

A “segurança da informação” – solução ou preocupação?

Apresentação do Contra-Almirante Mário Carmo Durão
No Seminário “2011: A Tipping Point for Data Security”
Embaixada dos EUA, Lisboa, 12 de Outubro de 2011

Enquadramento

Importância, abrangência e actualidade do tema “segurança da informação”

Como todos sabemos, a informação é um recurso vital para a generalidade das organizações ...

No entanto,

De tudo o que se lê ... em Livros, Revistas, Estudos, Relatórios, Legislação ...

Ou de tudo o que se ouve, ou se comenta ... em Notícias nos mais variados média, Conferências, Seminários ...

Verifica-se que há uma preocupação generalizada com a “segurança da informação” ...

Esta preocupação, hoje em dia, e como veremos mais à frente, é largamente potenciada pela utilização generalizada do ciberespaço (genericamente a Internet) ...

Desta forma, todos nós, mas sobretudo os que trabalham ou estão de alguma forma ligados às TI ...

Devem manter-se atentos ... sem que lhes seja possível ignorar o tema da “segurança da informação” ...

Tema, que ainda por cima, é muito vasto ... + de 45 tópicos diferentes no último ESORICS (European Symposium on Research in Computer Security)

É por isso natural que perante este cenário (de importância, actualidade e vastidão da “segurança da informação”) a principal questão, para a generalidade dos responsáveis de TI é simplesmente ... Que fazer?

E é esta a questão, a que certamente este Seminário, se propõe ajudar a responder ...

Proposta pessoal para a abordagem do tema

Pessoalmente, não sou um especialista de “segurança da informação” ... pelo que seria estultícia pretender falar perante tão insigne plateia sobre qualquer tema específico da “segurança da informação”

No entanto, sou também responsável de TI ... no MDN ... e tenho naturalmente grandes preocupações com a “segurança da informação” ...

Assim, perante o tema do Seminário ...

Optei por partilhar convosco essas minhas preocupações, que são certamente as da maioria dos responsáveis de TI ...

Preocupações baseadas na forma como vejo e sinto toda a problemática da “segurança da informação” ... em geral e em Portugal

para na parte final vos falar do caso concreto do MDN (que é o que conheço melhor)

mas que não deixa de ser o caso de:

uma organização grande e complexa ...

que é responsável por informação importante, volumosa e sensível ...

que, como qualquer outra organização, está sujeita a ameaças e ataques ...

que tem necessidade de garantir a “segurança da sua informação” ...

e em que é necessário saber o que fazer?...

Segurança da informação em geral

Falando então de “segurança da informação” ...

Como já falámos, a informação é vital para a vida dos Estados, das organizações e dos indivíduos ...

E como sabemos, as TIC são o suporte para o processamento, armazenamento e transporte dessa mesma informação ...

No que diz respeito à “segurança da informação”

Nos últimos 30 anos, a segurança da informação evoluiu de uma disciplina técnica para um conceito estratégico ...

A natureza das ameaças não mudou mas a utilização crescente do ciberespaço, de que tanto dependemos, possibilitou um novo mecanismo que permite aumentar a velocidade, a escala e a potência dos ataques dos cibercriminosos ...

A generalidade dos SI passou a estar em risco ...

As próprias infra-estruturas críticas, mesmo em tempo de paz, passaram igualmente a estar em risco ...

Em geral, a “segurança da informação” passou da previsibilidade para uma segurança orientada para riscos diversos ... mais difusos, na forma, na origem, no espaço e nos atores ...

E quando a “segurança da informação” é a principal preocupação, temos de optar entre estar ligado ou estar desligado ...

Naturalmente, numa sociedade globalizada, temos necessidade de estar ligados ...

Pelo que temos é de proteger a informação, fazendo uma cuidada gestão do risco ...

Nos dias de hoje, porém ...

Um outro aspecto a ter em conta, é o actual estado de crise de muitas economias ...

