UNIVERSIDADE SANTO AMARO

Superior de Tecnologia em Analise e Desenvolvimento de Sistemas

Alice Assis, Danilo Lima, Eduardo de Oliveira, Lucas Santos, Nicole Costa

SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MOBILE: ANALISE DE REDES SOCIAIS

SÃO PAULO

2020

Alice Assis, Danilo Lima, Eduardo de Oliveira, Leandro Dias, Lucas Santos, Nicole Costa

SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MOBILE: ANALISE DE REDES SOCIAIS

Projeto integrador apresentado à Universidade Santo Amaro, como requisito para aprovação na Disciplina Projeto Integrador: Segurança em Sistemas de Informação.

Orientador: Prof. Clausia Mara Antoneli

São Paulo

2020

RESUMO

Este estudo visa analisar a segurança de informação em aplicativos para dispositivos portáteis, como celular ou tablet, com o foco em redes sociais. O celular é uma ferramenta essencial nos tempos atuais, porém quanta informação é coletada de cada usuário? E como essas informações são utilizadas? A maioria dos processos que anteriormente eram feitos de forma manual ou analógica estão dando lugar a tecnologia, como por exemplo ter uma agenda de compromissos ou telefones, Os dispositivos portáteis tem facilitado levar todas as informações e até mesmo documentos consigo a todo momento, porém manter todas as informações em um aparelho eletrônico nem sempre é a melhor opção, durante a última década tivemos diversas polêmicas quanto a coleta e uso de dados na internet e em dispositivos mobile, nesse trabalho serão analisados dois casos que receberam muita atenção nos últimos anos, o aplicativo de redes sociais Facebook e a empresa de consultoria eleitoral Cambridge Analytica.

Palavras-chave: Segurança da Informação. Redes Sociais. Dispositivos Mobile. Coleta de dados.

SUMÁRIO

1 INTRODUÇÃO

2 OBJETIVOS

3 METODOLOGIA

4 CONCEITO DE SEGURANÇA DA INFORMAÇÃO

O Conceito de segurança da informação nada mais é do que a proteção contra as ameaças que possam colocar em perigo a integridade, disponibilidade e a confidencialidade.

Para que todo o processo de segurança ocorre existe inúmeros meios de proteção dessas informações.

Normalmente elas são divididas em vários outros tópicos, mas para algo mais “bruto” ela é explicada basicamente como integridade que é para garantir que pessoas não autorizadas tenham acesso a tal, disponibilidade que é para garantir que pessoas não autorizadas não tenham acesso facilmente e a confidencialidade que é para as informações permanecerem guardadas para não prejudicar ninguém.

No nosso mundo atual tem dedicado uma atenção para a informação por conta de sua importância para os negócios e as realizações de novos empreendimentos entre pessoas, empresas, nações etc.

Uma informação valiosa abre oportunidades para quem possui e podendo se tornar um cenário de negócios mais acirrados em buscas de novos mercados, acordos internacionais, poder e qualidade. O que gera competitividade e transformar assim então a informação como o principal elemento desse ambiente competitivo, gerando assim um cuidado especial de proteção.

Em outra perspectiva a falta de informação pode desencadear uma ameaça, podendo levar empresas a falência. Isto tudo graças a uma informação ruim, por isso informações tem valor, dá para transforma-las em um ativo importante para os negócios de uma informação.

Por conta de sua tamanha importância a confidencialidade tem que ser uma garantia e ser somente acessível a pessoas autorizadas a terem acesso.

Quando ocorre uma quebra de confidencialidade da informação ocorre grandes prejuízos, como o exemplo abaixo:

> Em um caso recente, um cliente de uma empresa australiana descobriu que suas informações estratégicas e de grande valor

> confidencial tinham sido vazadas por um concorrente. O vazamento foi a fonte de considerável sentimento de culpa e perdas financeiras, não apenas para o cliente da empresa, mas sim pela empresa que prestava serviços ao mesmo. Com o objetivo de preservar a relaxam com o cliente e a reputação de seus negócios a empresa começou uma investigação para determinar a causa e a fonte do vazamento. Agencias de lei também foram envolvidas na investigação.
>
> A investigação por fim mostrou que um funcionário falhou ao não segui o padrão de uma proteção adotado para documentos confidenciais. O mesmo percebeu as importâncias de tal informação e acabou as vendendo para a concorrência.
>
> O caso demonstrou que por questões de negligencias podem afetar empresas e contribuindo para suas perdas inestimáveis.
>
> Fonte: 2002 Australian computer crime and segurity Survey.

A classificação da informação da informação contribui para que exista uma espécie de filtro para a recomendação que a mesma seja classificar considerando o seu calor, requisitos, sensibilidade e critica para uma organização.

> O decreto federal n° 4.553/2002/, que disciplina no âmbito da administração pública federal, [...] estabelece que os dados considerados sigilosos ou informações cujo o conhecimento tem que ser irrestrito ou divulgação possa acarretar qualquer risco para a sociedade e do estado, bem como aqueles necessários ao resguardo da inviolabilidade do intimidar da vida privada, da honra e da imagem das pessoas, e o seu acesso e restrito e condicionado a necessidade de conhecer.
>
> Este decreto em seu art 5º, classifica os dados ou informações quanto ao grau de sigilo em quatro categorias:
>
> Ultrassecreto: aquele cujo o conhecimento não autorizado possa acarretar dano excepcionalmente grave a segurança da sociedade e do estado;
>
> Secreto: aquele cujo conhecimento não autorizado possa causar dano grave a segurança da sociedade e do estado
>
> Confidenciais: aqueles que, no interesse do poder executivo e das partes, devam ser de conhecimento restrito, e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do estado
>
> Reservados: aqueles cuja revelação não autorizada possa comprometer planos, operações ou objetivos, neles previstos ou referidos.

