Medidas de Controlo de Incidentes de Segurança Informática

Política de atuação do RCTS CERT para mitigação de impacto de incidentes de segurança informática

Serviço RCTS CERT

INT/Abr-2016/RCTS CERT/v5.1

ÍNDICE

LISTA DE TABELAS

1 INTRODUÇÃO

A principal atividade do RCTS CERT é o tratamento de incidentes de segurança informática. As medidas de controlo dos incidentes na RCTS constituem um instrumento essencial para mitigar os efeitos de incidentes de segurança e também para aumentar a probabilidade de resolução atempada dos mesmos.

Neste sentido, passamos a definir o âmbito de aplicação deste serviço, assim como a identificar a tipologia de incidentes mais relevantes e os critérios e medidas a aplicar tendo em vista a sua resolução e/ou a minimização de impacto para os eventuais alvos.

Entende-se por fim que os incidentes de segurança na rede RCTS consubstanciados, designadamente, no uso indevido da mesma, configuram também uma violação aos termos da Carta do Utilizador da RCTS (AUP), pelo que serão tratados nos termos do previsto neste documento e na referida AUP.

2 ÂMBITO

O âmbito de aplicação do presente documento restringe-se à comunidade servida pela RCTS - Rede Ciência, Tecnologia e Sociedade, tal como definida tecnicamente no documento disponível no endereço Internet https://www.trusted-introducer.org/directory/teams/rcts-cert.html, na secção "Constituency", sempre que esteja em causa a aplicação de medidas de controlo de incidentes.

O RCTS CERT é um serviço integrante da RCTS - Rede Ciência, Tecnologia e Sociedade, enquanto rede de investigação e ensino nacional cujo planeamento, gestão e operação é da responsabilidade da FCT|FCCN.

3 CRITÉRIOS

O critério de decisão quanto à medida de controlo a aplicar numa dada situação será ditada pelos seguintes fatores: (a) tipo de incidente e criticidade associada (ver capítulos 4 e 6); e (b) contexto do incidente (ver capítulo 8).

A prioritização nos meios de comunicação utilizados dependerá da resposta por parte da(s) entidade(s) envolvidas (ver capítulos 5 e 7).

4 TIPOS DE INCIDENTE DE SEGURANÇA

O RCTS CERT adota, para efeitos de classificação de criticidade de incidentes de segurança, a seguinte tabela em que se faz corresponder a cada tipologia um grau de criticidade, recorrendo a uma escala de 1 a 4, em que 4 é o grau mais elevado, e 1 é o grau de menor criticidade.

Classe do Incidente	Tipo de Incidente	Criticidade
Malware	Distribuição	2
	C&C	3
Disponibilidade	DoS/DDoS	4
	Sabotagem	3
Recolha de Informação	Scan	1
	Sniffing	2
	Phishing	3
Tentativa de Intrusão	-	2
Intrusão	-	3
Segurança da Informação	-	3
Fraude	-	2
Conteúdo Abusivo	SPAM	1
	Direitos de autor	1
	Pornografia infantil, racismo e apologia da violência	3
Vulnerabilidade	-	3
Outra	-	(*)

Tabela 1 - Criticidade por Tipo de Incidente

(*) Nos casos em que a determinação da criticidade do incidente não seja à partida definida, esta será realizada pelo RCTS CERT em função de fatores como:

- Potencial de risco para a RCTS ou redes externas;
- Potencial de risco para a segurança de pessoas, bens ou organizações;
- Abrangência.

A classificação de criticidade do incidente será dada a conhecer à entidade da RCTS que vier a ser notificada pelo RCTS CERT, bem como as ações que dela se esperam.

O grau de impacto associado a cada incidente pode ser alterado pela FCT|FCCN, em função de outras características do incidente de segurança analisado que se venham a conhecer.

De acordo com a criticidade de cada incidente, estabelecem-se valores de referência que determinarão o tempo de resposta para a primeira interação (ver tabela 2), bem como o tempo de resolução com informações referentes às ações tomadas para a resolução/mitigação do incidente (ver tabela 3). Qualquer dos tempos é entendido como tempo de referência, pelo que pode variar em função de cada situação concreta. A resposta inicial pode passar por diligências como a escalagem do incidente ou simples notificação suplementar. Os tempos apresentados nas tabelas seguintes são aplicáveis quando a entidade da RCTS é a origem do incidente em causa.

Note-se que os tempos definidos nas tabelas 2 e 3 são contados a partir do momento em que a notificação sobre o incidente é emitida pelo RCTS CERT.

Criticidade	Tempo de Resposta para 1ª Interação	Meio de Comunicação
1	3 dias úteis	email
2	2 dias úteis	email
3	1 dia útil	email
4	2h úteis	telefone e email

Tabela 2 - Tempo de Resposta para 1ª Interação

Criticidade	Tempo de Resolução	Meio de Comunicação
1	4 dias úteis	email
2	3 dias úteis	email
3	2 dias úteis	email
4	1 dia útil	telefone e email

Tabela 3 - Tempo de Resolução

5 COMUNICAÇÃO COM ENTIDADES DA RCTS

A comunicação com entidades da RCTS é realizada através dos meios de comunicação referidos nas tabelas 2 e 3 de acordo com a criticidade do incidente. O objetivo da diferenciação dos meios de comunicação é melhorar a eficácia no tratamento de incidentes.

