Reação a incidentes

Roadmap para a criação de capacidades mínimas

Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de cibersegurança têm-se mostrado mais frequentes e complexos.

Com o objetivo de dotar as entidades do Estado, os operadores de serviços essenciais e os prestadores de serviços digitais com as valências mínimas para a análise, a mitigação e a resolução de incidentes de segurança no ciberespaço, o Centro Nacional de Cibersegurança (CNCS) definiu um conjunto de capacidades – técnicas, humanas e processuais – que constituem uma base harmonizada e desejável nesta matéria.

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

GLOSSÁRIO

CMDB – Configuration Management Database

CNCS – Centro Nacional de Cibersegurança

CSIRT – Computer Security Incident Response Team

ECO – Elemento de Contacto Operacional

GNS – Gabinete Nacional de Segurança

IOC – Indicator of Compromise

IP – Internet Protocol

IRT – Incident Response Team

ISAC – Information Sharing and Analysis Center

LIR – Local Internet Registry

PGP – Pretty Good Privacy

RFC – Request for Comments

RIPE – Réseaux IP Européens Network Coordination Centre

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Índice

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Sumário Executivo

Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de cibersegurança têm-se mostrado mais frequentes e complexos. Neste cenário, interessa mitigar o impacto e reduzir os danos decorrentes de incidentes desta natureza.

Com o objetivo de dotar as entidades do Estado e os operadores de infraestruturas críticas nacionais com as valências mínimas para a análise, a mitigação e a resolução de incidentes de segurança no ciberespaço, o Centro Nacional de Cibersegurança (CNCS) definiu um conjunto de capacidades – técnicas, humanas e processuais – que constituem uma base harmonizada e desejável nesta matéria. Este documento apresenta a visão e o modelo que o CNCS pretende desenvolver em cada uma das entidades do Estado e operadores de infraestruturas críticas para atingir esse objetivo. O modelo apresentado permitirá avaliar as várias entidades quanto ao seu grau de maturidade em matéria de resposta a incidentes.

Neste sentido é igualmente apresentado um plano, composto por cinco fases, para o desenvolvimento das várias capacidades. A primeira fase é preparatória e o seu objetivo é estabelecer os alicerces para a cooperação entre a entidade e o CNCS. Na fase seguinte irão ser desenvolvidos os meios técnicos de deteção e análise de incidentes. Posteriormente, numa terceira fase, serão formados os recursos humanos da entidade para que tirem partido desses mesmos meios. A penúltima fase consiste em criar procedimentos e políticas que definam e otimizem as capacidades da equipa que estará encarregue da resposta a incidentes. Finalmente, a última fase é opcional e consiste em criar uma equipa dedicada à reação a incidentes que participe em exercícios que ponham à prova os seus procedimentos e capacidades e contribua para a comunidade nacional de cibersegurança. O processo de desenvolvimento de capacidades mínimas para a reação a incidentes de cibersegurança permite uma avaliação contínua de cada uma das entidades relativamente ao seu grau de maturidade numa escala de 1 (um) a 5 (cinco).

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Capacidades mínimas para reação a incidentes de cibersegurança

O CNCS tem como objetivo estratégico assegurar a existência de capacidades técnicas e humanas, bem como os processos necessários para uma eficaz deteção, bloqueio e resposta a incidentes de cibersegurança, nas entidades do Estado e operadores de infraestruturas críticas. Este documento centra-se nas capacidades de resposta a incidentes de cibersegurança.

Para concretizar este objetivo foi estabelecido um plano para o desenvolvimento faseado de um conjunto de capacidades mínimas em todas as entidades do estado e, com isto, melhorar a sua capacidade de deteção e resposta a incidentes. O plano descrito no presente documento visa igualmente integrar as entidades no ecossistema nacional de cibersegurança e criar condições para uma melhoria sustentada das mesmas.

Finda a execução deste plano é esperado que cada uma das entidades possua as seguintes capacidades/funcionalidades desenvolvidas:

- Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança;
- Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança;
- Tenha identificadas as áreas de atividade e serviços considerados críticos e realize gestão de ativos para as mesmas;
- Colete e armazene metadados de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes;
- Possua um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos ciberataques mais comuns;
- Possua os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses necessárias e articule com eficácia com o CNCS;
- Tenha aprovados e implementados procedimentos internos de resposta a incidentes de cibersegurança;

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

- Tenha definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de cibersegurança.

As entidades de maior dimensão ou que executam funções críticas deverão ter a sua função de resposta a incidentes assegurada por uma equipa dedicada, vulgarmente designada de CSIRT. Estas entidades deverão possuir ainda as seguintes capacidades:

- Uma equipa dedicada à reação a incidentes de cibersegurança – CSIRT;
- Colaboração em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT;
- Participação em exercícios nacionais e internacionais de cibersegurança.