Assim toda informação tem um ciclo de vida, ela nasce com a produção, tem um tempo de vida útil, na qual ela é manuseada, utilizada internamente e externamente, armazenada e morre com a sua destruição.

5 VULNERABILIDADE DA INFORMAÇÃO

As vulnerabilidades estão sempre relacionadas com as fragilidades. Estas podem estar nos processos, equipamentos e nos recursos humanos.

Elas não provocam incidentes, pois são elementos fracos, necessitando de um agente causador ou de condição favorável, já que se trata de ameaças

Um ponto de desperta atenção que, apesar da evolução da segurança da informação, os ataques ainda permanecem em patamar preocupante, os ataques por meio de vírus ainda ocorrem.

Outro ponto de vulnerabilidade é sobre os funcionários e prestadores de serviços, sabendo-se que as informações e a sua exposição involuntária podem ocorrer em momentos simples do dia a dia de uma empresa, o que torna os recursos humanos uma das maiores preocupações para a implementação de segurança e treinamentos voltados para essa proteção. Por conta disso o ambiente de negócios é um dos lugares mais preocupantes para os especialistas de segurança, tudo isso por conta do crescimento das teologias, pessoas que não são especialistas m segurança de informações podem ser facilmente enganadas.

A vulnerabilidade pode vir de vários aspectos: instalações físicas e desprotegidas contra incêndios, inundações e desastres naturais, materiais inadequados, ausência de políticas se segurança para o RH (funcionários sem um treinamento devido) ausência de procedimentos de controle de acesso e de utilização de equipamentos.

Para um melhor entendimento é necessário dividir os mesmos em oito grupos:

Vulnerabilidade natural: está relacionada com a condição do ambiente, que pode colocar em risco as informações, pode ser local sujeitos a incêndios em determinado período do ano, locais próximos a rios que são propensos a inundações, áreas onde se verificam manifestações da natureza como terremotos.

Vulnerabilidade organizacional: que se diz respeito a políticas, planos e procedimentos, e a tudo que possa constituir numa infraestrutura de controles de uma organização.

Ausência de políticas de segurança e treinamento, falhas ou ausência de processos, falta de planos de contingencia, recuperação de desastres e de continuidade, ausência de deficiência da CIPA (Comissão interna de prevenção de acidentes), etc.

Vulnerabilidade física: são aos ambientes que estão sendo processadas ou gerenciadas as informações. Podendo ser, instalações inadequadas, ausência de recursos para o combate a incêndio, disposição desordenada dos cabos de energia e de rede, não identificação de pessoas e locais, portas destrancadas, acesso desprotegido as salas de computado, sistema deficiente de combate a incendido etc.

Hardware: possíveis defeitos de fabricação ou de uma configuração errada dos equipamentos podendo permitir o ataque ou a alteração dos mesmos.

Softwares: os aplicativos que possuem pontos fracos que permitem acesso indevidos aos sistemas de computadores, inclusive sem o conhecimento de um usuário administrador de redes.

Meios de armazenamento: suporte físico ou magnético utilizado para guardar informações tais como: disquetes, cd rom, fita etc

Humanas: A vulnerabilidade humana é a que mais preocupam os especialistas já que os conhecimentos de medidas de segurança são desconhecidos por pessoas que não são profissionais.

Comunicação: os pontos fracos relacionados a trafego de informações, tais como, cabo, satélite, fibra ótica, onda de rádio, telefone, internet, wap, fax , etc.

O risco tem várias origens, pode ser de eventos da natureza a uma ação intencional. Os Mesmos podem ser classificados em várias categorias, como: incontroláveis, técnicos, de mercado, de credito, operacionais, legais e humanos.

Classificar os riscos em categorias objetivas para que ajude a ter possível melhor visibilidade.

Riscos naturais são aqueles de fenômeno da natureza.

Os involuntários são os que resultam em ações não intencionais, relacionado a vulnerabilidade humana, física, de hardware, de software, dos meios de armazenamentos e das comunicações.

Os intencionais são aqueles que foram provocados por ações humanas.

6 IMPACTOS DE ROUBO DE DADOS

Quando um roubo de informações ou de dados ocorre ele cria impactos os quais são confidencialidade, modificação, perda, destruição e interrupção.

Primeiro passo antes de tudo é identificar o impacto, deve levar em consideração as atividades e os critérios definidos para o requisito confidencialidade, integridade e disponibilidade.

Ao identificar deve-se observar o que pode ocorrer se determinado requisito for quebrado. Os mais comuns são a venda de informações que podem prejudicar a empresa que foram roubados os seus dados.

> O método OCTAVE (operational Critical Threat, Asset, and Vulnerabilty Evaluation) apresenta um esquema simples, que pode facilitar a identificação de impactos.
>
> OCTAVE é um método avaliativo de riscos de segurança da informação que foi desenvolvido pelo software *Engineering Institute* da *Carnegie Mellon University.* [...], este método é baseado num conjunto de critérios. Ele define os elementos fundamentais para uma avaliação de riscos de segurança de uma organização.
>
> Livro: segurança da informação pag 96

Esses impactos devem ser classificados em níveis, alto, médio, baixo e desprezível, esses quatro níveis devem ser utilizados na análise dos riscos identificados.

