PLANO DE SEGURANÇA

Carlos Almeida (1181132)
André Teixeira (1190384)
SEGSI – Segurança de Sistemas e Informação

Índice

Índice Figuras

Introdução

Este plano de segurança foi desenvolvido para a cadeira de Segurança de Sistemas e Informação, visando assegurar a proteção dos ativos e sistemas vitais da organização, em conformidade com as orientações da diretiva **NIS2** da União Europeia. No nosso país, a **Lei 46/2018** e o **Decreto-Lei 65/2021** adaptaram esta diretiva, requerendo que todas as entidades elaborem um plano de segurança devidamente documentado e aprovado pelo **CISO**. Este documento ainda segue as orientações do Centro Nacional de Cibersegurança (**CNCS**), visando garantir a conformidade com as normas nacionais e europeias para uma estratégia segura e resiliente em segurança da informação.

Preâmbulo

Este trabalho tem como objetivo elaborar um plano de segurança que atenda às exigências da política de defesa ciberdefesa da UE (União Europeia), mais concretamente após a publicação da NIS2. Este trabalho tem um sistema a ter em conta, como é apresentado na figura em baixo, onde se consegue ver a sua estrutura:

- Server1: serve como frontend da página pública.
- Server2: serve de base de dados para e-commerce e contabilidade.
- Server3: serve exclusivamente para contabilidade.
- Switch1 e Switch2: são conexões de rede para servidores e clientes.
- Router1: conecta a rede à internet.
- Client: clientes que podem ser internos (acedendo via Switch2) ou externos (acedendo via Switch1).

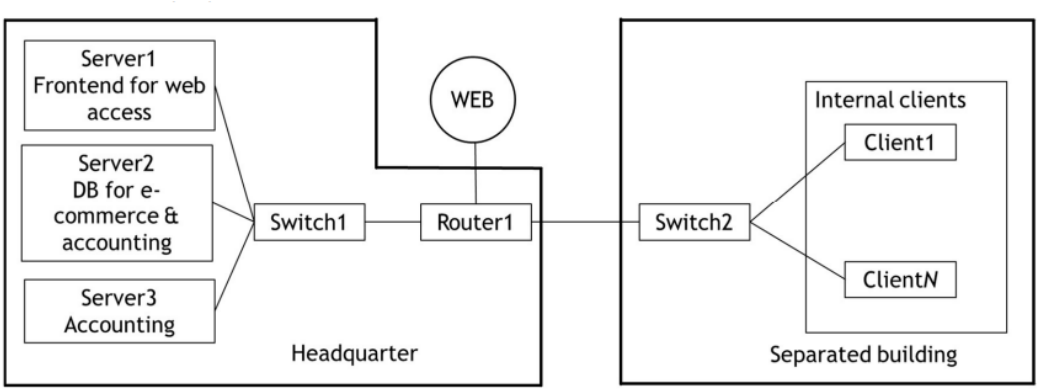

Figura 1: Arquitetura do sistema

Um plano de segurança em conformidade com a política de ciberdefesa, especialmente com a diretriz NIS2 é crucial para proteger a organização contra ameaças cibernéticas, garantir a continuidade dos negócios e evitar penalidades legais. Além disso, demonstra compromisso com a segurança, aumentando a confiança de clientes e parceiros.

Política Geral de Segurança

A Política Geral de Segurança estabelece os princípios e orientações para resguardar os ativos e informações da organização. Este conjunto de regras é crucial para todas as atividades de segurança e está em conformidade com as diretrizes da NIS2.

1) Objetivo

A finalidade da Política Geral de Segurança é estabelecer um ambiente seguro, reduzindo riscos e ameaças à integridade, disponibilidade e confidencialidade dos ativos da organização. Isso engloba a defesa da entidade contra ataques cibernéticos, fraudes, perdas de informação e incidentes que possam impactar negativamente as operações e a imagem da organização.

