

Online Media Sector

Source: Deloitte Report



Case 3

Hackers redirect readers to fake news

Organization

A large news organization, with a strong presence both online (websites) and offline (newspapers).

Scenario

A hacker group with political ties tricked employees of a third-party domain registrar into revealing information that was then used to access domain name server (DNS) records, allowing the group to redirect all incoming web traffic to its own website.

Attackers and motivation

The attackers were hacktivists spreading propaganda and wanting to influence public opinion about events occurring in their region.

Techniques used

The attackers used social engineering, in particular spear phishing, to gain access to the reseller's DNS account. It then altered DNS records to redirect web traffic to its own server, which hosted a visually identical copy of the news website but presented altered facts.

Business impact

The attack tarnished the organization's reputation and credibility, which because of the organization's size and name recognition, also had a ripple effect on other news organizations. This caused readers to question the legitimacy of news stories they viewed online, and likely drove some to other news sources.