aplicação de conhecimentos científicos e empíricos, criando-se uma estrutura adequada para o atendimento de uma necessidade humana e Social, que tem a ver com relativo ao uso da sociedade. Assim, a Engenharia Social, nada mais é do que a prática de construção de táticas para se obter informações sigilosas, de modo indevido (MARTORINI, 2012).

Engenharia social é uma manipulação psicológica que o indivíduo utiliza para obter informações a algo que ele deseja, este conceito tem uma aplicação muito mais voltada para sistemas de informação. Começaram a utilizar este termo na computação devido à descoberta de senhas de computadores, informações a respeito de contas bancárias, em fraudes na internet (PEIXOTO, 2006).

Este termo de uma forma geral está sempre voltado para obtenção de informações de uma maneira indesejada por quem se torna alvo daquele de quem está utilizando.

Conforme Silva (2008), engenharia social é o termo usado para conceituar a prática de obter informações sigilosas de empresas e pessoas com o objetivo de enganá-las ou de tirar algum proveito. Em 1990, esta prática ficou conhecida por meio de um *hacker* chamado Kevin Mitnick.

Visto utilizar conhecimentos tecnológicos para acessar informações, invadindo a vida social das pessoas, parece pertinente este ato ser chamado de Engenharia Social (SANTOS, 2004).

Segundo Peixoto (2006, p. 36), “A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação”. Assim, o engenheiro social combina vários fatores com o propósito de manipular e causar estragos financeiros profundos.

Para Peixoto (2006, p. 37), os ataques da engenharia social podem ser classificados como: diretos e indiretos:

Ataques diretos: De maneira que o nome diz, são aqueles realizados pelo contato direto no meio do engenheiro social e a vítima por intermédio de telefonemas, fax inclusive pessoalmente. Isso faz com que o engenheiro social faça uma ação de planejar antecipadamente e nem esmiuçado, diante de um segundo meio para caso o primeiro não se concretize, além de muita inovação e junção para que o esquema seja bem prosseguido. Ataques indiretos: dar consistência pela utilização de softwares, ou ferramentas para invadir como, por exemplo, vírus, cavalos de troia ou por meio de sites e e-mails inverídicos para sim alcançar informações almejadas.

Segundo Martorini (2012), o Engenheiro Social, irá reunir suas capacidades técnicas com o objetivo de enganar sua vítima, de modo persuasivo, levando a total credulidade. Assim, esse profissional possui talento, tanto tecnológico, como de persuasão, com o propósito de enganar pessoas.

Nota-se então que qualquer ataque de engenharia social é exclusivo, com a probabilidade de abranger diversas fases/ciclos ou até aquele acréscimo o uso de outros meios de ataque mais corriqueiras para alcançar a conclusão desejada. Assim

se faz relevante que as empresas invistam em segurança, não somente no que se refere a softwares, mas também no treinamento e na capacitação dos seus funcionários, uma vez que eles podem apresentar alguma vulnerabilidade.

2. A VULNERABILIDADE DO ELEMENTO HUMANO

Às vulnerabilidades relacionadas à segurança da informação estão presentes nas organizações das instituições, técnicas, físicas e humanas. É possível dividir a vulnerabilidade humana em três aspectos, são eles: Humanas, Físicas e Técnicas.

Falhas Humanas - O erro do usuário pode expor dados confidenciais criando pontos de acessos onde invasores acessem o sistema. Acontece de o próprio usuário acessar arquivos maliciosos que facilita a intrusão na rede e a perda de dados e informações, isso pode acontecer por falta de conhecimento, falta de atenção ou mesmo intenções maliciosas dos colaboradores.

Falhas Físicas – Acontecem através da desatualização dos processos gestão da segurança, essa fragilidade se manifesta em diversos pontos, como software, nos hardwares e equipes despreparadas. Importante o usuário memorizar sua senha para não ficar anotada em condições de ser usada por terceiros, a senha deve ser pessoal e intransferível. A falta de controle minucioso dos acessos autorizados a usuários, falha no backup.

Falhas Técnicas – Não estabelecer regras claras de políticas de segurança, é necessário determinar e documentar qual conjunto de ações práticas e técnicas relacionadas ao uso seguro dos dados, estabelecer o que não pode ser feito com relação as informações internas, não se deve acessar e-mail pessoal ou redes sociais no ambiente corporativo essa liberdade faz com que a empresa perca o controle dos sites acessados pelos funcionários.

Á ciências destaca o ser humano como elemento mais vulnerável, sendo ele indispensável na gestão de segurança. Não tem como criar ferramentas que protejam o humano, igual se cria para componentes técnicos e físicos. Como foco nas ameaças e incidentes causados pelo fator humano.

A falha humana sendo a mais frágil e fácil de ser explorado, os erros humanos podem expor dados confidenciais, em pontos de fácil exploração pelos invasores. A falha na rede com hardware ou software expõe uma possível invasão de terceiros. Ex. ponto de acesso wi-fi inseguros, firewall mal configurado. A vulnerabilidade de software ou sistema operacional expõe riscos que pode ser utilizado para ataques. Ex. software desatualizados.

Físicas – Instalação do prédio, controle de acesso.

Naturais – Fatalidades como incêndio, falta de energia.

Humanas – Não haver treinamentos frequentes, não deixar clara a política de segurança da empresa, equipamentos de segurança espalhados, funcionários insatisfeitos, isso tudo é uma ameaça.

Hardware - Mau instalação e falta de manutenção podem causar problemas na produção.

Software – software desatualizado pode causar impacto nos negócios é importante mantê-lo atualizado, dentro dos padrões de qualidade.

Mídias Digitais – Não utilizar dispositivo externo não autorizados, pois, pode comprometer confidencialidade, integridade e a disponibilidade do sistema.

Os Principais Tipos de Ataque

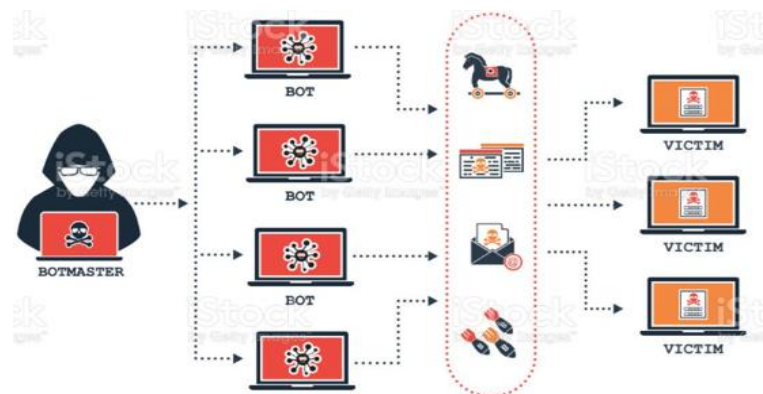
Dos ataques maliciosos existe o que sobrecarrega um servidor ou computador, esgota seus recursos como memória e processamento, tornando-os indisponíveis. Além de outros ataques cibernéticos que são uma tentativa de desabilitar computador as vezes concluído, rouba dados ou usa um sistema de computador para lançar ataques adicionais. Os criminosos virtuais usam de métodos diferentes para atacar sistemas entre eles estão: malware, phishing, ransomware, ddos, cavalo de tróia, dma, sql injection.

Injeção de sql – ocorre quando um invasor insere um código malicioso em um servidor que usa sql e força o servidor a revelar informações que normalmente não são reveladas. Um invasor pode injetar um código malicioso para caixa de pesquisa de sites vulneráveis.

Phishing – envia comunicação fraudulentas que da impressão de ser fonte de confiança, através de e-mail o objetivo é roubar ou obter dados confidenciais, como cartão de crédito e informações de login ou instala um malware na máquina da vítima.

