Ransomware
medidas de prevenção

Rogério Raposo

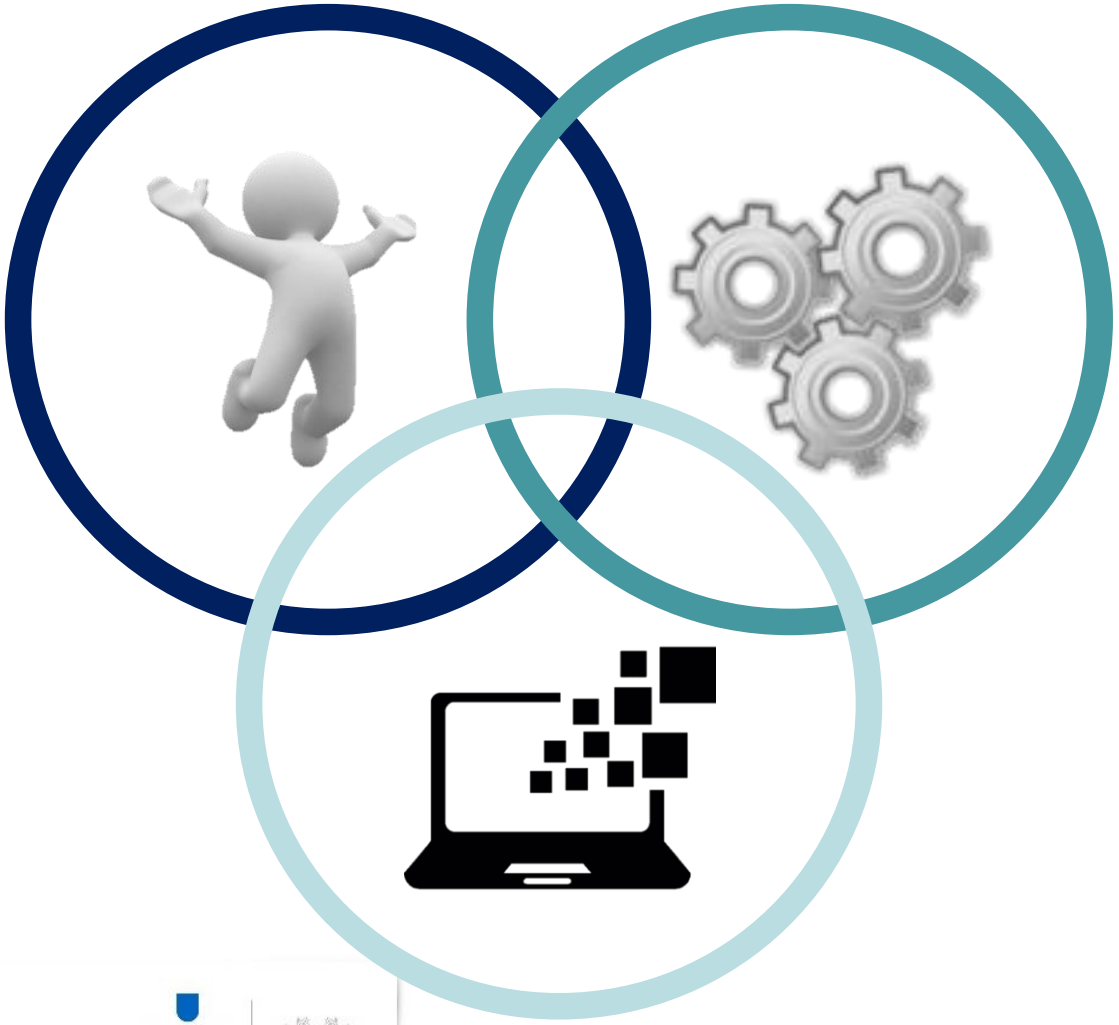
Departamento de Operações

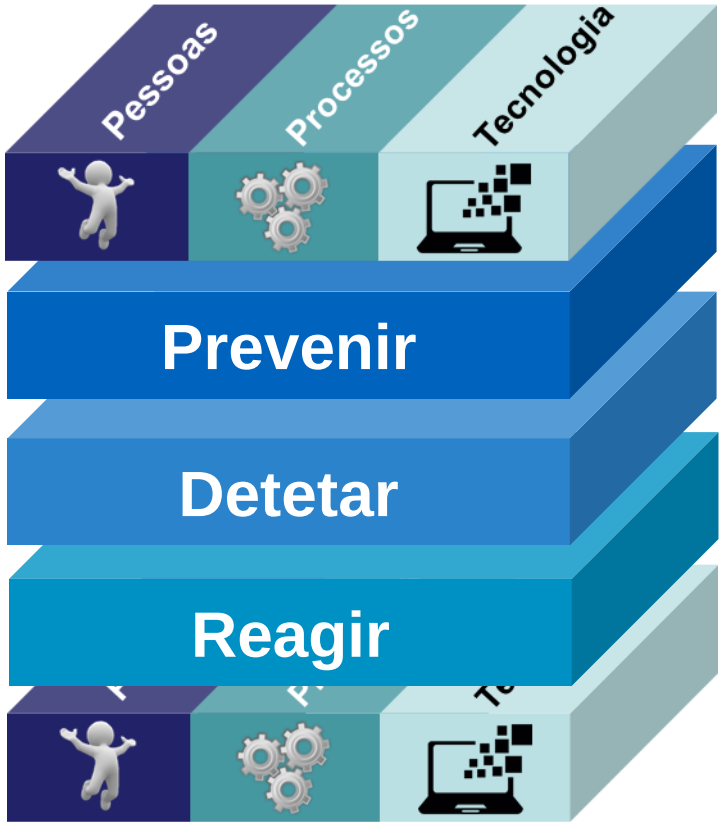
GNS | 27 Jan 2017

CNCS

Centro Nacional
de Cibersegurança
PORTUGAL

Prevenir – Detetar - Reagir





Medidas de Prevenção - Deteção

Ensinar, formar, treinar

- ✓ Uso da tecnologia
- ✓ Possíveis efeitos (diretos/colaterais) das ameaças
- ✓ Identificar potenciais ameaças
- ✓ Reportar potenciais ameaças
- ✓ Agir perante potenciais ameaças

Pensar, definir, aplicar

- ✓ Políticas, procedimentos
  - ✓ pessoas
  - ✓ redes e sistemas de informação (o que liga ao quê e porquê)
  - ✓ áreas de negócio da organização
  - ✓ Informação
    - ✓ Conhecer
    - ✓ Identificar
    - ✓ Priorizar
    - ✓ Proteger

Implementar, configurar, gerir

- ✓ Sistemas de prevenção
- ✓ Cópias de segurança (de tudo?)
- ✓ Paridade acesso–necessidade
  - ✓ privilégios de acesso
  - ✓ gestão de acessos
- ✓ Robustez da tecnologia
  - ✓ redes e sistemas associados (dependências - segregação)
  - ✓ funcionalidades (*javascript*, macros, etc)
- ✓ Atualizações

CNCS

Medidas de Prevenção - Deteção




Ensinar, formar, treinar