O desenvolvimento de todas estas capacidades deverá ser feito de uma forma faseada, correspondendo cada uma das fases a um grau de maturidade da entidade:

FASE	CAPACIDADES
Preparação (Maturidade 1)	Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança. Tenha identificadas as áreas de atividade e serviços considerados críticos e realize gestão de ativos para as mesmas.
Técnica (Maturidade 2)	Colete e armazene metadados de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes. Possua um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos tipos de ciberataques mais comuns.
Humana (Maturidade 3)	Possua os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses necessárias e articule com eficácia com o CNCS.
Processual (Maturidade 4)	Tenha aprovados e implementados procedimentos internos de resposta a incidentes de cibersegurança.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

	Tenha definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de cibersegurança.
Organizacional (Maturidade 5)	Possua uma equipa dedicada à reação a incidentes de cibersegurança – CSIRT. Colabore em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT. Participe em exercícios nacionais e internacionais de cibersegurança.

Para cada uma das fases, o CNCS disponibiliza um conjunto de instrumentos para ajudar a entidade a desenvolver cada uma destas capacidades, nomeadamente serviços de consultoria e aconselhamento, ações de formação técnica e a organização de workshops temáticos.

Os custos envolvidos na execução deste plano são da responsabilidade da entidade. O plano detalhado apresenta uma estimativa dos custos envolvidos, bem como uma previsão dos recursos humanos necessários para a sua execução. O CNCS poderá facilitar a agregação das necessidades das várias entidades para atingir os objetivos propostos.

Plano de desenvolvimento das capacidades mínimas

O *roadmap* aqui apresentado tem por base quatro fases distintas (com uma quinta fase opcional) para a capacitação de uma entidade.

Uma primeira fase preparatória visa criar as condições base para a cooperação entre a entidade e o CNCS. A segunda fase é dedicada aos aspetos técnicos a desenvolver em cada uma das entidades. A terceira fase visa dotar os recursos humanos para a realização das ações de análise forense mais comuns. A quarta fase é dedicada à criação dos processos e procedimentos internos de reação a incidentes. A quinta e última fase, opcional, visa criar uma equipa dedicada à reação a incidentes.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Fase 1 – Preparação

A fase preparatória consiste no conjunto de ações que são a pedra basilar da cooperação entre o CNCS e a entidade.

Objetivos

Os objetivos desta fase inicial de preparação são a definição dos canais de comunicação entre a entidade e o CNCS, a identificação do âmbito material de colaboração e articulação e o arranque dessa mesma colaboração.

No final desta primeira fase é suposto que a entidade passe a reportar sistematicamente, através de canais específicos, incidentes de cibersegurança ao CNCS. Por outro lado, é suposto que o CNCS, no quadro da sua atividade de coleção de eventos de cibersegurança, consiga relacionar um determinado evento à entidade, conheça os principais sistemas informáticos da entidade e as suas dependências funcionais, e possua um Elemento de Coordenação Operacional (ECO), dentro da entidade, para contactar em caso de necessidade.

Ações

As ações previstas para atingir os objetivos propostos para esta fase são:

Ação
A 1.1 – Formalização de Protocolo de Colaboração
A 1.2 – Identificação de ECO e levantamento de serviços críticos
A 1.3 – Estabelecimento de canais de comunicação
A 1.4 – Procedimento de notificação de incidentes
A 1.5 – Registo de endereços IP no Local Internet Registry (LIR)

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

A 1.1 – Formalização de Protocolo de Colaboração

O sucesso do processo que é aqui proposto, envolvendo investimentos e disponibilidade de recursos humanos das várias áreas de atividade dentro da entidade, depende, em grande medida, do compromisso e do suporte da respetiva administração ou direção.

A evidência desse compromisso é feita mediante a formalização de um Protocolo de Colaboração entre a entidade e o CNCS. Esta formalização marca o início do processo de desenvolvimento das capacidades mínimas aqui proposto.

A 1.2 – Identificação de ECO e levantamento de serviços críticos

O ECO é o ponto de contato da entidade para qualquer assunto junto do CNCS. Este deverá conhecer bem a entidade quer do ponto de vista técnico, quer de "negócio". Deverá ser capaz de reencaminhar internamente as solicitações para responder ao CNCS. Por outro lado, é esperada disponibilidade para contatos de emergência fora do horário de expediente. Adicionalmente a entidade poderá indicar um conjunto de técnicos que asseguram ou poderão vir a assegurar a função de analistas de cibersegurança. A designação do ECO é feita com o preenchimento do Formulário de Identificação de Entidade.

