The Role of Security Breach Notifications in Improving Cyber Security

Steve Purser

Attended the universities of Bristol and East Anglia where he obtained a BSc. in Chemistry and a PhD in Chemical Physics respectively. He started work in 1985 in the area of software development, subsequently progressing to project management and consultancy roles. From 1993 to 2008, he occupied the role of Information Security Manager for a number of companies in the financial sector. He joined ENISA in December 2008 as Head of the Technical Department and is currently responsible for all operational activities of ENISA. Steve is co-founder of the 'Club de Securité des Systèmes Informatiques au Luxembourg' (CLUSSIL) and is currently the ENISA representative on the ISO SC 27 working group. He frequently publishes articles in the specialised press and is the author of 'A Practical Guide to Managing Information Security' (Artech House, 2004).

Resumo

O Papel das Notificações de Violação de Segurança na Melhoria da Cibersegurança

Neste artigo analisa-se como os procedimentos de Security Breach Notification (SBN) podem ser utilizados na melhoria da cibersegurança numa envolvente transfronteiriça. A ideia central assenta no pressuposto de que dados quantitativos são necessários para melhor se compreender as ameaças envolventes, ainda que se reconheça existirem fortes condicionantes que requerem a implementação de uma recolha estruturada de dados e uma análise cautelosa de tendências.

É feita uma distinção entre SBN e Data Breach Notification (DBN). Ambos os conceitos serão relevantes para os futuros desenvolvimentos de uma política de cibersegurança da União Europeia, sendo a sua implementação requererá a adoção de requisitos específicos e economicamente viáveis em ambos os processos. Por fim, serão descritas questões relacionadas com a implementação de tais processos num contexto transfronteiriço e transcomunitário.

Abstract

This article examines how Security Breach Notification (SBN) procedures can be used to improve cyber security in a cross-border environment. The central idea is that quantitative data is necessary in order to better understand the evolving threat environment, although there are some strong limitations on this statement and it is extremely important to implement the data collection in a structured way and to analyse any trends cautiously.

A distinction is made between SBN schemes and Data Breach Notification (DBN) schemes. Both schemes are likely to play a role in future EU policy developments relating to cyber security and implementations will need to take account of the specific requirements on both processes whilst remaining economically viable. Finally, issues related to implementing such schemes in a cross-border and cross-community environment will be presented.