CSIRT

IP Telecom

RFC2350

CONTEÚDO[1]

[1] Tabela de conteúdos estabelecida de acordo com a RFC-2350

1. Informação do Documento

Este documento descreve o CSIRT da IP Telecom de acordo com a RFC 2350[2]. A informação essencial que é disponibilizada sobre o CSIRT da IP Telecom, onde são descritos os canais de comunicação, os cargos e as respetivas responsabilidades.

Data da Última Atualização

A primeira versão do documento foi disponibilizada a 24 de março de 2010.

A segunda versão foi disponibilizada a 30 de abril de 2021.

A terceira versão foi disponibilizada no dia 12 de julho 2021.

A quarta versão foi disponibiliza no dia 29 de novembro de 2021.

Lista de Notificações

Não existem notificações assinalar.

Localização do Documento

Este documento pode ser encontrado na sua última versão no website da IP Telecom. O endereço para acesso:

https://www.iptelecom.pt/csirt/

Autenticação deste documento

O documento é assinado pela chave PGP do CSIRT da IP Telecom. A Assinatura pode ser visualizada no endereço https://www.iptelecom.pt/csirt/.

Identificação do Documento

Título do documento: "IPT-CSIRT-RFC2350-PT_v1.3"

Versão: 1.3

Data do Documento: 29-11-2021

2. Informação de Contacto

Informação do Documento

Nome Completo: IP Telecom CSIRT

Nome Curto: CSIRT-IPT

Endereço

CSIRT IP Telecom

[2] http://www.ietf.org/rfc/rfc2350.txt

Rua Passeio do Báltico nº4 , 1990-036 Lisboa – Portugal

Fuso Horário

Portugal (Continente) está no fuso horário da Europa Ocidental. *Western European Standard Time (WET) is Greenwich Mean Time (GMT) .* O horário de verão é observado em Portugal, com um avanço de 1 hora, 1 hora antes do horário de Greenwich (GMT + 1), iniciando no último domingo de Março e finalizando no último domingo de Outubro. Após esse período, o tempo é atrasado 1 hora para o horário da Europa Ocidental (WET) ou (GMT) novamente.

Número de Telefone

+351 211 024 016

16122 (24 horas por dia, 365 dias por ano)

Número de Fax

Não disponível.

Outro contacto de telecomunicações

Não disponível.

Endereço de Email

Qualquer informação relevante sobre incidentes de cibersegurança ou ameaças de cibersegurança que envolvam a IP Telecom, é importante notificar através do endereço de mail csirt@iptelecom.pt.

Para informações referentes a atividades e serviços relacionados com a área de cibersegurança, contacte-nos através do mesmo endereço de email.

Chaves Públicas e Informação de Encriptação

O Identificador da chave é C2E17B6D6175F315 e deve ser utilizado quando a informação a enviar necessitar de ser transmitida de forma segura e encriptada para o CSIRT da IP Telecom.

PGP Fingerprint: BD5A ADF2 41F1 A85E 88D1 44FA C2E1 7B6D 6175 F315

Esta chave está disponível no endereço https://www.iptelecom.pt/csirt/.

Membros da Equipa

A equipa do CSIRT da IP Telecom é composta por analistas de cibersegurança e de inteligência de ameaças cibernéticas. O líder da equipa é Ricardo Conceição M. Ferreira. O responsável de segurança da informação é José Carlos da Silva Gonçalves.

Outras Informações

Informações gerais relacionadas com o CSIRT da IP Telecom podem ser pesquisadas através do seguinte endereço:

https://www.iptelecom.pt/csirt/

PONTO DE CONTACTO PARA CLIENTES

O método mais indicado para reportar incidentes é através do seguinte endereço de email:

csirt@iptelecom.pt

Os membros da equipa do CSIRT da IP Telecom estão disponíveis para responder e ajudar durante o horário estabelecido pelo NSOC. O horário de disponibilidade é 24 horas por dia, 365 dias por ano. Em caso de urgência utilizar o termo [Urgência] no assunto da mensagem.

3. CARTA

DESCRIÇÃO DA MISSÃO

A equipa do CSIRT-IPT é a equipa de resposta a incidentes de cibersegurança da organização IP Telecom. Esta unidade tem na sua responsabilidade toda a área de Análise Forense e Resposta a Incidentes (DFIR).

A missão do CSIRT-IPT é suportar e proteger, nos seus negócios, interesses e reputação contra qualquer tipo de ataque malicioso que possa prejudicar o seu pleno funcionamento.