Por outro lado, é importante, para a atividade do CNCS, uma descrição dos serviços críticos prestados pela entidade, bem como os endereços IP públicos associados a cada um deles. Esta informação permite ao CNCS conseguir, a partir de eventos de cibersegurança recolhidos de outras fontes, identificar quer a entidade envolvida, quer o serviço vital associado.

A 1.3 – Estabelecimento de canais de comunicação

O ECO e o conjunto de técnicos que vão trabalhar na execução deste plano ou que poderão vir a assegurar a função de analistas de cibersegurança deverão fazer parte de uma lista de distribuição de correio eletrónico interna da entidade. Este será o canal de comunicação privilegiado usado pelo CNCS para comunicar informação de cibersegurança relevante para a entidade.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Por outro lado, alguma da informação trocada por correio eletrónico é sensível, nomeadamente detalhes sobre ameaças, incidentes ou vulnerabilidades que dizem respeito exclusivamente à entidade. Para esse efeito, é necessário usar algum tipo de encriptação. Na comunidade de cibersegurança o padrão utilizado é o PGP, donde deverá ser criada uma chave PGP associada ao endereço de correio eletrónico da lista de distribuição atrás referida. Opcionalmente, o ECO e cada um dos técnicos poderão possuir chaves de PGP próprias.

A 1.4 – Procedimento de notificação de incidentes

Criar e fazer aprovar pela direção da entidade, um procedimento de notificação obrigatória de incidente de cibersegurança que não seja estritamente interno. Por estritamente interno consideram-se os incidentes que envolveram, apenas, sistemas da própria entidade. A não ser que o ECO entenda como relevante, excluem-se incidentes relacionados com violação de direitos de autor, SPAM ou tentativas de intrusão. O CNCS presta o apoio necessário na definição e operacionalização deste procedimento de notificação de incidentes de cibersegurança.

A 1.5 – Registo de endereços IP no Local Internet Registry (LIR)

A base de dados do RIPE é a principal fonte de informação de contato para a comunidade internacional de resposta a incidentes e para o CNCS em particular. Por este motivo é extremamente importante que a entidade tenha esta informação atualizada junto do LIR de forma a poder receber notificações e outra informação de cibersegurança relevante para as redes e sistemas sob sua administração. Caso não seja possível este registo na base de dados do RIPE, o CNCS opera uma base de dados privativa que poderá ser utilizada pelas entidades para este registo.

Assim sendo, a entidade deverá atualizar a informação de contato junto de uma destas duas bases de dados ou pedir ao respetivo fornecedor de Internet para o fazer. O CNCS pode constar como contato para resposta a incidentes (IRT) das redes da instituição até que esta possua a capacidade de criar um CSIRT próprio.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Recursos necessários da parte da entidade

Tempo de recursos humanos previsto:

- Equivalente a 1HM (Homem/mês).

Recursos materiais necessários:

- Não aplicável.

Instrumentos e apoio do CNCS

O CNCS apoiará a entidade com os seguintes instrumentos:

a) Minuta de PROTOCOLO DE COLABORAÇÃO;
b) FORMULÁRIO DE IDENTIFICAÇÃO DE ENTIDADE;
c) Lista de distribuição para disseminação de alertas e de outra informação de cibersegurança relevante;
d) Base de dados de contatos de segurança para as entidades do Estado e operadores de infraestruturas críticas;
e) Workshop DEFINIÇÃO DE FUNÇÕES CRÍTICAS;
f) Instruções para pedido de registo no LIR;
g) Ação de formação CAPACIDADES MÍNIMAS PARA RESPOSTA A INCIDENTES;
h) Procedimento e FORMULÁRIO PARA NOTIFICAÇÃO DE INCIDENTES;
i) Documento TAXONOMIA COMUM PARA CLASSIFICAÇÃO DE INCIDENTES.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Fase 2 – Técnica

Nesta fase são reunidas as ações que dotam a entidade dos meios técnicos necessários para a análise e a resposta aos incidentes de cibersegurança mais comuns.

Objetivos

O objetivo desta fase é a criação de instrumentos, sistemas e documentação que permita o conhecimento dos recursos críticos da entidade e suas dependências, a salvaguarda de registos de forma centralizada e visibilidade dos padrões de comunicação dos sistemas da entidade.

No final desta fase a entidade deverá possuir as capacidades tecnológicas mínimas para assistir com eficácia a reação a ciberincidentes.