As análises de riscos desenvolvem um entendimento sobre os riscos e impactos nas atividades de negócios e ativos envolvidos, no sentido de orientar as melhores estratégias para o tratamento dentro da relação custo benefício. Assim com base na análise são realizadas e estabelecidas o estado de impacto, após este momento entra a avaliação de riscos.

A avaliação de riscos é realizada uma comparação entre a classificação de cada risco analisado e o critério estabelecido pela organização quando da escolha do método de avaliação.

Esses parâmetros são referências escolhidas para organizar e decidir o tipo de segmento que iram tomar.

Abaixo, citamos alguns casos de roubos e vazamentos de dados

7 TENDÊNCIAS DE SEGURANÇA

Em 1994 foi emitido relatório, onde já se estabelecia um consenso da necessidade de mecanismos de segurança para usuários e empresas ao utilizar a internet, como autenticação e criptografia.

Desde 1995, os ataques vêm crescendo, nos diversos sistemas operacionais e roteadores, por exemplo, a falsificação de IP, para explorar aplicações que usam autenticação, tendo acesso as informações transmitidas como, logon e conteúdos do bando de dados.

Com o aumento dos usuários de internet e com maior complexidade dos protocolos e aplicações da rede, as invasões tem sofrido um crescimento exponencial, cada vez mais sofisticados e exigindo menos habilidades dos invasores.

8 A ARQUITETURA DE SEGURANÇA OSI

A arquitetura de segurança OSI (open systems interconnection), é útil para que gerentes possam organizar meios de seguranças, afim de, evitar quebra e vazamento de dados. Pelo fato de ser uma arquitetura de utilização internacional, é utilizada para desenvolver recursos de segurança para muitos equipamentos. Abaixo temos as características de Arquitetura de Segurança OSI:

- Ataque à segurança: Qualquer ação que comprometa a segurança da informação pertencente a uma organização.
- Mecanismo de segurança: Um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou permitir a recuperação de um ataque à segurança.
- Serviço de segurança: Um serviço de processamento ou comunicação, que aumenta a segurança dos sistemas de processamento de dados e as transferências de informação de uma organização. Os serviços servem para frustrar ataques à segurança e utilizam um ou mais mecanismos de para prover o serviço.

Definições para Ataque e Ameaça, segundo a RFC 2828 (Request for Comments)

- Ameaça: Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Portanto, a ameaça é um possível perigo que pode explorar uma vulnerabilidade.
- Ataque: Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços e violar a política de segurança de um sistema.

8.1 ATAQUES À SEGURANÇA

Ataques à segurança são divididos entre passivos e ativos. Ataques passivos tem como objetivo espionar e ou monitorar transmissões, com a finalidade de coletar dados trocados em uma conversa e troca de e-mails, tudo isso ocorre sem que as pessoas envolvidas notem a terceira pessoa observando o conteúdo, pois, esse ataque geralmente não deixa rastro e não realiza nenhuma alteração nos dados transmitidos.

Ataques ativos são subdivididos em quatro categorias: disfarce, repetição, modificação de mensagens e negação de serviço.

- Disfarce: ocorre quando uma entidade finge ser outra com privilégios, podendo usar sequências de autenticação captadas e reproduzi-las, depois que ocorrer uma sequência válida, fazendo assim se passar pela entidade com privilégios
- Repetição: captura uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado.
- Modificação de mensagens: simplesmente ocorre quando uma mensagem é alterada, reordenada ou adiadas para produzir um efeito não autorizado, como, por exemplo, dar acesso a algum arquivo ou conteúdo a alguém com poucos privilégios.
- Negação de serviço: ataca instalações de comunicação, no qual afeta o fluxo de dados e informações transmitidas com a interrupção de uma

rede inteira, utilizando a desativação ou sobrecarga do sistema com mensagens para prejudicar a performance.

Apesar de os ataques passivos serem difíceis de detectar, eles podem ser impedidos com pouca dificuldade, ao contrário dos ataques ativos que podem ser detectados, porém, devido a sua variedade e a vulnerabilidade dos softwares eles podem causar grandes transtornos e possíveis danos. Mas quando detectados e os softwares de proteção possuírem recursos de defesas necessárias elas podem contribuir para intimidar e prevenir novos ataques.

8.2 SERVIÇOS DE SEGURANÇA

São serviços de processamentos fornecidos com algumas especificações distintas, onde trabalham de formas diferentes afim de proteger comunicações e dados transmitidos por seus usuários. Esses serviços são divididos em cinco categorias para distintas funções autenticação, controle de acesso, confidencialidade de dados, irretratabilidade e disponibilidade.

- Autenticação: O serviço de segurança garante que o remetente dos dados são realmente quem diz ser, assim como o receptor seja quem se apresenta, afim de evitar que um terceiro possa se passar por qualquer uma das partes.
- Controle de acesso: realiza o controle de acesso a determinadas áreas de acordo com os privilégios do usuário.
- Confidencialidade de dados: faz a proteção de dados transmitidos contra ataques passivos, obstruindo um possível intruso de observar ou até coletar dados em uma transmissão ou conversa.
- Irretratabilidade: serviço que confirma o envio ou recebimento de mensagens, mesmo que o emissor ou o receptor aleguem não ter enviado ou recebido.
- Disponibilidade: serviço que garante a proteção de ataques cujo o intuito é derrubar ou causar lentidão em um servidor de acesso mutuo, garantido assim o acesso e proteção aos usuários.

