Novo CSIRT.UEVORA

CSIRT UEVORA

UNIVERSIDADE DE ÉVORA
SERVIÇOS DE INFORMÁTICA

Tiago Sousa
Universidade de Évora

4ª Reunião da RAC - 2018/11/20

Introdução

- A Universidade
- Caminho percorrido
- Incidentes e divulgações
- Motivação
- O CSIRT.UEVORA

Universidade de Évora

- 8450 alunos
- 1136 funcionários
- 11 colégios/edifícios (Évora)
  + Pólo da Mitra (Valverde)
  + outros
- 7 residências

Infraestrutura

- 160 switches com gestão
    - E *incontáveis* microswitches :-)
- 257 access points
- 84 servidores físicos (em espaços dos SI)
    - Muitos outros de departamentos, etc
- 89 VMs
- 4854 endereços IPv4 (espaço total) + IPv6 /48

Historial

- 2013 – Criação do e-mail csirt@uevora.pt
- 2013 – Início do projecto “Gestão de Serviços TI” (ISO 20000 / ITIL)
    - Segurança da Informação
    - Incidentes e pedidos de serviço
- 2014 – Parametrização do OTRS (ferramenta de apoio ao projecto)
- 2015 – Checkbox “Incidente de segurança” no OTRS

Ênfase crescente na segurança

- Projecto “Gestão de Risco e da Segurança de Informação” (ISO 27001)
  - Auditoria
  - Workshop
- Projecto RGPD (levantamento dos dados pessoais e respectivos tratamentos)
- Conferência Cibersegurança (iniciativa no âmbito de Outubro - Mês Europeu da Cibersegurança)
  - Marco Matias (PGR) / António Gameiro Marques (GNS)

Segurança + RGPD

- Constituição do Conselho de Segurança da Informação e Proteção de Dados Pessoais
  - «O CSIPDP tem por missão promover e contribuir para a definição e consolidação de políticas e práticas visando a salvaguarda da informação na Universidade, bem como a gestão dos dados pessoais com respeito pela privacidade dos titulares.»
  - Encarregado da Protecção de Dados (DPO)
  - Responsável pela Segurança de Informação (CISO)

Tratamento de incidentes

- 97 Tickets registados desde 2015
  - Sem contar com violações de copyright
- 23 em 2018 (até agora)
  - Páginas comprometidas
  - Contas comprometidas
  - Serviços inseguros, Spamming, Brute force...
- Nem todos foram registados…
  - Alertas RCTS-CERT :-)

Divulgação à comunidade

- 7 alertas de segurança enviados em 2018 à comunidade académica
    - Phishing
    - Software vulnerável
- Blocos de notas distribuídos em eventos
- Posters (em preparação)
- https://www.si.uevora.pt/Seguranca

Motivação

- SIADAP: “Pensem em segurança”
- Já processamos incidentes via csirt@...
- Já temos um historial de processos noutras áreas…
- Segurança está na ordem do dia...
- Porque não formalizar?
- CSIRT.UEVORA!

Legitimidade

- Aguardamos o despacho reitoral como mínimo
- Seria desejável (em fase de revisão) uma menção no Regulamento dos Serviços de Informática por estar aqui integrado
- Talvez definir uma eventual relação com o Conselho de Segurança da Informação e Proteção de Dados Pessoais

Equipa

Tiago Sousa	tiagosousa@uevora.pt	Linux / Redes
Rui Paz	rpaz@uevora.pt	Windows
Mário Filipe	mjnf@uevora.pt	Chefe da DIS
Joaquim Godinho	jjg@uevora.pt	Director dos SI

...Nenhum de nós em exclusivo!

Missão

- Compete ao CSIRT.UEVORA dar uma primeira e rápida resposta a incidentes de cibersegurança na Universidade de Évora, focando-se na salvaguarda da informação contida nos seus sistemas informáticos, bem como ajudar a colmatar eventuais falhas identificadas.

- Procura também, proactivamente, minimizar riscos e vulnerabilidades nos sistemas informáticos da Universidade de Évora e fomentar boas práticas de segurança de informação na sua comunidade académica.

Vamos a isso :-)

Obrigado!

www.csirt.uevora.pt

csirt@uevora.pt