Após entendermos como um ataque é feito em um serviço de autenticação de contas e como é muito fácil ter acesso ao login de um usuário inserindo um banco de dados que pode ser criado ou até vazado de algum outro lugar, temos que pensar em uma forma para mitigar esse problema, um jeito em que mesmo que seja feito esse ataque o site se comporte de forma que possa bloquear ou até mesmo um jeito que esse ataque seja totalmente falho, tudo isso, para que possamos garantir um dos pilares que é muito importante na área de segurança da informação: a confidencialidade.

É muito importante que uma organização pense nesse fator quando contratar um serviço de segurança da informação, a quebra da autenticidade pode causar prejuízos enormes, como perda de clientes, indenizações por vazar informações não autorizadas e principalmente a perda de crédito diante o mercado corporativo. Sendo assim, vamos mostrar como podemos proteger desse ataque automatizado feito através do software SentryMBA.

Método “Anti-Automação”

O que faz o ataque automatizado ser tão perigoso e eficiente é justamente porque o software consegue testar milhares de usuários e senhas em apenas alguns segundos conseguindo ser eficiente após milhares de solicitações de autenticação. Então, a primeira forma de mitigar será através do método de “anti-automação”, nele podemos pensar em formas que em cada solicitação, o site irá pedir um requisito a mais, que pode ser algo muito simples para uma pessoa física (humano) mas para a máquina pode ser praticamente impossível. Inicialmente vamos explorar o “Captcha”.

Implementando o “Captcha” em nosso site, a ideia é que após 3 solicitações falhas de autenticação, será necessário mais um requisito para se “logar”, além do usuário e senha. Será apresentado uma imagem aleatória com caracteres aleatórios onde o usuário terá que digitar o conteúdo em uma caixa de texto, caso as informações tiverem corretas, terá sucesso na autenticação. Esse método praticamente quebra o ataque automatizado, ele não conseguirá mais fazer muitas tentativas por segundo pois além do usuário e senha tem um terceiro requisito que não consta no banco de dados e é totalmente aleatório.

Apesar desse método se mostrar muito eficiente e é utilizado em muitos sites atualmente, ele pode se tornar falho com o avanço da inteligência artificial onde os computadores estão cada vez mais capazes de interpretar diferentes imagens como os que são gerados pelo “captcha”. Dessa forma, vamos explorar um pouco da segunda ideia que será a autenticação em dois fatores.

Com o mundo globalizado e como hoje em dia praticamente todos possuem um smartphone, a autenticação em dois fatores tem se mostrado um método muito eficiente de mitigação de ataques automatizados não autorizados. Nele, após a autenticação sendo feita com êxito, o site irá solicitar mais uma informação para poder acessar as informações que você deseja. Essa informação pode ser um “sms” enviado para um celular previamente cadastrado no sistema, um “token” que é gerado através de aplicativo ou código enviado para o e-mail. Com esse método, apesar de ser um pouco mais demorado par ao usuário final conseguir acesso ao site, fica bem difícil um sistema automatizado conseguir sucesso na invasão.