Ddos – (Distribute Denial of Service) esse ataque derruba sistemas e servidor on line sobrecarregando a conexão, essa técnica consiste em derrubar um IP específico direcionando um grande tráfego de requisições em pouco tempo, aumentando as tentativas repentina de conexão utilizando máquinas invadidas por malwares chamado de zumbi. Ultimamente tem se falado muito desses vírus por derrubar grandes sites e redes sociais como twitter, esse aumento se deu por conta da internet das coisas, assim quanto mais dispositivos para se conectar mais chances de ser vítima desse ataque, sendo realizados a partir de sites de empresa esse tipo de ataque torna o servidor indisponível aos usuários. Para executa este ataque, os hackers contam com um grupo de máquinas denominadas BOTNETS.

Figura - 3 Extraída em 27/05/2022 do site: <https://sempreupdate.com.br/google-usa-aprendizado-de-maquina-para-impedir-ataques-ddos/>. a imagem configura o ataque do Botmaster infectando outras máquinas com diversos tipos de malware, cavalo de tróia, phishing entre outros.



BOTNETS é uma rede de computadores infectados que podem ser controlados remotamente e forçados a enviar spam, espalhando malwares ou ataques Ddos sem o consentimento dos usuários dos dispositivos.

Tipos de ataques Ddos

Inundação syn – Pacotes acima de 250 bytes ao mesmo tempo esgotam os recursos do servidor e os grandes saturam a rede.

Cortina de Fumaça – Distrai atenção de um outro ataque mais potente na cama OSI distinta, assim o executa em outro vetor da rede.

Ataque Mult-Vetorial – Explora a vulnerabilidade em uma tentativa de erro.

Ampliação e Reflexão de Tráfego – Ataca a vulnerabilidade em serviços respondendo ao protocolo DNS (Domain Name System) e NTP (Net Work Time Protocol), potencializando esses ataques para um servidor, dessa forma ataques de reflexão inundam o alvo com dados indesejados.

ATAQUES VOLUMÉTICOS – Máquinas Zumbi são infectadas por phishing, induzem a usuários clicar em links maliciosos, na maioria das vezes reproduzem o layout de empresas confiáveis.

ATAQUE A CAMADA 7 HTTP SSL DNS – De acordo com Gartner cerca de 25% dos ataques serão baseados em aplicativos, onde diversos comandos são enviados para atingir a capacidade de processamento dos servidores, tornando essas aplicações indisponíveis, recomenda-se fazer instalação do Appliances para combater ataques Ddos.

4. ALGUNS TIPOS DE ATAQUES

Cavalo de Tróia

A partir da sua instalação é possível modificar, excluir, instalar arquivos, mandar e-mail. O cavalo de troia buscam gerar estragos nos dispositivos dos usuários sem serem percebidos, atuam lendo ser baixado no computador, sendo capaz de executar um arquivo e atuar conforme foi programado.

Ataque Dma

DMA (Direct Memory Access) permite que alguns componentes de hardware interajam diretamente com a memória RAM de um computador e transfiram dados para a partir desta sem intervenção do processador. Esta funcionalidade é utilizada para acelerar o tempo de processamento e aumentar a taxa de transferência do computador.

A configuração incorreta de firewall, não usar o antivírus e a falta de atualização torna a rede vulnerável. O firewall trabalha com bloqueio de dados para proteger o computador por regras que o usuário cria, firewall pode se tornar sensível a ransomwares e malwares de toda espécie, o sniffing é um método que captura pacotes de dados em uma rede o software sniffers pode ser utilizado pelo administrador para procurar pacotes intrusos em suas redes, também pode ser usado para coletar informações a respeito de dados conectados na mesma rede local.

SQL injection um invasor que acrescenta códigos SQL em um formulário, para obter informações do usuário. Atualmente, criam-se ataques que atingem a comunicação do servidor que está sendo utilizados por ciber criminosos, uma forma de modificar esses dados é o uso de software que interceptam tráfego numa rede.

Skype e Whatsapp podem funcionar como vetores de links e anexos maliciosos, basta clicar no link ou anexo para infectar seu aparelho e a rede que estiver conectado.

5. COMO PREVENIR AS VULNERABILIDADES DE UMA REDE

Para evitar ataques Ddos deve seguir boas práticas de segurança, o que não garante 100% de eficácia, contudo aumenta a segurança da empresa. Na segurança em nuvem (Cloud Computing), a empresa escala diversos servidores inibindo a tentativa de sobrecarregar o mesmo servidor e ainda pode bloquear o número da requisição pelo IP. Monitoramento por especialistas com uma equipe sempre de olho no tráfego de rede dos servidores.

Durante o ataque Ddos uma solução é usar a conexão reserva, ter um bom firewall combate ameaças e controla os acessos que rondam a infraestrutura.

Ex. se um site de rede varejista for atacado existirá perdas nas vendas foi o que aconteceu com as lojas americanas em 2021, onde a empresa perdeu 12% em valor no mercado. (ISTO É 2021)

Deve ter cuidado ao descartar informações corporativas, pois isso é uma vulnerabilidade, existe formas de recuperação das informações contidas no HD, nessus e nmap são software usados para monitoração de vulnerabilidade de ambiente.

ambiente de redes. Nessus realiza o scan, que scaneia algo usando o software. Nmap realiza mapeamento do range faz um scan completo na rede para saber quais hosts estão ativos.

As empresas devem tratar a questão da gestão de vulnerabilidade com prioridade.

Os ciber criminosos buscam sempre tirar proveito da falha de segurança por motivos diversos, eles representam uma ameaça constante.

Segundo a ISO 27000, portarias do sistema de gestão de segurança da informação, reza que as vulnerabilidades são fraquezas a serem exploradas por várias ameaças, podendo acontecer durante a concepção, implementação ou configuração de um controle, pode ser gerada por falha humana, por parte da tecnologia não atualizadas ou com má intenção.

- Falha humana
- Vulnerabilidade de rede
- Vulnerabilidade de aplicação
- Vulnerabilidade de processo

Os erros dos usuários podem expor dados confidenciais até mesmo usuários internos podem executar arquivos maliciosos facilitando a invasão. O hardware ou software podem facilitar a invasão através de pontos de acesso wi-fi inseguros.

As empresas devem olhar com mais seriedade para as vulnerabilidades de segurança, evitando que aconteça problemas e só depois dar a devida atenção. É importante definir o que é necessário proteger, quais metas a seguir, identificar fontes de ameaça, redefinir as proteções de segurança, escolha de feeds de inteligência de ameaças cibernéticas e estratégia de ataques, saber quais são as maiores ameaças à segurança da rede, é mantendo a proteção cibernética atualizada.

WLANS é um acesso conveniente que pode abrir brecha de segurança. O uso de SSID aumenta a chance de alguém tentar quebrar a segurança, pois é fácil encontrar o cracking além do SSID revelar sua localização.

WPS também abre brechas para invasores, o crack com um pin de 8 dígitos recupera a senha WPS, o WPA2 é mais indicado para uso corporativo. O firewall trabalha com bloqueio para proteger o computador, por regras controladas pelo usuário, um firewall pode torná-lo mais suscetível a *ransomwares* e *malwares* de toda espécie.

Os Sniffing é um método que verifica pacotes de dados de uma rede, podendo ser utilizado para procurar intruso em suas redes ou coletar informações a respeito de todos conectados na mesma rede local mesmo se passarem por outros aparelhos com a intenção de roubo.

Como Encontrar a Vulnerabilidade de Segurança

É importante para as empresas terem esses cuidados:

- Priorizar que é necessário proteger;
- Criar regras para segurança geral;
- Avaliar fontes de ameaças;
- Aprimorar as proteções de segurança cibernéticas, escolha lista de inteligência de ameaças e monitorar as novas estratégias de ataque.

5.1. Como proteger a rede

Falha na Segurança ao Armazenar Dados

Importante manter data center para armazenar arquivos confidenciais, esses data centers são sistemas de tecnologias atuais de virtualização muito utilizada em computação em nuvem. Sendo mais uma segurança que as empresas podem utilizar. Ter um bom firewall baseado em host. Algumas empresas acham desnecessários, partem do ponto que só usuários confiáveis tem acesso a ele, maneira de garantir a segurança neste aspecto é que todos os hosts possuam um firewall ativo configurado.

