Proposta de anexo à AUP RCTS

Controlo de Incidentes e Eventos de Segurança na RCTS

Carlos Friaças
Jorge Carvalho

cfriacas@fccn.pt
jcarvalho@fccn.pt

2017-04-19

CERT RCTS

INTRODUÇÃO

JORNADAS FCCN2017

- Carta ao Utilizador da RCTS (AUP)
- Melhoria contínua

OBJETIVOS

JORNADAS FCCN2017

- Melhorar reputação da(s) organização(ões)
- Melhorar tratamento de incidentes **e** eventos
- Regras homogéneas para todos e do conhecimento de todos

"I have some paperwork to catch up. If I'm not back in two days, organize a search and rescue team!"

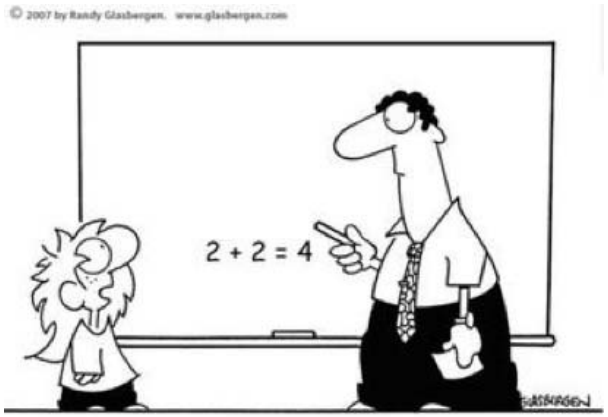
HOJE

JORNADAS FCCN2017

Documento em vigor (Fev/2013):

http://arquivo.pt/wayback/20151125134625/http://fccn.pt/fotos/editor2/medidas_de_controlo_de_incidentes_de_seguranca_informatica_v4.7.pdf

- Apenas relativo a incidentes
- Critérios
  - Tipo de incidente
  - Gravidade associada
- Apenas definida **uma** iteração



"How can I trust your information when you're using such outdated technology?"

PROPOSTA

JORNADAS FCCN2017

- Relativo a incidentes **e** eventos
- Critérios
  - **Fidedignidade** da fonte;
  - **Detalhe** da informação enviada;
  - **Severidade** do incidente/evento de segurança informática

    => Resultam num **Nível de alerta**
- **Duas** iterações com base no nível de alerta

FIDEDIGNIDADE

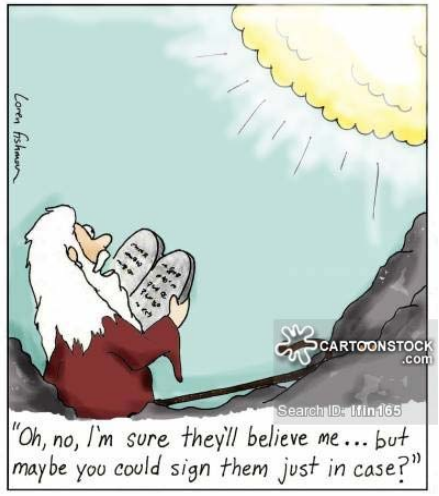
JORNADAS FCCN2017

Valor	Nível de confiança	Descrição
1	Médio	• Fontes de informação anónimas • Indivíduos singulares • Entidades não credenciadas • Informação isolada • Chats • Forums • Pastebin
2	Alto	• Entidades não credenciadas mas consideradas de confiança pelo RCTS CERT (Entidades RCTS, Operadores, Bancos, CSIRT nacionais e estrangeiros não acreditados) • Sites de segurança conhecidos • Informação recolhida de várias fontes, num mínimo de duas
3	Muito alto	• Entidades credenciadas (Agências policiais ou de *intelligence* nacionais ou internacionais, CSIRT estrangeiros acreditados internacionalmente (TI, ENISA ou FIRST) • Membros da rede Nacional de CSIRT) • Testado pela equipa do RCTS CERT

CRITÉRIO DE FIDEDIGNIDADE

- *Feedback* das instituições
- Análises aos registos de incidentes ou eventos
  - Totalidade - Com automatismos, desde que não cause impacto no cliente
  - Por amostragem – Manualmente