2) Âmbito

Esta política abrange todos os sistemas e processos da organização, incluindo:

- **Sistemas de Informação**: Aplicações críticas, bases de dados, sistemas de backup e plataformas em nuvem.
- **Infraestrutura de Rede**: Todos os aparelhos de comunicação e direcionamento de informações.
- **Informações Sensíveis**: Dados pessoais, financeiros e outras informações consideradas confidenciais.
- **Recursos Humanos**: Funcionários, contratados e terceiros com acesso aos ativos.

3) Princípios de Segurança

Esta política é direcionada por princípios específicos:

- **Confidencialidade**: Garantir o acesso controlado aos dados, permitindo que apenas pessoas autorizadas tenham acesso a informações confidenciais.
- **Integridade**: Preservar a exatidão dos dados ao longo do armazenamento, processamento e transmissão.
- **Disponibilidade**: Assegurar que os sistemas e serviços essenciais estejam disponíveis e acessíveis quando necessário.
- **Conformidade**: Garantir que as práticas de segurança estejam em conformidade com normas internacionais e a diretiva NIS2, realizando auditorias regulares.

Figura 2: Triade da Segurança

4) Declaração de Intenção

Esta política demonstra o empenho da empresa em aplicar uma estratégia de segurança abrangente e incentivar a sensibilização de todos os colaboradores, independentemente dos seus níveis hierárquicos.

5) Papéis e Responsabilidades

- **Diretor de Segurança da Informação (DSI):** Coordena a aplicação da política e revê periodicamente o plano.
- **Gestor de Tecnologia de Informação:** Supervisiona a instalação dos controlos técnicos, conduz auditorias de segurança e avalia ameaças e vulnerabilidades.
- **Equipa de Cibersegurança:** Vigia constantemente os sistemas, deteta potenciais ameaças e atua perante incidentes.
- **Colaboradores:** Devem obedecer às normas de segurança, participar em formações e informar sobre atividades suspeitas.

6) Atualização e Revisão

A política será revista anualmente ou sempre que houver mudanças significativas nas operações ou nas regulamentações. Auditorias internas e externas verificarão a conformidade e a eficácia do plano, promovendo ajustes conforme necessário.

Inventário de Ativos

A criação de um Inventário de Ativos é essencial para identificar os elementos que precisam de proteção, priorizando-os de acordo com sua criticidade e sensibilidade. Estes ativos incluem dados, equipamentos, software, infraestrutura e até mesmo pessoal e propriedades físicas.

1) Identificação e Classificação dos Ativos

Cada ativo foi categorizado com base na sua importância para a operação organizacional:

- **Servidores Críticos**: Hospedam dados e sistemas essenciais para o funcionamento dos serviços.
    - **Classificação**: Alta criticidade e sensibilidade, pois uma falha nesses servidores afeta diretamente as operações.
- **Base de Dados de Clientes**: Armazena informações pessoais e financeiras dos clientes.
    - **Classificação**: Sensibilidade elevada, impacto muito significativo em caso de violação, como sanções legais e desconfiança.
- **Plataforma de comunicação Empresarial**: Ferramenta de comunicação interna e externa.
    - **Classificação**: Média criticidade, mas com impacto significativo em caso de comprometimento.
- **Equipamentos de Rede**: Inclui routers, switches e firewalls essenciais.
    - **Classificação**: Alta criticidade, pois o seu comprometimento pode expor dados a invasores.

2) Propriedade e Localização

- **Servidores Críticos:** Localizados no data center principal, acessíveis apenas a pessoal autorizado.
- **Base de Dados de Clientes:** Localizada em servidores com controlo de acesso rigoroso e sistemas de auditoria.

- **Equipamentos de Rede:** Localizados em áreas seguras e monitorizadas para evitar acessos não autorizados.

3) Valor e Impacto

O comprometimento de ativos, como servidores críticos ou dados de clientes, acarretaria consequências significativas, incluindo perda financeira, prejuízo à reputação e possíveis sanções legais.

