Auditorias LTDA

Relatório de Auditoria de Segurança da Informação

Auditorias LTDA

Sumário

Auditorias LTDA

1 - APRESENTAÇÃO

Este documento trata sobre a auditoria efetuada na LojaVirtual LTDA que teve como abrangência a análise do documento Sistemas de Gestão de Segurança da Informação em sua versão 1.0 e seus controles no tratamento dos ativos.

2 - COMPOSIÇÃO DA EQUIPE DE AUDITORIA

Abaixo a relação dos componentes desta auditoria realizada na LojaVirtual LTDA.

- Gustavo Henrique Da Rocha Reis (líder da equipe de auditoria)
- Jonathas Borges Cavalcante (membro da equipe de auditoria)

3 - ITENS AUDITADOS

Controle ISO 27002	Descrição do controle	Implementado?
5	Política de Segurança da Informação	sim
6.1.1	Responsabilidades e papéis pela segurança da informação	sim
8.1.1	Inventário dos ativos	sim
8.1.2	Proprietário dos ativos	sim
8.2.1	Classificação da informação	sim
8.2.3	Tratamento dos ativos	sim
9.4.2	Procedimentos seguros de entrada no sistema (log-on)	sim
9.4.3	Sistema de gerenciamento de senha	sim

Descrição do controle	Implementado?
Backup do banco de dados	não
Teste do backup do banco de dados	não
Atualização do gerenciador do banco de dados	não
Atualização do sistema web LojaVirtual	sim
Controle de acesso/usuário	sim
Atualização do sistema de hospedagem de páginas	não

1. Política de Segurança da Informação: A organização deve desenvolver e implementar uma política claramente definida e documentada que estabeleça diretrizes para a proteção dos ativos de informação. Essa política deve ser comunicada a todos os funcionários e partes interessadas relevantes.

2. Responsabilidades e papéis pela segurança da informação: Deve ser atribuída a responsabilidade pela segurança da informação a indivíduos específicos dentro da organização. Os papéis e responsabilidades de cada um devem ser claramente

definidos, estabelecendo a autoridade necessária para implementar e manter as medidas de segurança adequadas.

3. Inventário dos ativos: A organização deve manter um inventário completo de todos os ativos de informação relevantes, incluindo hardware, software e dados. Isso ajuda na identificação e no gerenciamento adequado dos ativos de informação.

4. Proprietário dos ativos: Cada ativo de informação deve ter um proprietário designado que seja responsável por sua proteção. O proprietário deve ser identificado e ciente de suas responsabilidades em relação à segurança desses ativos.

5. Classificação da informação: A informação deve ser classificada com base em seu valor, sensibilidade e criticidade. Isso permite que a organização aplique medidas de segurança adequadas para proteger a informação de acordo com sua importância.

6. Tratamento dos ativos: Os ativos de informação devem ser adequadamente protegidos ao longo de seu ciclo de vida, desde a criação até o descarte. Isso inclui medidas de proteção física, controles de acesso, criptografia e outras práticas relevantes para garantir a confidencialidade, integridade e disponibilidade dos ativos.

7. Procedimentos seguros de entrada no sistema (log-on): Deve haver procedimentos seguros de autenticação para controlar o acesso aos sistemas de informação. Isso pode incluir a exigência de senhas fortes, autenticação de dois fatores ou outras medidas de autenticação adequadas para garantir que apenas usuários autorizados acessem os sistemas.

8. Sistema de gerenciamento de senha: A organização deve estabelecer um sistema de gerenciamento de senha para garantir que senhas fortes sejam usadas e que sejam alteradas regularmente. Isso inclui diretrizes para a escolha de senhas seguras, restrições sobre o compartilhamento de senhas e o uso de técnicas criptográficas apropriadas para armazenar senhas.

4 - AVALIAÇÃO DAS EVIDÊNCIAS COLETADAS

Com base na análise realizada, verificou-se que a empresa possui o Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a norma ISO 27002. No entanto, alguns quesitos não estão em conformidade com o documento. A seguir, apresentamos os resultados da análise:

1. Durante a análise, constatou-se que não foram encontrados os **scripts de backup/testes do banco de dados**, registros de execuções agendadas e nem cópias armazenadas em outros dispositivos, conforme estabelecido no Sistema de Gestão de Segurança da Informação (SGSI). Essas responsabilidades são atribuídas ao Gerente do Banco de Dados e são consideradas de alto impacto para a organização, apresentando um **risco alto** de impacto.

