A Faculdade de Tecnologia de Sorocaba
Tecnologia em Análise e Desenvolvimento de Sistemas

SEGURANÇA DA INFORMAÇÃO (SI)

Prof.º Denilce de Almeida Oliveira Veloso
Disciplina: Programação para WEB

Vinicius Antony Ferreira 0030482011029

Sorocaba - SP

Agosto/2021

SUMÁRIO

1. Introdução

Hoje, pela internet podemos fazer inúmeras coisas, uma dessas coisas são as negociações com empresas. Empresas essas que vão ter seus dados e de outras milhares de pessoas. Assim é de grande importância que essas empresas possam garantir a segurança de nossos dados.

Para garantir essa segurança as empresas podem optar por diversos meios, protocolos, regras, políticas, profissionais ou empresas terceirizados podem ser uma solução. Nesse trabalho, será abordado um pouco mais sobre a segurança da informação e os meios para garantir essa segurança.

2. Segurança da Informação

Segurança da informação é um conjunto de ações e boas práticas que têm como finalidade proteger um grupo de dados. De tal maneira, essas medidas de segurança podem ser aplicadas em todas as empresas que trabalham com dados, uma vez que toda organização gera informações próprias.

A segurança da informação se baseia em quatro pilares que sustentam todas as medidas tomadas para garantir a proteção dos dados, que são: Confidencialidade, Autenticidade, Integridade e Disponibilidade.

2.1. Importância

O avanço da tecnologia fez com que grande parte dos processos empresariais passassem a serem feitos por meios eletrônicos. Logo é de extrema importância que esses processos e troca de informações sejam o mais seguro possível.

A última Pesquisa Global de Segurança da Informação da PwC, realizada em 2018, revela que 46% dos impactos sofridos pelas empresas por conta de ataques cibernéticos comprometeram informações sobre seus clientes. Com base nesses dados, dá para entender o tamanho da criticidade e prejuízos que esses ataques podem proporcionar às empresas.

3. Gerenciamento do Firewall

Uma das ferramentas utilizadas para tentar garantir a SI é o firewall, que funciona como uma barreira a fim de impedir a entrada de elementos estranhos no sistema. Em sua configuração, é possível determinar quem pode ou não pode acessar o ambiente, o que evita o acesso indevido aos dados.

Para garantir uma proteção eficiente é preciso fazer o gerenciamento de maneira adequada, que tanto pode ser por forma de bloqueio nas entradas, quanto por meio de permissão de acesso. Além disso, é preciso fazer um acompanhamento constante para garantir que as políticas definidas sejam mantidas.

Outro ponto importante é sempre executar testes antes de implementar alguma alteração em suas configurações. O ideal é criar um plano de reversão para situações em que seja preciso voltar as configurações em um estado anterior.

3.1. Benefícios

A utilização de firewall protege a empresa de inúmeras ameaças, algumas dessas ameaças são:

3.1.1. Evitar ataques DDoS

Os ataques DDoS — Distributed Denial of Service — que significa Negação Distribuída de Serviço, ocorre quando diversos computadores tentam acessar um servidor simultaneamente.

Esses computadores, que são chamados zumbis, são controlados por hackers. Com a sobrecarga por conta das diversas tentativas de acesso, o servidor fica indisponível ou lento. Um dos benefícios da utilização de um firewall é se proteger contra esse tipo de ataque.

Basicamente, isso é possível porque no firewall são determinados quais endereços IPs podem ter acesso ao servidor. Com base nesses dados, o firewall faz uma barreira aos outros endereços que não constem nos registros de conexões autorizadas.

3.1.2. Proteção contra ataques Ransomware

Um dos maiores temores de muitas empresas é o ataque Ransomware, no qual os criminosos virtuais sequestram os dados, criptografam e solicitam o pagamento de resgate para devolvê-los.

O modo de infiltração do ataque é por meio de arquivos ou programas instalados nos computadores vindos de fontes não confiáveis, por meio de e-mails com arquivos contaminados, entre outras formas possíveis.

O Ransomware tem algumas variações, como GoldenEye, WannaCry, Locky, entre outros. A utilização de ferramentas de proteção, como firewall e antivírus são essenciais para evitar esse tipo de ataque. Por meio delas, é possível restringir a transferência de arquivos que possam oferecer riscos para o sistema, como arquivos do tipo executáveis, compactados, entre outros. Além disso, é preciso criar políticas de segurança que devem ser adotadas por todos os colaboradores, como forma de prevenção.

3.1.3. Segurança de Blockchain

Tecnologias como cloud computing e a utilização de dispositivos móveis para acessar sistemas corporativos proporcionaram às empresas uma maneira mais prática de trabalho, pois a facilidade de acesso permite que os colaboradores possam trabalhar a partir de qualquer local.