Gestão de Riscos

A gestão de risco é a identificação e priorização, com base no impacto para o negócio, de eventos e questões imprevistas, seguida de atividades para mitigar e controlar resultados negativos que possam ter danos inaceitáveis para a rentabilidade, reputação ou sucesso do negócio. Ferramentas, processos e estratégias são implementados ou desenvolvidos para apoiar estas atividades. Foram definidos dois riscos principais com suas respetivas medidas de mitigação.

1) Risco 1: Ataque de Ransomware

- **Descrição**: Ataques de ransomware podem comprometer a disponibilidade e a integridade dos dados da organização, criptografando informações críticas.
- **Probabilidade**: Alta
- **Impacto**: Muito Alto, com a possibilidade de interrupção completa das operações.
- **Medidas de Mitigação**:
    - **Backups**: Manter backups atualizados em locais separados e testar a recuperação dos dados periodicamente.
    - **Software de Segurança**: Implantar antivírus e ferramentas antimalware avançadas com deteção em tempo real.
    - **Políticas de Conscientização:** Formação dos colaboradores sobre riscos de phishing.

2) Risco 2: Falha de Sistema

- **Descrição**: Falhas nos servidores críticos devido a falhas técnicas pode ocasionar interrupções nas operações e perda de dados.
- **Probabilidade**: Média
- **Impacto**: Alto, pois existe possibilidade de paralisação de operações.
- **Medidas de Mitigação**:
    - **Manutenção Preventiva**: Realizar revisões periódicas e substituição de hardware crítico conforme necessidade.
    - **Plano de Continuidade de Negócios (PCN)**: Desenvolver um PCN que inclua redundância, como servidores em diferentes locais e backups regulares, ajudará a reduzir os danos causados por falhas de sistema ou desastres naturais.
    - **Monitorização Proativa**: Implementação de monitorização em tempo real, 24 horas por dia, 7 dias por semana, com o objetivo de identificar falhas precocemente e corrigir problemas de forma antecipada.

Gestão de Incidentes

A gestão de incidentes é uma série de etapas tomadas para identificar, analisar e resolver incidentes críticos que podem levar a problemas numa organização. Um incidente, por definição, é um acontecimento que pode interromper ou causar a perda de operações, serviços ou funções. A gestão de incidentes descreve as ações necessárias a serem tomadas por uma organização para analisar, identificar e corrigir riscos, enquanto implementa medidas que podem prevenir futuros incidentes, tais como invasões de rede, problemas tecnológicos e perda de dados sigilosos.

Portanto, a Gestão de Incidentes é essencial para garantir uma resposta rápida e efetiva a qualquer incidente de segurança, minimizando os danos e simplificando a recuperação.

1) Incidente 1: Invasão de Rede

- **Descrição**: Tentativa de acesso não autorizado à rede da organização.
- **Deteção**: Vigilância permanente através de sistemas de deteção de intrusão (IDS) que avisam sobre possíveis tentativas suspeitas.
- **Resposta**:
    - **Contenção:** Separar de imediato os dispositivos comprometidos para evitar a disseminação.
    - **Análise e diagnóstico**: Descobrir a fonte do ataque e verificar o grau de comprometimento.
    - **Erradicação e recuperação**: Eliminar o agente malicioso e recuperar os sistemas comprometidos.
- **Relatório**: Documentar o incidente para revisão.

2) Incidente 2: Perda de Dados por Funcionário

- **Descrição**: Perda ou roubo de dispositivo contendo dados sensíveis da organização.
- **Deteção**: Colaborador comunica imediatamente a perda do dispositivo.
- **Resposta**:
    - **Contenção e bloqueio**: Bloquear acesso ao dispositivo e, se possível, apagar remotamente o dispositivo.
    - **Análise**: Avaliar se houve acesso a dados sensíveis por terceiros.
    - **Notificação**: Informar partes interessadas, como clientes e autoridades, quando aplicável.
- **Relatório**: Documentar o incidente e revisar políticas de segurança para minimizar futuras ocorrências.

