**Relatório de Análise de Segurança e Auditoria de**

**Tecnologia da Informação**

**N° 1/2023**

Cliente: TechNova 16 junho de 2023

1. **Introdução**

A partir do ataque realizado em um site web da empresa fictícia TechNova no dia 01 de março de 2023, apresenta-se o seguinte Relatório de Análise de Segurança e Auditoria de Tecnologia de Informação, com o objetivo de investigar o ocorrido a partir do levantamento das vulnerabilidades do sistema e da aderência às normas regulamentadoras, a citar NBR ISO 27001 e 27002, responsáveis por fornecer as diretrizes sobre a implementação de controles de segurança,.

A fim de promover a proteção dos dados e sistemas críticos da organização, bem como reduzir os riscos de ameaças cibernéticas, este trabalho busca destacar as falhas de segurança levantadas, e propõe recomendações de aprimoramento, onde possível.

O trabalho foi realizado no período de 06/05/2023 a 20/06/2023, executado de acordo com os procedimentos de auditoria em conhecimento da equipe. Os termos introduzidos neste relatório serão apresentados no dia dd/mm/aaaa, para avaliação da equipe responsável, e posterior homologação do relatório pelos mesmos.

1. **Contexto e Escopo**

A Empresa Fictícia TechNova atua no setor vendas online de produtos tecnológicos e possui uma infraestrutura de sistemas de informação crítica para suas operações. O escopo desta auditoria abrange a análise da segurança da informação dos sistemas afetados, bem como os recursos de tecnologia da informação utilizados pela organização.

1. **Metodologia**

A auditoria foi realizada a partir da análise e revisão documental, contando com apoio de entrevistas e encontros, tanto síncronos quanto assíncronos, com o monitor, responsável pelas informações de segurança da informação e análise técnica, além de discussões propostas nos fóruns do ambiente virtual *Moodle.*

Para o desenvolvimento do relatório, foi feito um aprofundamento teórico com pesquisas sobre o tema e assuntos relacionados ao incidente, além de consultas às normas NBR 27001 e NBR 27002 como referência.

Por fim, ao cruzar os dados obtidos dessas pesquisas, é feita a avaliação do estado da segurança do sistema atual, ao documentar as hipóteses levantadas pela equipe de auditoria neste documento. Como apoio nessa etapa, foi utilizado exemplos de relatórios de auditoria de tecnologia da informação encontrados na internet.

1. **Não Conformidades**

Tendo como referência as normas NBR 27001 e NBR 27002, foram identificadas, a partir da análise do incidente, algumas não conformidades, discutidas em maiores detalhes nas seções seguintes:

* 1. **Controle de Acesso**

Foram identificadas duas não conformidades relacionadas à configuração inadequada do controle de acesso na TechNova, as quais permitiram a disseminação do ransomware. Essa discussão se baseia no item 9 da NBR 27002, a qual trata das diretrizes associadas ao controle de acesso para segurança da informação. Esse item abrange, em seus subtópicos: requisitos do negócio para controle de acesso, gerenciamento de acesso do usuário, responsabilidades dos usuários e controle de acesso ao sistema e à aplicação. A partir do controle de acesso, entende-se que é possível limitar o acesso de usuários externos ao sistema, prevenindo o acesso à informações sensíveis e a articulação de ataques e atividades mal intencionadas.

* + 1. **Política de controle de acesso**

A seção NBR 27002 - A.9.1 busca limitar o acesso à informação e aos recursos de processamento da informação, considerando a visão de negócio. Com isso, estabelece os critérios de implementação de políticas de controle de acesso, no item 9.1.1. Nesse ponto, recomenda-se a definição e devida documentação de políticas de controle de acesso, com base nos requisitos de segurança da informação e dos negócios.

Com as políticas de controle de acesso definidas, é possível realizar o gerenciamento de contas de acordo com as respectivas permissões de acesso, restringindo os direitos de acesso com a declaração de regras e requisitos para solicitação e análise dos mesmos.

Diante disso, observa-se uma não conformidade com os termos destacados, fazendo-se necessário que a organização avalie a implementação de uma política de controle de acesso e realize revisões regulares, a fim de prevenir incidentes de segurança e proteger os sistemas e dados sensíveis da organização.

* + 1. **Gerenciamento de acesso do usuário**

Ainda sobre o controle de acesso, a seção NBR 27002 - A.9.2 dedica-se ao gerenciamento de acesso do usuário, com o objetivo de assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

Esse tópico rege as diretrizes relacionadas ao gerenciamento de acesso do usuário, a começar pelo processo formal de registro e cancelamento de usuário. Ainda assim, trata também das permissões para concessão ou revogação dos direitos de acesso entre os usuários do sistema, bem como o gerenciamento de direitos de acesso privilegiados. Isto é, restringir e controlar a concessão e o uso de determinados acessos considerados privilegiados.