As portas de entrada para os ataques virtuais podem ser as mais diversas, inclusive por meio de dispositivos móveis, como smartphones ou tablets. Em função disso, é preciso proteger esses acessos para evitar que essa seja a forma em que os criminosos possam acessar os dados corporativos.

Uma maneira de garantir essa segurança é por meio da tecnologia blockchain, a mesma utilizada para garantir a proteção da criptomoeda Bitcoin. Basicamente, a tecnologia funciona por meio de cadeia de blocos, que são relacionados entre si, de modo que o cada novo bloco precisa da validação dos blocos anteriores. Ela trabalha como uma rede distribuída, em que não há um único administrador central.

Dessa forma, se um invasor consegue entrar em um ponto da rede, não há como seguir adiante, pois é preciso que haja a validação dos outros blocos.

4. Certificados SSL e seus benefícios

O certificado SSL — Secure Sockets Layer — funciona como uma camada extra de proteção para as informações trafegadas na internet. Basicamente, ele utiliza a criptografia para assegurar a conexão e transmissão de dados entre o cliente, o servidor e vice-versa. Em tecnologias como cloud computing, o protocolo sempre é utilizado para garantir a proteção das informações armazenadas na nuvem.

O certificado SSL é utilizado para criar um canal seguro de comunicação por meio de uma sessão criptografada. Existem diversos tipos de certificados SSL, com características e funcionalidades diferenciadas.

4.1. Validação de domínios

O certificado de validação de domínio é um dos modelos mais básicos e muito utilizado em hospedagens de sites mais simples. Utiliza um tipo básico de criptografia, capaz de conferir e validar o endereço do site e garantir que os dados trafegados nesse domínio estejam em segurança.

É mais indicado para sites que utilizam formulários para comunicação com seus clientes, mas que mesmo assim necessitam que essas informações trafeguem em segurança. Esse protocolo também fornece proteção para dispositivos móveis e subdomínios.

4.2. Validação da organização

Esse tipo de certificado proporciona uma validação maior. Além da validação de domínio, inclui também a certificação da empresa. Dessa forma, o certificado indica que aquela empresa realmente existe. Para isso, confirmam a veracidade de seus dados por meio da validação do CNPJ junto à Receita Federal.

Esse modelo é muito utilizado em grandes sites ou lojas virtuais para transmitir maior segurança ao cliente. Sua utilização é recomendada em sites que armazenam dados de login de usuário, além de informações pessoais e financeiras sobre seus clientes.

4.3. Validação estendida

Esse é um dos modelos mais completo de certificação SSL. A criptografia utilizada nesse modelo é a mesma que em outras alternativas. Entretanto, para obter esse certificado, é preciso atender a outras exigências, como:

- ser uma empresa devidamente registrada nos órgãos competentes;
- deve estar em operação;
- o endereço e telefone devem ser verificados.

Com esse certificado, o endereço do site é exibido ao lado do cadeado na barra de endereço, o que permite sua fácil identificação.

Uma das grandes vantagens desse modelo é proteger a empresa e seus clientes de ataques como o Spear phishing. Nesse tipo de ataque, os clientes recebem e-mails ou falsas comunicações para que sejam redirecionados a sites maliciosos. Ao atender a essa solicitação maliciosa, o cliente pode se tornar uma vítima dos criminosos e fornecer informações sigilosas, como dados pessoais ou financeiros.

O certificado de validação estendida garante mais segurança ao site, pois ajuda ao usuário na identificação de que está no ambiente correto. Outra razão para utilizar esse modelo é estar em conformidade com padrões e normas de segurança importantes utilizados pelo mercado, como o PCI-DSS — Payment Card Industry Security Standards Council.

5. Erros cometidos

Um dos erros mais comuns no departamento de TI é negligenciar aspectos importantes da segurança da informação, o que aumenta sua vulnerabilidade.

5.1. Falta de investimento

Deixar de investir em segurança da informação é um erro muito grave que, além de causar prejuízos financeiros, pode prejudicar a imagem da empresa perante o mercado.

Para uma boa gestão de TI é necessário que haja a conscientização de que esse investimento será revertido em benefícios para o negócio. Isso porque uma empresa que se preocupa com a SI demonstra aos seus clientes que preza pela qualidade dos serviços prestados por ela.

A proteção dos dados deve ser uma prioridade nas empresas. Para isso, ela deve contar com ferramentas como antivírus, firewall e outras tecnologias que atendam essa necessidade.