8.3 MECANISMOS DE SEGURANÇA

Aqui abordaremos mecanismo de criptografia que são divididos entre reversíveis e irreversíveis.

- Criptografia reversível permite a alteração no envio e reorganização no recebimento.
- Criptografia irreversível incluem algoritmos de hash e código de autenticação de mensagens.

Mecanismos de segurança específicos

Podem incorporar camadas de protocolos a fim de oferecer serviços de segurança OSI

- Cifragem: utiliza algoritmos matemáticos convertendo dados em um formato que não seja decifrável, a transformação e recuperação de dados depende de um algoritmo e algumas chaves de criptografia.
- Assinatura digital: dados anexados a um arquivo ou unidade de dados que permite ao destinatário comprove a veracidade do mesmo.
- Controle de acesso: uma série de mecanismos que impõe direitos de acesso aos recursos.
- Integridades de dados: série de mecanismos que garantem a integridade e ou fluxo de dados.
- Troca de informações de autenticação: mecanismo que tem objetivo de identificar um usuário por troca de informações.
- Preenchimento de tráfego: realiza inserção de bits em um fluxo de dados para interferir tentativas de análise de dados.
- Controle de roteamento: permite controlar as melhores rotas para tráfego de dados e analisar a melhor rota em caso de suspeita de rota comprometida.
- Certificação: utiliza uma terceira entidade que garante propriedades especificas em uma troca de dados.

Mecanismos de segurança pervasivos

Mecanismos que não são específicos a serviços de segurança OSI ou camadas de protocolo especifica

- Funcionalidade confiável: considerada sendo correta em relação a alguns critérios.
- Rótulo de segurança: estabelece vínculo a um recurso que nomeia ou constitui atributos de segurança a esse recurso.
- Detecção de evento: relevantes à segurança.
- Registros de auditoria de segurança: coleta dados e pode utiliza-los para abreviar uma auditoria de segurança, que revisa e examina registros e atividades do sistema.
- Recuperação de segurança: lida com tratamentos e gerenciamentos de eventos solicitados por mecanismos, e realiza medidas de recuperação.

9 UM MODELO PARA SEGURANÇA DE REDE

Os modelos para segurança de rede incluem chave de criptografia no qual a mensagem enviada sofre alterações e fica ilegível caso seja interceptada, e só possa ser reorganizada pelo receptor destinado. Porém, modelos de segurança não se concentram apenas em criptografia de dados em uma conversa ou troca de dado, ela também está presente na parte de proteção contra vírus ou vermes (worms), que são utilizados em sua grande maioria com o intuito de roubar dados, prejudicar de alguma forma a empresa que utilize o servidor que sofreu o ataque, ou em alguns casos por hackers que os utilizam pelo único motivo de se satisfazer por ter rompido o sistema de segurança de determinado servidor.

Para essas situações entram em ação os modelos de segurança que utilizam procedimentos de login e senha, que tentam barrar o acesso a intrusos, caso essa primeira barreira seja rompida entra em ação procedimentos de filtragem e analise de atividade para detectar o intruso indesejado.

10 CRIPTOGRAFIA DE DADOS EM REDES SOCIAIS

A criptografia de dados já existe no mundo a milhares de anos, datada desde o Egito antigo, até os dias atuais em vários momentos. Atualmente ele é muito utilizado em aplicativos de conversa instantânea como Whatsapp e Telegram, onde se faz muito importante para a confidencialidade do assunto em discussão entre o destinatário e o remetente.

Nesses casos a criptografia utiliza algoritmos matemáticos para substituir e embaralhar o conteúdo da conversa, transformando em códigos que apenas o destinatário consegue decodificar e reorganizar o conteúdo na maneira correta.

Porem outros aplicativos de redes sociais como Facebook e Instagram ainda pecam nessa área de criptografia de dados, principalmente em suas ferramentas de conversa instantânea (Messenger e Direct). Mesmo após o anuncio do CEO Marck Zuckerberg em 2019 informando a implementação de Criptografia em suas redes sociais, hoje esse sistema de segurança ainda não foi implementado, tendo em vista a complexidade necessária para a atualização. Tendo em vista que o próprio Messenger precisaria ser reformulado quase que por completo, o que pode levar mais tempo do que o planejado inicialmente.

11 PORQUE É IMPORTANTE CONHECER CÓDIGOS?

Desde os primórdios da humanidade, houve a necessidade de se comunicar, seja por desenhos, sons ou linguagens verbais. Cada linguagem hoje conhecida é um tipo de código, o português que falamos hoje é um código que foi estruturado para facilitar a compreensão, há também códigos de leis, de programação, de comunicação visual, entre outros. Dessa mesma forma, para que os computares e demais dispositivos eletrônicos possam entender os nossos comandos, são utilizados códigos, sejam eles binários, hexadecimais, ou alguma linguagem de programação, como Java, Python, entre outros.