A seção declara, ainda, que o uso inapropriado de privilégios de administrador de sistemas (qualquer característica ou recursos de sistemas de informação que habilitam usuários a exceder o controle de sistemas ou aplicações) pode ser um grande fator de contribuição para falhas ou violações de sistemas.

Analisando o incidente de segurança em questão, observa-se que a TechNova não está em conformidade com os termos declarados neste item, a começar pelo acesso indevido do invasor ao sistema, realizado através de SQL injection. Ao garantir privilégios de administrador, foi possível obter o acesso indevido a todos os dados e arquivos da empresa, incluindo informações sensíveis de usuários, como senhas e contas bancárias.

Com isso, faz-se necessário revisar as diretrizes de gerenciamento de acesso, a fim de implementar as regras e restrições de acordo com o estabelecido na norma. Com isso, pretende-se reduzir o risco de acesso indevido ao sistema, e especialmente aos dados sensíveis da organização.

* + 1. **Controle de acesso ao sistema e à aplicação**

De forma similar, observa-se, no item 9.4 da mesma norma, diretrizes sobre o controle de acesso ao sistema e à aplicação, com o objetivo de prevenir o acesso não autorizado aos sistemas e aplicações. Esse item estabelece, entre outros, os critérios para especificar as restrições do sistema de acordo com a política de controle de acesso. Deste modo, inclui também o sistema de gerenciamento de senhas, com o objetivo de assegurar senhas de qualidade, conforme especificado na seção NBR 27002 - A.9.4.3.

Ao analisar as diretrizes da norma, observa-se a preocupação com a elaboração de senhas de qualidade, que devem ser alteradas regularmente, mas também estabelece critérios para armazenamento das mesmas, devendo estar separadas dos demais dados do sistema da aplicação, garantindo proteção e segurança também na transmissão das senhas dos usuários.

Neste contexto, observa-se a não conformidade da TechNova na adoção das políticas de senha da empresa, adequadamente com as diretrizes estabelecidas na norma. Assim, dificulta a invasão do sistema por usuários não autorizados, bem como o acesso aos dados de armazenamento das senhas em conjunto com outros dados. Com isso, é imperativo a definição de políticas de senhas fortes, a partir de critérios mínimos de complexidade, e principalmente a atualização regular das mesmas, impedindo a reutilização de senhas antigas.

* 1. **Atualizações de Segurança**

No contexto de atualizações de segurança a norma NBR 27002 no item 12 traz regras para garantir que o software seja desenvolvido e mantido com atualizações regulares de segurança, corrigindo vulnerabilidades conhecidas. Além disso, deve seguir as práticas recomendadas de desenvolvimento seguro, como implementar recursos e funcionalidades para garantir a segurança do software.

Nesse item identificamos que o site da TechNova não está em conformidade, primeiro falando da linguagem de programação utilizada para o desenvolvimento, o PHP v7.3, versão que já deixou de receber atualizações de segurança em 2018 e tem vulnerabilidades conhecidas: Vulnerabilidades de execução remota de código (RCE): RCE ocorre quando um invasor consegue executar comandos arbitrários no servidor; Vulnerabilidades de Cross-Site Scripting (XSS): O XSS ocorre quando um invasor consegue inserir código malicioso em um site, que é então executado no navegador dos usuários; Alocação de Recursos sem Limites ou Throttling: se refere a uma situação em que recursos de um sistema ou serviço são alocados ou utilizados sem restrições ou limitações adequadas.

Além das vulnerabilidades para o qual o site foi exposto ao utilizar a versão antiga do PHP o site também sofreu ataque de injeção de SQL que ocorrem quando as consultas SQL são construídas de forma insegura, permitindo que um invasor injete código SQL malicioso e obtenha acesso não autorizado ao banco de dados. O que indica que o time de desenvolvimento não seguiu boas práticas para criação das consultas feitas no banco de dados.

1. **Recomendações de Melhoria**

Diante desse contexto, como resposta às vulnerabilidades encontradas e discutidas em relação às normas regulamentadoras, são propostas algumas recomendações para prevenir reincidências do ataque, e, com isso, promover maior segurança dos sistemas da organização.