E em tempos de crise, o dilema da segurança vs investimento, é sempre uma questão importante...

No entanto ...

De acordo com o Global State of Information Security Survey® de 2011 da PWC, e das revistas CIO Magazine e CSO Magazine ...

Ainda que

se vivam tempos de rigoroso controlo das despesas ...

alguns sistemas de segurança comecem a ficar perigosamente obsoletos ...

os incidentes de segurança tenham diminuído mas os que ocorrem sejam muito mais preocupantes e devastadores ...

surjam constantemente novas ameaças e novos riscos ...

existem sinais de:

maior preocupação e consciencialização a todos os níveis das organizações com as implicações da segurança da informação ...

maior conhecimento e interesse pelas causas e as origens dos incidentes de segurança ...

maior disposição das administrações para investir em “segurança da informação” ...

E aqui temos certamente

um ponto de cruzamento com o tema do Seminário ...

“2011 ... Um ponto de viragem na segurança da informação”

Mas quais são as ameaças?

As Ameaças têm evoluído ... embora a natureza não se tenha alterado ...

Olhando apenas para os últimos 30 anos ...

Até meados dos anos 80's as ameaças eram essencialmente físicas ...

A comunicação de dados era essencialmente através de informação impressa ... o correio era o principal meio de comunicação de documentos ...

Nos anos 90's, com a Internet, o panorama alterou-se substancialmente ... passou a estar tudo "online" ...

No entanto, enquanto houve um enorme incremento na conectividade ... os aspectos da segurança nas redes foram deixados para trás ...

E as ameaças à "segurança da informação" passaram a ser veiculadas através das redes ... em consequência da sua generalização ... e das suas vulnerabilidades ...

Só no final dos anos 90's é que as organizações começaram verdadeiramente a investir em pessoas, processos e tecnologias orientadas para a "segurança da informação" ...

No início dos anos 2000 muitas organizações passaram a utilizar intensamente, por questões de produtividade, o email, as aplicações webizadas e o wireless, que passaram a constituir os principais veículos dos ataques ...

Hoje em dia, temos de acrescentar as redes sociais ...

De acordo com o Trustwave's Global Security Report 2011:

"Em 2010 o panorama da segurança da informação mudou. O alvo dos ataques mudou da infra-estrutura para os dispositivos ao dispor dos utilizadores finais que muitas vezes, pela sua acção, permitem aos atacantes o acesso a informação privada e sensível"

O que nos conduz a um novo cruzamento com o tema do Seminário ... "O ponto de viragem na segurança da informação"

No entanto, e procurando sumarizar as ameaças ...

A fraude, o roubo de identidade, o software malicioso (malware) e o spam (com as acções de "denial of service") continuam a ser as principais ameaças através das quais se materializam a maior parte dos ataques ...

Os riscos

Naturalmente para as organizações e decorrente das ameaças, os principais riscos serão:

A perda de operacionalidade ...

A negação de serviço ...

As implicações na continuidade do negócio ...

A protecção da imagem da organização ...

A importância do Ciberespaço

Neste enquadramento, de ameaças e riscos para a "segurança da informação" ...

Assume particular importância o ciberespaço ... de que já fomos falando ... mas sobre o qual é importante ainda realçar ...

O ciberespaço ... é essencialmente a Internet ... mas também as redes móveis (telemóveis, pagers), etc.

A importância da Internet na globalização da sociedade ... sociedade em rede

A importância dos serviços que disponibiliza ... correio electrónico, WEB, acesso remoto, trabalho colaborativo, transmissão de áudio e vídeo, educação, marketing ...

Hoje em dia, a nível empresarial, o "cloud computing" está na moda

O Social networking cresce exponencialmente ...

Os blogues e as redes sociais são um sucesso ...

No entanto, ...

A utilização generalizada do ciberespaço coloca inúmeros problemas de segurança potenciados muitas vezes pela própria internet ...

