EASYAUDIT WHITE PAPER

Reporting a Breach: Tighter Deadlines in the EU

Every day, IT service companies report sensitive-data breaches to the competent authorities. Yet a long time can pass between the breach and the actual report, slowing the response of the people involved in the attack.

The issue had been debated for some time: in Europe there was no time limit requiring providers to report an attack, which caused complaints from many customers. It is not simple, however, to define the correct deadline for informing judicial authorities of a breach.

In the United States, where the issue was addressed earlier, each state has its own rules. In some states, notification "sooner or later" is enough; in others the deadline is around 45 days. The twenty-eight EU states therefore decided to tackle the problem directly, imposing a very tight deadline on IT service companies: no more than one day between the breach and the report to the authority.

Providers quickly responded to criticism over slow notifications: working with such short deadlines is impossible, they say, and consumers would pay the price. The reason is the difficulty of recognizing a cyberattack quickly and identifying who has actually been affected.

Imposing a twenty-four-hour limit risks making it impossible to truly understand the type of threat, inevitably creating false alarms. It would also be impossible to provide precise and complete notifications. Todd Hinnen, a Perkins Coie partner interviewed by SCMagazine, supports a maximum notification deadline only if it does not prevent proper investigation. The right timing may vary, he says, "but it should still not exceed 72 hours".