5.2. Falta de políticas de segurança

Outro problema comum encontrado nas empresas é a falta de políticas de segurança. Elas são essenciais para prevenir e evitar uma série de problemas.

Uma das falhas mais comuns é a falta de política de definição de senhas. Negligenciar esse procedimento oferece um risco muito grande, pois facilita a entrada de potenciais invasores. Em função disso, é preciso elaborar uma política clara e bem definida, que deve ser distribuída a todos os colaboradores para que cada um entenda o tamanho de sua responsabilidade.

5.3. Profissionais inexperientes

A falta de profissionais especializados é outro problema sério com relação à segurança da informação. Com a grande variedade de ameaças virtuais é preciso entender quais ferramentas são mais adequadas a cada uma delas.

Ao capacitar um profissional de TI para atender às necessidades de SI, as empresas garantem que seus sistemas estarão sob a supervisão de pessoas especializadas. Isso contribui para reduzir a vulnerabilidade e os riscos de ataques.

6. Importância da infraestrutura

Atualmente, as empresas trabalham com um volume de dados extremamente alto. Em razão disso, há uma grande preocupação com relação à integridade e segurança dessas informações. Além delas serem importantes para o negócio, muitas são confidenciais, pois se referem a informações pessoais de clientes ou da própria empresa.

É preciso contar com uma infraestrutura eficiente, que garanta a recuperação das informações, tanto em casos de ataques virtuais, quanto em outro tipo de problema que cause a indisponibilidade dos dados.

Em uma infraestrutura eficiente há uma série de políticas de segurança que garantem a blindagem do data center. Além disso, é feita a realização de backups de dados com frequência, o que garante a recuperação das informações com facilidade.

Em uma infraestrutura bem planejada, os acessos às informações são feitos de acordo com a necessidade de utilização de cada usuário. Isso oferece mais proteção a dados sigilosos, que só podem ser acessados por usuários pré-determinados.

7. Dicas de garantia

Manter um ambiente seguro é essencial para o negócio, tanto para proporcionar a proteção dos dados, quanto para conservar a boa imagem da empresa no mercado. Para isso, a empresa deve seguir algumas dicas para implementá-la da melhor maneira.

7.1. Segurança de dispositivos móveis

Os dispositivos móveis são cada vez mais utilizados em ambientes corporativos. Há diversas ferramentas e sistemas que permitem que os colaboradores utilizem esse recurso para trabalhar de forma remota. Entretanto, é preciso atenção para garantir a segurança desses dispositivos, de modo que eles não sirvam como porta de entrada para o ambiente corporativo.

Uma das formas de oferecer isso é por meio da adoção de um padrão de acesso com segurança. Para isso, todos os dispositivos que acessam a rede corporativa devem ser registrados e monitorados.

Dessa forma, é possível identificar acessos e padrões de comportamentos indevidos. Além disso, os colaboradores devem se conscientizar de que não devem utilizar redes públicas para o acesso aos sistemas corporativos.

7.2. Ferramentas de proteção

Existem diversas ferramentas no mercado que garantem a proteção ao sistema e que as empresas devem investir, como antivírus, firewall e antispyware.

Além disso, elas também devem ser instaladas em todos os dispositivos utilizados pela corporação, como em notebooks, smartphones e tablets. O uso dessas ferramentas permite a configuração dos dispositivos que acessarão a rede, bem como a definição das conexões permitidas.

Essas configurações são essenciais para mitigar ataques DDoS e evitar ataques Ransomware. A utilização de tecnologia blockchain também deve ser considerada. Isso porque por meio dela é possível interromper um ataque de hacker, pois, ao invadir um nó da rede, os outros não permitirão que a invasão continue.

7.3. Computação em nuvem

Uma forma de garantir um ambiente extremamente seguro é utilizar a computação em nuvem. Entre os benefícios da hospedagem em cloud está o ambiente seguro e a proteção eficiente aos mais variados tipos de ataques cibernéticos.

Além disso, o ambiente na nuvem conta com ferramentas que facilitam a aplicação de políticas de segurança, como o controle de senhas e de acesso.

7.4. Softwares atualizados

Complementando a dica anterior, se os criminosos virtuais estão ligados nas inovações em relação à segurança da informação, eles também sabem das atualizações dos softwares, principalmente em relação às vulnerabilidades que foram sanadas. Ao manter os softwares e plugins atualizados, você eliminará as brechas para a ação dos cibercriminosos e trabalhará sempre com a versão mais moderna e completa.

7.5. Políticas de controle de acessos

Outra maneira eficiente de garantir a segurança da informação é com um bom controle de acesso, afinal, boa parte dos problemas relacionados a segurança da informação são causados por erros humanos — seja por desconhecimento ou negligência. O controle de acessos limita a ação de cada usuário de acordo com as suas necessidades, ou seja, quando ele faz login, a sua conta não se torna uma porta de entrada para o sistema inteiro.