Ações

As ações previstas para atingir os objetivos propostos para esta fase são:

Ação
A 2.1 – Inventariação de ativos
A 2.2 – Produção de um diagrama de rede
A 2.3 – Implementação de sistema de recolha e armazenamento de flows
A 2.4 – Recolha e armazenamento centralizado de registos (logs)
A 2.5 – Criação de instrumentos de correcção e mitigação de incidentes

A 2.1 – Inventariação de ativos

A grande parte das entidades já executa a função de inventariação de ativos e possui uma *Configuration Management Database* (CMDB) com os mesmos. Muitas outras possuem um catálogo de serviços informáticos aprovados. Esta base de dados fornece toda a informação necessária para o analista de cibersegurança – a pessoa responsável por reagir a um incidente – perceber o impacto, direto ou indireto, deste na atividade da entidade.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

No contexto da reação a ciberincidentes, interessa particularmente registar na CMDB, ou em qualquer outro suporte, a lista dos principais ativos informáticos de suporte às funções críticas identificadas na ação A 1.2. Para cada um destes ativos deve ser armazenado informação de endereçamento IP, versões de sistema operativo, versões de aplicações que comunicam com o exterior e dependências funcionais com outros serviços críticos. Deve ainda ser feita uma avaliação da criticidade de cada um dos ativos baseada no impacto decorrente de uma eventual falha de segurança.

Adicionalmente, a entidade deverá ter procedimentos instalados e verificados para atualização regular desta informação e para introdução de novos ativos, com uma periodicidade mínima de 6 meses, ou sempre que seja relevante.

A 2.2 – Produção de um diagrama de rede

Da mesma forma que é necessária uma inventariação de ativos, também é importante manter atualizado um diagrama com as principais infraestruturas de comunicações de dados e os sistemas de suporte aos serviços críticos da entidade. Num cenário de reação a um ciberincidente, possuir um diagrama de rede é essencial, quer para perceber como se desenvolveram os diversos momentos do ataque, quer para desenhar as soluções de mitigação e identificar o melhor local para a sua aplicação.

Do diagrama de rede deverão constar, no mínimo, todos os segmentos de rede da entidade, endereçamento IP usado em cada um deles, endereços IP de interligação, equipamento de interligação entre os vários segmentos e políticas de acesso entres estes.

Adicionalmente, a entidade deverá colocar em prática procedimentos com vista à atualização regular desta informação, com uma periodicidade mínima de seis meses, ou sempre que for relevante.

A 2.3 – Implementação de sistema de recolha e armazenamento de flows

A tecnologia de exportação e armazenamento de flows permite recolher, através de amostragem, metadados das comunicações que atravessam um equipamento de comunicações eletrónicas. É um instrumento essencial para identificar padrões de

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

comunicação com sistemas potencialmente comprometidos e realizar análise de tráfego considerado malicioso, no contexto da reação a incidentes de cibersegurança.

O CNCS sugere o armazenamento, com uma amostragem de 1:10, dos metadados de comunicações durante um período mínimo de um ano. A recolha dos metadados deve ser feita no router/switch ou outro equipamento de acesso à internet. No entanto, se a entidade pretender uma maior visibilidade das suas comunicações internas, poderá recolher metadados de outros equipamentos.

A implementação de recolha de flows requer um servidor dedicado, cujas características dependem da velocidade de acesso à internet. Como referência, para uma ligação de 100Mbps serão necessários 6TB de armazenamento. Os requisitos para dimensionamento deste servidor são apresentados no anexo II a este documento.

Existem soluções em regime de software aberto para o tratamento e análise dos metadados recolhidos.

A 2.4 – Recolha centralizada de registos (logs)

Os logs produzidos pelo sistema operativo e pelas aplicações de suporte à atividade são o principal instrumento de análise e investigação de um incidente de cibersegurança. Neste contexto é essencial que a entidade possua um repositório central para estes logs com um período mínimo de armazenamento de um ano. Em complemento, é importante que cada servidor tenha a capacidade de armazenar os seus próprios logs por um período de um mês.

A recolha centralizada de logs pressupõe a identificação dos principais sistemas informáticos de suporte aos serviços críticos da entidade, a configuração destes sistemas para exportar os registos e a instalação de um servidor dedicado para o seu armazenamento. O anexo IV descreve as principais características deste servidor, bem como o conjunto mínimo de logs a armazenar.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

A 2.5 – Criação de instrumentos de correção e mitigação de incidentes

Uma vez identificada a origem de um incidente é necessária a aplicação de medidas corretivas ou de mitigação do mesmo. Para o tipo de situações mais comum pode ser necessário aplicar um remendo para colmatar uma falha de segurança num sistema operativo ou aplicação; pode ser necessário bloquear determinado tráfego de entrada ou de saída da entidade; pode ser necessário corrigir uma vulnerabilidade no sítio web da organização; ou ainda assegurar que outros sistemas ou dispositivos não foram afetados pela mesma situação ou falha.

