Sumário

Histórico					
Versão	Elaborado por	Data	Revisado por	Data	Principais Alterações
1.0	Edenilton - ejsoares	17.05.2021			

Objetivo

Prover aos membros da equipe de infraestrutura um framework para avaliar o nível de requerimentos de segurança que deve ser utilizado e guiar a equipe de segurança operacional na seleção destes requisitos para sua implementação, garantindo assim uma maior segurança.

Introdução

A implementação de uma metodologia que possa auxiliar no desenvolvimento seguro é um dos principais pontos dentro de um processo de segurança. Os requisitos apresentados neste documento foram definidos com base nas especificações propostas pelo Open Web Application Security Project® (OWASP) e Center For Internet Security (CIS).

Níveis de Implementação

O documento apresenta três níveis de verificação que devem ser observados durante o processo de configuração do serviço. Cada um dos níveis aqui apresentados tem sua particularidade e profundidade.

Nível 1 - Segurança Mínima Necessária	Nível 2 - Padrão para web	Nível 3 - Alto Valor, Garantia, Segurança e Resiliência
Para níveis baixos de garantia de segurança. Apresenta o nível mínimo de segurança esperado para qualquer aplicação web.	Para aplicações que contêm dados sensíveis. É o nível recomendado para a maioria das aplicações.	Para as aplicações mais críticas, que requerem o mais alto nível de confiança.

Nível 1 - Segurança mínima

Para se adequar a este nível, a aplicação não deve possuir vulnerabilidades de fácil descoberta e exploração, bem como as listadas no TOP 10 da OWASP ou mesmo em outras listas de vulnerabilidades similares classificadas como críticos e altos.

O nível 1 é considerado o mínimo de segurança para qualquer aplicação, no entanto, se os dados que devem ser protegidos por sua aplicação são críticos, raramente somente o Nível 1 trará o nível de proteção recomendado de segurança.

Nível 2 – Segurança Recomendada

Um serviço atinge o nível 2 se tiver resiliência suficiente contra a maioria dos riscos associados a ataques através de recursos externos. Portanto, deve ser utilizado como o nível padrão de segurança. Este nível, que é apropriado para aplicações que tratam dados sensíveis, garante que os controles de segurança existem, funcionam e são utilizados dentro da aplicação.

Ameaças a aplicações neste nível serão tipicamente feitas por atacantes habilidosos e motivados, focando em alvos específicos, utilizando ferramentas e técnicas efetivas para o descobrimento e exploração de fraquezas dentro de aplicações.

Características da Aplicação
Armazena, transmite ou processa dados pessoais, confidenciais ou sensíveis de funcionários, parceiros de negócio, terceiros ou prestadores de serviço
Aplicações cuja integridade é crítica.

Nível 3 – Segurança Alto valor, garantia e resiliência

Este nível é o mais alto e é normalmente reservado para serviços que requerem níveis significativos de verificações de segurança, como em situações de infraestrutura crítica, quando realizam processos críticos para o negócio ou funções sensíveis, quando é necessária a garantia da sua integridade para o funcionamento do negócio, ou seja, nível de segurança 3 é exigido em cenários onde uma falha pode provocar um impacto significativo nas operações da organização.

Características da Aplicação
Aplicações que executam funções críticas, onde a falha pode afetar significativamente as operações. Ex: uma aplicação interna que seja utilizada por várias outras, Sefaz Identity, Portal de Assinaturas, etc Aplicações que manipulam informações sigilosas ou que realizam processos críticos para o negócio ou funções sensíveis. Ex.: manipulação de informações sujeitas ao sigilo fiscal.

Seleção dos Requisitos de Segurança

Para o processo de seleção dos requisitos de segurança ser eficiente, deve-se aplicar uma avaliação mista, levando em consideração os ativos que devem ser protegidos e os riscos mapeados.

O anexo 1 apresenta uma lista de requisitos de segurança propostos, divididos nos três níveis de segurança. Além disso, os requisitos propostos nos anexos, não deverão ser tratados como únicos. Caso seja notada a necessidade de adição de um requisito, o mesmo pode e deve ser adicionado à sua respectiva tabela dentro do respectivo anexo.

