ENISA Takes on Cloud Security

Written by Marco Attard
21 February 2013

What happens if a cloud service on which the organisation of the future depend fails or gets hacked? This is the Critical Information Infrastructure Protection (CIIP) perspective ENISA takes in its latest report.

"From a security perspective, the concentration of data is a ‘double-edged sword’" Dr Marnix Dekker says. "Large providers can offer state-of-the-art security and business continuity, spreading the costs across many customers. But if an outage or security breach occurs, the impact is bigger, affecting many organisations and citizens at once."

Over the past few years we have seen examples of failures affecting large sites with millions of users, such as the 2012 Windows Azure leap year bug outage.

ENISA reaches 3 key conclusions:

- Critical infrastructure: Cloud services are becoming critical information infrastructure, since soon enough most organisations will use the cloud in critical financial, energy and transport sectors.
- Natural disasters and DDoS attacks: The cloud proves resilient in the face of both natural disasters and DDoS attacks difficult to mitigate through traditional approaches (servers on site or single data centres).
- Cyber attacks: Software flaw exploits can cause large data breaches affecting millions of users due to large concentration of users and data, despite physical redundancy.

ENISA has 9 recommendations for bodies responsible for critical information infrastructures, chiefly the inclusion of large cloud services in national risk assessments, the tracking of cloud dependencies and collaboration with providers on incident reporting schemes.

"Cloud computing is a reality and therefore we must prepare to prevent service failures and cyber attacks on cloud services," ENISA director Professor Udo Helmbrecht comments. "The European Cyber Security and Cloud Computing Strategies provide a roadmap for this."

Go Critical Cloud Computing-- A CIIP Perspective