- ✓ Abrir ligações e executar ficheiros ~~suspeitos~~
  - ✓ O que são ficheiros executáveis
  - ✓ Identificar disparidades nas ligações sugeridas
- ✓ Efeitos do "*contornar*" medidas de segurança implementadas

Pensar, definir, aplicar

- ✓ Auditorias e inspeções
- ✓ Partilha de informação
- ✓ Criação de capacidade para prevenir e detetar incidentes na organização
- ✓ Laços e ligações com outras entidades (apoio, complementaridade)
- ✓ Processos de validação da segurança (das cópias, da tecnologia, da consciência, …)

Implementar, configurar, gerir

- ✓ Visibilidade sobre a tipologia dos ficheiros (**Nota.doc.exe, recibo.pdf.scr**)
- ✓ Permissões restritas (racionais) de escrita e leitura sobre informação sensível
- ✓ Instrumentos específicos para deteção de indicadores de ameaças de *ransomware*
- ✓ Gestão de vulnerabilidades *vs* diligência prévia rigorosas
- ✓ Registo e conservação de *logs* de auditoria

CNCS

Obrigado.

rogerio.raposo@cncs.gov.pt

Departamento de Operações

Lisboa

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Ransomware
medidas de prevenção

Rogério Raposo

Departamento de Operações

GNS | 27 Jan 2017

CNCS

Centro Nacional
de Cibersegurança
PORTUGAL