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

High Technology Sector

Source: Deloitte Report

Case 1

Fraudulent certificates lead to bankruptcy and a national security breach

Organization

A certificate authority that signs security certificates for organizations globally.

Scenario

The internet is based on trust and certificate authorities are at the heart of this trust. Hackers with ties to a foreign government obtained illegal access to the certificate authority's servers and used it to generate fraudulent security certificates. These certificates were then used to enable fraudulent servers posing as the original servers belonging to highly used web services. This allowed the attackers to perform man-in-the-middle attacks, possibly intercepting and decrypting a tremendous amount of confidential communications.

Attackers and motivation

The individual who claimed the attack said he was driven by political beliefs. However, the way the fraudulent certificates were used and the fact that the attack took place over a relatively long period of time suggests state actors were also involved.

Techniques used

Apart from known hacker tools, some very complex attack scripts were used that were specifically developed to attack the certificate authority in question.

Business impact

The hackers generated more than 500 fraudulent certificates, which were then used to perform man- in-the-middle attacks against many well-known global services. The certificate authority could not guarantee revocation of the fraudulent certificates, which was completely unacceptable given that the organization's sole reason for existence is to provide certification that is 100% trustworthy. The certificate authority declared bankruptcy shortly after the breach was made public.