Segurança em Computação: Trabalho Pensamento de Segurança

Rafael Begnini de Castilhos (20205642)

10 de maio de 2022

Resumo

Steam, a plataforma de mídias digitais e como é estruturada pensando em segurança da computação. Quais são os ativos que demonstram ser expressivos? Qual o perfil do adversário que cometeria um ataque? Como é realizado o gerenciamento de risco ponderando o custo/benefício? Existem contra medidas para mitigar os problemas?

Sumário

1 Introdução

O presente relatório possui como objetivo estudar e analisar o sistema da Steam (software de gestão de direitos digitais), com a finalidade de exercitar a forma de pensar como um profissional de segurança em computação

2 Sistema Escolhido

O sistema escolhido para este trabalho foi a Steam, que é uma das lojas de games para computador mais populares e foi originalmente uma ideia para resolver problemas de atualizações dos títulos da Valve, lançado em 2002.

A Steam é um sistema no qual seus usuários podem ter o acesso ao jogos de modo gratuito ou pago, além disso, dentro de cada jogo o usuário possui um inventário, na qual possui itens que podem ser utilizados dentro do jogo de maneira à customizar a experiência do jogador. Ela também funciona como uma espécie de rede social onde usuários podem trocar mensagem de texto, buscar e comparar perfis de outros jogadores.

Para abordar situações indesejadas ao que tange os aspectos de segurança computacional, a Steam possui uma política rígida de punição para os usuários que cometem ações ilícitas nos diferentes serviços do sistema. As punições variam de punições de suspensão ao perfil do usuário até o banimento completo da conta de usuário. Como todo sistema já existente, o sistema de segurança da Steam não é impenetrável.

3 Ativos

O ativo mais importante dentro do sistema é o banco de dados, contendo informações e arquivos-fonte de jogos, vendas, além dos dados de outros usuários envolvidos no ecossistema. Apesar de nenhum desses ativos ser financeiramente mensurável, é evidente que a perca, alteração ou uso indevido dos dados pode acarretar em problemas para a reputação da empresa.

Outro ativo expressivo é as informações de cartão de crédito, pois as compras feitas na plataforma dão como opção ao usuário, guardar as informações do cartão, a fim de que nas próximas compras não seja necessárias digitar as informações novamente toda vez que uma compra for efetuada, inclusive a senha do cartão.

Por fim, mas não menos importante, as contas dos usuários também é um ativo pois possuem informações pessoais do usuário, jogos digitais, histórico de mensagens de conversas, configurações pessoais, itens no inventário e entre outras informações cuja visualização é limitada para apenas o dono da conta.

4 Adversários

Um dos possíveis adversários seria os funcionários das empresas concorrentes como Origin e Epic Games. Esses funcionários, sob ordem maior poderiam atacar o sistema com objetivo de afetar moralmente e a médio prazo ser desvalorizada no mercado. Nesse viés, os concorrentes conquistariam os usuários que até então estavam usando o sistema da Steam, ampliando a quantidade de usuários ativos, e consequentemente ampliando a renda. O tipo do perfil desse adversário, possui conhecimentos técnicos para contornar a segurança e procuram formas para quebrar o mecanismo de segurança, além disso pode possuir poder computacional.

Outros prováveis adversários seriam os usuários da própria plataforma que buscam achar falhas de segurança dentro do sistema, para que assim consigam se beneficiar por intermédio de acesso dos conteúdos digitais sem nenhum tipo de custo, podendo ser considerado um vazamento. Entretanto esse tipo de adversário possui um perfil menos técnico e com pouco poder computacional, mas que mesmo assim se dispõem a conquistar novos conhecimentos para conseguir as vantagens indevidas.

Além disso, um possível adversário seria o usuário que possui elevado conhecimento técnico na área de segurança da computação, mas não detêm nenhum objetivo em específico, mas que por interesse em encontrar brechas pode identificar os problemas que a empresa cometeu. Este perfil pode ser denominado com duas frentes, um deles almeja explorar o sistema com objetivo de aprender e obter maior conhecimento nas vulnerabilidades e diferentes classes de ameaças, mas não busca retorno lucrativo. O outro não é um perfil ético, e almeja por meio das vulnerabilidades encontradas obter lucro.