6. OS PILARES DA SEGURANÇA DA INFORMAÇÃO

Figura 4 extraída em 29/05/2022 do site: <https://www.fabiobmed.com.br/site/em-seguranca-da-informacao-o-que-significa-cidal/> a figura mostra o conceito da base da segurança do uso de dados nas redes.



Sobre estes pilares da segurança da informação, estão a proteção de dados processados pela empresa que atendem as regras da ISO. Regras que tem sido fundamental para atrair investidores, clientes e colaboradores. Essas regras falam do cuidado que as empresas devem ter com seus os bancos de dados, tendo essa atenção dispensada para todos os pontos as portas certamente estarão fechadas para possíveis invasões. Existe outras formas de ameaças não sendo necessariamente de hackes, são os desastres naturais como queda de raios, incêndios e queda de energia, são fatores externos que podem prejudicar o sistema. Arquivar seu banco nas nuvens é uma solução segura com menos riscos de ataques uma vez que armazenamento em nuvens conta com diversos servidores assim a tentativa de sobrecarregar um servidor não acontece e ainda pode bloquear a requisição pelo IP.

A base de defesa das empresas são senhas fortes, softwares homologados, criptografia, firewalls entre outras. As ameaças surgem por diversos fatores, como ataque de malwares, usar software não homologados, o não uso de senhas criptografadas, engenheiros sociais persuadir funcionários e ter acessos a informações privadas e senhas, roubo de aparelhos móvel. A cibe segurança está em constantes atualizações e sendo tratada com prioridade nas áreas gerenciais.

6.1 Propriedades de Segurança

Previne que invasores de sistemas consigam entrar acessando computadores e redes (HAWARD1997), quando utilizam algoritmos de criptografia é possível garantir as seguintes propriedades de segurança (STALLINGS,2015)

- A- CONFIDENCIALIDADE
- B- INTEGRIDADE
- C- AUTENTICIDADE
- D- NÃO REPÚDIO


- **CONFIDENCIALIDADE:** Somente pessoas autorizadas tem acesso à informação, a criptografia simétrica pode ser utilizada para garantir a confidencialidade de arquivos armazenados (HOWARD,1997)

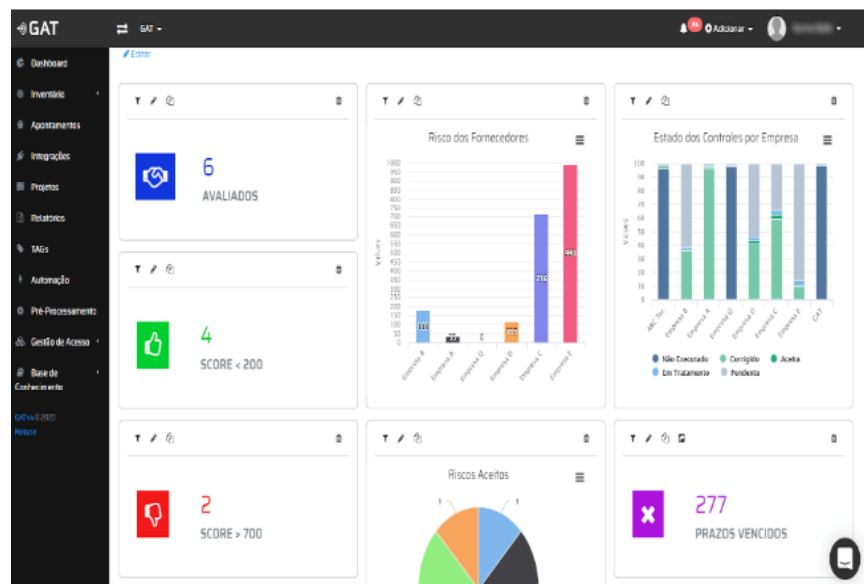
- **INTEGRIDADE:** Não deixar a informação ser alterada por pessoas não autorizadas, as funções hash e as assinaturas digitais podem ser utilizada para verificar se determinada mensagem foi alterada durante a transmissão.
- **AUTENTICIDADE:** Verifica se o emissor é quem diz ser, isso pode ser feito utilizando certificados digitais ou alguém mecanismo de autenticação com usuário e senha (STALLINGS, 2015).
- **NÃO REPÚDIO:** Garante que o ator de uma ação não possa negar que a executou, a utilização de assinatura digitais e certificados digitais, garantem o não repúdio por parte de um emissor sobre envio de uma mensagem (HOWARD,1997).
- **TRIADE CIA:** Os três pilares tiveram outros dois elementos acrescentados dados. Controle de acesso criptografia, senhas entre outras estratégias e confiabilidade é um dos requisitos da lei LGPD.
- **DISPONIBILIDADE:** É fundamental que seus dados estejam disponíveis sempre que necessário e que garante acesso em tempo integral(24x7) de uma equipe autorizada, o TI deve permanecer robusto e funcionando o tempo todo reforçando mais uma vez a escala (24x7) é preciso garantir a estabilidade e acesso permanente as informações dos sistemas por processos de manutenção rápidos, eliminando falhas de software, atualizações constantes, planos para administração de crises.
- **IRRETRABILIDADE (NÃO REPUDIO):** O remetente dos dados recebe um comprovante de entrega e que o destinatário recebe um comprovante da identidade do remetente de forma que ambos não possa negar o envio, o recebimento ou acesso aos dados. Os princípios da Segurança devem ser usados para provar a identidade e validar o processo de comunicação.

A plataforma GAT CORE (Plataforma de gestão integrada de risco cibernético e conformidade que otimiza sua gestão. É possível gerenciar ameaças, priorizar as correções de acordo com riscos e centralizar procedimentos, conformidades, check lists e prazos, com total integração as ferramentas de segurança da empresa.

O primeiro passo para construção de programa de segurança da informação é o gerenciamento da superfície (permanece em alerta em tempo real, na tentativa de aplicar soluções a análise de riscos de superfície de ataque externo mantendo a segurança do servidor). A visibilidade prioriza riscos, deve traçar metas para alcançar esse objetivo. A identificação, classificação e o monitoramento contínuo de ativos digitais que contêm ou enviem dados vitais entre redes a medida que surgem, esse método percebe maior transparência ajudando a fortalecer a relação clientes e parceiros comerciais por isso, deve criar programa de gerenciamento de superfície de exposição.

Figura 5 figuras extraída em 29/05/2022 do site <https://www.b2bstack.com.br/product/gat-core> trata-se de um gráfico onde é analisado riscos de fornecedores e controle dos riscos dentro de uma empresa, mostrando passo a passo a evolução até antes de ser detectado algum tipo de risco.

-  Detectado
-  Em Treinamento
-  Corrigido
-  Pendente
-  Aceito



6.2 Inventário Digital

É uma gestão do estoque de peças, o seu princípio é basicamente que em vez de estocar um depósito físico com grandes quantidades, que podem ou não estar em demanda, os arquivos de design para essas peças podem ser armazenados digitalmente e fabricado sob demanda. A impressão 3D ou manufatura aditiva, vem ganhando espaço entre as tecnologias ágeis que permitem a adoção de inventários digitais.

Fatores de Riscos: Após a identificação do inventário digital da empresa, o sistema realiza uma busca por possíveis problemas de segurança relacionados a cada um desses ativos. São quatro fatores de risco.

Risco de imagem de marca -> problemas que podem acarretar perdas de credibilidade da marca. Ex. má configuração do DNS

Vazamento de dados -> Verificação das contas de e-mail corporativas para checar vazamento de dados.

Problemas de Websites -> Má configuração de servidores web, tecnologia web inseguras. (o sistema não realiza nenhuma varredura intrusiva).

Problemas de rede -> Questões relacionadas ao IPs encontrados, como portas abertas.