A partir destes anexos, o PO irá gerar a Lista de Requisitos de Segurança, que será passada para a fase de sprint de desenvolvimento. Para gerar esta Lista de Requisitos de Segurança do Projeto, considere utilizar ferramentas, Kanban boards, Scrum ou tabelas que facilitarão na seleção e acompanhamento da implementação dos requisitos.

Anexo 1 – Requisitos de Segurança para Configuração

Este anexo apresenta os controles que devem ser avaliados, e caso atendam às necessidades de segurança da solução, devem ser aplicados. Esta lista de requisitos foi baseada primordialmente no CIS (Center For Internet Security) que apresenta uma lista das técnicas de boas práticas que deveriam ser incluídas em toda configuração inicial de recursos com finalidade de desenvolvimento de software.

1. Requisitos de Configuração Windows

1.1. Configuração WebServer

1.2. Configuração de Autenticação e Autorização

1.2.1.	Recomenda-se que 'regra de autorização global' esteja definida para restringir o acesso. Configurar uma regra de autorização global que restringe o acesso garantirá a herança das configurações na hierarquia dos diretórios da web; se esse conteúdo for copiado em outro lugar, as regras de autorização fluem com ele. Isso garantirá que o acesso ao conteúdo atual e futuro seja concedido apenas aos responsáveis apropriados, reduzindo o risco de acesso acidental ou não autorizado. CIS: IIS.10 – Pag 25				
1.2.2.	Recomenda-se que o acesso aos recursos confidenciais do site ocorra de forma autenticada. A configuração da autenticação ajudará a reduzir o risco de usuários não autorizados acessarem dados e / ou serviços e, em alguns casos, reduzir o dano potencial que pode ser causado a um sistema. CIS: IIS.10 – Pag 28	✓			
1.2.3.	Recomenda-se que a autenticação de formulários exija SSL A exigência de SSL para autenticação de formulários protegerá a confidencialidade das credenciais durante o processo de login, ajudando a mitigar o risco de roubo de informações do usuário. CIS: IIS.10 – Pag 32	✓			
1.2.4.	Recomenda-se que a autenticação de formulários esteja configurada para o uso de cookies. O uso de cookies para gerenciar o estado da sessão pode ajudar a reduzir o risco de tentativas de sequestro de sessão, evitando que o ASP.NET precise mover as informações da sessão para a URL. Mover identificadores de informações de sessão para a URL pode fazer com que IDs de sessão apareçam em logs de proxy, histórico de navegação e sejam acessíveis para scripts de cliente por meio de document.location. CIS: IIS.10 – Pag 34	✓			

1.2.5.	Recomenda-se que o “modo de proteção de cookie” esteja configurado para autenticação de formulários. Ao criptografar e validar o cookie, a confidencialidade e integridade dos dados dentro do cookie são garantidas. Isso ajuda a mitigar o risco de ataques, como sequestro de sessão e falsificação de identidade. CIS: IIS.10 – Pag 36	✓			
1.2.6.	Recomenda-se que a segurança da camada de transporte “autenticação básica” esteja configurada. As credenciais enviadas em texto não criptografado podem ser facilmente interceptadas por código malicioso ou por pessoas. Reforçar o uso do Transport Layer Security ajudará a reduzir as chances de credenciais sequestradas. CIS: IIS.10 – Pag 38	✓			
1.2.7.	Recomenda-se que as informações sensíveis (senhas e tokens) não estejam armazenadas em texto claro em arquivos de configuração. Informações sensíveis sempre devem ser protegidas para reduzir o risco vazamento. Por razões de segurança, é recomendado que informações sensíveis não sejam armazenadas em nenhum arquivo de configuração do IIS.Isso removerá todas as referências a usuários armazenados nos arquivos de configuração. CIS: IIS.10 – Pag 42	✓			

1.3. Configuração do ASP.NET

1.4. Solicitação de Filtragem e Módulos de Restrição

1.5. Restrições de IP

1.6. Configuração registro de LOG IIS

1.7. Solicitações de FTP

1.8. Criptografia de Transporte