5 Gerenciamento de Risco

Com a finalidade de impossibilitar um adversário de atacar, para gerenciar os riscos de um sistema como a Steam, deve-se primeiramente analisar os ativos

detalhados previamente. Em um possível cenário em que um atacante consegue escalar sua permissão para ter acesso ao banco de dados, tendo acesso aos arquivos-fonte das mídias digitais, informações de outros usuários e vendas, o atacante poderia realizar um vazamento desses dados ocasionando grandes prejuízos para a Steam, pois poderá impactar em contratos de sigilo com empresas produtoras de jogos. Além disso, os outros usuários que tiveram seus dados expostos poderiam exigir explicações, reembolso, deixar de usar a plataforma, e entre outras ações. Havendo um custo e consequência de reputação, podendo impactar negócios futuros e bem estar

Abordando o cenário apresentado acima, as questões financeiras não seria um problema para a Steam, visto que é a plataforma dominante no momento atual, possuindo valor de mercado de aproximadamente 16 bilhões de dólares [2], estando localizada na 16ª posição na lista das maiores empresas produtoras de jogos eletrônicos. Entretanto a cada casa decimal adicionada no número (99,999...) representa um investimento exponencial da segurança da plataforma.

A probabilidade de riscos como esse se concretizarem em problemas reais depende de vários fatores, dentre eles o quanto que o usuário malicioso pode ganhar. Dificilmente, alguém atacaria um sistema como esse apenas para ganhar jogos de graça. Geralmente usuários que invadem esse ramo de plataformas só querem ter seu nome lembrados como os responsáveis por burlar segurança de empresas gigantes. Outro fator importante a se considerar é analisar quantas vezes softwares similares já foram invadidos. A Steam não possui um histórico de invasões com grande magnitude, de acordo com UOL Notícias [1], o último registro foi em 2011 com um vazamento das informações contendo nomes dos usuários, endereço de e-mail e informações criptografadas de cartões de crédito.

6 Contra medidas

Como contra-medida, existe alguns protocolos e normas que a Steam implementa para mitigar o risco de usuários mal intencionados terem acesso aos ativos mencionados acima.

Além disso, todas as ações executadas perante o domínio da Steam, é utilizado a criptografia HTTPS, isso significa que qualquer informação enviada aos servidores do Steam é ilegível para qualquer pessoa que possa interceptá-la. Somente você e o Steam podem ver os dados.

Outrossim, outro ponto que é importante destacar é que a Steam oferece o Steam Guard, que é um recurso de segurança para manter sua conta apenas para seu uso. É uma forma de autenticação de dois fatores: depois de inserir seu nome de usuário e senha, você também precisará inserir um código de seu e-mail ou aplicativo móvel Steam para fazer o login.

7 Custo/Benefício

Os custos e benefícios das fragilidades identificadas no sistema variam de acordo com a situação. Evidentemente, esses benefícios possuem algum tipo de custo. Certificado HTTPS possui a mensalidade, Steam Guard teve o custo de desenvolvimento e manutenibilidade. Além disso, toda a infraestrutura de servidores e auditoria, treinamento e proteção, demandam um custo mensal, entretanto a Steam consegue balancear o custo e o risco, possibilitando estar na zona de lucro.

Uma vez que a Steam implementa essas e outras contra-medidas de risco, o sistema tende a ficar menos propenso ataques. Atacantes que queiram invadir a plataforma, terão que encontrar outro meio além do online, visto que a comunicação interna entre as máquinas estará totalmente criptografada. Uma possível alternativa seria o usuário tentar rodar algoritmos brute force para tentar descobrir qual algoritmo criptográfico está sendo utilizado, mas esse processo é tão caro que dificilmente alguém tentaria colocá-lo em prática.

Realizando a lição de casa e limpando a área, torna-se possível que o sistema da Steam tenha consistência e credibilidade, e consequentemente lucro, podendo ampliar a área da segurança na computação em seus serviços, pois conforme a escalabilidade novos métodos e abordagens são necessários para permitir a interoperabilidade e maturidade do sistema como um todo.

8 Conclusão

Realizando esse trabalho foi possível observar os principais ativos da Steam, ponderando os atacantes e o que deve ser feito para mitigar as vulnerabilidades do sistema. Além disso, também foi possível esclarecer como é dado o gerenciamento do risco tendo em consideração o custo / benefício de determinado serviço.

Referências

[1] UOL. Steam foi invadido por hackers dados podem ter vazado, diz valve... https://www.uol.com.br/start/ultimas-noticias/2011/11/10/hakers-invadem-banco-de-dados-do-steam-valve-admite-possivel-vazamento-de-dado htm, 2022. [Online; acessado em 08 de maio].

[2] Wikipedia. Lista das maiores empresas produtoras de jogos. https://pt.wikipedia.org/wiki/Lista_das_maiores_empresas_produtoras_de_jogos, 2022. [Online; acessado em 09 de maio].