ISO

Agora será descrito normas de segurança da ISO, uma organização não governamental independente, desenvolve e promove normas abrangendo segmentos, como indústria, comércio, tecnologia, alimentação, agricultura e saúde.

ISO 27000 É a proteção de dados para empresas e órgãos públicos, tem como base a criação de um sistema de gestão de segurança da informação SGS1.

SGS1 É a reunião políticas procedimentos, diretrizes e recursos de proteção de informação de uma organização.

ISO 27001

Avalia riscos, identificando as oportunidades, conscientiza toda as empresas sobre a importância da segurança da informação, controla eliminando e diminuindo os riscos citados, são realizadas auditorias internas para verificar resultado da implantação dos controles operacionais, visando a melhoria do processo após a certificação da avaliação de controle de riscos.

ISO 27002

Deve ser usada em conjunto com a ISO 27001, pois trata-se de política de segurança que contém formas de controle, planejamento de estrutura que fará a gestão da organização, identificação de ativos, criação de um plano de segurança para recursos humanos e fornecedores, garantir a segurança física dos equipamentos e instalações de processamento de dados, criando planos de continuidade dos negócios após um incidente.

ISO 27701

Esta é a certificação mais recente da 27000 para se adequar as normas LGPD. A ISO 27701 da lei 13 709 de 14 de agosto de 2018 trata-se da regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais, além de mudar a maneira como as instituições privadas coletam, armazenam e disponibilizam informações de usuários. A lei LGPD é destinada as instituições públicas, portanto devem ser seguidas pela união do estado, distrito federal e municípios.

Baseado em compartilhamento de dados que levam a indústria movimentar bilhões de reais, pois o mercado preparado conseguir manipular essas informações e garimpa seu público alvo, contudo na controvérsia o ambiente virtual sofre um aumento considerável no cibercrime, isso levou as autoridades do mundo a criar solução para coibir essas atitudes, a nova lei estabelece regras claras sobre coleta de dados, armazenamento, tratamento e compartilhamento de dados pessoais, impondo uma padronização na proteção desses dados com penalidades significativas caso descumprem as normas.

6.3 LGPD Os principais pontos dessa lei são:

Passa ser visto como dados pessoais todos os documentos, telefone, endereço, localização via gps, retrato, prontuário de saúde, cartão bancário, histórico de pagamentos, preferência de lazer, IP e até cookies, caso esses dados trafeguem nas redes sem autorização dos usuários, pode resultar e multa de 2% do faturamento anual da empresa, no limite de R\$ 50 milhões por infração, a lei garante o direito do cidadão pedir para deletar os dados sobre penalidade. A lei LGPD já está em vigor aqui no Brasil, chega um pouco atrasada em comparação com outros países, mas representa um grande avanço na consolidação dos direitos do cidadão. As instituições têm um grande desafio no que se refere a implantação desse mecanismo que garanta o exercício dos direitos do titular dos dados.

A lei Carolina Dieckman nº 12.737/2012 é uma alteração no código penal brasileiro para crimes virtuais e delitos de informática, alguns pontos dessa lei são:

- Invasão de dispositivo informático
- Falsificação de cartão
- Produzir, oferecer, distribuir, vender ou difundir um programa de computador ou dispositivo que permite a prática também sofrerá as consequências do crime. A pena do crime de invasão de dispositivo é de 3 meses a 1 ano mais multa, com um aumento de 1/6 caso ocasione prejuízo econômico a vítima, a pena tem um aumento de 2/3 se houver divulgação ou comercialização dos dados

O objetivo da ISO 27001 é criar um modelo padronizado para restabelecer, implementar, operar, monitorar, analisar criticamente, manter o melhorar os sistemas e processos de segurança da informação de uma empresa. Nenhuma organização é obrigada a ter o CERTIFICADO ISO /IEC 27001, mas essa pode ser uma exigência dos clientes e parceiros de negócio antes de fechar contrato com determinadas empresas, portanto, adotar o padrão de normas pode ser uma estratégia, a ser tomada de acordo com as necessidades e atuação do negócio.

A certificação da ISO 27001 estabelece padrões dos sistemas de gerência de forma que as empresas protejam seus sistemas de gestão da segurança da informação de acordo com os padrões estabelecidos a auditoria é feita por uma terceira parte, garantindo a credibilidade, a independência a transparência. Deve verificar a existência de documentos chaves para gestão, a auditoria faz uma

avaliação profunda e detalhada que inclui a existência e a eficácia de aplicação dos controles ISMS (Information Security Management System) é um padrão para sistema de gerência da segurança da informação, seu objetivo é usado em conjunto com ISO 17799 código de práticas para gerência da segurança da informação ou qual lista controle de segurança e recomenda um conjunto de especificações de controles de segurança. Os controles são etapas executadas para analisar os riscos de negócio.

Exemplo de controle familiar:

- Política que requer o uso de um VPN;
- Ter cartões de acesso de segurança para entrar em um edifício;
- O uso de software antivírus.

Figura 6 extraída em 18/05/2022 <https://www.tecmundo.com.br/seguranca/220645-lgpd-lei-geral-protacao-dados-pessoais.htm> a figura destaca pontos referente a lei 13709 de 14 de agosto de 2018.



Os Benefícios da Certificação da ISO para Empresas

É importante comprovar oficialmente que sua empresa obedece aos mais altos padrões do setor. É uma garantia que aos clientes e investidores que está seguindo

as regras da lei, com isso se opera com mais confiança. Importante ter a segurança da informação como elemento estratégico, os avanços da tecnologia impactam todos os setores, sendo assim trabalhar dentro dos padrões da ISO 27001 é a forma de alcançar novos horizontes. Nos trâmites da segurança da informação está a CRIPTOGRAFIA.

7. CRIPTOGRAFIA

O crescimento desenfreado da internet, as diversas atividades pessoais e profissionais, através principalmente das redes móveis, levou a população a ter um cuidado redobrado com seus dados. A criptografia proporciona a proteção da identidade de cada indivíduo quanto ao conteúdo de arquivos e de mensagens trocadas.

Impossível a sociedade atual ignorar a garantia sigilosa das transações bancárias, dados dos clientes, informação de investidores e colaboradores. É fato que os dados devem estar protegidos com excelência, levando em consideração que qualquer vazamento de informação pode ser fatal. Para que a comunicação na internet aconteça, o computador e celulares precisam acessar outro computador e serem acessado, essa comunicação é uma exposição constante, que possibilita acesso a captura de informações confidenciais. A criptografia é uma ferramenta de segurança das informações trafegadas, pois a internet original não foi projetada para prover essa segurança.

A criptografia é a segurança necessária para que os tráfegos na rede operam de maneira segura, pois um arquivo protegido com a criptografia evita desvio de dados pessoais e de mensagens. A codificação das mensagens se torna ilegível para invasores. Os primeiros algoritmos desenvolvidos aplicavam uma função matemática repetidamente e um dado para cifrá-lo, essa técnica não era muito robusta o que facilitava a quebra do código.

Criptografia simétrica: essa técnica usa a mesma chave para criptografar e decifrar código o que não é seguro, a criptografia assimétrica se usa uma chave para criptografar e outra para decifrar o código, isso aumenta a segurança da navegação,

fazendo com que seja quase impossível a invasão de hackers.

Vantagem dos algoritmos de criptografia simétrica

As criptografias simétricas possuem uma série de vantagens (AMARO, 2019):

- Criptografia simétrica são capazes de cifrar uma grande quantidade de informações em pouco tempo;
- Podem usar chaves simples e ainda assim ter um mecanismo robusto;
- Fáceis de utilizar na proteção de dados armazenados em dispositivos.

Desvantagens dos algoritmos criptografados simétrica

- A chave privada precisa ser distribuída em segredo, neste caso tanto o emissor quanto o receptor devem buscar uma forma segura para o envio das chaves;
- Como essa chave é usada para cifrar e decifrar mensagens, se um invasor tiver acesso a ela, toda a mensagem estará comprometida.

