e-Jornadas 2020

PORTUGAL INCoDe.2030

Construir um CSIRT

Carlos Friaças

Agenda

e-Jornadas 2020

- O que é um CSIRT ?
- Os Quatro Eixos
- Ecosistema(s)

e-Jornadas 2020

Queremos motivar a criação **formal** de novas equipas CSIRT na RCTS

O que é um CSIRT ?

e-Jornadas 2020

- **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam
- Principal Missão: Responder a Incidentes de Segurança.
- Na Prática: Muito trabalho de prevenção para tentar minimizar o número de Incidentes.
- É um conjunto de pessoas, processos e ferramentas devidamente enquadrados na organização.

O que é um CSIRT: Partir do (quase) Zero

e-Jornadas 2020

- A dimensão da equipa depende do contexto
- Tempo Integral vs. Tempo Parcial
- Integração de elementos de várias Áreas/Departamentos
- Começar com um conjunto mínimo de ferramentas
    - Ticketing, Contactos, Visibilidade sobre a infraestrutura

O que é um CSIRT: Começar pelo «BI»

e-Jornadas 2020

- Começar pela definição e publicação do RFC2350 da Equipa pode ser um bom primeiro passo.
- Esse documento deve ser revisto periodicamente.
- Não se pode pretender ter tudo no momento Zero.

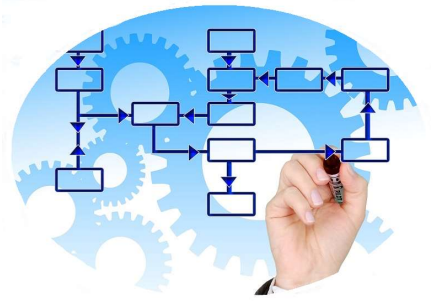
Os Quatro Eixos

- Organizacional

- Ferramentas

- Humano

- Processos



Os Quatro Eixos: Organizacional

e-Jornadas 2020

- Definir o âmbito
- Ter um claro mandato da gestão de topo
- Níveis de Serviço
- Tipificação de Incidentes
- Política de Segurança

Attack Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.

Os Quatro Eixos: Humano

e-Jornadas 2020

- Código de Conduta
- Descrição de Funções (com Resiliência)
- Formação
- Comunicação
- Cooperação com outras Equipas

Os Quatro Eixos: Ferramentas

e-Jornadas 2020

- Inventário IT
- Fontes de Informação
- E-Mail, Sistema de Ticketing, Telefone e Internet
- Ferramentas de Detecção
- Ferramentas de Prevenção e Resolução

Os Quatro Eixos: Processos

- Escalagem – Topo, Comunicação e Legal
- Prevenção
- Detecção e Resolução
- Auto-Auditoria, Reporting e Estatísticas
- Manuseamento Seguro de Informação

Ecosistema(s)

- RCTS: Rede Académica de CSIRT
  - ❖ https://cert.rcts.pt/pt/rede-academica-de-csirts
- Portugal: Rede Nacional de CSIRT
  - ❖ https://www.redecsirt.pt
- Europa: TF-CSIRT
  - ❖ https://tf-csirt.org
- Global: FIRST
  - ❖ https://first.org

Rede Académica de CSIRTs

e-Jornadas 2020

A RAC é a Rede Académica de CSIRTs

- RCTS CERT @FCCN [RFC2350]
- CSIRT.UPorto @Universidade do Porto [RFC2350]
- CSIRT.UMINHO @Universidade do Minho [RFC2350]
- CSIRT.UTAD @UTAD [RFC2350]
- CSIRT.UBI @Universidade da Beira Interior [RFC2350]
- CSIRT.UEVORA @Universidade de Évora [RFC2350]
- CSIRT@UA @Universidade de Aveiro [RFC2350]

1ª Reunião da RAC

2ª Reunião da RAC

3ª Reunião da RAC


MEMBROS DA REDE NACIONAL DE CSIRT
CERT RCTS
NOS
nowo
claranet
altice
DOGNÆDIS
U.PORTO
IP Telecom
Millennium
IGFEJ
edp
INESC
RNSI
PTServidor
vodafone
LAYER8
CERT.PT
NOVO BANCO
bancoctt
multicert
.pt
axians
Universidade do Minho
utad
cybersafe
S21SEC
outsystems
truphone
CSIRT.UBI
Santander
EURONEXT
universidade de aveiro
Secur.Net
UNIVERSIDADE DE ÉVORA
warpcom
EY
Building a better working world

Referências

- SIM3
  - https://www.trusted-introducer.org/SIM3-Reference-Model.pdf
- Modelo de Maturidade de Reacção (CNCS)
  - https://www.cncs.gov.pt/certpt/capacitacao-csirt/modelo-de-maturidade-de-reacao

Obrigado!