Capítulo 7

Aspectos de segurança na arquitetura de software

Com um mundo cada vez mais conectado e avançado no cenário tecnológico, um fator que tem ganhado cada vez mais evidência é a segurança da informação. Construir um sistema nos dias de hoje não é apenas criar uma boa arquitetura, realizar uma boa modelagem, utilizar os padrões de projetos corretos; é, além disso, garantir a integridade da informação e permitir o acesso apenas às pessoas que realmente estão autorizadas a terem contato com aquelas informações.

Todos esses fatores importantes para garantir que esse bem mais valioso dos últimos tempos, a informação, seja protegido agora também ganham respaldo por meio da Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709, de 14 de agosto de 2018) (BRASIL, 2018). A LGPD não penaliza a pessoa que consegue acesso a uma informação indevida, mas a empresa ou sistema que não consegue manter a privacidade do seu usuário intacta.

São muitos os assuntos que merecem reflexão. É preciso entender como e onde cada técnica é importante para construir um sistema que atenda aos requisitos de segurança e garanta a privacidade do usuário/cliente. Por mais que exista a certeza de que não existem sistemas à prova de falhas, quais passos devem ser dados para minimizar a falta de segurança e maximizar a integridade da informação? Todas essas reflexões devem ser feitas durante a construção do sistema. Neste capítulo, abordaremos alguns pontos importantes para o profissional de desenvolvimento de sistemas.

1 Princípios da segurança da informação

Antes de iniciar qualquer parte de proteção do sistema, o planejamento de hardware e software, sempre visando à integridade e segurança da informação, tanto de elementos externos quanto de elementos internos, é preciso entender os fundamentos básicos de segurança, recomendados para toda empresa. Os princípios da segurança da informação são apresentados na figura 1.

Figura 1 – Princípios da segurança da informação

1.1 Confidencialidade

A confidencialidade é o primeiro pilar para atingir um nível de segurança maduro para a empresa e o sistema. Esse pilar tem relação com o controle de acesso à informação. Isso significa que apenas as pessoas autorizadas podem acessar a informação. O acesso deve ser controlado por quaisquer meios, virtuais ou físicos (HUMPHREYS, 2016).

Geralmente, isso é assegurado por meio de um sistema de autenticação e autorização. O procedimento faz com que sejam impostas limitações às informações sigilosas, que, quando vulneráveis, acabam expondo a empresa, pois podem ser divulgadas em razão de roubos e ataques cibernéticos, o que pode resultar em um déficit financeiro da empresa e de seus clientes (HUMPHREYS, 2016).

1.2 Integridade

O segundo pilar da segurança da informação é a integridade, que significa a preservação dos dados armazenados para produzir determinada informação. Para que essa propriedade seja atendida, é preciso realizar a manutenção em todo o sistema de armazenamento de dados que a empresa utiliza. Isso quer dizer que se deve cuidar para que a origem da informação seja mantida e ainda se possa rastrear todas as alterações que os dados sofram ao longo do seu ciclo de vida, sempre capturando a identificação da pessoa, a data e o horário em que a operação foi realizada (HUMPHREYS, 2016).

Esse procedimento é importante pois, quando aplicado de maneira correta no sistema, garante que ferramentas especialistas possam efetuar o processo de recuperação dos dados e, o mais importante, a qualquer momento, por motivos de perda ou de dano (HUMPHREYS, 2016).

1.3 Disponibilidade

A disponibilidade garante que a informação estará acessível para o usuário autorizado, a qualquer momento que ele necessite. Esse terceiro pilar tem dependência direta da eficácia da infraestrutura da empresa. A rede de acesso e os servidores são os principais elementos que mantêm esse pilar (HUMPHREYS, 2016).

Para que seja atendida a disponibilidade, a empresa precisa contar com links de internet e servidores redundantes. Eles devem ser configurados para, em caso de falha dos equipamentos primários, automaticamente entrarem em ação, até mesmo quando há sobrecarga de acesso – por exemplo, em épocas de eventos comemorativos –, além de fornecerem os dados para a auditoria sempre que o sistema for avaliado. Esse é um ponto importante para o crescimento de uma empresa (HUMPHREYS, 2016).

1.4 Autenticidade

O último pilar dos fundamentos da segurança da informação é a autenticidade. Nesse pilar, através da identificação e do registro da pessoa que incluiu ou alterou algum dado no sistema, podemos determinar quão autêntica é essa informação. Sem essa documentação realizada entre as operações de manipulação de dados, não é possível comprovar se a origem destes é verdadeira ou se constituem dados falsos ou poluídos. Assim, esse também é um processo importante para a segurança da informação, que anda de mãos dadas com o primeiro pilar, a confidencialidade (HUMPHREYS, 2016).

2 Aplicação dos princípios de segurança na arquitetura de software

Dentre todos os princípios da segurança da informação, existe um que sempre deverá ser tratado dentro da arquitetura do sistema, a confidencialidade. Nesse princípio, é necessária a construção de um controle de acesso às informações da empresa e/ou sistema em questão. Esse, sem dúvidas, é o ponto focal da grande maioria dos ataques cibernéticos aos sistemas de informação.

O primeiro ponto que pode garantir a confidencialidade, por meio do controle de acesso, é o uso de um método de acesso e autenticação, como senhas, tokens ou biometria (reconhecimento de impressão digital, reconhecimento facial, etc.). Entretanto, o uso de apenas um desses métodos não é mais aconselhável para sistemas. Os ataques evoluíram tanto nos últimos anos que esses métodos isolados já não são mais problemas para os invasores (HUMPHREYS, 2016).