As principais atividades desenvolvidas pelo CSIRT-IPT são:

- Reduzir o risco geral da organização, através de medidas proativas, preventivas e de forma antecipada, suportando a continuidade de negócio;
- Resposta e recuperação eficiente para incidentes de segurança cibernética, por via de abordagens técnicas de alta qualidade, permitindo uma mitigação de problemas rápida e eficiente;
- A promoção de um contexto segurança corporativo holístico e integrado, de acordo com os mais altos padrões de ética, integridade e honestidade;
- Criação, manutenção e desenvolvimento de informações e partilha de conhecimento para as comunidades em geral e as suas plataformas, bem como a promoção da cooperação entre a IP Telecom, o Grupo Infraestruturas de Portugal (Grupo IP) e restantes associados;
- Fornece uma pesquisa de alta qualidade, serviços de análise a potenciais ameaças relacionadas com a cibersegurança;
- Persegue o objetivo de ser reconhecida como um centro de excelência de segurança da informação para organizações nacionais e internacionais.

CONSTITUIÇÃO

A constituição do CSIRT-IPT é composta por todos os elementos da IP Telecom, na área de sistemas de informação e gestão de negócio: utilizadores, sistemas, aplicações e redes.

O CSIRT-IPT, não obstante os serviços cooperativos acima, também podem ser fornecidos acordos de cooperação específicos com entidades regulamentares na área da segurança informática.

AFILIAÇÃO

CSIRT-IPT está afiliado à IP Telecom e ao Grupo IP, mantém afiliações com vários CSIRTs e CERTs em Portugal, na Europa de acordo com as necessidades, a troca de informações e os princípios de cooperação em conjunto com as suas missões e valores.

AUTORIDADE

O CSIRT-IPT opera sobre a gestão do Diretor Geral da IP Telecom.

4. POLÍTICAS

TIPOS DE INCIDENTES E NÍVEL DE SUPORTE

O CSIRT-IPT tem a autoridade de coordenar, gerir e responder a todos os tipos de ameaças cibernéticas, ciberataques e incidentes de segurança da informação, que ocorrem ou ameaçam ocorrer e que possam ser prejudiciais para os negócios, interesses e reputação da IP Telecom.

COOPERAÇÃO, INTERAÇÃO E DIVULGAÇÃO DE INFORMAÇÕES

O CSIRT-IPT considera importante a coordenação operacional e as informações partilhadas entre CERTs, CSIRTs, SOCs e entidades semelhantes, bem como outras organizações, que possam contribuir para fornecer os serviços ou que fornecem benefícios para o próprio CSIRT-IPT.

O CSIRT-IPT irá cooperar com outras entidades em todos os assuntos relacionados aos sistemas de informação e á segurança dos mesmos. Essa cooperação inclui a troca de informações vitais sobre ameaças, incidentes de segurança, campanhas de ataque e vulnerabilidades, bem como técnicas de mitigação. No entanto, o CSIRT-IPT promoverá a partilha de informações de forma anónima.

O CSIRT-IPT irá utilizar as informações fornecidas para ajudar a resolver incidentes de segurança, como fazem todos os CERTs. Por princípio comum, as informações que são distribuídas posteriormente às partes apropriadas será feita de acordo com o princípio da necessidade de ter conhecimento e de preferência de forma anónima.

O CSIRT-IPT reconhece, e apoia o uso do protocolo de partilha de informação através do *"Traffic Light Protocol"*[3] , classificando e gerindo as informações de forma adequada em conformidade com o protocolo com as siglas *"WHITE", "GREEN", "AMBER" e "RED".*

COMUNICAÇÃO E AUTENTICAÇÃO

Para uma normal comunicação (que não contenha informação sensível) o CSIRT-IPT irá utilizar métodos convencionais como emails não encriptados. O CSIRT-IPT protege a informação sensível de acordo com as regulamentações e políticas Portuguesas e da União Europeia. Em particular, o CSIRT-IPT respeita as marcações de toda a informação sensível comunicada para o CSIRT-IPT.

As informações confidenciais e a segurança das comunicações (incluindo encriptação e autenticação) é estabelecida através do uso de PGP.

5. SERVIÇOS

ATIVIDADES PROATIVAS E ANÚNCIOS

Através de uma operação de vigilância, o CSIRT-IPT realiza análises preventivas de segurança e controlo para detetar possíveis ataques, violações e ameaças, bem como de ataques á reputação e

[3] https://www.cncs.gov.pt/content/files/cncs-guia_de_uso_e_definicoes_tlp_protocol.pdf

riscos sobre a marca, vulnerabilidades ou configurações incorretas que podem ser aproveitadas nos ataques cibernéticos. Podem ser efetuadas análises de incidentes em progresso em conjunto com outras organizações.

Anúncios sobre vulnerabilidades e respetivas informações (por exemplo inteligência de ameaças) também são fornecidas como parte deste tipo de serviço. O serviço proativo do IPT-CSIRT também inclui observação da tecnologia, avaliação e adoção.