Silva, Araújo e Azevedo (2014, p. 02), observam:

> Com base na obra “O livro dos códigos), de Simon Singh (2001), observa-se que desde o antigo Egito a informação é vista como elemento de valor, cuja importância se revela segundo os interesses culturais, políticos e econômicos da sociedade. Observa-se, assim, a existência e a evolução de uma “batalha intelectual” entre os criadores de códigos e os decifradores, ou seja, de um lado o emissor que transmite a mensagem em códigos, quando aplicável, para que ela possa chegar de uma forma segura ao seu receptor – povos, governos, pessoas ou organizações, e do outro, os decifradores, que buscam decodificar as mensagens a de obter vantagem da informação decodificada, seja para fins militares, pessoais ou para corporativos.

Como citado pelos autores, a informação sempre foi e ainda é uma ferramenta valiosa, podendo ser utilizada de diversas formas, sejam elas econômicas, políticas ou culturais, aquele que detêm o conhecimento desses códigos possui de certa forma uma vantagem sobre aqueles que não a possuem. Aplicando tal conceito a segurança de informação, pode se entender que, quem compreende essa emissão e compreensão de códigos se torna menos vulnerável, por exemplo, compreendendo o funcionamento e a estrutura de um código computacional é possível encontrar falhas e até mesmo notar modificações na estrutura dos códigos, tornando-se assim menos vulnerável a ataques, sejam ele movidos por falhas no corpo do código ou por um malware.

Outra vantagem que conhecer códigos e linguagens de programação proporcionam, é a opção de criar softwares que proporcionem uma maior segurança para seus usuários, sejam eles pessoas físicas ou empresas, de forma que contenham o menor número possíveis de bugs.

Estamos a todo tempo cercados de tecnologia, a todo momento estamos com nossos celulares, tablets, laptops ou qualquer outro dispositivo que está conectado a internet, portanto é importante se proteger cada vez mais, pois a sociedade tem se tornado cada vez mais vulnerável graças a tecnologia.

Sabemos que nem todas as pessoas que possuem conhecimentos sobre códigos computacionais vão utiliza-las de forma benéfica, alguns hackers utilizarão esse conhecimento para tirar vantagem e até mesmo cometer crimes, esses hackers se aproveitam de qualquer falha que encontram, sejam bugs ou através de vírus.

12 O QUE É UM BUG?

Bug é um termo muito utilizado nas áreas da informática para descrever falhas inesperadas que podem causar mal funcionamento ou danos em um software ou hardware.

A origem do termo bug vem do inglês que significa inseto, não é certo o porque desse termo ser usado para falhas, mas a explicação com maior aceitação diz que em 1947 houve uma falha no computador MARK II, utilizado pela marinha dos Estados Unidos da América, ao verificar o computador o operador William Burke encontrou uma mariposa, então escreveu em seu diário de bordo que havia encontrado um inseto no computador.

Ao lançar um software, os desenvolvedores precisam realizar diversos testes para que haja o menor número possível de falhas, e quando essas falhas são descobertas é necessário conserta-la o mais rápido possível. Para que essas falhas não passem para a versão final do software, é comum que os desenvolvedores forneçam antes uma versão beta para ser testada por uma parcela dos usuários.

Os bugs caracterizam vulnerabilidades no sistema, que podem ser graves ou não. Invasores ou Hackers, como são mais conhecidos, podem encontrar tais vulnerabilidades e utiliza-las de alguma forma. Muitas empresas gratificam invasores que as enviam falhas de acordo com a gravidade da falha.

Os softwares atuais, sejam eles redes sociais, ou programas que são utilizados no computador ou celular, contém cada vez mais bugs, pois estão cada vez mais complexos, mas isso não quer dizer que estejam mais seguros, exatamente o contrário, quando um software se torna mais complicado, automaticamente se torna maior, quando se trata de códigos e portanto contém cada vez mais bugs, para estimar essas falhas é utilizada uma métrica chamada de KLOC.

13 O QUE É E PARA QUE SERVE O KLOC?

KLOC ou Kilo Lines Of Codes, em tradução livre significa mil linhas de código. O Kloc é uma métrica de analisa o número de bugs a cada mil linhas de código, geralmente a cada KLOC temos de 5 a 50 bugs.

Um software que passar por uma análise de qualidade rigorosa pode conter em torno de 5 bugs por KLOC, já um software que passa apenas por uma analise básica, onde são testadas as funções principais, podem conter em torno de 50, o que é o caso da maioria dos softwares dos mercado.

Por mais que os desenvolvedores acreditem que fizeram um teste que qualidade rigoroso, na maioria das vezes, apenas verificaram superficialmente.

Devido a crescente complexidade dos sistemas de software, há cada vez mais bugs, por exemplo, em 1983 o software Microsoft Word continha em torno de 27 mil linhas de códigos, levando em consideração que a maioria dos softwares passam apenas por testes superficiais, podemos estimar em torno de 1 milhão de bugs. Um bug não necessariamente representará uma falha 4grave de segurança, porém quanto mais bugs, maior a possibilidade de se encontrar uma falha grave. Já em 1995, o mesmo software continha em torno de 2 milhões de linhas, aumentando assim o potencial de bugs.

Todo software está vulnerável a conter bugs, seja ele um sistema operacional, como por exemplo o Windows XP, que em 2002 foi lançado com 40 milhões de linhas de código, e poucos meses depois foram encontradas falhas graves, ou seja uma rede social.

Com todos os sistemas conectados em uma rede de internet, como é comum hoje, essas falhas podem se tornar um problema ainda maior.

