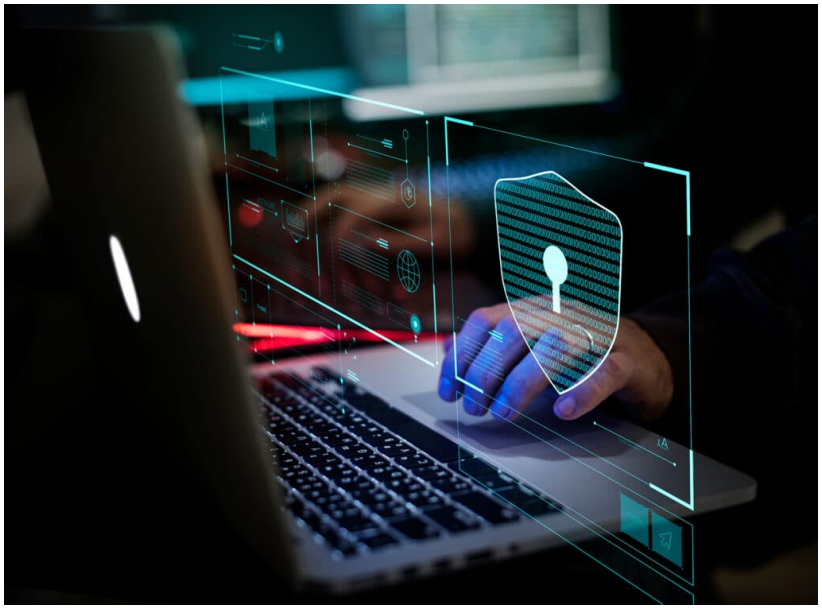
FMBusinessDaily

Report reveals UK financial services companies exposing ports to the Internet

3 years ago



A recent report by cybersecurity firm Rapid7 has confirmed financial services companies within the FTSE 350 are still leaving a number of ports, such as Telnet, RDP, and SSH, exposed to the Internet. This poses a significant risk to the security of financial and other sensitive data, as these ports are vulnerable to exploitation by cyber attackers.

The company recommends that financial services organisations take immediate action to secure their networks, including:

- implementing multi-factor authentication
- using firewalls to allow only trusted traffic to these ports
- regularly reviewing and updating their security protocols

By doing so, FTSE 350 firms can significantly reduce the likelihood of a breach and protect the tremendous amount of data they handle.

The report also found that financial services companies are particularly vulnerable to cyber attacks due to their reliance on online platforms and the sensitive data they store. Despite this, many organisations are still exposing vulnerable ports, putting themselves and their clients at risk. “Financial services companies handle some of the most sensitive information in the world, from personal and financial data to trade secrets and intellectual property,” said principal researcher Erick Galinkin. “It is concerning to see that many of these organisations are still exposing ports that are known to be vulnerable to attack. This puts them at risk of data breaches, which can be incredibly costly and damaging to both the company and its clients.”