

Assignment 3

Plano de Contingência

Marco Querido - 1220268

Pedro Oliveira - 1220495

Mestrado em Engenharia Informática

Docentes

Nuno Pereira, Pedro Rodrigues, Jorge Pinto Leite, António Costa ([nap | dcr | jpl | acc]
@isep.ipp.pt)

Índice

Abstract	3
Propósito e Âmbito	4
Pessoal Responsável	4
Potenciais Riscos/Ataques	4
Resposta	6
Teste e Treino	10
Revisão e Futuras atualizações	10
Sitografia	11

Abstract

Em qualquer organização é fundamental contar com mecanismos que permitam à mesma estar em constante funcionamento. Quando há uma interrupção inesperada, um plano de contingência adequado pode fazer uma enorme diferença.

Depois do impacto do Covid-19 no mundo, e do número de ataques informáticos a empresas e singulares divulgados através dos media, a segurança informática teve uma maior importância na conceção e desenvolvimento de novas tecnologias, e cada vez mais é uma preocupação atualmente. Verifica-se que segundo o Centro Nacional de Cibersegurança(CNCS) as principais ameaças que mais atingem as empresas são: Phishing/Smishing, Ransomware, Fraude/Burla Online, Comprometimento de contas ou tentativa e Vulnerabilidades e a sua exploração.[1]

Este documento tem como propósito descrever um plano de contingência para uma instituição de saúde portuguesa que armazena toda a informação relacionada com o Covid-19, incluindo as notícias sobre a doença, e o plano de vacinação de cada cidadão. A informação deve ser classificada e acessível via página web. A infraestrutura do sistema já está implementada e consiste num servidor de autenticação, um servidor web e um servidor de ficheiros. Os canais de comunicação são públicos, e não está planeada a criação de canais privados.

As seguintes medidas visam auxiliar a empresa a fazer com que os seus processos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível.

Keywords: Contingency planning, Training, Incident Response, Cyberattacks.

Propósito e Âmbito

O propósito deste plano de contingência é garantir que a organização está preparada e habilitada para responder a eventos, emergências ou até falhas que podem impactar as operações e/ou serviços.

O plano pretende diminuir as consequências dos incidentes inesperados, ao referenciar como atuar e como efetuar a recuperação perante alguns riscos/ataques.

Este plano abrange potenciais riscos/ataques, incluindo e não limitado a desastres naturais, cyberattacks e falhas de equipamentos. Com este plano pretende-se que toda a organização apresente uma garantia de preparação em vários níveis.

Por fim, abrange todos os Sistemas IT, softwares, base de dados, aplicações e recursos de rede necessários pela organização para realizar o negócio.

Pessoal Responsável

De forma a garantir que a continuidade das operações ou serviços os papéis de cada indivíduo pertencente à instituição devem estar bem definidos.

Estes papéis são assim determinados:

- Coordenador do Plano – Esta pessoa está encarregue de verificar e testar durante um certo período o plano de forma a mantê-lo sempre atualizado.
- Diretor de TI – Esta pessoa fornece apoio técnico à equipa de recuperação, quer seja a restaurar serviços até coordenar a entrega de possível equipamento e software de reposição.
- Diretor de Avaliação de Danos – Esta pessoa está encarregue de avaliar os danos existentes, bem como determinar a causa. Também prevê o tempo que a instituição possa demorar a recuperar e contacta suporte adicional caso seja um caso necessário para isso;
- Diretor de Equipa Legal – Esta pessoa está encarregue de todas as questões legais relacionadas aos dados afetados bem como a possível interrupção dos serviços. Também aconselha quais os passos legais a tomar;
- Coordenador de Comunicações – Esta pessoa é responsável por comunicar com pessoas ou empresas externas sobre as possíveis interrupções.

Potenciais Riscos/Ataques

Esta secção aborda a análise dos possíveis riscos ao qual a organização está vulnerável. O processo de avaliação de riscos tem como finalidade fornecer informações para a tomada de decisões e assim determinar a ordem de prioridade na aplicação das medidas. Está dividida em 3 fases: identificar os riscos, analisá-los e por fim avaliá-los.

Classificação dos Riscos

SEVERIDADE	Extremamente Prejudicial	Risco Moderado	Risco Substancial	Risco Intolerável
	Prejudicial	Risco Tolerável	Risco Moderado	Risco Substancial
	Levemente Prejudicial	Risco Trivial	Risco Tolerável	Risco Moderado
		Altamente Improvável	Improvável	Provável
		PROBABILIDADE		

Figura 1- Classificação dos Riscos[2]

De seguida está evidenciada uma tabela que representa a classificação de possíveis riscos da organização utilizando a ajuda da figura acima representada.