14 O QUE ISSO TEM A VER COM REDES SOCIAIS?

Atualmente a sociedade está cada vez mais conectada, estão sendo criadas cada vez mais redes sociais, como por exemplo o Facebook, TikTok, Instagram entre outras. Essas redes sociais são usadas em computadores pessoais, celulares, tablets e até mesmo em computadores de empresas.

Como visto no tópico anterior, quanto maior um software é em linhas de código, maior a possibilidade de se encontrar um bug. Em 2015 o aplicativo Facebook já continha em torno de 62 milhões de linhas de código. Levando em consideração o Kloc, o Facebook pode ter de 310 milhões a 3.1 bilhões de bugs, mesmo que nem todos esses bugs sejam graves, ainda assim é possível encontrar diversos erros graves dentre eles.

Segundo os termos do Facebook:

> Conforme descrito abaixo, coletamos informações de e sobre computadores, telefones, TVs conectadas e outros dispositivos conectados à web que você usa e que se integram a nossos Produtos, e combinamos essas informações dos diferentes dispositivos que você usa. Por exemplo, usamos as informações coletadas sobre seu uso de nossos Produtos em seu telefone para personalizar melhor o conteúdo (inclusive anúncios) ou os recursos que você vê quando usa nossos Produtos em outro dispositivo, como seu laptop ou tablet, ou para avaliar se você, em resposta a um anúncio que exibimos em seu telefone, realizou.
>
> As informações que obtemos desses dispositivos incluem:
>
> Atributos do dispositivo: informações como o sistema operacional, as versões do hardware e software, nível da bateria, força do sinal, espaço de armazenamento disponível, tipo de navegador, nomes e tipos de arquivo e de aplicativo, e plugins.

> Operações do dispositivo: informações sobre operações e comportamentos realizados no dispositivo, tais como se uma janela está em primeiro ou segundo plano, ou movimentos do cursor (que podem ajudar a distinguir humanos de bots). uma ação em um dispositivo diferente. [..]
>
> Rede e conexões: informações como o nome de sua operadora móvel ou provedor de serviço de internet, idioma, fuso horário, número do celular, endereço IP, velocidade de conexão e, em alguns casos, informações sobre outros dispositivos que estão nas proximidades ou em sua rede, de forma que nós possamos fazer coisas como ajudar você a realizar o streaming de um vídeo de seu celular para sua TV.
>
> Dados de Cookies: dados de cookies armazenados em seu dispositivo, inclusive configurações e IDs de cookies. Saiba mais sobre como usamos cookies na Política de Cookies do Facebook e na Política de Cookies do Instagram.

Como podemos observar, o Facebook coleta diversas informações sobre o nosso uso, não somente da rede social, mas do dispositivo que está sendo usado, localização entre outras informações, portanto levando em consideração a estimativa de bugs que o aplicativo pode conter, podemos entender o porque tais bugs são tão relevantes.

Atualmente o Facebook recompensa aqueles que descobrem e reportam as falhas, porém sabemos que nem todas as pessoas possuem boas intenções, por consequência já houveram diversos ataques a rede, sendo o ultimo deles em 2018, onde foram resetados os tokens, que permitem que o aplicativo permaneça logado, de 50 milhões de contas, dando assim o controle das contas para os hackers.

De acordo com o Facebook essa falha já foi removida.

15.1 Uso de Redes Sociais

Vivemos em um tempo em que a popularização da internet tem avançado a ponto de ser incomum alguém não possuir smartphones e redes sociais, seja este de qualquer idade ou classe social, pessoas que não possuem tais coisas são consideradas quase incomunicáveis.

Segundo estudos realizados pelas empresas *We Are Social* e *Hootsuit*, cerca de 2/3 da população brasileira está conectada a internet, gastando cerca de 9 horas conectadas, dessas 3 são usadas exclusivamente para uso de redes sociais, um estudo da *GlobalWebIndex* aponta o Brasil como segundo no ranking de uso de redes sociais, gastando em 2019 cerca de 225 minutos de uso por dia, pouco a mais que o ano anterior, a utilização de mídias sociais ainda é predominante entre os jovens, estes tem certa tendência a serem mais engajados, e os criadores de conteúdo sabendo dessa propensão ao uso da internet têm trabalhado em algoritmos cada vez mais inteligentes e assertivos na hora de recomendar aquilo que pareça agradável aos nossos gostos e forma de pensar.

Passando tanto tempo “conectados” ficamos expostos a alguns problemas, além de mudanças psicológicas e comportamentais negativas, dentro desses ambientes virtuais fazemos um grande compartilhamento de dados pessoais e/ou profissionais como: círculo social, lugares que frequenta, endereço, número de telefone e fotos em redes sociais. Seja de forma pública ou em conversas privadas, o grande problema é que não sabemos exatamente até que ponto isso é seguro para nossa privacidade, diversas pessoas já sofreram com ataques cibernéticos feitos por pessoas mal intencionadas, que fazem o uso das mesmas redes sociais e enxergam a vulnerabilidade que existe na exposição de tantos dados pessoais.

15 EXEMPLOS DE ATAQUES EM REDES SOCIAIS.

15.1 FACEBOOK:

Segundo investigações que foram feitas pelo jornal americano The New York Times, que cerca de 30 milhões de contas de usuários do Facebook tiveram seus dados como nome, conversas privadas e preferências vazadas à empresas privadas. (GAUCHAZH,2018).