Neste contexto, a fase técnica deste plano de desenvolvimento de capacidades de reação a ciberincidentes termina quando a entidade possui, de forma autónoma ou mediante contratação de serviços os seguintes instrumentos:

a) Serviços de anti-DDoS contratados ao operador de comunicações eletrónicas;
b) Mecanismos de bloqueio de tráfego para IPs e portas específicas (por exemplo, mediante configuração de firewall);
c) Mecanismos para identificação de IOC no parque de dispositivos da entidade (por exemplo através de sistema de instalação e execução remota de aplicações);
d) Quando aplicável, contratos de manutenção corretiva para todos os componentes de software presentes na CMDB;
e) Quando aplicável, contratos de manutenção corretiva para as aplicações chave na mão de suporte aos serviços críticos.

Recursos necessários da parte da entidade

Tempo de recursos humanos previsto:

- Equivalente a 3HM;

Recursos materiais necessários:

- Servidor para armazenamento de flows;
- Servidor para armazenamento de logs.

Instrumentos e apoio do CNCS

O CNCS apoiará a entidade com os seguintes instrumentos:

f) INSTRUÇÕES DE INSTALAÇÃO E CONFIGURAÇÃO DO NFSEN

g) INSTRUÇÕES DE CONFIGURAÇÃO DE EXPORTAÇÃO DE FLOWS NOS ROUTERS/SWITCHES

h) INSTRUÇÕES DE INSTALAÇÃO E CONFIGURAÇÃO DO SPLUNK

i) INSTRUÇÕES DE INSTALAÇÃO E CONFIGURAÇÃO DE SPLUNK FORWARDERS

j) Workshop INSTALAÇÃO DE NFSEN;

k) Workshop INSTALAÇÃO DE SPLUNK;

l) Template PROCEDIMENTO DE INVENTARIAÇÃO DE ATIVOS E MAPEAMENTO DE REDE

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Fase 3 – Humana

A terceira fase incide, essencialmente, na vertente humana, na sua formação e na sua especialização para operação dos instrumentos técnicos criados na fase anterior e a sua utilização no contexto da reação a incidentes. Para esse efeito, o CNCS promoverá um conjunto de ações de formação especializadas.

Objetivos

Esta fase tem como objetivos formar as pessoas afetas à resposta a ciberincidentes e treiná-las para essa mesma função. No final desta fase é esperado que a entidade seja autónoma na análise e resposta aos tipos de incidente mais comuns. Esta capacidade permitirá à entidade partilhar informação de cibersegurança dentro da comunidade nacional e com o CNCS com eficácia.

Ações

As ações previstas para atingir os objetivos propostos para esta fase são:

Ação
A 3.1 – Formação em análise de artefactos
A 3.2 – Formação em análise de tráfego
A 3.3 – Formação em resposta a incidentes
A 3.4 – Formação em bases legais para reação a ciberincidentes

A 3.1 – Formação em análise de artefactos

A análise de artefactos informáticos é uma das principais tarefas de um analista de cibersegurança no contexto da resposta a incidentes. Assim sendo, é essencial que as pessoas indicadas pela entidade para realizarem esta função recebam periodicamente formação específica nesta matéria, de forma a desenvolverem, com autonomia, investigações forenses em sistemas operativos Windows e Linux.

Esta ação de formação termina com um conjunto de exercícios práticos para avaliação das capacidades adquiridas.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

A 3.2 – Formação em análise de tráfego

Do mesmo modo, o analista de cibersegurança pode ter a necessidade de identificar ou confirmar a origem de um ataque, ou, ainda, determinar o momento em que este ocorreu. Para esse efeito poderá ter que recorrer a informação de metadados de comunicações armazenada ou realizar uma captura de tráfego específica. Assim, o analista de cibersegurança deverá receber formação específica na utilização das principais ferramentas de análise de flows, captura de tráfego e análise de tráfego capturado.

Esta ação de formação termina com um conjunto de exercícios práticos para avaliação das capacidades adquiridas.

A 3.3 – Formação em resposta a incidentes

Esta ação de formação tem como objetivo dotar os analistas de cibersegurança indicados pela entidade com as noções básicas em resposta a incidentes, o seu enquadramento nas principais normas internacionais de segurança da informação, as noções básicas de gestão de vulnerabilidades, os meios de comunicação interna e externa dentro das comunidades de cibersegurança e com as ferramentas comumente usadas para a resposta a incidentes.

