Cibersegurança e Cibercrime

Carlos Pinto de Abreu

23 de Março de 2017

Cooperação: palavra chave

“*a Internet nasceu na encruzilhada insólita entre a ciência, a investigação militar e a cultura libertária*”

Castells

Ciberespaço: o alargamento do universo

- ”espaço virtual no qual existe informação e ocorre a comunicação através de redes de computadores” (estruturas físicas, software, dados, utilizadores, acessos, comunicações…)

  ↓

  telemóveis, computadores, televisões, electrodomésticos, equipamentos médicos.

  ↓

  avanços/desafios vs vulnerabilidades/danos

Ciberespaço: oportunidades e desafios

▪Oportunidades

- Democratização da informação
- Redução dos custos de produção e de gestão de informação
- Decréscimo dos custos e das dificuldades de utilização
- Crescimento ilimitado
- Elevada adaptabilidade às mais variadas actividades (*v.g.* direito, medicina, política, indústria militar, educação, segurança e operações de socorro)

▪Desafios

- Evitar erro, dispersão, futilidade e manipulação da informação
- Protecção das infraestruturas críticas e da integridade das redes
- Salvaguardar a privacidade e a protecção de dados pessoais
- Dar resposta ao anonimato
- Investimento em meios e técnicos especializados a fim de garantir a operacionalidade do ciberespaço
- Prevenir e combater o cibercrime

Cibersegurança: riscos e ameaças

- Conjunto de tecnologias, processos e práticas utilizadas para protecção de redes, computadores, programas e dados (no ciberespaço) de perdas, ataques, acessos não autorizados ou sabotagem
- São dispersas e múltiplas as fontes de ameaça e de destruição de valor: desastres naturais, avarias, negligência humana, ataques intencionais
- Cibercrime, ciberterrorismo, ciberespionagem
- “Hacktivismo” – fenómeno recente
- Motivações políticas, sociais, económicas, criminais

Crises no ciberespaço: o cibercrime

- A elevada disseminação e utilização de sistemas de informação acabou por acentuar a importância e a perigosidade das crises informáticas e de alguns dos métodos de ataque: Backdoors, DoS, Spoofing, Phishing, Bullying... (a imaginação humana não tem limites para o mal… cibernético!)
- Apesar da maioria dos ataques informáticos exigir algum conhecimento técnico-científico são inúmeros e crescentes os ataques típicos dirigidos a cidadãos individualizados e a empresas -> cibercrime(s)

Crises no ciberespaço: o cibercrime

- “todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto de crime” - *Garcia Marques*
- **Crimes informáticos (Lei 109/2009, de 15.09)**
  - Falsidade informática (art. 3º)
  - Dano relativo a programas ou dados (art. 4º) e sabotagem informática (art. 5º)
  - Acesso ilegítimo e intercepção ilegítima (arts. 6º e 7º)
  - Reprodução ilegítima de programa protegido (art. 8º)

Crises no ciberespaço: o cibercrime

- Código Penal
  - Devassa por meio da informática (art. 193º)
  - Violação de telecomunicações (art. 194º)
  - Gravações e fotografias ilícitas (art. 199º)
  - Burla informática e nas comunicações (art. 221º)

  - Responsabilidade penal das pessoas colectivas
  - Obtenção de prova digital (pesquisa, apreensão, intercepção e acções encobertas) - medidas especiais (preservação expedita de dados, revelação expedita de dados de tráfego e injunção para apresentação de dados ou concessão de acesso a dados)
  - Cooperação judiciária nacional e internacional

Legislação especial essencial

- Lei do Cibercrime (Lei 109/2009, de 15.09)
- Lei da Conservação de Dados (Lei 32/2008, de 17.07)
- Lei da Protecção de Dados Pessoais (Lei 67/98, de 26.10, Rectificação 22/98, de 28.11, e Lei 103/2015, de 24.08)
- Lei das Comunicações Electrónicas (Lei 5/2004, de 10.02)
- Lei do Tratamento de Dados Pessoais e Privacidade no Sector das Comunicações Electrónicas (Lei 41/2004, de 18.08, e Lei 46/2012, de 29.08)
- Regime de Protecção Jurídica dos Programas de Computador (DL 252/94, de 20.10) e das Bases de Dados (DL 122/2000, de 4.07)

Outros diplomas, jurisprudência e doutrina

- Identificação e Protecção de Infraestruturas Essenciais (DL 62/2011, de 9.05)
- Lei 52/2003, de 22.08 (Lei de Combate ao Terrorismo)
- Estratégia Nacional de Combate ao Terrorismo (Resolução do Conselho de Ministros nº 7-A/2015, de 20.02
- DL 81/2016, de 28.11 (Unidade Operacional Especializada da PJ)
- Orientação Política para a Ciberdefesa (Despacho do Ministro da Defesa nº 13692/2013)

- Tabela de Jurisprudência e Bibliografia (remissão)

Gestão de crises

- Desde intrusões em websites à divulgação de mensagens de correio electrónico, são várias as possibilidades de ataque a sistemas informáticos e, por isso, é essencial a criação de protocolos de defesa e de resposta eficaz aos diversos ataques e suas consequências
  - *Prontidão* – a antecipação dos possíveis cenários de ataque é fundamental para uma resposta pronta e eficaz
  - *Resposta* – uma não reacção ou uma reacção errada pode potenciar os efeitos de determinado ataque, sendo a contenção o objectivo imediato
  - *Recuperação* – a análise posterior dos efeitos das crises é essencial ao aperfeiçoamento dos métodos de resposta

Gestão de crises

- É essencial a elaboração de um plano de acção
  - Avaliar riscos, vulnerabilidades, estabelecer prioridades, preparar os recursos e agir em conformidade
  - Assegurar o cumprimento de todas as obrigações legais (protecção dos dados, das infraestruturas, dos acessos)
  - Elaborar novos procedimentos e comunicações em caso de incidente e retirar daí as consequências de conduta
  - Basear toda a actuação na cooperação com todas as partes envolvidas (clientes, fornecedores, autoridades)
- Para o sucesso da cibersegurança é necessário ter como ponto de partida a adequada e sã cooperação interna e com as diversas entidades competentes

Acção e Cooperação

- Ministério Público e Órgãos de Polícia Criminal (PJ) / SIS
- CNS – Centro Nacional de Cibersegurança (tem como objectivo a coordenação operacional em matéria de cibersegurança entre as entidades do Estado, operadores de serviços essenciais e prestadores de serviços na área digital)
- Rede Nacional CSRIT (Resposta a Incidentes de Segurança)
- ➢ Responsável pela interligação entre as diversas entidades responsáveis pela segurança informática (entes públicos e privados)
- ➢ Criação de ferramentas úteis para a prevenção e repressão de incidentes (cibercrime, ciberterrorismo, ciberespionagem)
- Cooperação internacional (EUROJUST, INTERPOL, EUROPOL, UE, NATO, OSCE)

IDEIAS FINAIS

- A legalidade compensa e a cooperação previne
- Os direitos só se exercem plena e legitimamente quando se cumprem e fazem cumprir os deveres
- Nem o direito resolve todos os problemas da vida, nem todas as acções em matérias litigiosas terão que ser necessariamente de natureza penal, mas todas as ofensas a direitos fundamentais têm que ter uma resposta jurídica justa e eficaz
- A um direito ilegitimamente negado, restringido ou retirado corresponde uma acção legalmente prevista para o afirmar, repor ou reconstituir

Cibersegurança e Cibercrime

Carlos Pinto de Abreu

23 de Março de 2017