15.2 GOOGLE+:

Devido a dois incidentes ocorridos em 2018 e 2019, cerca de 50 milhões de usuários da rede social Google+, uma rede social da Google que entrou no mercado para competir com outras redes sociais, devido a um erro em suas APIs, tiveram seus dados como profissões, nomes, e-mails, idade vazados para 38 aplicativos conectados à rede social, ocasionando o seu encerramento para agosto de 2019 (TECHTUDO, 2019).

15.3 TWITTER:

tiveram acesso a conversas privadas e posts protegidos onde o seu autor delimita quem pode ter acesso a elas, devido a um bug encontrado na API da plataforma. O site afirma que o problema pode ter ocorrido devido aos desenvolvedores possuirem as suas assinaturas digitais configuradas para domínios que foram resolvidos para o mesmo IP7 público. Segundo o Twitter apenas 1% dos seus 335 milhões de usuários foram afetados (TIINSIDE, 2017).

Segundo a Cartilha de Segurança para internet, que foi criada para orientar os usuários de redes sociais, (Cartilha cert.br)

> Os principais riscos de algum ataque devido à falta de cuidado na internet são: furto de identidade (perfil *fake*); invasão de perfil (através do uso de páginas falsas ou computadores infectados); uso indevido de informações (incluindo o uso de questões de segurança usadas para recuperação de senhas); vazamento de informações (conteúdos sigilosos de empresas divulgados na internet); vazamento de informações confidenciais (persuasão para fornecimento de e-mail, endereço, telefone, etc); sequestro (através da localização do usuário por meio do uso de aplicativos para fazer check-in em lugares como restaurantes, cinemas e outros); furto de bens (comentários de que está fora de casa num determinado período); recebimento de mensagens maliciosas; acesso a conteúdos impróprios ou ofensivos; danos a imagem e à reputação (ex.: calúnia e difamação)

16 COMO SE PROTEGER?

Um fato é que estamos o tempo vulneráveis a sofrer ataques e ter os nossos dados e até mesmo documentos comprometidos, mas existem algumas formas de dificultar os ataques.

Para empresas, a melhor medida é criar testes de segurança mais rigorosos, pois as invasões geralmente possuem um padrão de ataque, então é

necessário testar todas as possibilidades de invasão além das funcionalidades principais.

Já para usuários individuais, existem diversas formas de se proteger, usar antivírus sempre é uma boa opção, mas além disso pode-se recusar diversas permissões em aplicativos, como acessar seus contatos, localização, câmera, rodar em segundo plano, entre outros.

Atualmente diversos aplicativos possuem a opção de verificação em 2 ou mais etapas, como aplicativos de banco, Facebook, e-mail e assim por diante. A verificação de duas etapas torna seus aplicativos mais seguros pois precisam de uma segunda validação fora do aplicativo, para garantir que é realmente é o usuário tentando acessar o aplicativo.

Uma das opções mais importantes é não salvar suas senhas no dispositivo ou navegador de internet, pois, caso seu computador ou dispositivo móvel seja invadido ou infectado com um vírus, todas as suas contas e informações estão comprometidas e acessíveis ao invasor.

Por último, downloads de fontes duvidosas são na maioria das vezes um problema, pois além de muitas vezes ser algo ilegal, você ainda está correndo o risco de comprometer todos os dados e arquivos do seu dispositivo.

Em suma, podemos concluir que, é impossível estar cem porcento seguro na internet, porém é necessário tomar o máximo de precauções para que o ambiente virtual seja sempre pacifico e com o mínimo de riscos possíveis.

16.1 CRIPTOGRAFIA E SEGURANÇA

> A criptografia refere-se ao processo matemático de tornar uma mensagem impossível de ser lida, é um conjunto de regras que visa fazer a codificação da informação onde apenas o emissor e o receptor conseguem ter acesso a elas (Surveillance Self-Defense, 2018)
>
> .

Quando uma mensagem é enviada a partir de um aplicativo de troca de mensagens, quer dizer que estamos enviando informações de um lugar para outro, isso é chamado de “dados em movimento”, significa que a informação sai

do dispositivo, passa pelos servidores da empresa prestadora do serviço até chegar no outro lado que seria o destinatário. Hoje, temos métodos de criptografia que nos auxiliam a fazer a proteção desses dados em movimento: TLS (*Transport Layer Security*) que em português seria a segurança na camada de transporte e o ponta-a-ponta.

16.2 ENCRIPTAÇÃO TRANSPORT LAYER SECURITY

A encriptação TLS, faz a proteção das mensagens durante seu trajeto, o remetente faz o envio da mensagem, que é encriptada e transmitida para uma torre de comunicação, que passa pela empresa provedora do serviço, que faz a desencriptação, mantem uma cópia da mensagem e reencripta para que chegue até o destino da mensagem, onde é feito novamente a desencriptação para que possa ter acesso ao conteúdo.

Hoje, é assim que o *Facebook* faz o tratamento das nossas conversas nos aplicativos de bate-papo, sempre mantendo um “histórico” das mensagens com o pretexto de usabilidade, caso precisemos de alguma informação, vai estar lá pois já a enviamos previamente. Com isso elas conseguem manter uma cópia desse conteúdo caso alguma autoridade faça a requisição ou até mesmo se tornem vulneráveis a vazamentos caso os servidores sejam alvo de ataques de *crackers* ou brechas nos sistemas.