Dessa forma, o método que muitas empresas têm adotado para solucionar essa vulnerabilidade é a autenticação em dois fatores para controle de acesso. Inclusive, essa é uma das recomendações da norma

de segurança ISO 27001, na qual são apresentados os benefícios de trabalhar com esse método (HUMPHREYS, 2016).

A autenticação possui um papel muito importante no controle de acesso. Ela representa o segundo passo de três para um controle de acesso robusto (HUMPHREYS, 2016). Esses três passos são:

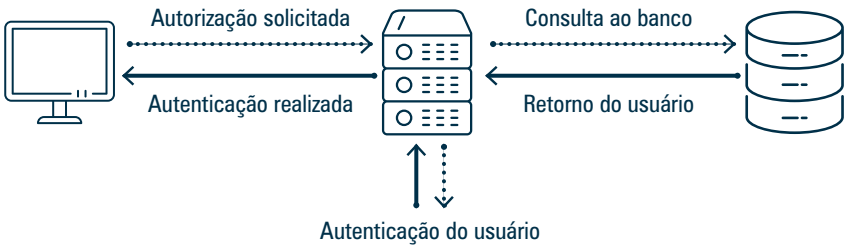
- **Identificação:** fornece à pessoa uma identidade que possa ser reconhecida no sistema. Exemplos: conta de usuário, número do CPF, passaporte, etc.
- **Autenticação:** assegura a identidade da pessoa, determinando que ela é quem afirma ser. Exemplos: senha, token, impressão digital, etc.
- **Autorização:** permite o acesso de uma pessoa autenticada no sistema a determinada informação. Exemplos: listas de permissões, grupos de permissões, etc.

No passo da autenticação do controle de acesso, é possível utilizar um ou mais métodos. Eles podem ser combinados de maneira paralela ou em sequência, como um processo de autenticação em várias etapas (HUMPHREYS, 2016). Por exemplo, pode ser combinado algo que a pessoa sabe (senhas e PINS), algo que a pessoa possui (smart cards, tokens, chave de acesso) e algo que faz parte de quem a pessoa é (padrão de voz, reconhecimento de retina, impressão digital, reconhecimento facial).

Nesse caso, foram apresentados os métodos do menos seguro para o mais seguro. O foco está na autenticação, pois essa etapa tem controle dentro do software e de sua arquitetura. Afinal, mesmo quando criamos um serviço, precisamos autenticar o acesso para entregar somente a informação desejada pela empresa à pessoa correta.

Sendo assim, vamos entender como funciona o processo de autenticação de um fator apenas, por meio da figura 2.

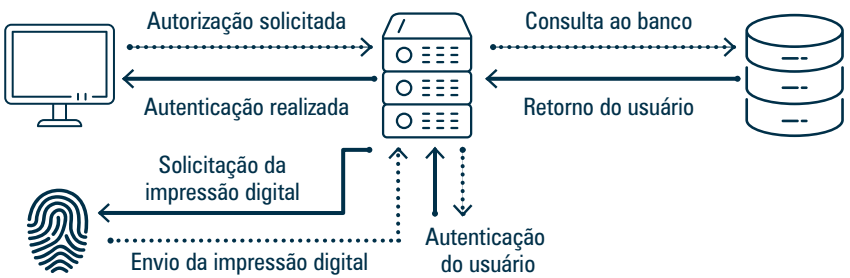
Figura 2 – Autenticação com apenas um fator



Se observarmos e analisarmos com calma o cenário proposto na figura, é possível identificar algumas falhas comuns de segurança que tornam o sistema vulnerável. As pessoas nem sempre têm cuidado com as informações pessoais. Elas compartilham senhas, escrevem em locais de fácil acesso e não estão atentas à aplicação de técnicas de engenharia social. Smart cards, tokens ou chaves de acesso podem, então, substituir as senhas, entretanto, esses itens todos podem ser roubados. Do mesmo modo, os padrões biométricos podem ser facilmente reproduzidos com as tecnologias atuais.

Porém, perceba que isso ocorre pois é utilizado apenas um método de autenticação. O que acontece se esses métodos forem combinados? Esse é o princípio da recomendação da ISO 27001 para o sistema de autenticação. A autenticação em dois fatores consiste basicamente em combinar dois dos métodos apresentados para essa tarefa. A figura 3 apresenta como seria o método de autenticação em dois fatores.

Figura 3 – Autenticação em dois fatores



Realizando o processo de autenticação em dois ou mais fatores, criam-se camadas extra de proteção, dificultando assim o acesso não autorizado às informações. É muito mais difícil que um invasor possua todas as informações dos fatores utilizados, e isso torna o sistema mais seguro.

Considerações finais

Neste capítulo, apresentamos os princípios da segurança da informação. Compreendemos como devemos tratar os pontos principais do controle de acesso em nosso sistema para deixá-lo cada vez mais seguro. Mesmo que um sistema não seja à prova de falhas, podemos dificultar ao máximo as ações de pessoas mal-intencionadas. Fique sempre atento para construir sistemas cada vez mais seguros para seus usuários.

Referências

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 dez. 2020.

HUMPHREYS, Edward. **Implementing the ISO/IEC 27001 ISMS Standard**. Norwood: Artech House, 2016.