* 1. **Implementação de Medidas de Segurança Técnica**

Para garantir a segurança técnica, é importante implementar várias medidas, conforme estabelecido na norma NBR 27002. Uma delas é a instalação de firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS) e antivírus atualizados em todos os dispositivos. Além disso, é essencial utilizar criptografia em comunicações e dados sensíveis, tanto em repouso quanto em trânsito. Estabelecer políticas de controle de acesso, com autenticação forte e gerenciamento adequado de senhas, também é fundamental. Por fim, é necessário monitorar de forma contínua os sistemas em busca de atividades suspeitas ou anormais.

* 1. **Elaboração da Política de Segurança da Informação**

No que se refere à liderança, é responsabilidade da Alta Direção estabelecer uma política de segurança da informação em conformidade com os requisitos para criação da política de informação estabelecidos na norma NBR 27001 - 5.2.

Em primeiro lugar, a política deve ser formalizada em um documento registrado por escrito, garantindo que todos na organização tenham acesso a ela. Isso proporcionará clareza, compreensão e adesão à política por parte de todos os envolvidos.

Em segundo lugar, é essencial comunicar amplamente a política dentro da organização, alcançando todos os funcionários, contratados e outras partes relevantes. Uma comunicação eficaz garantirá que todos estejam cientes da política e compreendam suas responsabilidades em relação à segurança da informação.

Por último, a política também deve ser disponibilizada para as partes interessadas externas, como clientes, fornecedores, parceiros de negócios e outras entidades relevantes. Isso demonstra o comprometimento da organização com a segurança da informação e contribui para o estabelecimento de confiança mútua.

Dessa forma, ao estabelecer e comunicar adequadamente a política de segurança da informação, a Alta Direção promove a conscientização, a conformidade e o compromisso de todos os envolvidos, fortalecendo a postura de segurança da organização.

* 1. **Criação de uma política de backups**

Para garantir a integridade e segurança dos dados contra possíveis ataques, é essencial implementar uma política de backups em conformidade com as normas NBR27002.

Essa política deve abranger backups totais, que englobam todos os dados, que serão executados em intervalos regulares definidos pela política. Isso garante que todas as informações sejam protegidas e restauradas integralmente em caso de perda ou corrupção dos dados originais.

Além dos backups totais, os backups parciais podem ser implementados para permitir a recuperação seletiva de partes específicas dos dados e backups de atualização devem ser realizados regularmente para acompanhar as mudanças nos dados.

Também é fundamental testar periodicamente a eficácia dos backups, verificando sua integridade e a capacidade de recuperação dos dados. Isso pode ser feito por meio de restaurações de teste, simulando situações de recuperação reais e avaliando a confiabilidade do processo.

Por fim, a criptografia deve ser aplicada aos backups para proteger os dados armazenados. A utilização de algoritmos criptográficos robustos e o gerenciamento adequado das chaves de criptografia são essenciais para garantir a confidencialidade e a integridade das informações durante o armazenamento e a transferência dos backups.

Ao adotar uma política de backups a organização estará fortalecendo sua postura de segurança, minimizando o risco de perda de dados e garantindo a prontidão para enfrentar possíveis ameaças futuras.

* 1. **Criação do Sistema de Gestão da Segurança da Informação (SGSI)**

A criação do Sistema de Gestão da Segurança da Informação (SGSI) para a TechNova é essencial após o ataque cibernético sofrido pela empresa. O SGSI englobará ações para contemplar os riscos e oportunidades relacionados à segurança da informação, de acordo com o critério estabelecido na norma NBR 27001 - 6.1. Isso inclui a avaliação completa dos riscos, definição de políticas e procedimentos, implementação de controles de segurança e treinamentos de conscientização. Com o SGSI, a TechNova poderá fortalecer sua proteção, garantindo a disponibilidade, integridade e confidencialidade dos dados, prevenindo futuros ataques e preservando a confiança dos clientes.

1. **Conclusão**

Em conclusão, observa-se que o ataque enfrentado pela TechNova foi resultado de falhas de segurança nos sistemas internos da empresa, devido à não conformidade com as diretrizes estabelecidas pelas normas regulamentadoras de segurança da informação. Tem-se, então, a oportunidade de implementação de medidas para proteção da privacidade e dos dados críticos da empresa. Reforça-se, ainda, a importância dessas medidas, em conformidade com os critérios estabelecidos pelas normas vigentes.

Recomenda-se fortemente a criação do Sistema de Gestão da Segurança da Informação (SGSI) que servirá como um protocolo para uma gestão de segurança mais estruturada que junto a criação de uma política de segurança da informação irão evitar futuros problemas.

16 de junho de 2023

**Thiago Coutinho**