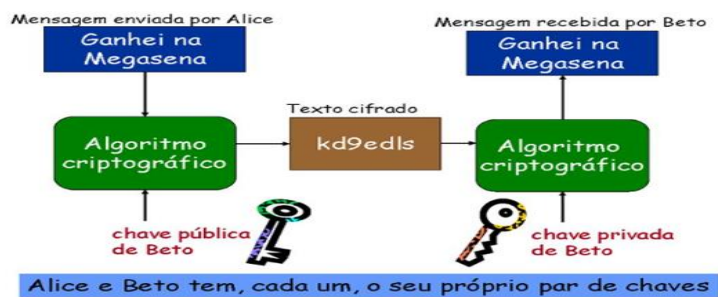
Criptografia e Certificação Digital

Para que duas pessoas consigam se comunicar utilizando a criptografia assimétrica, precisa de alguma forma de troca de chaves públicas e privadas, podendo utilizar o e-mail para enviar essa chave, a figura abaixo é da criptografia assimétrica, a mensagem é sempre criptografada com a chave pública do destinatário e a mensagem só será decifrada com o uso da chave privada.

Figura 7 extraída em 16/05/22 do site: <https://slideplayer.com.br/slide/4024622/>

Representa a comunicação entre duas redes, onde a mensagem é enviada com a chave pública e descriptografada com uma chave privada.

Criptografia Assimétrica



VPN

O VPN atua como firewall que protege o computador criando um túnel exclusivo para que os dados trafeguem pela rede. As empresas precisam fornecer a VPN para que mesmo de casa o trabalhador e os dados estejam seguros.

Categoria de VPN:

- VPNS protocolo PPTP

Desenvolvida pela Microsoft, seu uso não é mais recomendado porque a criptografia usada é fraca suscetível da força bruta.

- VPNS protocolos IPSeC

Adotado no tcp/ip responsável pelo funcionamento da internet, com recursos para criptografia dos dados transmitidos, autenticação dos emissores e receptores do pacote de controle de integridade.

- VPNS protocolos SSL/TLS

São protocolos utilizados para garantir segurança de protocolos HTTPS, proteger dados trafegados na web.

A da categoria de VNP utilizada, todas fazem o uso algoritmos de chave simétrica e assimétrica na construção de rede virtual.

PROTOCOLOS HTTP e HTTPS CERTIFICADOS DIGITAIS

Protocolos usados para transferência de hipertexto, carregam páginas da web (World Wide Web www) o http e https tem a mesma função de transferir dados, o https são sites criptografados, esse site garante que seus dados estão protegidos, o certificado digital é um requisito da segurança de protocolação eletrônica de documentos e certificado digital, comprova de forma eletrônica a identidade do usuário. Quase todas as empresas hoje estão na internet, a tecnologia virou essencial para a humanidade. Empresas possui website, onde facilita o acesso do cliente, a internet é uma vitrine das empresas aliadas à venda, existe alguns protocolos que possibilitam essa navegação com rapidez e segurança, os protocolos TCP/IP controla a transmissão de dados, permitindo a comunicação entre as redes, o protocolo HTTP possibilita acesso à internet, mas não garante o sigilo dos dados e quem permite a navegação protegida com recursos criptografados é o HTTPS, o certificado digital é um documento que garante que uma chave pública pertence a uma determinada entidade ou pessoa (STALLINGS,2015), este certificado é emitido e também revogado por uma instituição chamada autoridade certificadora (Certification Authority-CA).

Existem vários tipos de certificados digitais, utilizados na internet, e cada um é apropriado e identificado com uma determinada entidade. (GARFINKEL, 1997).

- **CERTIFICADO DE AUTORIDADE**, contém chave pública de uma CA o nome da CA e os serviços que serão certificados;
- **CERTIFICADOS DE SERVIDORES**, contém chave pública de um servidor, esse deve suportar protocolo SSL;
- **CERTIFICADOS PESSOAIS**: possuem basicamente o nome da pessoa e sua chave pública, pode conter outras informações.

Os navegadores permitem acessar um certificado digital de um servidor web que provém de páginas seguras.

PROTOCOLOS SSL e TLS e SUAS FUNÇÕES

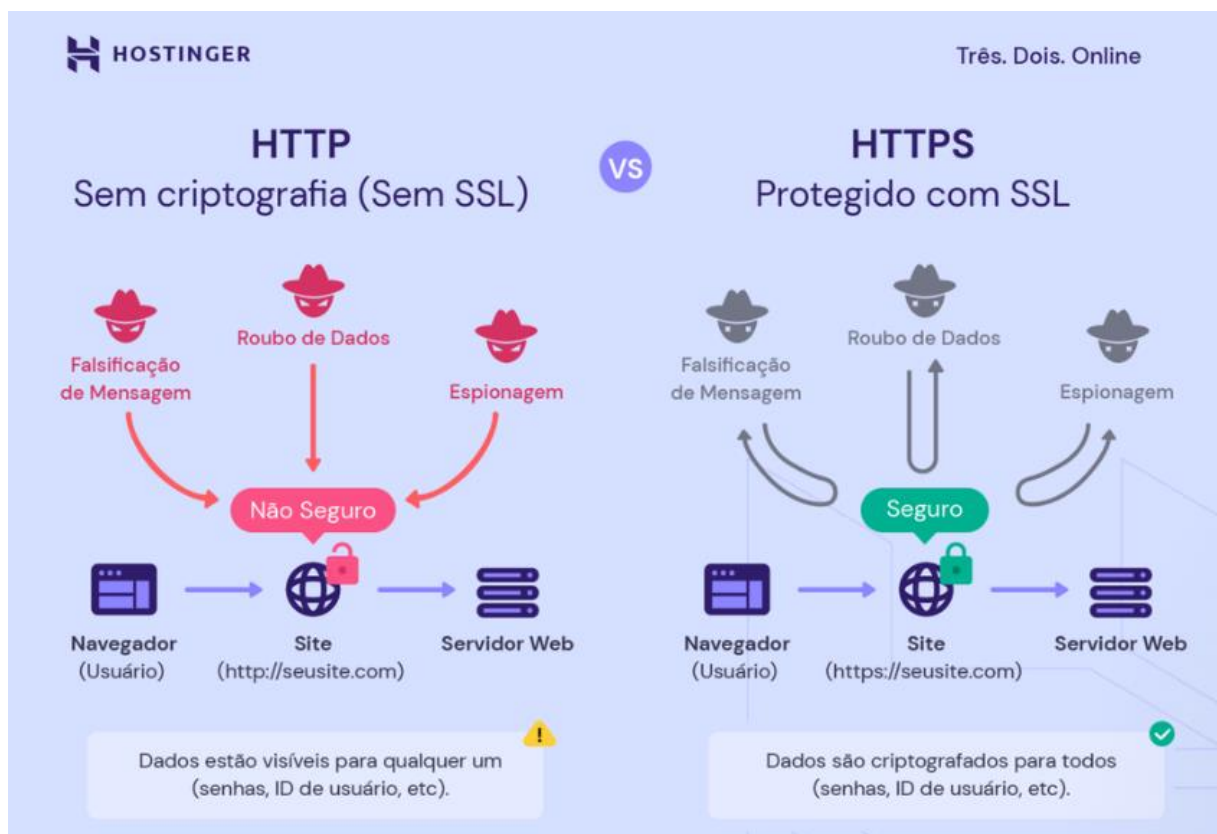
SSL (Secure Sockets Layer) é um tipo de segurança digital que permite a comunicação criptografada entre um domínio de site e um navegador, essa tecnologia

está sendo substituída pelo TLS significa (Transport Layer Security) que certifica a proteção de dados semelhantes ao SSL. O objetivo do SSL/TLS é tornar segura a transmissão de informações sensíveis como dados pessoais, de pagamento ou de login. É uma alternativa à transferência de dados em texto simples no qual a conexão ao servidor não é criptografada e torna mais difícil para que hackers possam interceptar a conexão e roubar dados.