Dado que a internet não tem fronteiras ... não tem legislação universal ... não é governada por uma organização

Expressões como “phishing” ou “spyware” tornaram-se correntes e surgiram novos conceitos como cibercriminalidade ou mesmo ciberterrorismo ...

Neste enquadramento e mais uma vez a questão que se coloca é

como é que os países, as organizações ou mesmo os indivíduos, podem prevenir as ameaças à “segurança da informação” e combater a cibercriminalidade no ciberespaço?

Segurança da informação em Portugal

Qual é a situação em Portugal?

Baseado no Portugal Country Report de 2011 da ENISA (European Network and Information Security Agency) ...

Política de segurança da informação

Não temos definida uma política nacional de “segurança de informação” ... estamos na fase inicial ...

Não há uma iniciativa de gestão de risco a nível nacional ...

Existem apenas acções no sentido de definir uma estratégia nacional de “segurança de informação” ... mas sobretudo para o sector público ...

Entretanto, foi promulgada a Lei 109/2009 de 15SET, lei do cibercrime ...

Não existe um CERT nacional ... apenas o CERT.PT ...

CERT.PT responsável pela rede das universidades e pelo domínio. PT...

No âmbito do Plano Tecnológico têm sido promovidas várias iniciativas dispersas ...

Têm sido tomadas várias medidas de sensibilização para a importância da “segurança da informação” no ciberespaço, pelas autoridades e por organizações privadas e académicas ...

Iniciativas como “Internet segura”, (UMIC, ME, FCCN, Microsoft), “Linha Alerta” (Parte da Internet Segura) e “Segurinet” inserem-se nesta linha de acção ...

No entanto, apesar das medidas, Portugal é um país onde não existe informação generalizada e disponível sobre a utilização segura do ciberespaço ...

Por outro lado existem vários “players” ...

As autoridades: ICP-ANACOM, UMIC, CNPD

Os CERT: CERT.PT, CSIRT.FEUP ...

As organizações académicas: FCCN ...

Outras entidades: GNS, OSCOT, IPQ, DECO ...

Recentemente, surgiu uma iniciativa importante do IDN no sentido de contribuir para a definição de uma Estratégia Nacional de Informação

Mas se não temos uma política própria, estamos inseridos na União Europeia e numa política europeia de “segurança da informação” institucionalizada pela ENISA ...

Estamos por outro lado, inseridos na NATO que recentemente reviu o Conceito Estratégico tendo considerado prioritário o desenvolvimento de uma capacidade de ciberdefesa

Na área policial, através da Polícia Judiciária e da ASAE estamos inseridos em redes internacionais ...

O mesmo acontece em muitas outras áreas desde a banca á economia ... com ligações internacionais e preocupações de “segurança da informação” ...

De tudo isto, o que parece fundamental é a necessidade de definir e implementar uma Estratégia Nacional de informação ...

Que nos proteja de ciberataques, protegendo essencialmente:

as infraestruturas críticas

as redes informacionais

Para tal, será necessário um esforço concertado, nas áreas da cibersegurança, e da ciberdefesa do País

Segurança da informação no MDN ...

Entretanto vamos vivendo ...

O MDN sendo uma organização grande e complexa (Ramos, EMGFA, SCS's, IASFA) depende das TIC para o processamento, transporte e armazenamento da informação que lhe é vital para a operacionalidade ...

No MDN, em termos dos principais SI, existe essencialmente informação de gestão (na esfera de competência da SG) e informação operacional (na esfera de competência dos Ramos e do EMGFA) ...

Naturalmente, para qualquer tipo de informação, a “segurança da informação” é uma preocupação permanente ...

Relativamente à informação de gestão na competência da SG/MDN ...

