ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Telecommunications Sector

Source: Deloitte Report

Case 2

False claims do real damage to a major ISP

Organization

A large internet service provider (ISP), hosting a nation's critical infrastructure.

Scenario

A teenage hacker gained access to hundreds of the ISP's servers and then published a list of user names and passwords he claimed to have stolen from them. This forced the company to temporarily suspend the email accounts of all affected users. It later turned out the data was obtained from a different company and not the ISP.

Attackers and motivation

The attacker was an individual teenager who was hacking for fun and ego gratification, bragging about his accomplishments in online forums.

Techniques used

A vulnerability in a website not related to the affected company was exploited to export data from the database containing customer information. The attacker then selected all users having email addresses from the ISP's domain in order to make the public (and the ISP itself) believe the ISP had been compromised.

Business impact

The ISP did not have the proper processes in place to determine if it had been compromised or not, and thus had to assume the published data had been stolen from its systems. In response, it was forced to suspend all affected email accounts, which angered a lot of customers and prompted many to switch to another email provider. Also, the fact that the ISP could not conclusively determine if the leaked data had actually originated from its systems gave the impression the company did not have a very good handle on security breaches.