manchete

Diário Económico
Universidades & Emprego
25-01-2016

Periodicidade: Diário | **Temática:** Recursos Humanos
Classe: Economia/Negócios | **Dimensão:** 348
Âmbito: Nacional | **Imagem:** S/Cor
Tiragem: 18714 | **Página (s):** 3

OPINIÃO

Como proteger a informação?

AGOSTINHO ABRUNHOSA
Associate Professor da AESE Business School

Somos internet-o-dependentes: facebook, compras, emails, estudo, música, rádio, televisão, etc. e um site em baixo tem potencial para incomodar e ser notícia. No entanto, não é apenas o risco de ficar em baixo, há o risco de informação ser roubada, vendida ou usada para fins menos lícitos. É também uma forma de protesto.

Se muitas pessoas começarem, a ligar de 5 em 5 segundos para um telefone podem bloquear todas as comunicações de entrada nesse número. É uma analogia simples para um tipo de ataque comum conhecido como DDoS (Distributed Denial-of-Service). Se um servidor receber um número de pedidos exagerado e sem nexo pode ir abaixo ou ficar vulnerável.

Inúmeras infraestruturas estão hoje automatizadas com base em sistemas informáticos. É remota a possibilidade, mas o que pode acontecer se esses sistemas ficam comprometidos? Que impacto pode ter numa sociedade se alguns serviços "falham"? São frequentes as notícias sobre ataques informáticos, mas existem outros riscos. Recordo um presidente que se esqueceu de códigos nucleares secretos no casaco que foi para a lavandaria.

A segurança absoluta não existe, até porque, por vezes, os ataques podem não ser no local onde estão as defesas. Usando uma analogia antiga, é possível comprometer a segurança de um castelo usando uma simples escada pela calada da noite. Uma password partilhada, ou usada numa rede sem fios vigiada, podem ser o elemento final para o ataque. Numa crise informática é preciso pensar em todas as vertentes: legal, concorrencial, fiscal, imagem, perda de confiança, mercados, etc. e saber como cobrir cada uma delas. Um caso de Harvard usado na AESE Business School refere três momentos críticos de gestão destas crises: o antes, o durante e o depois. No antes a palavra-chave é prevenção. É desenhar sistemas que reduzam o risco e procedimentos robustos para alterações nos mesmos. É convencer a gastar dinheiro para que nada aconteça. No durante é preciso resiliência. (...)No pós crise é preciso por "trancas à porta" e mitigar as consequências.

A AESE realizou uma conferência com o título "Conhece o risco de IT da sua organização?" orientada por Francisco Fonseca da Anubisnetworks e que esclareceu estas e outras questões nesta área tão crítica para a operação e continuidade das organizações.■