Está subordinada à implementação de uma “política integradora” dos SI, architectada em:

Um sistema integrado de gestão ... (SIG)

Um Centro de Dados único ... (CDD)

Um sistema de comunicações integrado ... (SICOM a cargo do EMGFA)

No âmbito desta “política integradora” o SIG e o CDD assumem um papel relevante e decisivo no que diz respeito à informação de gestão ...

Importância do SIG

É um SI integrado (ERP SAP), estruturante para o MDN e de grande abrangência

As entidades ... , as áreas funcionais ...

Fundamental para a gestão do MDN

A dependência crítica para as entidades do MDN

Importância do CDD

A infra-estrutura fundamental de suporte do SIG

Aloja os sistemas legacy do MDN, EXE e MAR

Aloja ADM do IASFA

Aloja Intranet e Correio electrónico do MDN

Gere a Internet no MDN

Principal infra-estrutura de serviços partilhados da Defesa

Centro de Dados de grande dimensão que se pretende “uma referência na AP”

As preocupações em matéria de segurança da informação

Perante a importância do SIG e da maioria da informação alojada no CDD ...

Perante as ameaças à “segurança da informação” ...

Numa altura de crise na economia ... Sem grande margem de manobra para investimentos ...

As principais prioridades da “segurança da informação” no MDN são:

Continuidade do negócio

Criação de um Centro de Dados Alternativo (CDA)

Protecção da imagem do MDN

Conformidade regulamentar

Neste enquadramento ... a questão fundamental continua a ser

Que fazer? Que organização para a “segurança da informação”?

Como estamos organizados?

A organização da segurança aponta para:

Combater as ameaças externas e internas;

Com o objectivo de manter a integridade, disponibilidade e confidencialidade da informação;

As ameaças externas (Defesa do perímetro)

Intrusões

Negação de serviço

Seguimos as normas ISO 27001

Temos uma política definida e procedimentos estabelecidos

Temos uma DMZ para os serviços prestados ao exterior

Temos um ponto lógico único de acesso à Internet com várias ligações físicas

Temos instalado

Firewalls, IPS (log's e alarmes), VPN, WLC, Antivirus, Antispam

Não temos *um sistema integrado de monitorização e alerta de incidentes ...*

Não temos *uma ferramenta que tipifique ataques ...*

As ameaças internas

Acessos

Acesso dos utilizadores é controlado por gestão de identidade através do Directório

Rede está segmentada; cada entidade só tem visibilidade sobre o seu segmento

Recursos partilhados estão alojados no Data Center; acedidos com regras de acesso

Alteração obrigatória de passwords

Sistemas críticos

Redundância de equipamentos em todos os sistemas críticos

Servidores dos SI's críticos estão “clusterizados”

Desktop's e Laptop's

Sistema centralizado para gestão da configuração e monitorização (SCCM)

Sistema centralizado de distribuição de actualizações

Administração central do antivírus para todos os desktop no MDN

Backup's

Sistema de backup generalizado e centralizado

Armazenamento em 2 localizações distintas

Rotação de BK's diária, semanal, mensal e anual

Backup (on line) sem interrupção de serviço

Criadas imagens (SO + Aplicações) de todos os desktops/laptops

Armazenamento

Sistema de armazenamento redundante

Discos podem ser reconstruídos

Disaster Recovery

Existem planos de contingência ...

Existe a firme intenção e existem planos para a criação de um Centro de Dados Alternativo (CDA)

Considerações finais

A "segurança da informação" é uma preocupação ... não é uma solução ...

Está aqui a resposta ao título da apresentação ...

Mas é uma preocupação constante ...

Não existem organizações seguras, o que existe é um maior ou menor grau de segurança implementado ...

No entanto, é importante ter em consideração que mais segurança implica menos facilidade de acesso ... e a informação é para ser acedida ...

Donde, em cada momento, temos de nos organizar em função das ameaças ... e dos riscos ...

É importante que em cada organização exista uma estratégia para a "segurança da informação" ... e que se faça uma cuidada gestão do risco ...