MARINHA DO BRASIL

DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO DA MARINHA

BOLETIM TÉCNICO

DCTIMBOTEC 31/002/2020: Recomendações e Requisitos Mínimos de Segurança da Informação para Sistemas Digitais na MB

RESPONSÁVEL TÉCNICO:

ALISSON CAVALCANTE E SILVA
Capitão-Tenente (T)
Encarregado da Divisão de Gestão de Risco e Incidentes de Rede
ASSINADO DIGITALMENTE

APROVAÇÃO:

HUMBERTO FERREIRA RAMOS JUNIOR
Capitão de Fragata
Chefe do Departamento de Segurança das Informações Digitais
ASSINADO DIGITALMENTE

RATIFICAÇÃO:

MARIA CARNEIRO DE REZENDE
Capitão de Fragata (T)
Superintendente de Tecnologia da Informação
ASSINADO DIGITALMENTE

DATA: 02/06/2020.

ÍNDICE

1 - PROPÓSITO

Estabelecer e divulgar recomendações e requisitos mínimos de segurança para a homologação de Sistemas Digitais (SD) na MB.

2 - MOTIVAÇÃO TÉCNICA

Conforme estabelecido nos itens 3.7.1 e 14.2 da DGMM-0540 e no item 3.4 da DCTIMARINST - Norma sobre Conformidade, Homologação e Hospedagem de Sistemas Digitais (SD) na MB, a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) tem como atribuição singular a análise dos aspectos de segurança da aplicação para homologar um SD. A fim de orientar as OM que desejam homologar um SD e assim possibilitar a verificação prévia e simplificada das condições mínimas de segurança de um SD, divulgam-se as condições e configurações necessárias a um SD, para sua homologação, do ponto de vista da Segurança da Informação (SI).

3 - REQUISITOS MÍNIMOS DE SEGURANÇA

Neste tópico serão estabelecidas condições e/ou configurações consideradas mínimas para segurança de SD a serem homologados para utilização na MB. Os tópicos a seguir estão numerados conforme as características dos SD a serem avaliados ou situações a serem apreciadas, devendo-se verificar a aplicabilidade de cada item, especificamente no contexto do SD que se quer homologar.

3.1 - SD COM INTERFACE VIA NAVEGADOR WEB

Os SD que utilizam interface via navegador web para acesso a um sistema hospedado em um servidor de aplicações devem:

a) ser compatíveis com todos os navegadores e sistemas operacionais padronizados para uso na MB, conforme estabelecido na DCTIMBOTEC que trata da Estação de Trabalho Padrão da MB, considerando as últimas versões dos navegadores disponíveis.

b) utilizar o protocolo https (hypertext transfer protocol secure), com certificados atualizados e válidos, para realização de suas conexões. Conexões efetuadas por protocolos sem criptografia não devem ser aceitas. Em caráter excepcional e devidamente justificado, pode ser aceito um SD que utilize outro protocolo de rede quando houver apenas informações ostensivas e sem necessidade de autenticação e/ou controle de acesso;

c) caso o SD seja acessado apenas na RECIM, os certificados utilizados nos servidores do SD deverão ser emitidos pelo CTIM;

d) desabilitar o cache realizado no lado cliente nas páginas que contenham informações sensíveis. Para isso o parâmetro “Cache-Control: no-store” pode ser utilizado;

e) desabilitar a funcionalidade de autocompletar nos formulários que contenham informações sensíveis, incluindo o formulário de autenticação (se houver). Para isso, pode

ser utilizada a opção prevista no padrão HTML 5 e já implementada nos navegadores mais recentes: autocomplete="off", colocando-a no código do formulário e no dos controles propriamente; e

f) se houver autenticação de usuário no SD, deverão ser utilizadas neste processo apenas requisições POST e bloqueadas quaisquer tentativas de autenticação utilizando-se requisições GET.