Risco	Probabilidade	Severidade	Classificação de Risco
Sobrecarga de uso(energia)	Provável	Extremamente prejudicial	Risco Intolerável
DDos	Provável	Extremamente prejudicial	Risco Intolerável
Base de dados afetada	Improvável	Extremamente prejudicial	Risco Substancial
Sistema de Ficheiros afetado	Improvável	Extremamente prejudicial	Risco Substancial
Sobreaquecimento das salas de servidores	Improvável	Extremamente prejudicial	Risco Substancial
Ataque à página web	Provável	Prejudicial	Risco Substancial
Social Engineering	Provável	Prejudicial	Risco Substancial
Phishing	Provável	Prejudicial	Risco Substancial

Trovoadas	Improvável	Extremamente prejudicial	Risco Substancial
Malware	Improvável	Prejudicial	Risco Moderado
Falhas de energia	Improvável	Prejudicial	Risco Moderado
Terramotos	Altamente improvável	Extremamente prejudicial	Risco Moderado
Incêndio	Altamente improvável	Extremamente prejudicial	Risco Moderado
Cheias	Altamente improvável	Extremamente prejudicial	Risco Moderado
Ataques Físicos	Altamente improvável	Prejudicial	Risco Tolerável

Resposta

Risco/Ataque: Sobrecarga de uso(energia)

Descrição: Vários aparelhos eletrónicos ao utilizar energia criam uma sobrecarga.

Como atuar:

- Evacuar a divisão dependendo da origem calmamente e em segurança.
- Entrar em contacto com as autoridades competentes e seguir as ordens deles.
- Se houver indícios de sobrecarga, desligar os aparelhos eletrónicos que possam ser danificados das tomadas.
- Após a sobrecarga ter passado proceder á análise dos danos causados

Risco/Ataque: Ataque DDoS

Descrição: Pedidos dirigidos efetuados ao servidor de forma múltipla e consecutiva causando uma sobrecarga, levando ao sistema falhar.

Como atuar:

- Tentar a identificação da conexão e do IP do atacante.

Risco/Ataque: Base de dados afetada.

Descrição: Acesso não autorizado à base de dados, o que pode provocar a exposição de informações sensíveis, como por exemplo dados pessoais ou contas de utilizadores.

Como atuar:

- Verificação de direitos de acesso de todos os funcionários;
- Bloquear utilizadores que estejam inativos de forma a diminuir as chances de possíveis ataques;
- Informar os funcionários que foram comprometidos.

Risco/Ataque: Sistema de ficheiros afetado.

Descrição:

1: Acesso não autorizado ao sistema de ficheiros, quer seja por roubo de credenciais ou por direitos de acesso/privilégios errados.

2: Acesso a ficheiros que não estão confidenciais, mas deveriam estar.

Como atuar:

1: Identificar o utilizador a quem pertencem essas credenciais que foram utilizadas para acesso ilegal (roubo de credenciais) ou acesso errado (direitos de acesso/privilégios).

2: Identificar os ficheiros que estão expostos de forma errada.

Risco/Ataque: Sobreaquecimento das salas dos servidores

Descrição: Temperatura da sala dos servidores fora do normal.

Como atuar:

- Diminuir a temperatura da sala;
- Não mover o equipamento enquanto este estiver quente;
- Abrir portas (e janelas se existirem) de forma a arejar a divisão.

Risco/Ataque: Ataque página web.

Descrição: Atacantes poderão ganhar acesso a credenciais de utilizadores, o que pode significar a visualização e possível eliminação de informação sensível.

Como atuar:

- Identificar o utilizador cujas credenciais foram usadas para ganhar o acesso e alterar os seus dados;
- Informar o utilizador que foi alvo de roubo das credenciais;

- Identificar que dados foram expostos e por consequência possivelmente alterados/apagados;
- Alertar as entidades competentes.

Risco/Ataque: Social Engineering

Descrição: Um atacante coage um funcionário a ignorar medidas de segurança de forma a poder ter acesso ao sistema.

Como atuar:

- Identificar o funcionário que comprometeu o sistema;
- Informar o funcionário que foi vítima do ataque que comprometeu o sistema;
- Trocar as credenciais de acesso deste funcionário.