Além do problema de segurança, essa prática reduz os erros, pois não há o risco de um profissional, mesmo que de forma involuntária, excluir, alterar ou mover algum arquivo importante para outro colaborador.

7.6. Políticas de segurança

Uma coisa que deve ser bem clara é que a segurança da informação não é de exclusividade de um único setor ou profissional de TI. Todos os setores estão envolvidos, seja trabalhando de forma preventiva ou participando dos processos de criação de estratégias. São os profissionais que utilizam os ativos de TI, seja para acessar, criar, modificar ou eliminar os dados e isso pode acabar se tornando a porta de entrada para os malwares.

Uma boa política de segurança é aquela que normatiza as regras que todos deverão seguir, para reduzir os riscos trazido pela ação dos criminosos virtuais. Com a política de segurança o gestor poderá definir, por exemplo, os dispositivos que estão autorizados a acessar a rede corporativa, tanto dentro como fora da empresa.

7.7. Ferramentas de monitoramento

Não basta apenas criar as políticas de segurança, é importante que elas estejam alinhadas aos processos corporativos. Isso porque, algumas políticas de segurança vão exigir uma reestruturação da infraestrutura de TI, o que exigirá todo um planejamento prévio. Por exemplo, caso seja necessário modificar o sistema operacional, essa mudança deverá ser feita em todas as máquinas instaladas na empresa e isso demanda preparação e tempo. O mesmo vale para as mudanças na hierarquia de arquivos, backups entre outros.

Por isso, é importante que haja uma integração e as demais áreas, para que haja essa adequação de processos para que a política de segurança seja colocada em prática. Se essa integração não for feita, as falhas anteriores permanecerão e as políticas serão apenas burocracia em papel.

7.8. Criptografia de dados

Uma das tecnologias que mais ganha campo em relação à segurança da informação é a criptografia. É ele que impede que os arquivos sejam interceptados no meio do caminho entre o dispositivo de acesso e o servidor. Isso porque, com a criptografia, apenas as duas pontas têm a chave privada para decodificar os dados, ou seja, mesmo que o hacker consiga ter acesso aos dados, eles estarão indecifráveis.

7.9. Empresas especializadas

Nem sempre uma empresa pequena ou média tem um orçamento que permite a manutenção de uma equipe interna especializada em segurança da informação, principalmente as empresas que não têm o TI como seu core business. Nesse cenário, uma boa solução e a contratação de uma empresa especializada na área de segurança da informação, que ficará responsável pelos procedimentos estratégicos e essenciais, que garantam a privacidade e integridades das informações de sua empresa.

Dessa maneira, a sua empresa poderá focar em seu core business e o parceiro especializado, ficará atento às novidades, oferecendo sempre as melhores soluções que ajudarão a otimizar os mecanismos de proteção. Por exemplo, se a sua empresa optar por contar com armazenamento de backup em nuvem seguro oferecido pelo parceiro especializado, garantirá uma maior proteção de dados. Se a sua empresa for atacada por ransomware, a empesa especializada poderá dar as diretrizes para que os danos sejam mitigados.

8. Conclusão

Como visto, é de extrema importância hoje, que empresas invistam na segurança de suas informações e que que nossos dados fiquem seguros quando utilizados na internet. Além de evitar os prejuízos financeiros que um ataque cibernético proporciona ao negócio, esse procedimento ajuda a manter uma imagem positiva da empresa frente ao mercado.

Vimos os diversos meios pelo qual a empresa pode seguir para tentar garantir essa segurança. Partindo desde protocolos e regras até a parceria com empresas especializadas na área.

9. Referências

EVEO, Redação. Guia completo: segurança da informação. **EVEO**, 2019. Disponível em: https://www.eveo.com.br/blog/guia-seguranca-da-informacao/. Acesso em: 9 Agosto. 2021.

VELASCO, Ariane. O que é Segurança da Informação? **CANALTECH**, 2020. Disponível em: https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/. Acesso em: 9 Agosto. 2021.

VELOSO, Thássius. O que é Segurança da Informação? **TECNOBLOG**, 2010. Disponível em: https://tecnoblog.net/43829/o-que-e-seguranca-da-informacao/. Acesso em: 9 Agosto. 2021.

ZEFERINO, Denis. O que é Segurança da Informação e qual sua importância? **CERTIFIQUEI**, 2020. Disponível em: https://www.certifiquei.com.br/seguranca-informacao/. Acesso em: 9 Agosto. 2021.