SSL/TLS são utilizadas por webmasters para assegurar seus sites e oferecer uma opção segura para efetuar transferência. Quando se identifica um cadeado se sabe que a conexão é segura e possui certificado SSL/TLS.

Figura 8 extraída em 16/05/22 <https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https#:~:text=O%20SSL%2FTLS%20funciona%20atrav%C3%A9s,o%20servidor%20fazer%20uma%20conex%C3%A3o>

A figura mostra os riscos da conexão sem e com criptografia.



Código de criptografia

Código não implementado por mim, mas demonstra um código sendo cifrado e decifrado.

```
String EncryptData(string strData, string strKey)
```

```
{
```

```
    byte[] key={}; //Chave de Criptografia
```

```
    byte[] IV = {10,20,30,40,50,60,70,80};
```

```
    byte[] inputByteArray;
```

```
    try
```

```
    {
```

```
        Key= Encoding.UTF8.GetBytes(strKey)
```

```
        //DESCryptoServiceProvider é a classe de criptografia em c#.
```

```
        DESCryptoServiceProvider ObjDES=new DESCryptoServiceProvider();
```

```
        InputBytrArray=Encoding.UTF8.GetBytes(strData);
```

```
        MemoryStream Objmst = new MemoryStream();
```

```
        CryptoStream Objcs = new CryptoStream(Objmst, ObjDES.CreateEncryptor(Key,IV),
```

```
        CryptoStreamMode.Write);
```

```
        Objcs.Write(inputByteArray,0, inputByteArray.Length);
```

```
        Objcs.FlushFinalBlock();
```

```
        Return Convert.ToBase64String(Objmst.ToArray()); // string final
```

```
    }
```

```
    Catch(System.Exception ex)
```

```
    {
```

```
        throw ex;
```

```
    }
```

```
}
```

Código de Descriptografia

```
public string DecrypData(string strData, string strKey)
{
    bytes[] key = { };// chave

    bytes[] IV = (10,20,30,40,50,60,70,80);

    bytes[] inputByteArray = new byte[strData.Length];

    try
    {
        Key = Encoding.UTF8.GetBytes(strKey);

        DESCryptoServiceProvider ObjDES = new DESCryptoServiceProvider();

        InputByteArray = Converter.FromBase64String(strData);

        MemoryStream Objmst = new MemoryStream();

        CryptoStream Objcs = new CryotStream(Objmst,ObjDES.CreateDecryptor(key,IV),
CryptoStreamMode.Write);

        Objcs.Write(inputByteArray,0,inputByteArray.Length);

        Objcs.FlushFinalBlock();

        Encoding encoding = Encoding.UTF8;

        Return encoding.GetaString(Objmst.ToArray());
    }
}
```

```
catch (System.Exception ex)

{

    Throw ex;

}

:

}
```

8. INTELIGÊNCIA ARTIFICIAL e a SEGURANÇA DA INFORMAÇÃO

Figura 9 extraída em 16/05/2022 <https://infranewstelecom.com.br/inteligencia-artificial-na-seguranca-da-informacao/>

A figura simboliza um robô e um cadeado fechado, IA atuando na segurança



Com a velocidade com que as informações são disponibilizadas nas redes, há também o aumento de crimes cibernéticos. Crimes virtuais são avassaladores na contramão das leis e fragilidades da penalização aos culpados. A Inteligência Artificial realiza várias tarefas ajudando o departamento de segurança, com falta de pessoal preencher as habilidades especializadas melhorando a eficiência dos profissionais humanos protegendo de diversas ameaças a Inteligência Artificial coloca a segurança a frente. Tendo um alto poder analítico a IA será responsável por analisar rapidamente

uma grande quantidade de dados através de um parâmetro criado os sistemas de segurança identificarão riscos a infraestrutura interna; entre tantas vantagens, as desvantagens é a falta de ética, o custo inicial elevado o risco de aumentar o desemprego.

O benefício da IA é que ela pode agir de forma independente a ameaças, em uma velocidade que, humanamente, seria impossível.

Implantar a IA defensiva nos coloca a frente, contudo a sabedoria, governança e estratégia devem assumir sua parte com responsabilidade no negócio, a IA não substituirá a necessidade de profissionais da segurança qualificados, é necessário equilibrar a supervisão humana com a confiança que permite a IA atuar de forma autônoma. O futuro é agora, as ferramentas técnicas da IA devem ser úteis também em defesa para atores mal-intencionados. As organizações devem reduzir riscos e aproveitar as oportunidades, protegendo seu sistema inteligente e criar suas próprias defesas. A IA não está no futuro ela é real e as organizações devem começar a se preparar para uma guerra cibernética.

A INTELIGÊNCIA ARTIFICIAL e a SEGURANÇA DA INFORMAÇÃO ANDAM JUNTAS NA VIGILÂNCIA AO FUTURO

A comunicação por meio de computadores está cada vez mais presente, com isso cria facilidades e problemas.

No Brasil, 40% das empresas implantaram a inteligência artificial nos seus negócios, é necessário que as empresas estabeleçam um plano de segurança, a necessidade de a tecnologia ser usada em equipes, trabalhando em sintonia para proteger o bem maior das empresas, o banco de dados.

É nítido os avanços das empresas na tecnologia embarcada que se comunica com seus clientes por meio de assistência virtual, a automação no fluxo de trabalho e o gerenciamento da segurança da rede.

9. IA EM 2022 - TENDÊNCIA, RISCOS E BENEFÍCIOS

A perspectiva é que a rede 5G passará de um bilhão de assinatura já em 2022, devido a sua velocidade ser 100 vezes mais que a tecnologia anterior.

METAVERSO -> Espaço tridimensional virtual onde é possível logar, e usar 3D para interagir seja por lazer ou trabalho.

INTERNET DAS COISAS -> Rede de objetos físicos incorporados a sensores, software e outras tecnologia com o objetivo de conectar e trocar dados com outros dispositivos pela internet. Esses dispositivos variam de objetos domésticos comuns a máquinas industriais sofisticadas. São mais e 7 bilhões de dispositivos IoT conectados hoje, especialistas esperam que esse número cresça para 10 bilhões entre 2020 até 2022 (ORACLE).

SEGURANÇA DIGITAL -> Segundo a consultoria alemã Roland Berger, o Brasil ocupa o 5º lugar no ranking de ataques cibernéticos.

Investir na Transformação da Tecnologia

A empresa que quiser se manter viva e competitiva terá de investir nos avanços da tecnologia. O 5G vem com força, com uma cobertura e alta velocidade que fará a diferença aos usuários. 5G irá dispor de uma elevada segurança cibernética, dificultando a atuação dos hackers, o que facilitará a vida do engenheiro social será a falha humana, uma vez que a máquina não cansa, não fica doente, não se distrai e produzirá mais rápido que o homem.

É indiscutível o aumento da produtividade usando às máquinas, sem contar com a redução de custos, uma vez que não precisará admitir, demitir treinar etc. É verdade que a máquina substituirá o homem algumas vezes, porém a máquina funcional será dependente do homem a máquina não pensa, depende do homem para criar e ela executar, partirá do homem a manutenção e atualização de funções da máquina, é incontestável que a evolução da tecnologia se deve a uma máquina chamada cérebro que só o homem tem. Todo sucesso da inteligência artificial depende da mente humana,

Uma pesquisa feita por especialistas em ciências da computação mostrou que a inteligência artificial atingiu um ponto crítico em sua evolução, o professor de ciências da computação do Brown University Michael Littman que presidiu o relatório mostra um progresso substancial em diversas áreas. Outro pesquisador Mahammed

Gawdot acredita que sistemas conhecidos como inteligência artificial geral AGI sigla em inglês parecidos com skynet do filme o exterminador do futuro, são inevitáveis e representa um perigo real, deixando as pessoas mais perto de um apocalipse gerado por máquinas poderosas. Em um futuro não muito distante, esse cenário hipotético pode se transformar em realidade. A inteligência artificial onipresente se tornará a forma dominante de inteligência no planeta com programas de computador e robôs assumindo o controle dos humanos prevê (GAWDAT 2021).

