N.º de Páginas:	7
Data:	30.11.2020

DE:	Hardsecure, Segurança em Redes e Sistemas de Informação
PARA:	Rede Nacional CSIRT
ASSUNTO:	Serviço de resposta a incidentes de segurança informática da Hardsecure, de acordo com o RFC2350
CLASSIFICAÇÃO:	PÚBLICA

Índice

1. Informação acerca deste documento

O presente documento descreve o serviço de resposta a incidentes de segurança informática da Hardsecure, de acordo com o RFC2350.

1.1 Data da última atualização

Versão 1.0 publicada em 2020/11/30

1.2 Listas de distribuição para notificações

Não existe um canal de distribuição para notificar alterações a este documento.

1.3 Acesso a este documento

A versão atualizada deste documento está disponível em
https://www.hardsecure.com/pages/49/h-soc

1.4 Autenticidade deste documento

Este documento é assinado com a chave h-CSIRT Hardsecure. A chave PGP utilizada para assinar está disponível no ponto 2.7.

2. Informação de contacto

2.1 Nome da equipa

h-CSIRT Hardsecure – Computer Security Incident Response Team da Hardsecure

2.2 Morada

h-CSIRT Hardsecure
Rua Engenheiro Frederico Ulrich
nº3210, Maia, Portugal

2.3 Zona horária

Portugal/WEST (GMT+0, GMT+1 em horário de verão)

2.4 Telefone

+351 218 278 126 (Horário normal de funcionamento - 09h00 - 18h00).
+351 915 613 526 (Contacto de emergência, fora das horas normais de funcionamento).

2.5 Outras telecomunicações

Não existentes.

2.6 Endereços de correio eletrónico

csirt@hardsecure.com - Correio eletrónico para notificação de incidentes de cibersegurança e outros assuntos relacionados com os serviços do CSIRT.

2.7 Chaves públicas e informação de cifra

ID da chave PGP: 711C15DD
Impressão digital PGP: 0173 5C4D EB8D 3989 0545 F6BD B371 7D48 711C 15DD
A chave PGP pode ser recuperada em: https://pgp.mit.edu/

2.8 Membros da equipa

Coordenação: Nuno Arroz
Membros: Ivo Cunha, Vitor Magalhães, Rui Rodrigues

2.9 Outra informação

Informações gerais sobre o h-CSIRT Hardsecure podem ser encontradas em https://hardsecure.com.

2.10 Meios de contacto para utilizadores

O h-CSIRT Hardsecure dispõe dos meios de contacto elencados nas secções 2.4 a 2.6

3. Guião

3.1 Missão

Proteger a Segurança da Informação na Hardsecure e na comunidade, cooperando também no sentido de uma crescente resiliência da cibersegurança nas geografias onde a Hardsecure está presente, através do seu papel de apoio às organizações no sentido de ficarem preparadas para enfrentar ameaças ao nível dos ciberataques.

3.2 Comunidade Servida

O h-CSIRT Hardsecure gere a resposta a incidentes de segurança de informação de colaboradores e clientes processada ou arquivada na sua infraestrutura informática ou em sistemas informáticos externos, através de ações desenvolvidas a partir do IP 87.103.13.203, neste caso sujeito a cláusulas contratuais em vigor.

3.3 Filiação

O h-CSIRT Hardsecure faz parte do Centro de Operações de Segurança, unidade organizacional da Hardsecure.

3.4 Autoridade

As atribuições da h-CSIRT Hardsecure são definidas pelo seu CISO.

4. Políticas

4.1 Tipos de incidente e nível de suporte

O h-CSIRT Hardsecure responde a incidentes nas áreas de segurança informática, nomeadamente na intrusão ou tentativa de intrusão, código malicioso, disponibilidade, recolha de informação, segurança da informação, fraude, conteúdo abusivo e vulnerabilidades.

Para além de incidentes de segurança informática o h-CSIRT Hardsecure responde e intervém nas áreas autenticação segura, gestão do ciclo de vida de identidades digitais, cooperação, interação, definição e políticas de privacidade e proteção de dados.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do h-CSIRT Hardsecure prevê que informação sensível pode ser passada a terceiros, única e exclusivamente em caso de necessidade e com a autorização prévia expressa do indivíduo ou entidade a quem essa informação diga respeito.

4.3 Comunicação e autenticação

Dos meios de comunicação disponibilizados pelo h-CSIRT Hardsecure, o telefone e o correio eletrónico não cifrado são considerados suficientes para a transmissão de informação não sensível. Para a transmissão de informação sensível é obrigatório o uso de cifra PGP.

5. Serviços

A Hardsecure garante uma capacidade de fornecimento de serviços adequada à realidade de cada instituição, com recursos técnicos e operacionais adequados ao fornecimento de serviços avançados de segurança e cibersegurança, de forma a garantir a mitigação/bloqueio de vetores de ataque diferenciados e distintos.

5.1 Segurança Defensiva

Através da utilização de meios técnicos que permitem o bloqueio/mitigação de ataques à infraestrutura de TI de uma organização (NG Firewall, endpoint security, DLP, Gestão de Identidades, Proxy/Reverse Proxy, Anti-spam, SIEM, Autenticação Forte, Anti-target attack, …).

5.2 Auditorias de Segurança

Standards ISO27001, ISO27002, ISO22301, ISO27005, ISO27037 e PCI-DSS.

5.3 Pentest/Pentest as a Service

Vulnerability Assessement, Injeção de Incidentes (exploit DB, Zero-day/Zero-hour).

5.4 Análise Forense

Email Crime Investigation, Web Attacks Investigation, Operating System Forensics, Data Acquisition and Duplication, Cloud Forensics, Malware Forensics, Mobile Forensics, Network Forensics, Database Forensics.

5.5 Resposta a Incidentes de Segurança

SOC & SOC as a Service

5.6 Testes de Segurança e Controlo de Qualidade do Código

Utilização de frameworks OWASP, PTES, OWTF, NIST, ISSAF e OSSTMM.

5.7 Proteção de Dados

Adoção de mecanismos e políticas que abrangem Processos e Procedimentos, Dados Pessoais, Organização e o Sistema de Informação da Instituição (coordenação entre Segurança em TI vs. Legal).

5.8 Consultoria

Planeamento, Governance, Planos de Ação, Correção/Mitigação.

5.9 Investigação e Desenvolvimento

Investigação de Malware, Desenvolvimento de Exploits, Projetos de Cibersegurança.

6. Salvaguarda de responsabilidade

Embora todas as precauções sejam tomadas na preparação da informação divulgada quer no portal Internet, quer através das listas de distribuição, o h-CSIRT Hardsecure não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.