Segurança Informática

contexto, conceitos e desafios

Rotary Club Vizela
(http://rotaryclubevizela.blogspot.pt/)
18 de Junho de 2014

Luis Borges Gouveia
Professor Associado com Agregação
Universidade Fernando Pessoa

Rotary Club de Vizela
D. 1970 –Ano Rotário 2013/2014

"Segurança Informática"
pelo
Prof. Doutor Luís Borges Gouveia

Dia 18 de Junho
21h e 30m
Restaurante Águia d'Ouro

CONTEXTO

A ideia de mundo

Agora…

Sociedade da Informação

- Uso intensivo de computadores e redes
  (*do saber usar ao saber o que fazer com eles*…)
- A informação que conta é digital
  (*a informação já não é o que era e vale pouco*…)
- A organização que conta é a rede
  (*as hierarquias são uma simplificação a num momento*…)

O que significa?

Mudança…

Dois aspectos essenciais

- **Sustentabilidade**

Como garanto a minha liberdade ou como o valor gerado cobre o valor absorvido*
**(valor: económico, social, político e satisfação)*

- **Soberania**

*Como garanto a minha identidade** ou como posso ser reconhecido como eu próprio e ser o que quero/posso ser*
***(marca: pessoa, empresa, nação)*

Tempo e espaço

- **Tempo**

  24/7 sempre ligado, sempre presente

  MAS exige disponibilidade inteligente e bem gerida

  AFINAL o tempo humano é limitado

- **Espaço**

  em qualquer lugar, de qualquer forma

  MAS como estar presente?

  AFINAL a experiência é o memorável

Estratégias facilitadas pelo digital

- Capacidade de **projecção**
  - Chegar aos outros e exposição global
- Diferente e **dinâmico**
  - Ter capacidade de capturar a atenção
- Criativo e **inovador**
  - Ter capacidade de concretizar valor
- Inclusivo e **cumplice**
  - Perceber que a colaboração e a rede são essenciais

Contexto

- Mundo complexo
  - Computadores e redes (tudo ligado)
  - Mais gente com competências à escala gobal
- Exigidos novos cuidados ou o reforço dos existentes
  - …e alargado a mais pessoas e empresas
  - As instituições são alvo
  - As figuras públicas são alvo
  - No geral, quem pode contribuir (*) é alvo

CONCEITOS

Segurança…

- Um ativo central e não muitas vezes valorizado
  - Não existindo, sentimos muito a sua falta
  - Existindo, *continuamos como estamos…*
- Não tem retorno direto e funciona para um potencial risco que esperemos que não ocorra
  - Tal como um seguro (em que o risco é normalmente público – acidente. Em oposto a ser privado – incidente)
- Segurança e defesa
  - Conceito associado com muitas outras atividades e que determina a nossa qualidade de vida e nível de proteção
  - Ativo não tangível que afeta confiança (a moeda de esperança da economia…)

Informação...

- Apoia a tomada de decisão e torna possível a ação
  - É abstrato, mas central à atividade humana
- Pode ser um **recurso**
  - E portanto estratégico numa organização (por exemplo, informação comercial de clientes e fornecedores…)
- Pode ser um **ativo**
  - E pode ser transacionado (por exemplo, vender uma base de dados de clientes e suas caraterísticas…)
- Pode ser uma ***commodity***
  - Adquiriu um valor de mercado expetável (por exemplo, saber onde fica determinado lugar…)

Informática…

- Lidar com a informação digital
  - Processada, armazenada e comunicada por dispositivos eletrónicos
- Muito além do computador
  - Dispositivos móveis: tablets, smart phones, …
  - Sistemas de geolocalização e identificação e controle de acessos, …
  - Armazenamento de dados: USBs, discos, …
  - Cartões e outros meios de identificação
  - Internet, *Cloud* e plataformas digitais
  - Aplicações , serviços e jogos

Segurança informática

- Vírus e outras formas de ataque a computadores e dispositivos móveis
- Exploração de falhas de software cada vez mais complexas
- Engenharia social e exploração das características humanas (curiosidade, medo, ganância, etc.)
- Falha humana não intencional (desconhecimento, relaxamento ou desinteresse)
- Falha humana intencional (interesses e atividade criminosa)

Segurança da Informação

- Um maior nível de preocupação que inclui a informação digital, mas também a existente em suportes não digitais
- Preocupa-se com uma abordagem estruturada ao problema e à salvaguarda da informação
  - Qual a informação crítica?
  - Quais as infraestruturas críticas?
  - O que fazer para assegurar a continuidade do negócio/atividade?
- E temos ainda de lidar com a questão final:
  - *Quem guarda os guardas?*

Princípios

- Integridade
  - A informação deve ser completa, verificável e verdadeira
- Confidencialidade
  - A informação deve ser salvaguardada de quem não tive autorização para o seu acesso
- Disponibilidade
  - A informação deve ser fácil de obter onde e quando necessária e de forma entendível
- Não repudiação
  - Não deve ser possível a negação de autoria ou origem da informação

Termos associados: segurança da informação

- Vulnerabilidade
  - Existência de um potencial de falha de segurança
- Ameaça
  - Elementos concretos, potenciadores de exploração de falha de segurança
- Risco
  - Probabilidade efetiva de concretização de ameaças para as vulnerabilidades existentes
- Medida
  - Meio ou procedimento de combate ou minimização do risco
- Impacte
  - Prejuízo em caso de concretização da ameaça
- Incidente
  - Situação efetiva de aproveitamento de uma vulnerabilidade