16.3 ENCRIPTAÇÃO PONTA-A-PONTA

> Com a grande quantidade de incidentes de vazamento de informações que são compartilhados apenas em conversas privativas, o *Facebook* está com o projeto de implementar o *end-to-end* (ponta a ponta) como principal método de criptografia nos seus aplicativos de conversas e troca de mensagens entre usuários, sem que seja um recurso extra e sim um recurso que é ativado automaticamente (Newsroom Facebook, 2019).

A criptografia de ponta-a-ponta faz a proteção da mensagem durante todo o percurso, ela faz com que as informações contidas sejam transformadas em uma mensagem secreta, ela envia a mensagem como uma carta fechada, ninguém, nem mesmo o aplicativo por onde a mensagem está sendo enviada tem acesso ao conteúdo da mensagem.

Segundo o CEO6 do Facebook, Mark Zuckerberg.

> A criptografia de ponta-a-ponta é uma importante ferramenta no desenvolvimento de uma rede social centrada na privacidade. A criptografia ajuda a descentralizar – ela limita serviços como os nossos de ver o conteúdo que está fluindo através deles e dificulta muito o acesso de qualquer um às suas informações". 5.10 Exemplo de Aplicação de Criptografia Ponta-a-Ponta Assim como sugerido por Mark Zuckerberg em 2018, uma das possíveis soluções a se implementar nos seus aplicativos de bate-papo é a criptografia ponta-a-ponta que já foi mencionada, esse recurso já está disponível para utilização no aplicativo do Facebook, porém é necessário fazer a sua ativação manualmente.

16.4 VANTAGENS E DESVANTAGENS DA CRIPTOGRAFIA PONTA-A-PONTA

Vantagem: a aplicação desse tipo de criptografia, é se assegurar que apenas as pessoas inseridas na conversa vão ter acesso às mensagens enviadas, dando mais privacidade e confiança aos seus usuários, sabendo-se que nem mesmo o provedor do serviço de mensagens vai poder ter acesso ao conteúdo da conversa

> As mensagens enviadas estarão mais seguras pois cada uma delas terá um cadeado que somente as pessoas envolvidas terão acesso a chave secreta para desbloqueá-

> las e terem acesso ao seu conteúdo (Surveillance Self-Defense, 2018).

Desvantagem: esse tipo de serviço pode ser utilizado por terroristas e pessoas de má índole, para planejarem e executarem ações que possam prejudicar a sociedade.

17 RECOMENDAÇÕES E DICAS DE SEGURANÇA PARA O USO DE REDES SOCIAIS

Diante dessas informações devemos avaliar nosso uso de redes sociais, para que não caiamos em golpes e armadilhas para algum crime cibernético que possa vir a ferir nossa imagem ou causar outros tipos de prejuízo, abaixo listaremos alguns cuidados que temos que ter no uso para que nos tornemos menos vulneráveis a possíveis ataques.

17.1 VERIFICAR SE ESTA É A PÁGINA CORRETA

Se faz necessário devido a muitos *crackers* criarem páginas idênticas às originais para fazer o roubo de informações como e-mails e senhas de seus donos. Assim podendo acessar contas e se passando por seus usuários.

Hoje em dia podemos fazer a verificação de modo simples, em seu navegador, do lado onde é inserido o link do site, podemos ver um cadeado fechado na cor verde, que identifica que é um site seguro que permite que os dados inseridos pelos usuários estejam trafegando criptografados entre o computador e o servidor.

17.2 CONTROLAR QUEM TEM ACESSO A INFORMAÇÕES PESSOAIS

Dentro das redes sociais podemos adicionar outros usuários, muitas vezes adicionamos pessoas com o mesmo tipo de interesse ou até mesmo conhecidos de outros colegas para que possamos nos relacionar com novas pessoas, dando a elas acesso à informações privadas disponíveis no nosso

perfil, apenas pessoas que estão conectadas podem tem acesso às informações que compartilhamos no perfil, porém, a rede social permite separar em grupos tais como: família e colegas de trabalho e delimitar o acesso a determinado tipo de informação para cada um deles, dando mais controle ao dono do perfil..

17.3 PRIVACIDADE DO PERFIL

As redes sociais possuem configurações de privacidade, onde podemos definir quem pode acessar determinado tipo de conteúdo tais como: fotos, posts, vídeos e etc. Assim podemos evitar que pessoas indesejadas tenham acesso a esse conteúdo.

18 CONCLUSÃO

REFERÊNCIAS

Época Negocios. **Os 21 maiores casos de violação de dados de 2018**. 2018. Disponível em: < https://epocanegocios.globo.com/Empresa/noticia/2018/12/os-21-maiores-casos-de-violacao-de-dados-de-2018.html>. Acesso em: 31 ago. 2020.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI: da Estratégia à Gestão dos processos e Serviços**. 4ª ed., São Paulo: Brasport, 2014.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Pearson, 2015.

HOGLUND, Greg; McGRAW, Gary. **Como Quebrar Códigos: A Arte de Explorar (E Proteger)** Software. São Paulo, 2006.

Information is Beautiful. **Million Lines of Code**. 2015. Disponível em: <https://www.informationisbeautiful.net/visualizations/million-lines-of-code/>. Acesso em: 05 out 2020.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6ª ed., São Paulo: Pearson, 2015.

SILVA, Narjara Bárbara Xavier; ARÁUJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-americana de Ciência da Informação.** Disponível em : <http://eprints.rclis.org/23226/>