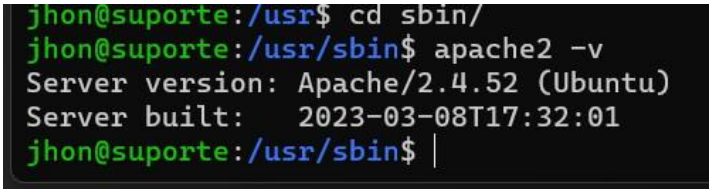
2. Durante a análise, verificou-se que a versão do SGBD MariaDB no servidor é a **10.6.12**. No entanto, é relevante destacar que já está disponível uma versão mais recente e estável, a **11.2.0**, que soluciona diversos bugs, incluindo vulnerabilidades de segurança listadas em. Conforme estabelecido no SGSI, é responsabilidade do Gerente do Banco de Dados manter o SGBD atualizado. Essas atualizações são classificadas como de alto impacto para a organização, apresentando um **risco alto** de impacto.

Data de acesso em 22/06/2023 - https://mariadb.org/mariadb/all-releases/

3. A plataforma de comércio eletrônico LojaVirtual encontra-se atualizada na versão 5.7 e está configurada para receber atualizações automáticas, conforme pode ser verificado em https://www.lojavirtual.com.br/wp-admin/update-core.php. No entanto, foi identificado que há 7 plugins desatualizados, conforme evidenciado em https://www.lojavirtual.com.br/wp-admin/plugins.php. Conforme as diretrizes do Sistema de Gestão de Segurança da Informação (SGSI), é de responsabilidade do Analista de Sistemas manter o sistema web atualizado. Ressalta-se que esse ativo possui uma classificação de baixo impacto para a organização, acarretando **um risco de baixo** impacto.

4. Durante a análise, constatou-se que o sistema possui o controle de acesso / usuários diferenciando permissões para usuários comuns e administradores, conforme segue orientações do SGSI.

5. O sistema de hospedagem de página (servidor web) encontrado, conforme print do console, foi:
   jhon@suporte:/usr/sbin$ apache2 -v
   Server version: Apache**/2.4.52** (Ubuntu)
   Server built: 2023-03-08T17:32:01



Contudo, já existe a versão estável **2.4.57** (released 2023-04-06) disponível em <https://httpd.apache.org/download.cgi> cujo anúncio pode ser comprovado em <https://downloads.apache.org/httpd/Announcement2.4.html> que corrige diversas brechas de segurança descritas em < https://downloads.apache.org/httpd/CHANGES_2.4.57.html>. Conforme o SGSI, é responsabilidade do Gerente de Redes manter o sistema de hospedagem atualizado. Este ativo possui classificação de médio impacto à organização e **risco médio** de impacto.

5 - CONCLUSÕES

Conclui-se que o protocolo SGSI apresentado deve ser atualizado para contemplar os ativos do Sistema Operacional, bem como seus responsáveis, suas classificações de riscos junto com a analise dos respectivos impactos que podem acarretar para a organização.

Para evitar possíveis vulnerabilidades decorrentes de bugs conhecidos em versões anteriores, recomenda-se a implementação de um plano de atualização dos seguintes componentes do sistema: sistema operacional ubuntu para a versão 23.04, sistema de hospedagem Apache para a versão 2.4.57, SGBD MariaDB para a versão 11.2, e também os plugins do sistema web. Isso garantirá a segurança e o bom funcionamento do sistema.

Com o objetivo de reduzir os riscos decorrentes da indisponibilidade do banco de dados, é altamente recomendável que sejam criados scripts de backup e testes de backup. Além disso, é importante agendar regularmente a execução desses backups, copiando o banco de dados para um dispositivo externo ao servidor. Essa medida garantirá a segurança dos dados e facilitará a recuperação em caso de falhas ou incidentes.

Após encerrar todas as observações descritas neste documento, a equipe de auditoria se coloca à disposição para futuras auditorias ou para acompanhar a resolução dos problemas atualmente relatados. A equipe se encontra disponível para qualquer suporte necessário e prontos para contribuir com as soluções necessárias

Gustavo Henrique Da Rocha Reis
Líder da equipe de auditoria

Jonathas Borges Cavalcante
Membro da equipe de auditoria