Continuidade de negócio

A continuidade de negócios é a capacidade de uma organização de manter ou retomar rapidamente níveis aceitáveis de entrega de produtos ou serviços após um evento de curto prazo que interrompa as operações normais. Exemplos de interrupções variam desde desastres naturais até falhas de energia. O MTD (Maximum Tolerable Downtime) é atribuido com base no impacto financeiro e reputacional, e neste caso em específico o e-commerce necessita de uma recuperação rápida, enquanto a contabilidade pode tolerar uma falha mais longa.

BIA (Business Impact Analysis)

Uma análise de impacto nos negócios é um processo sistemático para determinar e avaliar os potenciais efeitos de uma interrupção nas operações críticas de negócios como resultado de um desastre, acidente ou emergência.

Processos Críticos:

1. E-commerce:
    a. Impacto de falha: perda de receitas, reputação e clientes.
    b. MTD (Maximum Tolerable Downtime): 3 horas após isso, o impacto no negócio torna-se inaceitável.
2. Contabilidade:
    a. Impacto de falha: compromete relatórios financeiros.
    b. MTD (Maximum Tolerable Downtime): 24 horas, pois tem menos impacto imediato em comparação com o e-commerce.

Impacto dos componentes:

- Server1: afeta o frontend, o que tem impacto diretamente nos clientes externos (MTD = 3 horas).
- Server2: afeta o acesso à base de dados, é um ponto crítico, pois interrompe o e-commerce e a parte da contabilidade (MTD = 3 horas).
- Server3: afeta apenas a contabilidade (MTD = 24 horas).

Risk Assessment e Matriz de Risco

Como já relatado anteriormente foram identificados alguns riscos como:

- Ataques cibernéticos (por exemplo, ransomware).
- Falhas de hardware.
- Catástrofes naturais (por exemplo, inundações, incêndios, furações).

Ameaça	Probabilidade	Impacto	Nível de Risco

Ataque cibernético	Alta	Muito Alto	Muito Alto
Falha de hardware	Média	Alto	Alto
Catástrofes Naturais	Baixa	Muito Alto	Alto

BCM (Business Continuity Management)

A gestão da continuidade de negócios garante a recuperação dos serviços dentro dos tempos de tolerância definidos no BIA, tal como já referido anteriormente, existem algumas medidas para ajudar nestes processos, como a redundância (configurar servidores de backup para Server1 e Server2 e replicar os dados para uma localização secundária), planos de recuperação (garantir disponibilidade de equipamentos substitutos e estabelecer planos de recuperação para cada risco identificado) e monitorização (implementar ferramentas que consigam efetuar uma monitorização de modo a detetar falhas ou anomalias). De política todos os dados críticos (e-commerce e contabilidade) devem ser replicados diariamente para um servidor secundário, pois é essencial mitigar falhas críticas como estas perdas de dados, e garantir que os backups sejam testados mensalmente para verificar a sua integridade.

Recuperação de desastre

Um plano de recuperação de desastres (DRP) é uma abordagem estruturada que traça procedimentos e ferramentas para restaurar sistemas de IT críticos, dados e operações após um ciberataque, desastre natural ou outra interrupção. Ajuda a garantir a continuidade do negócio ao definir medidas para minimizar o tempo de inatividade e proteger ativos sensíveis. É um componente do BCP (business continuity plan) que especifica como restaurar operações após um desastre.

Prioridades de Recuperação

- Server1: Restaurar rapidamente o acesso ao site para evitar perda de clientes.
- Server2: Recuperar dados críticos, garantindo transações financeiras estáveis.
- Server3: Suporte interno, menos prioritário, mas deve ser funcional dentro do limite.

O objetivo do DRP é recuperar os sistemas críticos dentro dos tempos máximos toleráveis (MTD) para minimizar os impactos. Caso o MTD seja violado, é necessário que já haja uma preparação prévia, como manter backups atualizados em locais remotos para recuperação rápida. Como o Server1 e Server2 tem uma prioridade maior sobre o Server3, pode-se dizer que para restaurar as funções em caso de desastre, backups incrementais diários e um backup total semanalmente para o Server2, e soluções de snapshot para Server1 para restaurar rapidamente o frontend.