3.2 - SD COM CONTROLE DE ACESSO E AUTENTICAÇÃO DE USUÁRIOS

Quando existir um mecanismo de autenticação de usuários e controle de acesso, devem ser observados os seguintes requisitos:

a) quanto ao nome do usuário: utilizar, preferencialmente, o NIP, podendo, entretanto, ser aceita outra regra de formação, desde que justificada na documentação do SD;

b) quanto à constituição da senha dos usuários: deve-se exigir que contenha letras maiúsculas, letras minúsculas, números e caracteres especiais (simultaneamente), com, no mínimo, 10 caracteres e sem limite máximo de tamanho. Ressalta-se que dependendo do objetivo e das informações do SD, um maior grau de complexidade na criação da senha poderá ser exigido, a fim de manter as condições mínimas de segurança.

c) as senhas dos usuários não podem ser armazenadas em claro (legíveis) e também não devem permitir sua recuperação e/ou leitura em nenhuma hipótese. Para a consecução do processo de autenticação de usuário pode ser gerado um hash da senha digitada pelo usuário e compará-la ao hash armazenado no SD. E de maneira a tornar mais robusto armazenamento de senhas, deve-se incluir o ID do usuário junto à senha do usuário para a geração do hash, gerando assim uma cadeia salt. Como algoritmo de hash a ser utilizado sugere-se SHA-256, SHA-512, Whirpool ou outro definido por esta DE;

d) quanto a senhas padrão para usuários: somente é permitida a utilização de senhas padrão na criação de novos usuários, devendo o SD forçar o usuário a trocá-la na primeira autenticação no sistema;

e) a entrada de senha deve ser ocultada na tela do usuário utilizando-se campos especiais para esta finalidade (por exemplo, em HTML campos do tipo password);

f) a autenticação deve ser efetuada após o preenchimento de todos os dados necessários pelo usuário. Não pode ser emitida mensagem de erro especificando os motivos da recusa de uma autenticação. Isto é, quando ocorrerem erros na autenticação, as mensagens emitidas para o usuário e/ou registradas em arquivos de log, que podem ser acessados por usuários, não poderão conter indicações de qual parte dos dados de autenticação estão incorretos. Por exemplo, não podem ser utilizadas mensagens como "Nome de usuário inválido" ou "Senha incorreta", devendo-se usar algo genérico como "Usuário e/ou senha inválidos" para ambos os erros;

g) deve ser implementada, no SD, a desativação automática de contas de usuário após um número pré-definido de seguidas tentativas inválidas do login. Esta desativação da conta visa prevenir tentativas de invasão por força bruta. Recomenda-se que a autenticação seja travada:

I) após 3 (três) tentativas, para sistemas que hospedem assuntos de grau de sigilo RESERVADO e para o correio eletrônico adotado na MB; e

II) após 5 (cinco) tentativas para os demais sistemas.

3.3 - ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS EM BANCOS DE DADOS

Dados sensíveis que necessitem ser armazenados em Bancos de Dados (BD) necessitam de uma camada de proteção adicional aos mecanismos de segurança do próprio BD (por exemplo, devem permanecer cifrados). Para tal, podem ser utilizados os Algoritmos de Estado estabelecidos pela MB ou então o algoritmo AES, já disponível no Oracle e no PostgreSQL (BD padronizados para utilização em SD na MB).

3.4 - PROTEÇÃO E ATUALIZAÇÃO DO SISTEMA OPERACIONAL DE REDE

A OM responsável e hospedeira do SD deverá manter constante atualização dos softwares utilizados nos servidores de aplicação. As atualizações e patches de segurança devem ser aplicados com a maior celeridade possível, sendo necessária a instalação e utilização da solução de antivírus homologada para uso na MB. Maiores informações sobre o assunto estão disponíveis na página do CTIM na intranet (www.ctim.mb).

4 - ANÁLISE DE VULNERABILIDADES NOS SERVIDORES DO SD

Como parte do processo de homologação do SD, o CTIM realiza uma varredura de vulnerabilidades nos servidores. As vulnerabilidades identificadas serão informadas à OM solicitante para que sejam corrigidas. Posteriormente, o SD corrigido deverá ser novamente submetido à análise de vulnerabilidade, a fim de prosseguir com o processo de homologação.

