Segurança em Computação
Trabalho Individual I

Gustavo Figueira Olegário

21 de março de 2019

1 Sobre o Sistema Escolhido

O sistema escolhido para este trabalho foi a Xbox Live. O sistema da Xbox Live é um sistema de serviços online de jogos e marketplace criado em 2002 pela Microsoft para dar suporte ao seu primeiro console, o Xbox. A Live é um sistema no qual seus usuários pagam para utilizar e podem conversar entre si através de sistemas de party chat, jogar por meio dos servidores disponibilizados pela empresa e comprar jogos e conteúdo online no seu sistema de Marketplace, a Microsoft Store. Ela também funciona como uma espécie de rede social onde usuários podem trocar mensagem de texto, buscar e comparar perfis de outros jogadores.

No que se refere aos aspectos de segurança computacionais, a Xbox Live tem um histórico muito melhor do que sua principal concorrente, a Playstation Network. Ela nunca teve um ataque massivo como houve com a PSN no ano de 2011. Além disso, a Microsoft também tem uma política rígida de punição para quem comete ilicitudes em seus serviços. Os castigos variam desde uma simples suspenção de conta até banimento completo de console e conta de usuário. Evidentemente, o sistema implementado pela Microsoft não é impenetrável e já houve relatos no passado de ataques de Denial of Service, bem como casos de usuários que tiveram suas contas hackeadas e pontos virtuais pagos gastos sem consentimento.

2 Ativos

Um dos principais ativos dentro da plataforma são as informações de cartão de crédito dos usuários guardadas no sistema. 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.

Outro ativo são as próprias contas de usuário em si. As contas além de possuirem informações pessoais do usuário, possuem jogos digitais, assinaturas, mensagens de conversas passadas, configurações pessoais, estatísticas dentro dos jogos que podem ser visíveis somente para o dono da conta e histórico de pesquisa dentro da plataforma.

Por último, um ativo importante dentro do sistema é o banco de dados da própria Xbox Live. Contendo informações sobre jogos, vendas e informações de partidas. Apesar de nenhum desses ativos ser financeiramente mensurável, é evidente que a perca, alteração ou uso indevido dos dados pode acarretar em probelmas para a reputação da empresa.

3 Adversários

Um provável adversário seria usuários da própria plataforma que querem achar falhas de segurança dentro do sistema, para que assim possam se beneficiar ou beneficiar terceiros, através de jogos e conteúdos digitais sem nenhum tipo de custo. Geralmente esse tipo de perfil de adversário, possui um perfil menos técnico,

mas que, mesmo assim, sua motivação de se beneficiar é tão grande que se dispõe a conquistar novos conhecimentos para conseguir vantagens indevidas.

Outro possível adversário desse sistema seria funcionários das marcas concorrente, Nintendo e Sony. Esses usuários poderiam atacar a plataforma com o intuito de que sua concorrente fosse afetada moralmente pelos ataques e, a longo prazo, ficasse desvalorizada dentro do mercado. Nesse sentido, as plataformas concorrentes conquistariam os usuários que eventualmente abandonassem a Xbox Live.

Por último, um possível adversário seria usuários com grande conhecimento técnico na área de computação e que gostam explorar as falhas de segurança de um sistema. Podem não ter nenhum objetivo em específico, mas apenas gostam de procurar falhas nos sistemas e identificar quais os erros que a empresa cometeu.

4 Gerenciamento de Risco

Para gerenciar riscos de um sistema como a Xbox Live, deve-se primeiro analisar metodicametente os ativos mencionados previamente. Imaginando um cenário em que algum usuário acessou a conta de algum jogador com informações de cartão de crédito guardadas, o usuário poderia comprar diversos jogos online, até o limite do cartão não permitir mais compras. O usuário que teve sua conta invadida não somente exigiria de volta o dinheiro gasto em seu nome como também uma multa.

Um cenário como esse envolve, em uma primeira análise, questões financeiras, visto que a Microsoft teria que ressarcir o seu cliente. Isso não seria um problema para a Microsoft já que é uma das três empresas mais valiosas do mundo, mas ao longo do tempo ela seria desvalorizada dentro do mercado, pois uma vez que teve sua reputação manchada, os usuários tendem a ficar com uma impressão ruim da empresa por um bom tempo.

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 plataformas como a Xbox Live 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. O caso mais marcante, foi o da Playstation Network de 2011 e, certamente, serve como indicativo muito forte de que não se deve implementar um sistema dessa magnitude sem nehum tipo de estratégia de segurança.

5 Contra-medidas

Como contra-medida, existe alguns protocolos e normas que a Microsoft implementa para mitigar o risco de usuários mal intencionados terem acesso aos ativos mencionados acima. Sabe-se que a Xbox Live permite que somente consoles com firmware reconhecidos possam se conectar a rede. De acordo com a empresa, qualquer console com firmware desconhecido ou de origem duvidosa, tem o hardware e conta banidos permanentemente da plataforma.

Além disso, quanto a questão de cartões de crédito, a empresa implementa o PCI Security Standard. Esse modelo de segurança, exige que as empresas sigam algumas regras básicas de segurança como por exemplo: garantir two factor authentication, senhas dos sistemas sendo trocadas periodicamente, fazer com que toda comunicação entre os sistemas internos seja criptografada. Essa certificação é exigida de companhias que guardam informações de cartão de crédito ou implementam gateway de pagamento.

A Microsoft também implementa a ISO 27001 e tem seus servidores Azure auditados anualmente, serviço cloud no qual onde está instalado a principal parte da infraestrutura da Xbox Live. Dentre algumas das restrições da norma, destaca-se a questão de que a implementação da segurança da informação deve ser feita sempre de forma crítica e que esteja sempre sendo revisada. Outro ponto importante a ressaltar é que mudanças grandes, no que se refere a gerência da segurança da informação, devem ser sempre rastreáveis, testadas e seus potenciais impactos negativos mitigados.

6 Custo/Benefício

Uma vez que a Xbox Live 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. Um usuário mal intencionado que ainda queira hackear a plataforma, terá que, provavelmente, utilizar algum decompilador para reverter o binário da máquina para o código fonte original para poder entender melhor como funciona o sistema. Entretanto esse tipo de ferramenta não é nenhum um pouco de se encontrar e ainda que o usuário consiga fazer isso, ele provavelmente teria que alterar o firmware original do console. Outra 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 realizá-lo.

Outro benefício que essas contra medidas trazem é o banimento de hardware modificados. Ainda que o hacker detenha o conhecimento de como invadir o sistema e espalhe-o pela internet a fora, a prática do mesmo é muito cara, uma vez que adquirir um videogame é caro, financeiramente, e tem-se também o custo de assinaturas e jogos para criar uma nova conta. Além disso, espalhar o conhecimento na internet também não é a forma mais inteligente de compartilhar a informação com outros usuários mal intencionados, uma vez que cedo ou tarde a empresa também teria a acesso à informação e, nesse sentido, trabalharia o mais rápido possível para resolver a falha.

Evidentemente, esses benefícios possuem algum tipo de custo. Normas ISO são certificações caras, uma vez que possuem reconhecimento internacional. Além disso, como os sistemas de nuvem são auditados anualmente, deve-se considerar não somente o custo de conquistar a certificação, mas de renová-la a cada ano. O reconhecimento e autenticação de firmware também deve ser incluído nos custos, já que é um projeto de integração software e hardware nem um pouco trivial. Por último, ainda deve-se considerar os custos de se manter funcionários bem preparados e treinados para que sejam capazes de implementar essas e outras normativas de segurança.