  ⇒ Comunicação com instituição:
    - Intrusivas a nível de confidencialidade de dados
    - Degradação do serviço prestado pela instituição



DETALHE DA INFORMAÇÃO

JORNADAS FCCN2017

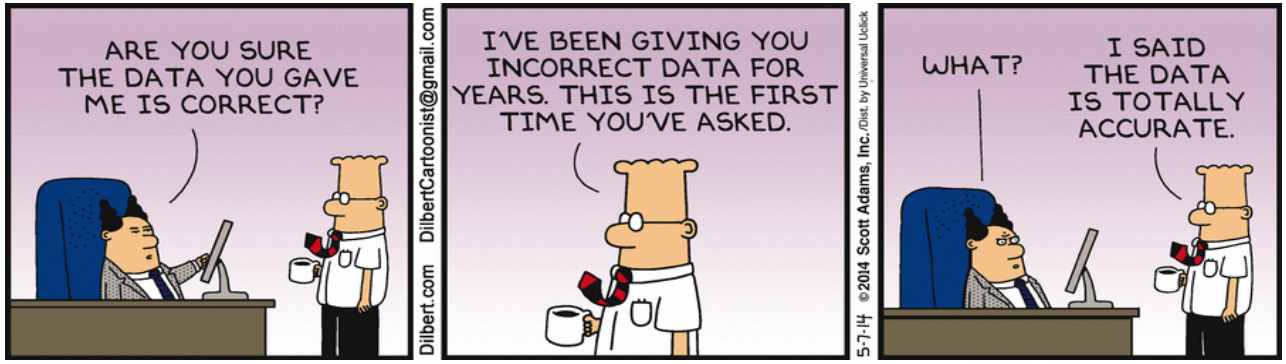
Valor	Classificação	Descrição
1	Pouco detalhado	Os dados fornecidos não permitem que os responsáveis pelas infraestruturas identifiquem com precisão os sistemas afetados.
2	Detalhado	Os dados fornecidos permitem a identificação precisa do sistema ou sistemas afetados, mas não o problema em concreto.
3	Muito detalhado	Os dados fornecidos permitem a identificação precisa do sistema ou sistemas afetados, e o problema em concreto.

"You're asking for pretty detailed information. Have your hackers gotten more demanding?"

SEVERIDADE DO TIPO DE ATAQUE

JORNADAS FCCN2017

- Tem em conta se afecta:
  - **Confidencialidade**
  - **Integridade**
  - **Disponibilidade**



NÍVEL DE ALERTA

Fidedignidade	Detalhe	Severidade	Nível de alerta
1	1	1	Verde
1	1	2	Verde
1	2	1	Verde
2	1	1	Verde
1	3	1	Verde
3	1	1	Verde
2	2	1	Verde
2	3	1	Verde
2	1	2	Amarelo
1	1	3	Amarelo
1	2	2	Amarelo
1	2	3	Amarelo
1	3	2	Amarelo
2	2	2	Amarelo
3	1	2	Amarelo
3	2	1	Amarelo
2	3	2	Amarelo
3	3	1	Amarelo

Fidedignidade	Detalhe	Severidade	Nível de alerta
2	1	3	Laranja
1	3	3	Laranja
3	1	3	Laranja
2	2	3	Laranja
3	2	2	Laranja
3	3	2	Laranja
2	3	3	Vermelho
3	2	3	Vermelho
3	3	3	Vermelho

NOTIFICAÇÃO & ATUAÇÃO (1ª ITERAÇÃO)

JORNADAS FCCN2017

1º Iteração	Incidentes		
Nível de alerta	**Tempo de Resposta para 1ª Iteração**	**Tempo de resolução após comunicação**	**Meio de comunicação**
Verde	Não aplicável	Não aplicável	Não comunicado
Amarelo	2 dias úteis	4 dias úteis	Email
Laranja	1 dia útil	3 dias úteis	Email
Vermelho	6 horas	12 horas	Email ou telefone
1º Iteração	**Eventos**		
Nível de alerta	**Tempo de Resposta para 1ª Iteração**	**Tempo de resolução após comunicação**	**Meio de comunicação**
Verde	Não aplicável	Não aplicado	IntelMq/Email
Amarelo	3 dias úteis	5 dias úteis	IntelMq/Email
Laranja	2 dias úteis	4 dias úteis	IntelMq/Email
Vermelho	Não aplicável	Não aplicável	Não comunicado

"No, I'm not angry at you, sir.
I'm angry at the random act of fate
that directed your call to my extension."