5 - DOCUMENTAÇÃO DE SI NO DESENVOLVIMENTO

Para os SD que se enquadrem no subitem 3.2 deste Boletim Técnico, deverá ser encaminhado à DCTIM um formulário de “Resumo de Definições de SI para Desenvolvimento de SD”, conforme modelo em anexo. Este formulário, devidamente preenchido e assinado, deverá ser encaminhado quando da solicitação de homologação do SD, acompanhado dos documentos definidos nas demais normas pertinentes.

6 - ESCOPO DA VERIFICAÇÃO DE SEGURANÇA PARA HOMOLOGAÇÃO

A segurança dos SD em utilização na MB deve ser uma preocupação conjunta da DE e da OM responsável pelo mesmo. As recomendações e requisitos estabelecidos neste Boletim Técnico não esgotam e nem restringem os requisitos de segurança que possam ser identificados como

necessários para um determinado SD. Assim, sempre que for preciso poderão ser propostos, implementados e/ou exigidos novos atributos e características de segurança.

7 - VIGÊNCIA

Este DCTIMBOTEC entra em vigor na presente data.

8 - CANCELAMENTO

Este DCTIMBOTEC cancela a de nº 31/002/2017.

MARINHA DO BRASIL

< Nome da OM >

RESUMO DE DEFINIÇÕES DE SEGURANÇA DA INFORMAÇÃO (SI)
PARA DESENVOLVIMENTO DE SISTEMA DIGITAL (SD)

1.0 – Dados do Sistema Digital (SD):

Nome do SD: ☐

Posto e nome do responsável pela definições de SI do SD:

☐

Classificação mais elevada dos dados manipulados pelo SD:
◯ Ultra-Secreto ◯ Secreto ◯ Reservado ◯ Ostensivo

2.0 – Regra para formação dos nomes dos usuários:

Utiliza o NIP como nome de usuário …….... ◯ Sim ◯ Não

Utiliza a função como nome de usuário..……. ◯ Sim ◯ Não

Utiliza qualquer nome de usuário..……... ◯ Sim ◯ Não

Caso utilize qualquer nome, exige um tamanho mínimo de ☐ e máximo de ☐ caracteres

3.0 – Regra para constituição das senhas dos usuários:

Exige utilização de letras maiúsculas, letras minúsculas, números e caracteres especiais (@#$%) (simultaneamente) …….. ◯ Sim ◯ Não

O SD diferencia maiúsculas de minúsculas na senha ……..... ◯ Sim ◯ Não

Exige um tamanho mínimo de ☐ e máximo de ☐ caracteres na senha

4.0 – Armazenamento das senhas dos usuários:

As senhas dos usuários são armazenadas: ◯ no banco de dados ◯ em arquivo separado

As senhas são criptografadas com o algoritmo: ☐

5.0 – Bloqueio automático de contas de usuários:

O SD bloqueia usuários quando há tentativas inválidas de acesso (erro de senha, por exemplo):
◯ Sim ◉ Não

O bloqueio automático é feito após quantas tentativas inválidas de acesso: ☐

6.0 – Protocolos de rede utilizados para acesso ao SD:

Protocolos utilizados: ☐ HTTP ☐ HTTPS ☐ TCP ☐ UDP outros
A.C. emitente de Certificados para o SD:

7.0 – Processo de autenticação de usuários:

Descreva como foi implementado o processo de autenticação de usuários no SD:

8.0 – Processo de recuperação de senhas de usuários:

Descreva como foi implementado o processo de recuperação de senhas de usuários no SD:

< local, data >

< Nome do responsável pelas definições de SI do SD >
< Posto do responsável pelas definições de SI do SD >
< Função do responsável pelas definições de SI do SD >

ASSINADO DIGITALMENTE