Risco/Ataque: Phishing

Descrição: Um atacante alicia uma pessoa a divulgar dados pessoais através de email ou websites aliciantes.

Como atuar:

- Identificar a informação que foi comprometida;
- Identificar o atacante e como ele atuou;
- Corrigir a validação existente na whitelist.

Risco/Ataque: Trovoadas

Descrição: Danificação de equipamentos devido a trovoadas.

Como atuar:

- Desligue equipamentos não especialmente necessários;
- Proteger equipamentos de forma a não sofrer danos elétricos;
- Esperar que a tempestade acalme para ligar equipamentos para não os danificar.

Risco/Ataque: Malware

Descrição: Equipamento afetado com Malware e com a possibilidade de infectar os outros equipamentos que possam estar conectados.

Como atuar:

- Analisar o equipamento afetado para identificar o malware;
- Usar software anti-malware de forma a remover o malware do equipamento afetado. Caso não seja possível remover então que seja feito o restauro de um ponto anterior. Se após estas duas tentativas o problema ainda exista então o equipamento deverá ser formatado.

Risco/Ataque: Falhas de energia

Descrição: Possíveis falhas de energia que interrompam o funcionamento ou danifiquem equipamentos

Como atuar:

- Ativar os geradores de backup de forma a repor a energia;
- Verifique se os servidores estão funcionais e execute os backups necessários.

Risco/Ataque: Terramotos

Descrição: Danificação de equipamentos devido a terremotos.

Como atuar:

- Se sentir um terremoto proteja-se debaixo de uma mesa até que tudo se acalme;
- Se algum equipamento estiver danificado não lhe toque pois pode ainda ter energia e dar choque;
- Esperar até ter alguma certeza que o terremoto parou e utilize as saídas de emergência.

Risco/Ataque: Incêndio

Descrição: Danificação de equipamentos devido a incêndios.

Como atuar:

- Se identificar um incêndio e este for ainda pequeno tente apagá-lo com segurança usando os equipamentos de emergência;
- Avise as entidades de emergência;
- Se o fogo não se estiver a propagar, tente prender os equipamentos eletrônicos de forma a não serem alcançados pelo fogo.
- Evacue as instalações em segurança pelas saídas de emergência;
- Após a sobrecarga ter passado, proceder á criação e análise dos danos causados pela entidade competente.

Risco/Ataque: Cheias

Descrição: Danificação de equipamentos devido a cheias.

Como atuar:

- Em perigo de cheias tente colocar os equipamentos eletrônicos a uma distância segura do chão, bem como barricar as portas para impedir a progressão da mesma.

Risco/Ataque: Ataques Físicos

Descrição: Roubo de equipamentos e danos físicos a equipamentos (servidores e outros hardwares).

Como atuar:

- Identificar a falha que originou o acesso não autorizado por parte do invasor;
- Verificar as câmaras de vigilância de forma a identificar o invasor que causou o estrago;
- Criação de um relatório do dano causado.

Teste e Treino

De forma a preparar todo o pessoal da organização sobre como proceder em caso de alguma situação anteriormente descrita acontecer, o coordenador do plano terá de efetuar testes e treinos através de exercícios e simulações de forma a garantir a sua eficácia. Isto inclui programas de treino para educar o pessoal da organização a saber o seu papel, responsabilidade e procedimentos, caso seja necessário ativar o plano de contingência.

Revisão e Futuras atualizações

Efetuada o planeamento, a equipa deve orientar os seus recursos para ter a certeza de que a mitigação dos riscos é bem-sucedida. A orientação dos recursos deve abordar a proteção das pessoas, bem como a instalação e infraestrutura da organização.

Uma vez feito este plano ele deve ser aceite pela alta administração.

De forma a manter o plano sempre atualizado e em dia, semestralmente o coordenador do plano deve efetuar uma revisão e atualizar o plano, utilizando lições aprendidas de eventos reais que aconteceram e/ou exercícios para garantir a sua relevância e a sua efetividade.

Sitografia

[1] <https://www.cnccs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cnccs.pdf>

[2] <https://www.sstonline.com.br/o-processo-de-avaliacao-de-riscos-e-o-seu-impacto-nas-medidas-de-prevencao/>

<https://www.lumiun.com/blog/perigo-para-empresas-ataque-de-ddos/>

<https://www.controle.net/faq/ataque-ransomware-tudo-o-que-voce-precisa-saber>

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltab7d19ca9100e50e/5e9dda e7674ec260f325c3ca/data_breach_response.pdf