Protecting Critical Information Infrastructures

Eduardo Gelbstein

Ed Gelbstein has over 40 years experience in information systems and technology, both in the private and public sectors. His experience includes being Information Technology Strategy Manager for the British Railways and Director of the United Nations International Computing Centre. He was also an advisor to the United Nations Board of Auditors and the French Cour des Comptes. Ed is currently Adjunct Professor at Webster University Geneva and the author of several books and articles as well as a regular speaker at international conference on security, risk, audit and governance.

Resumo
Proteção de Infraestruturas Críticas de Informação

O recurso aos sistemas de informação na gestão e operação de infraestruturas críticas cresceu exponencialmente em todo mundo, sendo que atualmente não existem infraestruturas críticas que não dependam fortemente de software, computadores e redes informáticas.
Nenhuma tecnologia é perfeita e lidar com erros de sistemas faz parte das responsabilidades daqueles que fornecem e operam esta tecnologia. A ubiquidade das redes globais como a internet criou um desafio adicional: tentativas, por vezes bem-sucedidas, de aceder a estas tecnologias por parte de terceiros com a intenção de interromperem estas operações ao abrigo de justificações que vão desde o simples desafio individual, ao ativismo e, potencialmente, a operações de natureza militar ou terrorista.
Os desafios associados à proteção de infraestruturas de informação crítica da qual a sociedade depende para funcionar, são variadas e complexas e têm de lidar com componentes passíveis de gerarem erros: pessoas, processos e tecnologia.
Este artigo fornece uma visão sobre estes desafios e aponta sugestões e referências quanto às melhores práticas.

Abstract

The use of information systems in the management and operation of critical infrastructures has grown explosively around the world and, today, there are such infrastructures that do not have a strong dependency on software, computers and networks.
No technology is perfect and dealing with malfunctions is part of the responsibilities of all those who supply and operate such technology. The ubiquity of global networks such as the Internet has created an additional challenge: attempts, often successful, to access such technologies by external parties intent in disrupting their operations for any of a number of reasons, ranging from "because I can" to activism and, potentially, military and/or terrorist.
The challenges of protecting the critical information infrastructures, on which society depends to function, are many and complex as they have to deal with three imperfect components: people, processes and technology. This article provides an overview of these challenges and includes pointers and references to established standards and good practices.