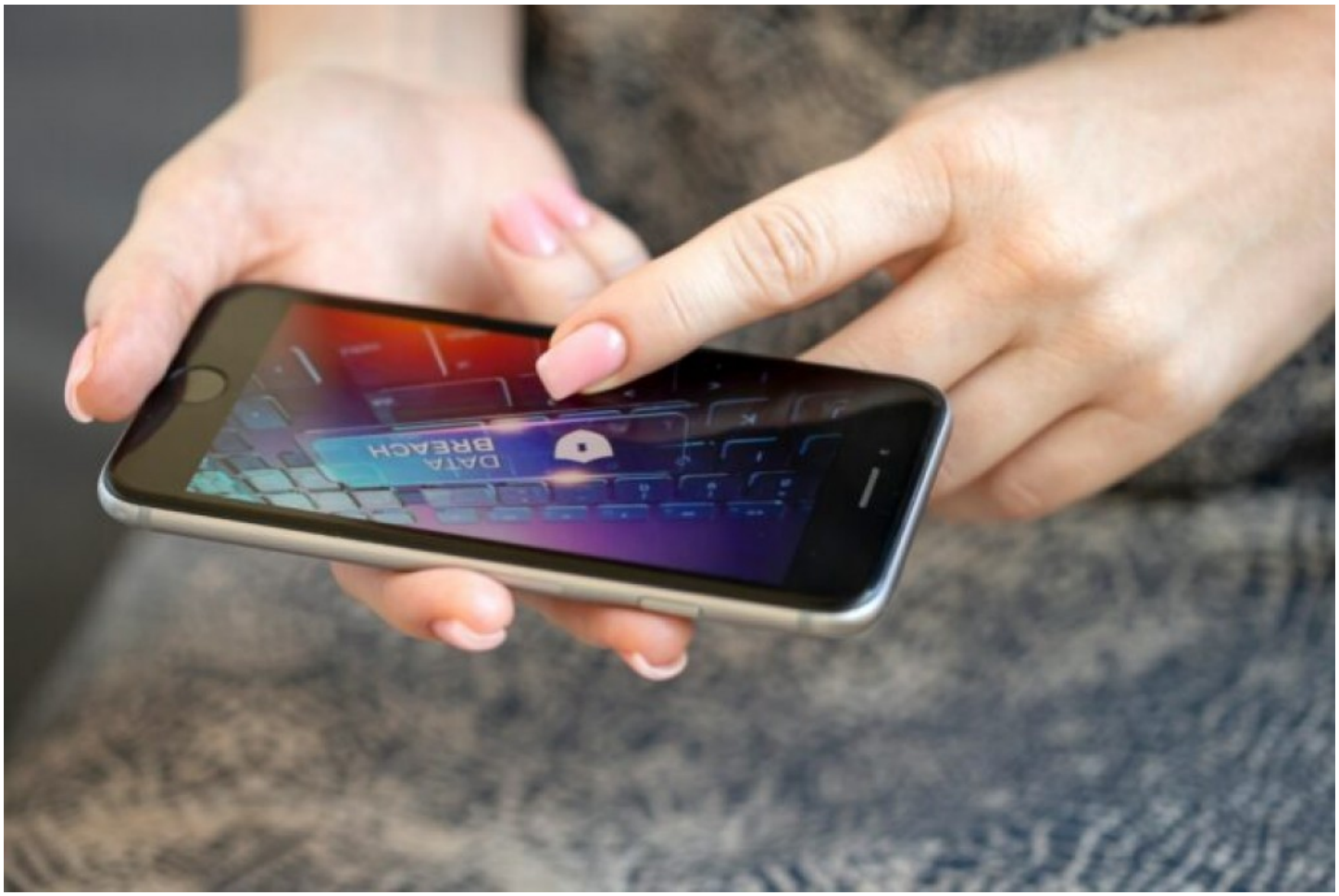
Geeky News Discusses the PSNI Data Breach and How Continuous Pen Testing Could Help

The breach has resulted in the information of over 10,000 personnel being exposed through a Freedom of Information request, which raises the question of how to safeguard against human error



Surrey, United Kingdom Aug 15, 2023 (Issuewire.com**)** - On the 9th of August, the Police Service of Northern Ireland (PSNI) faced a data breach. The incident—which is being called the worst data breach in the organisation's 22-year history—has revealed the identities of more than ten thousand staff members. Due to an internal error, the organisation gave out the names of all police and civilian personnel to a Freedom of Information (FoI) request.

The FoI request wanted a breakdown of staff ranks and grades, but the data provided also contained the surnames, initials, and some other information of over 10,000 people within the PSNI. Fortunately, the details don't include any private addresses. According to the report by the BBC, leaked addresses would have been "*catastrophic in terms of assisting terrorist groups to target officers.*"

Police officers in Northern Ireland used to be the target of violence from republican paramilitary groups during the Troubles. In the years after the Good Friday Agreement, they were attacked with guns and bombs. With the terrorism threat high in NI, this data breach could prove to be dangerous to the people affected by it.

Most members of the PSNI tend to keep their occupation and place of employment private. They are careful about who they share it with. Now, with this breach, several of them are concerned about their own safety and that of their loved ones. Geeky News, a technology and lifestyle platform, discusses the incident and how it might have been prevented.

The site reports that this year has seen several cyberattacks, the most notable being the ones on British Airways, University of Manchester, and Boots (the pharmacy chain). However, in those cases, the incidents were undertaken by threat actors using technology.

The issue is, this data breach happened due to human error—it's suspected that a junior employee published this information by accident in response to the FoI request. Now, questions are being raised about why there weren't any safeguards in place to prevent such a breach from happening.

However, security safeguards need to be reviewed and reevaluated continuously to be effective. Services like penetration and vulnerability testing from managed security service providers (MSSP) like DigitalXRAID have been said to prevent such cyber incidents. Penetration testing—or pen testing—is a service that tests an organisation's digital ecosystem for vulnerabilities that could be exploited. A comprehensive pen testing service will not only test networks, systems, devices, and applications, but also the human element.

Unfortunately, according to DigitalXRAID, pen testing "*only offers a snapshot of vulnerabilities found at the time of testing or vulnerability scanning.*" Instead, the company has recommended continuous pen testing as an alternative. The company claims this is a service that checks the organisation's cybersecurity on an ongoing basis. It allows the client to identify any weaknesses in its digital ecosystem as well as real-world processes before they can be exploited by cybercriminals.

Moreover, as evidenced by the PSNI data breach, information isn't just broken into through sophisticated hacks, claims the MSSP. It can also be stolen by exploiting unsuspecting people, through social engineering attacks. Pen testing, using features like red teaming, helps identify weaknesses in employee behaviour that could lead to compromised data. Such a service could help prevent incidents like the PSNI leak.

Media Contact

Geeky News

press@geekynews.co.uk

+44 20 3800 1212

Parallel House, 32 London Road, Guildford, Surrey

Source : Geeky News

See on IssueWire