Nome: Gustavo Hammerschmidt. Data: 27/ 08/ 2018

TDE - Boas Práticas, Normas e Padrões

Há várias ameaças que comprometem a segurança das informações e dados dos usuários, desde códigos mal projetados até malwares e vírus. Para que tais problemas de segurança sejam evitados, programadores utilizam métodos de abordagem para evitar furos em seus códigos, protegendo assim os dados de seus clientes. Será abordado nesse trabalho 3 boas práticas e 3 padrões de segurança de informação.

Práticas:

1. Dentre vários mecanismos, um dos mais utilizados é o Firewall (uma barreira contra o "fogo" proveniente de outros computares conectados à rede) são softwares responsáveis por administrar pacotes de dados que entram(por meio de uma rede externa ou a partir de um host na própria rede) ou saem de uma rede, eles filtram o tráfego de informações e, dessa forma, diminuem os riscos de programas maliciosos infiltrarem-se em networks privadas e afetarem a sua segurança eventualmente. O firewall encarrega-se da filtração de dados, para que isso aconteça, ele opera por meio de regras estabelecidas previamente e, portanto, autoriza o tráfego de dados parametrizando-se às limitações propostas; é importante que ele seja imune às ameaças. O firewall protege contra ataques como vírus e malwares, não protege de ameaças internas como funcionários (a menos que seja projetado para). Para solucionar os problemas, o firewall compara uma lista de políticas de segurança com o conteúdo do cabeçalho de algum pacote de dados, se houver alguma regra pertinente a alguma informação do pacote, a regra é aplicada e então ele pode permitir a passagem do pacote ou bloqueá-lo (depende da ação que lhe foi atribuída para resolver determinado problema).
2. Outra abordagem é a Criptografia de Chave Pública, esse sistema atribuí a cada entidade (usuário, empresa, rede etc.) um par de chaves, uma delas é mantida em segredo (chave privada) e a outra é publicada junto ao nome da entidade (chave pública) expondo assim seu valor. Uma mensagem criptografada com a chave pública só pode ser descriptografada com a chave privada e uma mensagem criptografada com a chave privada não pode ser descriptografada, apenas se descriptografá-la concomitantemente com a chave pública. Essa abordagem de criptografia evita que uma mensagem seja interceptada e alterada de forma efetiva – uma vez que quem não tem a chave privada não conseguirá mudar o arquivo ou a mensagem – dessa forma garante-se um grau de confidencialidade à transferência do arquivo; aquele que deseja manter certo sigilo, utiliza a chave pública para enviar o documento, pois, sabe que apenas o dono da chave privada poderá descriptografá-lo.
3. Um recurso utilizado em grandes empresas e suas centrais certamente é Redes Privadas Virtuais (VPNs), esse método uma conexão de baixo custo entre locais de uma organização; para que isto aconteça, a empresa aluga circuitos de dados que conectam seus sites entre si, cada uma dessas conexões é, também, conectada aos roteadores locais da companhia. Isso proporciona o fluxo direto de dados – de um roteador a outro – sem, necessariamente, terem de percorrer através da Internet, o que fornece maiores garantias de que os

dados permaneceram confidenciais. AS VPNs não são de baixo custo, entretanto, empresas telefônicas garantem que nenhuma outra companhia tenha acesso a elas, logo, os dados não estarem sujeitos a leitura de concorrentes. Todas as informações enviadas nesse ambiente também estarão sujeitas a criptografia, o que agrega maior confidencialidade; e ,para torná-lo ainda mais seguro, há a possibilidade de adicionar firewalls entre as conexões de um site ao outro, isso evita que haja entrada de conteúdo indesejado caso um dos PCs esteja conectado à internet e à VPN.

Normas e Padrões de Segurança:

1. Para que se defina segurança em redes, é necessário definir uma política de segurança. Uma dessas políticas é a Integridade de Dados. O objetivo dela é garantir que os dados sejam gravados exatamente como pretendido e que a recuperação dos dados seja exatamente igual aos dados garantidos. Por exemplo, a entrada de quanto dinheiro uma pessoa disponibiliza no banco virtualmente e qual é o valor limite de suas transações, afinal qualquer incremento ou decremento resultará em prejuízos para um dos dois lados. Para evitar a perda de alguns pedaços de dados, alguns arquivos utilizam o sistema RAID (Redundant Array of Inexpensive Drives), é um mecanismo interno do arquivo que pode reconstruir parte de dados corrompidos. Conhecido como proteção de dados de ponta a ponta.
2. Outra política é a Disponibilidade de Dados que consiste na relação entre tempo e acessibilidade de acesso a dados e/ou sistemas de empresas. Essa política demanda a compatibilidade entre dispositivos e softwares, eliminando possíveis conflitos de disponibilização de dados. A falta ou obliteração parcial dessa política resulta em atrasos, inconvenientes no tráfego de documentos da empresa, interrupção de atividades etc. Soluciona-se esse infortuno por meio da utilização de uma infraestrutura tecnológica voltada à autopreservação do acesso aos seus dados; isto é importante, pois, evita atrasos de re-efetuação de logins em um ataque virtual ou após um “blackout”.
3. Por fim, a política de Confidencialidade. Ela consiste na restrição de informações a pessoas conforme o seu nível de acesso, dividindo os níveis de atuação de profissionais em uma empresa como uma hierarquia. Dependendo do grau de confidencialidade poder-se-á adotar medidas de rigorosidades para conceder limitar ou expandir o acesso. Por que é importante restringir acesso às informações? Porque as empresas que possuem “leaks” de dados estão expondo os dados não apenas delas mesmas, mas também de seus clientes, funcionários e fornecedores, a perda de dados gera prejuízos financeiros e, às vezes, até processos. Então, para evitar esses vazamentos indesejados, há formas de implementar a estrutura da empresa processos de criptografia de dados, autenticação em dois fatores, uso de tokens e verificação por biometria.