NOTIFICAÇÃO & ATUAÇÃO (2ª ITERAÇÃO)

JORNADAS FCCN2017

2ª Iteração	Incidentes		
Nível de alerta	**Tempo de Resposta para 2ª Iteração**	**Tempo de resolução após comunicação**	**Meio de comunicação**
Verde	Não aplicável	Não aplicável	Não comunicado
Amarelo	12h	1 dia	Email
Laranja	6h	12h	Email ou telefone
Vermelho	2h	4h	Telefone

2ª iteração	Eventos
Nível de alerta	**Tempo de Resposta para 2ª Iteração**
Verde	Não aplicável
Amarelo	Passa a incidente nível alerta amarelo
Laranja	Passa a incidente nível alerta laranja
Vermelho	Não aplicado

MEDIDAS DE CONTROLO DE TRÁFEGO

JORNADAS FCCN2017

Medida	Órgão competente
Corte a conectividade IP/Porta (um ou vários pares)	Membro do serviço RCTS CERT
Corte a conectividade de um ou vários endereços IP	Gestor do serviço RCTS CERT
Corte total de acesso	Coordenador-Geral da Unidade orgânica da Computação Científica Nacional (FCCN) da FCT,I.P.

CONTACTOS REGISTADOS DA ENTIDADE

JORNADAS FCCN2017

- Os **contactos** indicados pela entidade na descrição tipo “RFC2350”, dos seus serviços de **segurança informática**, presentes no diretório de contactos do RCTS CERT
- Os **contactos de segurança** associados ao acesso RCTS (Serviço IP) da sua entidade
- Os contactos técnicos associados ao acesso RCTS (Serviço IP) da sua entidade

CSIRT@... / CERT@...

- cert@cert.rcts.pt
- cert@fmv.ulisboa.pt
- certreports@ipc.pt
- csirt@esenf.pt
- csirt@ipbeja.pt
- csirt@ipb.pt
- csirt@ipca.pt
- csirt@ipleiria.pt
- csirt@ipsantarem.pt
- csirt@ipt.pt
- csirt@iscte-iul.pt
- csirt@lisboa.ucp.pt
- csirt@reitoria.ulisboa.pt
- csirt@uab.pt
- csirt@uac.pt
- csirt@ua.pt
- csirt@ubi.pt
- csirt@uevora.pt
- csirt@uma.pt
- csirt@up.pt
- csirt@upt.pt
- rcts.cert@lneg.pt

TO-DO, «RAC»

- Existem cerca de 80 entidades ligadas à RCTS
- Muitos csirt@ / cert@ por criar
- «Rede Académica de CSIRT», a.k.a. «RAC»
  - Sessão de *Kickoff* no dia 21
- Objectivos: Listar equipas e promover publicação de RFC2350 de cada entidade

2ª VIA: SIMPLIFICAÇÃO

JORNADAS FCCN2017

- Foco apenas nos incidentes
  - Mantendo o «status quo»

- Não vamos ignorar os eventos, mas não os vamos associar a um nível de alerta

2ª VIA: SIMPLIFICAÇÃO

- Usar apenas 3 níveis de Alerta
- «Fusão» dos níveis Verde e Amarelo
- Ausência de resposta durante 3 dias (úteis) subirá o nível de alerta

2ª VIA: SIMPLIFICAÇÃO

JORNADAS FCCN2017

- Cortes serão executados após autorização dos contactos técnicos/segurança
  - Excepção:
    - sempre que o impacto seja relevante
    - não haja acção de mitigação por parte da entidade utilizadora
    - não exista outra forma de conter o incidente.

2ª VIA: SIMPLIFICAÇÃO, CONTACTOS

JORNADAS FCCN2017

- A necessidade de contactos actualizados é exactamente igual

- Mais comunicação = Resposta a Incidentes mais eficaz!

DISCUSSÃO

JORNADAS FCCN2017

JORNADAS FCCN2017

CERT RCTS

report@cert.rcts.pt

cert.rcts.pt