Como pré-requisito é necessário que o analista de cibersegurança tenha realizado as duas anteriores ações de formação.

Esta ação de formação termina com um conjunto de exercícios práticos para avaliação das capacidades adquiridas.

A 3.4 – Formação em bases legais para reação a ciberincidentes

Finalmente, de forma a realizarem as suas várias funções dentro do quadro jurídico nacional e articularem com eficácia com todas as autoridades nacionais relevantes nesta matéria, os analistas de cibersegurança deverão ter as noções básicas em aspetos jurídicos da cibersegurança.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Entre outros, esta ação de formação incidirá nos aspetos legais relativos à recolha e salvaguarda de prova, comunicação com os órgãos de polícia criminal e partilha de informação de cibersegurança.

Esta ação de formação termina com um conjunto de exercícios práticos para avaliação das capacidades adquiridas.

Recursos necessários da parte da entidade

Tempo de recursos humanos previsto:

- Equivalente a 1HM por técnico indicado pela entidade;

Instrumentos e apoio do CNCS

O CNCS apoiará a entidade com os seguintes instrumentos:

a) Ação de formação em ANÁLISE DE ARTEFACTOS;
b) Ação de formação em ANÁLISE DE TRÁFEGO;
c) Ação de formação em RESPOSTA A INCIDENTES;
d) Ação de formação em ASPECTOS LEGAIS NA REAÇÃO A CIBERINCIDENTES.

Fase 4 – Processual

Nesta fase desenvolvem-se as condições internas para uma eficaz reação a incidentes, nomeadamente através da criação de processos e da divulgação interna de procedimentos.

Objetivos

O objetivo desta fase é dotar a entidade dos processos necessários para a formalização interna de uma função de reação a incidentes de cibersegurança. Esta formalização pressupõe a identificação de um responsável, possibilidade de escalar na hierarquia de responsabilidades, divulgação e treinos internos para a reação a incidentes.

Ações

As ações previstas para atingir os objetivos propostos para esta fase são:

Ação
A 4.1 – Definição de cadeia de responsabilidade
A 4.2 – Definição de procedimentos de reação a incidentes
A 4.3 – Treino e sensibilização internos
A 4.4 – Realização de simulacro de cibersegurança

A 4.1 – Definição de cadeia de responsabilidade

Esta ação pressupõe a nomeação de um responsável pela reação a incidentes de cibersegurança dentro da entidade. Este responsável, que pode ou não ser o ECO (elemento de contato operacional com o CNCS), deve ser conhecido de toda a organização como o ponto de contato para notificação interna de eventos e incidentes de cibersegurança. Preferencialmente, o responsável pela reação a incidentes não deverá pertencer a uma área técnica.

Cabe ao responsável pela reação a incidentes de cibersegurança definir e fazer aprovar os processos de reação a incidentes, bem como, ouvidas as partes interessadas, determinar as medidas de mitigação necessárias para conter ou resolver o incidente.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

A 4.2 – Definição de procedimentos de reação a incidentes

Esta ação pressupõe a identificação dos tipos de ataque mais comuns e a criação de um procedimento para a respetiva mitigação ou resolução. O caderno de procedimentos que resulta desta ação deve ser aprovado pelo departamento jurídico e pela administração da entidade. Também deve ser criado um procedimento interno para notificação de incidentes que indique como deve proceder um colaborador perante um incidente ou um evento suspeito.

A 4.3 – Treino e sensibilização internos

Depois de criados e aprovados os processos e procedimentos, deverão ser realizadas ações internas de sensibilização em matérias de conduta de cibersegurança e dar a conhecer o caderno de procedimentos. É suposto todos os colaboradores receberem formação nesta fase.

A 4.4 – Realização de simulacro de cibersegurança

Por último, de forma autónoma ou com o apoio do CNCS, a entidade deverá realizar simulacros de cibersegurança para avaliação do nível de sensibilização dos seus colaboradores e do grau de preparação dos analistas de cibersegurança para lidar com os tipos de incidente mais comuns. Estes simulacros deverão ocorrer numa base semestral.

Recursos necessários da parte da entidade

Tempo de recursos humanos previsto:

- Equivalente a 2HM;

Instrumentos e apoio do CNCS

a) Consultadoria na definição de processos de reação a incidentes de cibersegurança;
b) Workshop TREINO E SENSIBILIZAÇÃO INTERNOS;
c) Workshop SIMULACROS DE CIBERSEGURANÇA;
d) Template PROCEDIMENTO GENERALIZADO DE RESPOSTA A INCIDENTES
e) Template PROCEDIMENTO PARA RESPOSTA A TIPOS DE INCIDENTE ESPECÍFICO.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Fase 5 – Organizacional (opcional)

A quinta fase compreende as ações necessárias para a operacionalização de um CSIRT na entidade. A decisão de criação de um CSIRT deve ter em conta a dimensão da entidade, a importância estratégica dos seus ativos informacionais, a capacidade financeira e o histórico de incidentes. Por este motivo, a execução desta fase deve ser objeto de avaliação conjunta entre a entidade e o CNCS.