RESPOSTA A INCIDENTES (TRIAGEM, COORDENAÇÃO E RESOLUÇÃO)

O CSIRT-IPT é responsável pela coordenação de eventos/incidentes de segurança envolvendo o GRUPO IP. O CSIRT-IPT, portanto, lida com os aspetos de triagem e coordenação também como resposta a incidentes. O desenvolvimento das técnicas de mitigação são responsabilidade da equipa de cibersegurança da IPT que em conjunto com o CSIRT-IPT agilizam todos os processos quer de resposta a incidentes quer de análise forense aos artefactos suspeitos.

ALERTA

O serviço de alerta do CSIRT-IPT visa divulgar informações sobre os ciberataques, interrupção de serviços, vulnerabilidades, propagação e atividade de malware, intrusão e tentativas de intrusão que aconteceram ou podem acontecer. O serviço de alerta é complementado com recomendações para lidar com as questões de segurança dos seus colaboradores. Este serviço pode ser fornecido a outras partes semelhantes, nomeadamente CSIRTs, CERTs, SOCs e outro tipo de entidades com o mesmo âmbito.

INTRUSÃO E DETEÇÃO DE VULNERABILIDADES

O CSIRT.IPT mantém e desenvolve um conjunto de tecnologias, sistemas e processos com o objetivo de detetar eventos com potencial de intrusão, bem como vulnerabilidades existentes. Os Relatórios do CSIRT-IPT sobre as descobertas de vulnerabilidades oferecem um suporte e aconselhamento de elevada qualidade no tratamento de incidentes. Dentro deste tipo de serviço, o CSIRT-IPT tem capacidade de desenvolver atividades de "*Blue team*" e "*Red Team*" para perseguir o objetivo de um ecossistema global de cibersegurança mais seguro e resiliente quer na própria organização, quer no exterior.

ANÁLISE FORENSE E RESPOSTA A INCIDENTES

O CSIRT-IPT executa todas as atividades de DFIR para a sua organização. O serviço de resposta a incidentes abrange 7 etapas: antecipação, preparação, identificação, contenção, erradicação, recuperação e lições aprendidas. O CSIRT-IPT possuí um laboratório, onde são efetuados vários tipos de análise, tais como análise de *software* malicioso, análise de IPs, análise de domínios, análise de tentativas de *phishing* entre outros. Este serviço é também fornecido a todo o Grupo IP.

DESENVOLVIMENTO DE FERRAMENTAS DE AMEAÇAS CIBERNÉTICAS E SEGURANÇA CIBERNÉTICA

O CSIRT-IPT desenvolve algumas das suas ferramentas de segurança para utilização interna, quando existem necessidades de aumentar as capacidades e funcionalidades da tecnologia existente, no âmbito de alcançar melhorias significativas na capacidade de ciberdefesa.

COOPERAÇÃO E PARTILHA DE CONHECIMENTO

O CSIRT-IPT considera extremamente importante a cooperação e partilha de informação a todos os níveis, entre CERTs, CSIRTs, SOCs e entidades semelhantes, bem como outro tipo de organizações. Este tipo de serviço visa contribuir ainda mais na antecipação e proatividade, resultantes de informações partilhadas sobre inteligência de ameaças a fim de melhorar globalmente a postura de segurança interna e externa. Este serviço visa o desenvolvimento e a promoção da partilha de informações através de plataformas, *frameworks* e bases de dados, criando assim laços de cooperação entre o CSIRT-IPT e outras partes.

6. FORMULÁRIO - RELATÓRIO DE INCIDENTE

Não existe ainda desenvolvido nenhum formulário para alertar sobre incidentes de segurança ao CSIRT-IPT. No caso de uma emergência ou crise, pode comunicar utilizando os contactos previamente definidos, fornecendo, no mínimo a seguinte informação:

- Detalhes do Contacto. Nome da pessoa, organização, endereço;
- Endereço de email e número de telefone fixo e móvel;
- Uma descrição sumária da observação/evento ou incidente;
- Anexos, evidências ou artefactos se existirem;
- Indicadores de Compromisso (IoCS), indicadores de ataque (IoAs), FQDN(s), e outro tipo de informação técnica relevantes para o incidente em causa;
- Se algum email for encaminhado para o CSIRT-IPT, todos os cabeçalhos e email, corpo da mensagem e anexos devem ser incluídos, se possível em conformidade com os regulamentos, políticas e legislação em vigor sob as quais opera a parte relatora.

7. ISENÇÃO DE RESPONSABILIDADE

Embora sejam tomas todas as precauções na preparação de informações, notificações e alertas, o CSIRT-IPT não assume nenhuma responsabilidade por erros, omissões, ou por danos resultantes da utilização das informações fornecidas.