O processo de notificação é o seguinte:

1. O RCTS CERT contacta a entidade participante no incidente solicitando-lhe genericamente o seguinte:
    a. Tomada de medidas com vista à resolução do incidente;
    b. Elementos adicionais necessários à gestão do incidente;
    c. Resposta com a indicação das medidas tomadas e elementos solicitados.
2. Caso não se obtenha resposta dentro do período previsto para a 1ª interação (ver tabela "Tempo de Resposta para 1ª Interação"), o RCTS CERT estabelecerá um contacto telefónico com a entidade participante no incidente.
3. A entidade participante no incidente deverá executar as medidas por si entendidas como necessárias para a resolução do incidente, bem como aquelas indicadas pelo RCTS CERT para o mesmo efeito, dentro do prazo estabelecido para a resolução do incidente (ver tabela "Tempo de Resolução").

O não cumprimento do prazo referido no ponto anterior levará o RCTS CERT a notificar a entidade participante no incidente das medidas de controlo de tráfego a aplicar na RCTS, com o pré-aviso de 60 minutos. A notificação será enviada via e-mail, e será realizada uma tentativa de contacto telefónico, tendo como destinatários os contactos apropriados (ver capítulo 10 - "Contactos registados da Entidade"), consistindo num relatório técnico explicativo devidamente fundamentado.

6 MEDIDAS DE CONTROLO DE TRÁFEGO

As medidas de controlo de tráfego são de caracter técnico e variam conforme os casos em análise. As medidas a aplicar neste âmbito implicam a realização de configurações técnicas, as quais deverão causar o menor impacto negativo possível para a entidade, e têm como objetivo a limitação de prejuízos e/ou danos causados pelo incidente. Dependendo do tipo de incidente as medidas possíveis a aplicar são:

- Corte de conectividade a um ou vários endereços IP;
- Corte de conectividade IP/Porta (um ou vários pares);
- Corte total de acesso à RCTS (e Internet).

Na tabela seguinte estão apresentados os órgãos responsáveis pela determinação definitiva da medida a aplicar:

Medida	Órgão competente
Corte a conectividade IP/Porta (um ou vários pares)	Membro do serviço RCTS CERT
Corte a conectividade de um ou vários endereços IPs	Gestor do serviço RCTS CERT
Corte total de acesso	Diretor da Unidade orgânica da Computação Científica Nacionaal (FCCN) da FCT,I.P.

Tabela 4 - Entidade Competente para Determinação de Medida de Controlo

7 REINCIDÊNCIA

Nos casos em que se venham a detetar várias ocorrências de um mesmo tipo de incidente para a mesma entidade (ou bloco de endereços), o processo de recurso a níveis superiores da situação refletir-se-à nos meios de comunicação utilizados pelo RCTS CERT para notificar a entidade que alegadamente está a originar os problemas. O recurso a níveis superiores traduz-se pela notificação aos contactos administrativos das entidades, associadas ao seu acesso à RCTS. A medida de controlo só será agravada caso se verifique tal ser estritamente necessário para conter os efeitos do incidente em apreço.

Assim sendo, o incremento de relevância terá como efeito no estabelecimento de comunicação:

1. Nos casos em que se enviaria inicialmente notificação por email, tentar-se-à de imediato o contacto telefónico;
2. Nos casos em que a notificação inicial regular já seria via contacto telefónico, o RCTS CERT continuará a tentar estabelecer a 1ª comunicação através desta via, sendo que será também enviada notificação por e-mail.

Este processo tem por objetivo reduzir, quer o número de iterações, quer o tempo de resposta das entidades. Note-se que o tempo máximo de resposta esperado continua a ser aquele definido na tabela 3 no capítulo 4.

8 MÚLTIPLOS INCIDENTES

Nos casos em que se venha a detetar mais que um tipo de incidente para a mesma entidade (ou bloco de endereços), o processo de recurso a níveis superiores da situação refletir-se-à na medida de controlo a aplicar, uma vez que a diversificação de atividade maliciosa aponta, usualmente, para uma situação de compromisso de segurança mais grave que o caso isolado, justificando medidas de controlo de maior abrangência.

A ativação do processo terá como efeito:

- Nos casos em que se adotaria corte de conetividade IP/Porto (um ou vários pares) para incidentes isolados, adotar-se-à um corte de conetividade de um ou vários endereços IP;
- Nos casos em que se adotaria corte de conetividade de um ou vários IPs (no mínimo 10) para incidentes isolados, adotar-se-à o corte total de acesso, na sequência de análise que leve a concluir que a situação em causa é de extrema criticidade, e uma vez obtida aprovação superior (ver tabela 4 "Entidade Competente para Determinação de Medida de Controlo ").

9 SUSPENSÃO E/OU LEVANTAMENTO DE MEDIDAS

As medidas de controlo de tráfego serão suspensas e/ou levantadas logo que se verifique que o incidente foi tratado de forma adequada, tendo daí resultado a cessação da atividade maliciosa em curso, e após pedido do contacto da entidade credenciado para o efeito.

O RCTS CERT manterá um registo atualizado do estado das medidas de controlo de incidentes aplicadas, podendo fornecer essa informação aos contactos credenciados para o efeito, pertencentes às respetivas entidades.

10 CONTACTOS REGISTADOS DA ENTIDADE

Para efeitos de aplicação dos termos do presente documento, designadamente para efeitos de notificação sobre uma situação que possa vir a justificar a imposição de uma medida de controlo de tráfego, entende-se por "contactos registados da entidade":

- Os contactos indicados pela entidade na descrição tipo "RFC2350", dos seus serviços de segurança informática, presentes no diretório de contactos do RCTS CERT;
- Os contactos técnicos associados ao acesso RCTS (Serviço IP) da sua entidade.

Para efeitos de corte total de acesso, e só nestes casos, notificar-se-á para além dos "contactos registados da entidade" o responsável hierárquico superior (contacto administrativo afecto ao Serviço IP) da entidade face ao acesso RCTS.

11 CONTACTOS DO RCTS CERT

Os contactos do RCTS CERT encontram-se publicados em http://www.cert.rcts.pt/index.php/institucional/contactos