Objetivos

O objetivo desta fase é criar uma estrutura operacional de resposta a incidentes (CSIRT) perfeitamente integrada no organigrama da entidade.

No final desta fase é suposto que a entidade possua um CSIRT operacional vocacionado para a sua comunidade específica e perfeitamente integrado nas comunidades nacional e internacional de CSIRT.

Ações

As ações previstas para atingir os objetivos propostos para esta fase são:

Ação
A 5.1 – Definir missão, comunidade servida e portfólio de serviços
A 5.2 – Elaborar e fazer aprovar o plano e orçamento para o CSIRT
A 5.3 – Montar e anunciar o CSIRT
A.5.4 – Afiliação nas comunidades nacionais de CSIRT
A.5.5 – Participação num exercício nacional de cibersegurança

A 5.1 – Definir missão, comunidade servida e portfólio de serviços

A primeira ação para a constituição de um CSIRT na entidade passa por definir a visão para esse mesmo CSIRT. Isto consiste em definir e validar com as partes interessadas uma definição clara da missão, uma identificação da comunidade servida e o desenho do portfólio de serviços adequado para atingir os objetivos propostos.

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Do portfólio de serviços deverá constar, no mínimo, o tratamento de incidentes de cibersegurança e a gestão de vulnerabilidades.

Para a construção desta visão contribuem muitos dos entregáveis produzidos nas fases anteriores, nomeadamente a gestão de ativos, a definição de uma cadeia de responsabilidade e os processos de mitigação de incidentes.

A 5.2 – Elaborar e fazer aprovar o plano e orçamento para o CSIRT

Um CSIRT deve ter uma estrutura capaz e sustentável. Para esse efeito é necessária a aprovação por parte da direção da entidade de um plano de ação e orçamento para montar e operar o CSIRT.

O sucesso do CSIRT depende da objetividade da sua missão e da adequação dos meios e dos instrumentos para atingir os seus objetivos.

Deste plano deverá constar uma proposta de enquadramento funcional do CSIRT dentro da estrutura orgânica da entidade, a definição atrás referida da missão, comunidade servida e portfólio de serviços; um plano de investimentos para a montagem inicial do CSIRT; um plano de formação e capacitação para os recursos humanos alocados e/ou a contratar; um plano de deslocações de representação e participação nas comunidades de cibersegurança; bem com um calendário para a sua operacionalização.

A 5.3 – Montar e anunciar o CSIRT

Aprovado o plano de ação, dá-se início à operacionalização do CSIRT. Esta ação prevê a aquisição e montagem das infraestruturas técnicas e operacionais, bem como a afetação, requalificação ou contratação dos recursos humanos necessários.

Tipicamente um CSIRT precisa de um sistema de registo de ocorrências e comunicações, de canais de comunicação (telefone e correio eletrónico), de mecanismos de cifra (eg. PGP) e de um conjunto de ferramentas de suporte à análise forense de artefactos. A maior parte destas ferramentas são de acesso livre e gratuito.

De forma a automatizar processos, será necessário integrar o sistema de ocorrências do CSIRT da entidade com os mecanismos de disseminação de eventos e de alertas do CNCS, utilizando uma ontologia e uma taxonomia comuns.

Por outro lado, é necessário formar os recursos humanos afetos ao CSIRT com as competências técnicas necessárias. Dependendo do objeto do CSIRT, as capacidades necessárias são: procedimentos de tratamento de incidentes, análise técnica de tráfego, análise técnica de artefactos e análise técnica de malware.

Por último importa anunciar o CSIRT à comunidade servida. Uma equipa de resposta a incidentes opera sobre as notificações internas e externas que lhe chegam, donde é essencial que o CSIRT se dê a conhecer aos seus utilizadores, bem com às várias comunidades de cibersegurança nacionais e internacionais. Para esse efeito é essencial assegurar presença regular nos principais fora de cibersegurança e participar ativamente nos seus planos de trabalhos.

O CSIRT deve, igualmente, solicitar ao prestador de serviços de comunicações eletrónicas a publicação de um objeto IRT (Incident Response Team) junto do LIR.

A 5.4 – Afiliação nas comunidades nacionais de CSIRT

O sucesso de um CSIRT depende da sua boa integração nas várias comunidades de cibersegurança e das relações de confiança que aí são criadas.