DESAFIOS

Conflitos na era da informação

INFORMATION *IN* WARFARE

- Inteligência
- Vigilância
- Reconhecimento
- Clima
- Geográfico
- Outro

INFORMATION WARFARE

- Influenciar atitudes
- Negar/Proteger
- Enganar/Esconder
- Explorar/Atacar

Potenciais vulnerabilidades da sociedade

- **Vulnerabilidades das democracias:**
  - tirando partido de liberdades e garantias e originando informação falsa ou confusa em campanhas organizadas com recurso aos media (imprensa, de massas e redes sociais);
- **Ataque de indivíduos criativos**:
  - com conhecimento, capacidade e determinação para explorar sistemas de comunicações e redes de computadores para ganhos ilegais ou simplesmente sabotar a sociedade;
- **Organizações criminosas:**
  - terroristas, traficantes de armas, ou de mão de obra escrava ou orgãos humanos que operam entre países;
- **Operações conjuntas:**
  - realizadas de forma combinada com ações militares mais tradicionais, ocultando interesses e atacando alvos considerados críticos para esses interesses;
- **Guerra psicológica:**
  - operações com foco na população de modo a minar a sua confiança nos seus lideres ou na sabedoria da suas ações, muitas vezes explorando clivagens étnicas, sociais, morais dessa sociedade

http://www.iwar.org.uk/iwar/resources/deterrence/iwdAppb.htm

Atores principais na guerra da informação

- **Nações mais poderosas**
  - depende de sistemas complexos, sujeitos a instabilidade política ou equilíbrios frágeis e possível perda de reputação
- **Organizações multinacionais e redes muito estruturadas**
  - Sujeitos a ações legais, roubo de propriedade intelectual, falha de sistemas e censura pública
- **Indivíduos e redes menos estruturadas**
  - Sujeitos a stresse legal e ilegal por governos e organizações, quando apanhados

O ciberpoder: 3 táticas (familiares, não?...)

- **A diz a B o que fazer**
  - se não, B não o pode fazer…
- **A não permite a escolha a B**
  - inclui a permitir a B aplicar as suas estratégias
- **A molda as preferências de B**
  - desta forma, B não considera algumas das estratégias possíveis

Ciberdefesa

- Conceito militar de resposta à guerra da informação
- Possui 3 componentes:
  - Ciberdefesa **defensiva**: orientada para assegurar a defesa de infraestruturas críticas
  - Ciberdefesa de **exploração**: orientada para explorar e conhecer vulnerabilidade de terceiros e próprias
  - Ciberdefesa **ofensiva**: orientada para realização de ataques a alvos específicos ou como meio de dissuasão (pode incluir o desenvolvimento de ciberarmas)

Cibersegurança

- A versão civil da ciberdefesa, orientada para as preocupações de proteger a sociedade nas suas vertentes de serviços públicos, economia e indivíduos
  - Existem ao nível dos Estados, preocupações crescentes com estas questões (em Portugal, é a ***estratégia nacional para a cibersegurança***, http://www.gns.gov.pt/new-ciberseguranca.aspx da responsabilidade do Gabinete Nacional de Segurança)
  - É organizada em rede e conta com a troca de informação entre interessados e com o reporte de incidentes e práticas de contingência comuns (em Portugal, o **CERT.PT** http://www.cert.pt/)
  - Cada um de nós, deve tomar precauções à sua escala…

Concluindo...

Incidentes (alguns exemplos…)

- Stuxnet (o caso do ataque com sucesso no Irão) e ?
  - Utilização de software malicioso como ciberarma
- Wikileaks e os EUA
  - Classificar informação e proteger informação, parece um ato impossível
  - Ainda existe confidencialidade possível?
- Snowden e a NSA
  - Afinal até eu sou espiado, registado e armazenado nas minhas mais diversas dimensões
  - Ainda existe privacidade?
- A China e os EUA
  - Dos relatórios Mandiant à acusação de Pensilvania
  - Cibersegurança diferente de ciberdefesa?
    E as relações EUA-China?

Numa escala mais humana…

- Como defender:
  - A esfera empresarial
  - A esfera pessoal
- Desafios:
  - Proteção e segurança da informação
  - Privacidade
- Mecanismos
  - Trabalho especializado
  - Formação, cautela e experiência

Como fazer?

- Avaliar os ativos de informação
- Classificar a informação
- Listar as infraestruturas críticas
- Listar as vulnerabilidades, as ameaças e os riscos para o contexto
- Formar e enquadrar os recursos humanos
  - Desde o controle de acessos e creditação, até à sensibilização e efetivação de políticas de segurança
- Realizar uma auditoria de segurança
  - Avaliar os riscos e capacidades existentes, refletindo sobre impactes e medidas de contingência
- Rever, partilhar e colaborar
  - A segurança é partilha de informação, rede e conhecimento…

Comentários finais

- A melhor maneira de estar seguro é estar informado
- As proteções tem de ser uma preocupação constante
  - Cada vez mais sofisticadas
  - Sempre em evolução
  - Os indivíduos são tão importantes como as empresas
- O conhecimento é a arma e a colaboração a defesa
  - As redes são importantes e as colaborações e parcerias estratégias
  - O nível de segurança corresponde ao nível associado com o nodo mais vulnerável da rede a que pertencemos