9.1 O Fenômeno chamado 5G

Figura 10 extraída em 18/05/2022 <http://blog.targetso.com/2020/08/12/primeiro-talk-target/>

A figura demonstra o 5G dominando todos os pontos da terra.



Esperado por muitos com grandes expectativas, o 5G vem inovar a era digital, um aumento expressivo de pessoas conectadas com uma excelente qualidade, o tempo de resposta fica estimado em 5 e 20 milissegundos, essa banda larga permite navegação com mais segurança e confiabilidade não existe resposta exatas da real segurança, o que se fala é dos planos de contingências, que será analisado a medida que vai evoluindo essa tecnologia, os cibercriminosos também tendem a evoluir por isso as práticas de segurança devem ser adotadas. A segurança da informação afirma que precisamos trabalhar em sintonia desde já, precisa-se combinar a tecnologia, políticas adequadas e capacitação das pessoas; a segurança da informação é pautada em uma ação coordenada, onde todos estejam envolvidos, serão necessários novos equipamentos compatíveis com a nova realidade. A segurança ultrapassado deverão ser revistos, utilizando mais camadas de proteção de diversos parâmetros

habilitados por equipes remotas. A consultoria Poneman (SINDSEGSP), em suas pesquisas, indicam que 2/3 de roubos e vazamentos de dados são por falha humana, falta de supervisão ou negligência. É necessário preparar as pessoas, treinar equipes conscientizando o real valor de cada um na luta pela segurança de dados. O 5G precisa vir acompanhado de precaução, diante dessa possibilidade sobreviverá quem usar a tecnologia com responsabilidade.

A tecnologia 5G está sendo considerada a estratégia da transformação digital, com potencial para gerar um forte crescimento econômico tem despertado uma preocupação em vários países com relação a segurança cibernética das redes 5G. A CPQD (Centro de Pesquisas e Desenvolvimento em Telecomunicação fundada em 1976 é um dos maiores centros de pesquisa da América Latina, com foco na inovação da tecnologia e comunicação, mantém um portfólio abrangente de soluções que são utilizadas nos diversos segmentos de mercado no Brasil e no exterior) apresentou uma proposta a Anatel de criar no Brasil laboratório nacional de referência em 5G multiusuário com a capacitação de realizar auditoria de segurança cibernética de equipamentos e soluções destinadas a redes de telecomunicação brasileira estes recursos poderá ser capitados com leilões para 5G, pela Anatel, que prevê destinar 5% dos recursos para o desenvolvimento tecnológico 5G essa iniciativa seria voltada a segurança cibernética nas redes.

10. OWASP TOP TEN

É a junção de alguns desenvolvedores que através de pesquisas chegaram a algumas vulnerabilidades mais comuns em se tratando de desenvolvimento de aplicação web, grupo sem fins lucrativos trabalham em prol da segurança da informação, deixando em destaque as dez falhas mais comuns do sistema no momento que permite invasores atacar. Por isto esses desenvolvedores, pesquisadores disponibilizaram conteúdos educacionais, incluindo artigos, documentações, ferramentas e códigos abertos, para auxiliar profissionais da área de desenvolvedores web, o objetivo da OWASP é diminuir a vulnerabilidade da segurança web, a listagem é atualizada com uma certa frequência, relacionando as brechas mais críticas e perigosas.

No RANKING, às vulnerabilidades comuns são:

- INJEÇÃO – Falha de injeção incluindo SQL, OS, LDAP se um interpretador for manipulado por um atacante que execute comandos maliciosos;
- QUEBRA DE AUTENTICAÇÃO – Problemas de implementação de recursos;
- EXPOSIÇÃO DE DADOS - Exposição de dados sensíveis a APIS mal configurado, podem expor dados pessoais.

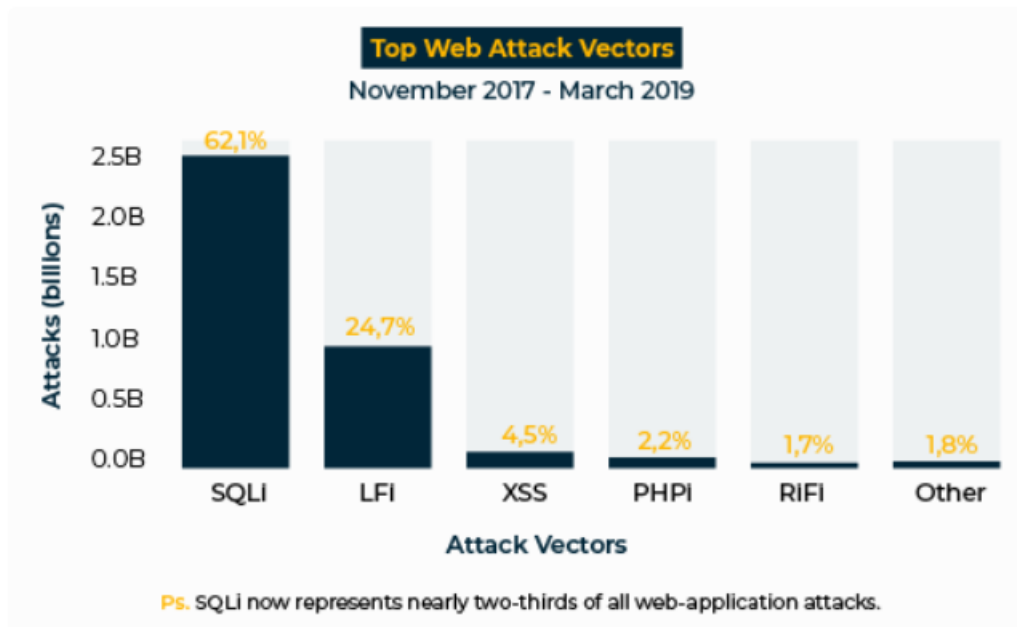
O OWASP top TEN é um guia disponível para qualquer desenvolvedor que trabalha em projetos web APP. Atualmente muitos programadores trabalham remotamente é importante que esses desenvolvedores usem recursos da OWASP durante o processo de desenvolvimento e manutenção. Esse projeto ajuda desenvolvedores a proteger seu sistema, seus dados e seus usuários, revisão de códigos, pontos de acesso de segurança. Host pots de segurança são usos de códigos sensível a segurança. À medida que os desenvolvedores interagem com os pontos de acesso de segurança, eles aprendem avaliar os riscos de segurança enquanto aprendem mais sobre codificação segura.

Vulnerabilidade de segurança precisa de ação urgente e o SonarQube (Uma ferramenta para garantir a qualidade do código fonte em desenvolvimento) fornece descrições minuciosas sobre problemas de código explicando o risco caso seu código esteja em perigo. É só fazer check-in de correção e proteção de aplicativos.

Um dos relatórios liberado pela OWASP (2007 trata da web attacks and Goming abuses, mostra que, embora o cenário seja grande, a maioria dos ataques estão focados em duas categorias SQLi e LFI 89% dos ataques.

Figura 11 extraída em 18/05/2022 <https://blog.convisoappsec.com/sql-injection-sao-como-baratas-digitais/>

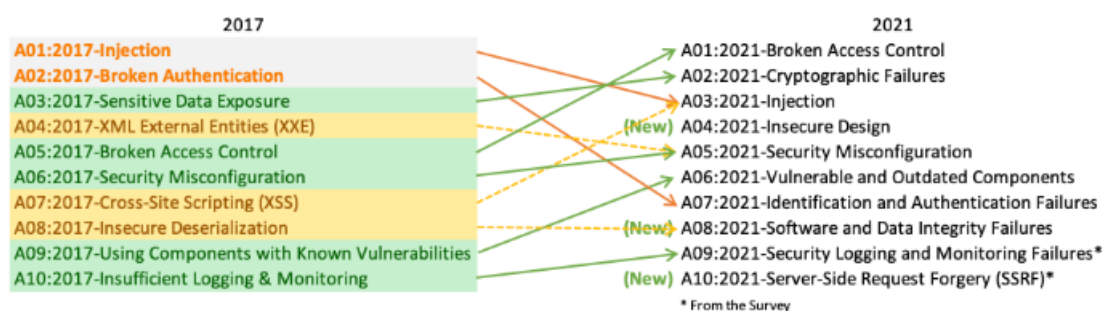
Esse gráfico mostra a porcentagem de ataques a cada tipo de malware.