Como medidas preventivas, é necessário implementar redundância para reduzir o impacto de falhas e elaborar simulações de cenários de falha de modo a testar regularmente os tempos de recuperação para cada serviço para assegurar que o RTO (Recovery Time Objective) está dentro do limite MTD.

Formação de Recursos Humanos

A organização manterá um programa de formação contínua, abordando:

- Segurança Digital: Procedimentos seguros e prevenção de phishing.
- Proteção de Dados: Responsabilidades de cada colaborador.
- Avaliação: Entrevistas e testes pós-formação, com registo das sessões.

Cronograma e Responsabilidades

1) Planeamento Temporal

Um cronograma específico será elaborado para garantir a implementação e a revisão periódica de cada medida de segurança, com prazos para atingir cada marco, monitorizando o progresso das ações de segurança.

2) Designação de Responsáveis

Cada etapa e medida de segurança terá responsáveis atribuídos. Isso inclui o acompanhamento e a supervisão das implementações, e um responsável específico será designado para coordenar a resposta a incidentes ou vulnerabilidades emergentes.

Identificação dos Responsáveis e Validade do Plano

1) Responsáveis pela Segurança e Pontos de Contato

Para garantir respostas rápidas e eficazes em caso de incidentes, o plano inclui os nomes e contactos do **Responsável de Segurança da Informação (CISO)** e de pelo menos um ponto de contacto adicional, como email e telemóvel, permitindo um contacto direto com a autoridade nacional ou parceiros em qualquer circunstância.

Exemplo de Identificação dos Responsáveis:

- **Nome do CISO**: [Nome Completo]

- **Email**: [email@empresa.com]
- **Telemóvel**: [+351 123 456 789]
- **Ponto de Contacto Adicional**: [Nome Completo]
- **Email**: [email@empresa.com]
- **Telemóvel**: [+351 987 654 321]

2) Validade e Revisão do Plano

Este plano de segurança é válido por um período de um ano, sujeito a revisões periódicas anuais ou adicionais, caso novas ameaças, regulamentações ou mudanças tecnológicas exijam adaptações. A versão atualizada do documento será assinada após revisões aprovadas pelo CISO.

Conclusão

Este Plano de Segurança foi criado para oferecer uma proteção sólida para os ativos vitais da organização, em conformidade com os princípios de confidencialidade, integridade e disponibilidade. Conforme a norma NIS2 e as diretrizes do CNCS, o propósito do plano é garantir a continuidade dos serviços e a resistência a riscos de segurança. Com uma implementação rigorosa e avaliações regulares, este plano pode servir como uma orientação segura para reforçar a segurança da entidade.

Referências

- **União Europeia**. Diretiva NIS2 sobre Segurança da Informação. Disponível em: https://eur-lex.europa.eu.

- **Centro Nacional de Cibersegurança (CNCS)**. Diretrizes para a elaboração de Planos de Segurança e gestão de ciberincidentes. Disponível em: https://www.cncs.gov.pt.

- **Decreto-Lei n.º 65/2021**. Estabelece medidas de segurança de redes e sistemas de informação, regulamentando a adaptação da Diretiva NIS2 em Portugal. Diário da República, 30 de junho de 2021.

- **ISO/IEC 27001**. Normas de Gestão de Segurança da Informação. Disponível em: https://www.iso.org.

- **ISO/IEC 27005:2018**. Gestão de Riscos em Segurança da Informação. Complemento à ISO/IEC 27001. Disponível em: https://www.iso.org.

- **NIST Cybersecurity Framework (CSF)**. Diretrizes práticas para segurança cibernética. National Institute of Standards and Technology. Disponível em: https://www.nist.gov/cyberframework.

- **ENISA (European Union Agency for Cybersecurity)**. Implementação da NIS2 e gestão de ciberincidentes. https://www.enisa.europa.eu.