
# RELATÓRIOS MENSAIS DE CIBERSEGURANÇA

Pedro Silva

27 de Junho de 2023

# AGENDA

- Âmbito
- Leituras - Categorias e Periodicidade
- Como funciona
- Relatório Final
- Novas Leituras

# ÂMBITO

- Porque foi criado?
- O que faz?
- Para quem?

# LEITURAS/CATEGORIAS/PERIODICIDADE

## Leituras - Métricas

### Periodicidade

- Diária
- Semanal
- Mensal


### Categorias

- Incidentes
- Vulnerabilidades
- Malware
- Direitos de Autor
- Defacements

- IDS
- CERT/CSIRT
- E-Mail
- Web
- Blacklist
- DNS

# COMO FUNCIONA

- Leituras
  - Periodicidade
  - Categoria
- Gerar o relatório
  - Fórmula matemática
    - Leitura
      - Média ou soma
- Valor final – Rating

# RELATÓRIO FINAL

CERT RCTS

RELATÓRIO DE CIBERSEGURANÇA - Abril 2023

## Fundação para a Computação Científica Nacional

Rating

A

971 / 1000

CERT RCTS

**Incidentes Abertos:**

| Incidentes | Data | Chave | Taxonomia |
|---|---|---|---|
| | 2023-03-03 | | Vulnerable - Vulnerable system |

CERT RCTS

| Número de Incidentes: | Número de IPv4 atribuídos: | Domínio testado: |
|---|---|---|
| 0 | | fccn.pt |

### COMO LER O SCORE

A tabela do lado direito detalha a avaliação de 18 parâmetros realizada com base em diversas leituras levadas a cabo no último mês. Cada linha tem um valor avaliado e um valor máximo possível de atingir com base no peso que o RCTS CERT atribui a cada parâmetro. Para atingir o valor máximo de 1000 pontos todos os parâmetros terão que ter leituras que reflictam configurações consideradas seguras.

Mais em: https://www.cert.rcts.pt/rating

### SERVIÇOS DE SEGURANÇA SUBSCRITOS

| | |
|---|---|
| Vulnerabilidades | Não |
| DNS Firewall | Sim |
| Auditorias | Sim |
| Campanhas de Phishing | Sim |

### CONTACTOS DE SEGURANÇA

| | |
|---|---|
| Carlos Friaças | chiacas@fccn.pt |
| Pedro Silva | pedro.silva@fccn.pt |

| TIPOLOGIA | SCORE |
|---|---|
| Malware | |
| Direitos de Autor | |
| Defacements | |
| IDS | |
| Blacklists | |
| Vulnerabilidades | |
| Equipa CSIRT formalizada | |
| E-MAIL - SPF | |
| E-MAIL - DMARC | |
| E-MAIL - DKIM | |
| Web - Headers | |
| Web - Server Signature | |
| DNS do domínio principal - Zone Transfer | |
| DNS do domínio principal - DNSSEC | |
| Web - SSL | |
| Incidentes | |
| **Total** | |

# NOVAS LEITURAS

- Certificados Expirados ou Self-Signed
- Portas abertas
  - RDP
  - SSH
  - NTP
  - SNMP
  - QOTD
  - PORTMAP
  - TELNET
  - MEMCACHE
  - REDIS
  - LDAP
  - MONGODB
  - MYSQL
  - POSTGRESQL
  - FTP/TFTP
  - VNC
  - ...

```
C:\>netstat -an |find /i "listening"
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1062           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2002           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2535           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2937           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
```

- HSTS (HTTP Strict Transport Security)

# OBRIGADO!

# Patrocinadores

## Platina

EBSCO

ELSEVIER

Microsoft

warpcom

cisco

FORTINET

axians

officelan

SECURNET

CHECK POINT

SYSCRUM

PAESSLER

THE MONITORING EXPERTS

ORACLE

NVIDIA.

paloalto

software one

## Ouro

ACS Publications

Most Trusted. Most Cited. Most Read.

Clarivate

CAMBRIDGE UNIVERSITY PRESS

DE G DE GRUYTER

HUAWEI

DIVULTEC

LOGICALIS

Architects of Change

Sage

SPRINGER NATURE

tp-link

wavecom

Bravantic

itcenter

reallife

## Prata

ROYAL SOCIETY OF CHEMISTRY

IOP Publishing

MEO EMPRESAS

aws

emerald PUBLISHING

IEEE

Logiser

## Organização

fct Fundação para a Ciência e a Tecnologia

FCCN