Owasp divulgou as maiores vulnerabilidades de 2021; o ranking foi feito com aproximadamente 500 mil aplicativos fornecidos por um número não revelado de organizações. Esta foi a maior e mais abrangente amostra, os principais fornecedores de dados foram AppSec Labs, GitLab, Micro Focus, Sqreen, Cabalt, Io entre outros.

Ranking atualizado 2017 x 2021

Figura 12 onde a OWASP fez um comparativo dos mesmos ataques sofridos em 2017 e 2021 <https://blog.convisoappsec.com/sql-injection-sao-como-baratas-digitais/>



11. ESTUDO DE CASO e ANÁLISE DOS RESULTADOS

Em junho de 2021, a Labs grupo FLEURY ficou por uma semana com o sistema fora e os clientes não conseguiam marcar exames (ITFORUM 2021) nem pegar o resultado de exames feitos. Segundo o site Bleeping Computer, (G1- GLOBO 2021) “diversas fontes” confirmaram que o ataque do tipo ransomware, o grupo Fleury não confirmou. Mas, de acordo com a publicação especializada em cibersegurança, o grupo criminoso REvil (G1-GLOBO 2021) estaria por trás desse ataque.

Outro caso ocorrido em 2021, relatado na revista (ISTO É 2021) o grupo das lojas americanas, detentora dos e-commerce Americanas, foi vítima, invadida e bloqueada por hacker, Americanas perdeu 12% em valor de mercado, os papéis oscilaram de R\$33,72 (sexta-feira, 18, véspera do ataque) para R\$29,69 (quarta-feira, 23) e fecharam uma semana depois a R\$32,45, números gigantescos como 398,3 milhões de transações e 49,98 milhões de clientes no acumulado de 12 meses, Guazzelli diz que toda ação tem que ser tomada antes de qualquer invasão “somente atuação preventiva é eficaz”, disse depois de consumida a invasão, o estrago está feito e o invasor dá as cartas, atualmente os invasores pedem resgate em criptomoedas. A Americana (InFoMoney 14/03/2022), em seu comunicado, disse que o e-commerce foi suspenso por causa de um incidente de segurança, disse que sua base de dados não foi comprometida, não disse que invasão sofreu, só quis manter seus parceiros informados do incidente sem dar maiores detalhes.

É necessário que as empresas adotem uma política de segurança preventiva, isso significa restringir acesso a seu banco de dados, só tendo a senha pessoas que realmente precisam acessá-lo. o funcionário ao sair de férias, deve ter seu acesso bloqueado, caso de demissão cancelamento imediato. Importante dividir com todos os funcionários a responsabilidade da segurança treinar a equipe, estarem sempre atentos a acessos desconhecidos, seguir às normas da ISO 27001, usar senhas criptografadas onde se mescla números, letras, símbolos e complicar ao máximo, tendo o cuidado ao guardá-la. Normalmente, as empresas escondem que sofreram ataques, isso para não passar aos seus clientes, acionistas, a fragilidade do negócio.

12. CONSIDERAÇÕES FINAIS

Notou-se por meio do presente estudo que a vulnerabilidade humana é o ponto mais explorado pelos engenheiros sociais. Visto então que a segurança da informação não só depende da tecnologia, mas de humanos preparados, foi abordado a necessidade do planejamento técnico e das ações humanas. É fundamental que se conheça os riscos e as consequências, para então tomar as precauções necessárias para inibir a invasão de intruso.

Investir em treinamento da equipe, ter um profissional da área atuando ativamente, investir em equipamentos, são medidas imprescindíveis. Assim se alcançará um nível de segurança que consiga minimizar os impactos dos invasores nas instituições. Não existe Segurança 100% eficaz. Seria importante analisar sobre se ter um setor voltado para profissionais da segurança da informação, a computação em nuvem e todo um mecanismo de proteção com auxílio da inteligência artificial contra novas ameaças.

13. BIBLIOGRAFIAS:

Cleórbete Santos, 2018
Segurança digital
amazon.com Services LLC

Eduardo Tomasevicius Filho (Coeditor)
A lei Geral de Proteção de Dados Brasileira: uma Análise Setorial
Editora : Almedina; 1ª edição (3 fevereiro 2021)

Maicon Balke (Autor), Lisandra M. Fontoura (Autor), Ruan Carlo B. Pozzebon
Gerenciamento colaborativo de riscos de segurança da Informação: Uma abordagem Colaborativa para Gerenciamento de Riscos de Segurança da Informação
Editora Novas Edições Acadêmicas (20 janeiro 2017)

Routo Terada (Autor)

Segurança de Dados: Criptografia em Rede de Computador
Editora : Blucher; 2ª edição (1 janeiro 2008)

Silva, Gilson Marques
Editora Ciencias Moderna, 2011
Segurança de Informação para Leigos

William Stallings
Editora
Addison-Wesley Professional
Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud

Sites:

<https://sustenere.co/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012>

Rodolfo Francisco Paz Freire
Centro Universitário Santo Agostinho
Humberto Caetano Cardoso da Silva
Universidade Federal de Pernambuco
<http://orcid.org/0000-0001-9584-4465>

Ricardo Gomes de Queiroz
Faculdade Santo Agostinho
Amélia Acácia de Miranda Batista
Faculdade Santo Agostinho

<https://tripla.com.br/entenda-o-que-sao-vulnerabilidade/>

<https://www.compugraf.com.br/quais-as-principais-vulnerabilidades-de-uma-rede-e-como-se-prevenir/>

<https://www.gat.digital/blog/5-pilares-da-seguranca-da-informacao/>

<https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>

<https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>

<https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd>

Extraído do site <https://blog.idwall.co/iso-27001>

Bibliografia

AMARO, G. Criptografia simétrica e criptografia de chaves publicas vantagens e desvantagens.FESP

Em <http://publica.fesp.br/index.php/rnti/issue/download/4/33>

OLIVEIRA,P.E;R ANDRADE,P.T.E; D'OLIVEIRA R.L.G.RSA. Instituto de Matemática e estatísticas da Unicamp

Disponível

https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/oliv_RSA.pdf

Extraído em 21/04/2022 <https://infranewstelecom.com.br/inteligencia-artificial-na-seguranca-da-informacao/>

Extraído do site: <https://tiinside.com.br/18/03/2022/ia-e-machine-learning-aliados-da-seguranca-da-informacao/>

Extraídos em 23/04/2022 do site <https://www.perallis.com/news/o-que-e-o-owasp-top-10-quais-sao-as-vulnerabilidades-mais-comuns>

<https://www.cpqd.com.br/noticias/seguranca-cibernetica-de-redes-5g-e-o-foco-de-laboratorio-de-referencia-proposto-pelo-cpqd-a-anatel/>

<https://itforum.com.br/noticias/06-ataques-ciberneticos-que-abalaram-o-brasil-em-2021/>

<https://www.oracle.com/br/internet-of-things/what-is-iot/>

<https://canaltech.com.br/inteligencia-artificial/ia-da-meta-consegue-replicar-movimentos-de-varias-partes-do-corpo-humano-217244/>

<http://www.sindsefsp.org.br/site/noticia-texto.aspx?id=24689>

<https://itforum.com.br/noticias/06-ataques-ciberneticos-que-abalaram-o-brasil-em-2021/>

webinar fgv <https://www.youtube.com/watch?v=tmmtb2sFGuc>