

Segurança da Informação: Imperativo Nacional

Por Tito de Moraes

Recentemente, na sua declaração ao país, o Presidente da República trouxe à ribalta o tema da segurança da informação com a questão das vulnerabilidades. De todo este "folhetim" resulta claro que a definição de uma estratégia de segurança da informação é um imperativo nacional.

Na sua «declaração ao país» do passado dia 29 de Setembro, o Presidente da República interrogou-se sobre se seria possível alguém do exterior entrar no seu computador pessoal e conhecer os seus e-mails e se estaria "a informação confidencial contida nos computadores da Presidência da República suficientemente protegida?". A estas duas interrogações, acrescentou: "Foi para esclarecer esta questão que hoje ouvi várias entidades com responsabilidades na área da segurança. Fiquei a saber que existem vulnerabilidades e pedi que se estudasse a forma de as reduzir." A expressão "vulnerabilidades" entrou assim no léxico dos portugueses.

O Início de Uma "Novela"

Perante isto, a edição do semanário Expresso do passado dia 2 de Outubro, titulava em primeira página: "Conseguimos entrar na rede informática do Governo". Nos dias seguintes vários órgãos de comunicação social noticiaram o aumento exponencial do número de tentativas de intrusão nos sistemas informáticos de órgãos de soberania e sobre o reforço de medidas de segurança para proteger as mesmas. Por outro lado, responsáveis pelas mesmas ou em seu nome, assim como especialistas em segurança informática desmultiplicaram-se a vir a público falar sobre o assunto. O país despertara para a questão da segurança da informação e para a questão das vulnerabilidades dos sistemas de informação e comunicação. Ao seu mais alto nível.

Alertas Antigos

Apesar de me debruçar em particular sobre a segurança de crianças e jovens na Internet, o que tenho feito desde 2003, a verdade é que a consciência dessa

necessidade nasceu em 2001, em resultado do meu envolvimento profissional em questões relacionadas com a segurança da informação.

Alertas Mais Recentes

O rastreio de vulnerabilidades visando a sua descoberta, é assim algo com o qual estou familiarizado desde esse tempo. Nunca escrevi sobre o assunto pois esse tipo de rastreios eram conduzidos para clientes após a obtenção da sua autorização por escrito e, invariavelmente, este é um assunto sobre o qual as organizações não falam em público. Por razões óbvias, como este caso agora o demonstrou. No entanto, desde meados de 2008, que o projecto Nonius vem alertando de forma sistemática e periódica para o nível de segurança da Internet Portuguesa. O alerta mais recente data de Julho de 2009, considerando-o como "perigoso". A este nível, são curiosas duas referências:

- As redes de infra-estruturas do Estado revelam um maior índice de perigosidade do que as do sector Privado.
- A FCCN (Fundação Para a Computação Científica Nacional), entidade responsável pelo planeamento, gestão e operação da Rede Ciência, Tecnologia e Sociedade (RCTS) que serve as escolas e universidades portuguesas, entidade competente para a gestão do serviço de registo de domínios de .pt e que é a entidade responsável pelo CERT.PT (Serviço de Resposta a Incidentes de Segurança Informática), surge entre os 3 primeiros operadores de serviços Internet em cuja rede de infra-estruturas foram detectadas mais vulnerabilidades.

Ameaças Externas vs. Ameaças Internas

Nos últimos dias tem-se falado sobretudo na vulnerabilidade dos sistemas de informação e comunicação a ataques vindo do exterior. No entanto, se estes devem ser motivo de preocupação, como o indicam os alertas do projecto Nonius, a verdade é que os especialistas em segurança da informação tendem a considerar as ameaças de segurança vindas do interior das organizações como constituindo hoje maior motivo de preocupação que ameaças externas. Na realidade, estudos indicam que 80% dos crimes relacionados com os sistemas de informação são cometidos a partir do interior. Algo que é fácil de perceber.

As Ameaças Internas

As organizações geralmente tentam descobrir as vulnerabilidades dos seus sistemas, "tapar os buracos" descobertos e torná-los impenetráveis. Mas quem

conhece por dentro estes buracos e estas vulnerabilidades? Os funcionários e ex-funcionários de uma dada organização são as pessoas que estão mais "por dentro" de eventuais falhas. Daí que, geralmente, os funcionários descontentes, ex-funcionários ou funcionários recentemente despedidos ou até funcionários ao serviço de fornecedores externos e outras pessoas na posse de informação interna, sejam os mais prováveis responsáveis por quebras de segurança.

Estas são as pessoas que melhor conhecerão as fraquezas dos sistemas de informação e comunicação de uma organização e como os ultrapassar. São geralmente pessoas que acedem a zonas de acesso restrito e que podem estar na posse de palavras-chave não autorizadas que lhes conferem acesso a informação confidencial. No entanto, apesar do que digo acima, é preciso ter bem presente que muitas vezes estas quebras de segurança interna não são resultado de actos deliberados, mas antes de acções e erros involuntários.

Pessoas, Processos e Tecnologias

Daí que, como escrevi no artigo "[Começar a Construir a Casa Pelo Telhado](#)", para além de uma questão tecnológica, a segurança informática é sobretudo uma questão de pessoas e processos. Em face de tudo isto, fica claro o que há muito venho afirmando: Portugal não tem uma cultura de segurança. Ao nível da segurança da informação impera o princípio do velho adágio "casa arrombada, trancas à porta".

Quando a segurança da informação em órgãos de soberania é questionada e posta à prova publicamente, a definição de uma estratégia de segurança é assim um imperativo nacional. E se assim é, com a segurança nacional, com a segurança interna, imagine-se como não será com a segurança online de crianças e jovens.

Pergunta a José Sócrates

Perante isto, compreende-se [a pergunta que fiz a José Sócrates](#) em finais de Julho passado, e se na altura já não fiquei muito sossegado com a resposta, agora ainda menos.

Perante isto, continuo a não compreender como é que apesar de aprovada por unanimidade em 11 de Julho a [Resolução da Assembleia da República Nº 38/2008](#) (PDF), recomendando "ao Governo que promova uma campanha nacional sensibilização e prevenção dos riscos da Internet para as crianças, no âmbito de um Sistema Nacional de Alerta e Protecção de Crianças Desaparecidas e Abusadas Sexualmente, a ser difundida na comunicação social e nas escolas" e apesar da sua

publicação em Diário da República a 29 de Julho, tal campanha ainda não tenha sido vinculada. É algo sobre o qual, decididamente os cidadãos devem pedir satisfações aqueles que elegeram para o Parlamento e que estes devem reiterar ao próximo Governo.

Por fim, não deixa de ser irónico que, enquanto em Portugal se desenrola esta "novela", nos Estados Unidos se celebre Outubro como o "Mês Nacional de Sensibilização Para a Ciber Segurança". Pela sexta vez.

A terminar, apesar de todo o ruído em torno deste assunto na comunicação social, para o cidadão comum, pouca ou nenhuma informação ou conselhos foram fornecidos sobre o que são essas tais "vulnerabilidades" e sobre o que se pode fazer para as minimizar. Disso tratarei no próximo artigo.