Neste contexto, o CSIRT da entidade deverá afiliar-se e participar ativamente nos programas de trabalhos das comunidades nacionais de CSIRT, tais como a Rede nacional de CSIRT e, se adequado, do Trusted Introducer for CSIRTs in Europe (TF-CSIRT). Adicionalmente, recomenda-se a participação em fora internacionais sectoriais, tais como o FI-ISAC (Financial Services – Information Sharing and Analysis Centre) para o sector bancário.

A 5.5 – Participar num exercício nacional de cibersegurança

Os exercícios de cibersegurança servem dois objetivos importantes: testar as capacidades, mas principalmente os procedimentos para resposta a incidentes, e melhorar a articulação interna e externa com as partes interessadas.

O CSIRT da entidade deve participar num exercício de cibersegurança pelo menos uma vez por ano, seja o mesmo de âmbito nacional ou internacional.

Recursos necessários da parte da entidade

Tempo de recursos humanos previsto:

- Equivalente a 6HM;

Instrumentos e apoio do CNCS

a) Consultoria para a criação de CSIRTs
b) EXERCÍCIO NACIONAL DE CIBERSEGURANÇA;
c) Documento ONTOLOGIA DE EVENTOS DE SEGURANÇA
d) Documento ONTOLOGIA DE ALERTAS DE SEGURANÇA

Anexo I – Sumário de ações por Fase

Ação
A 1.1 – Formalização de Protocolo de Colaboração
A 1.2 – Identificação de ECO e levantamento de serviços críticos
A 1.3 – Estabelecimento de canais de comunicação
A 1.4 – Procedimento de notificação de incidentes
A 1.5 – Registo de endereços IP no LIR
A 2.1 – Inventariação de ativos
A 2.2 – Produção de um diagrama de rede
A 2.3 – Implementação de sistema de recolha e armazenamento de flows
A 2.4 – Recolha e armazenamento centralizado de registos (logs)
A 2.5 – Criação de instrumentos de correção e mitigação de incidentes
A 3.1 – Formação em análise de artefactos
A 3.2 – Formação em análise de tráfego
A 3.3 – Formação em resposta a incidentes
A 3.4 – Formação em bases legais para reação a ciberincidentes
A 4.1 – Definição de cadeia de responsabilidade
A 4.2 – Definição de procedimentos de reação a incidentes
A 4.3 – Treino e sensibilização internos
A 4.4 – Realização de simulacro de cibersegurança
A 5.1 – Definir missão, comunidade servida e portfólio de serviços
A 5.2 – Elaborar e fazer aprovar o plano e orçamento para o CSIRT
A 5.3 – Montar e anunciar o CSIRT
A.5.4 – Afiliação nas comunidades nacionais de CSIRT
A.5.5 – Participação num exercício nacional de cibersegurança

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Anexo II – Lista de entregáveis por Fase

Fase 1 - Preparação
D 1.1 - Manifestação de interesse (partilhado com o CNCS)
D 1.2 - Estrutura de serviços críticos (partilhado com o CNCS)
D 1.3 - Procedimento de notificação de incidentes
Fase 2 - Técnica
D 2.1 - Inventário de ativos
D 2.2 - Mapa de rede (Partilhado com o CNCS)
Fase 4 - Processual
D 4.1 - Caderno de procedimentos para reação a incidentes
Fase 5 - Organizacional
D 5.1 - RFC2350

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Anexo III – Conjunto mínimo de registos a manter

Sistemas operativos

Microsoft Windows

Todos os Event Logs da máquina

Linux

syslog, messages ou equivalente

auth, secure ou equivalente

cron

yum.log ou equivalente

audit log

Serviços

Servidores web (IIS, Apache ou equivalente)

access log

error log

Servidores de bases de dados (Microsoft SQL Server, MySQL ou equivalente)

error log

Servidores de email (Exchange, Postfix ou equivalente)

Registos de SMTP (maillog ou equivalente)

Servidores de FTP (IIS, vsftpd ou equivalente)

Registos do serviço FTP

Servidores de SSH (OpenSSH ou equivalente)

sshd.log ou equivalente

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Anexo IV – Requisitos mínimos para os servidores

Serviço Associado	Característica	Mínimo recomendado
Recolha centralizada de registos	**Processador**	8 núcleos a 2.5Ghz
	Memória	128GB
	Armazenamento	16TB composto por discos de 10000RPM
Recolha de flows	**Processador**	4 núcleos a 2.5Ghz
	Memória	64GB
	Armazenamento	Discos de 10000RPM (6TB para link de 100Mbps)

Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt