HealthManagement
Promoting Management and Leadership

Cybersecurity tips for insider threats

Healthcare organisations need to take insider security threats seriously. As noted in a recent Verizon report, 60 percent of healthcare data breaches involve insiders.

There are two types of insider threats that healthcare organisations can face: malicious and accidental. Malicious actors aim to do harm; unintentional insiders are often employees that were trying to do the right thing but made a mistake or acted in ignorance.

"If an insider is bored, depressed, frustrated or angry based on a situation involving an organisation or workplace, there is a high likelihood that they may act out maliciously," says Mike McKee, CEO of insider threat management company ObserveIT. "Money is another significant motivator for malicious insider threats."

Even politics can contribute to security risks. Incidents of state-sponsored insider threat attacks and corporate espionage have been reported.

Meanwhile, unintentional insider threats are often caused by human error or ignorance. For example, an employee or contractor with access to the organisation's systems and data may be a risk for becoming an insider threat if they aren't necessarily tech-savvy or used to considering the security implications of their actions.

Healthcare organisations can take administrative countermeasures to protect themselves against insider threats.

"These include continuous workforce education, active training via simulated phishing emails with immediate feedback and training, and progressive disciplinary measures for repeat offenders, although this has been slow to adopt in my experience," says Fernando Martinez, chief digital officer at the Texas Hospital Association, which created and promotes a cybersecurity awareness programme.

In addition, technical countermeasures can be taken to protect the organisation's digital assets. These include disabling hyperlinks and document execution from emails, flagging emails from outside of the organisation, and using third-party security software, host-based intrusion prevention systems, according to Martinez.

For his part, McKee says the best way to mitigate risk associated with both intentional and unintentional insider threats is by monitoring user activity and implementing a formal insider threat programme to decrease risk. This view echoes a key recommendation included in HIMSS 2017 cybersecurity report: Implementing an insider threat management programme is more effective because rules, formal policies and sanctions can be applied and enforced consistently.

A monitoring solution should include a collection of data: capturing rich metadata including timestamp and duration of a session, login account, system name, the far endpoint the user came in from and more provides organisations the context of user actions before, during and after any incident or out-of-policy behaviour, McKee explains.

Such technology also helps in detecting risky activity and anomalous user behaviour, McKee adds. Behavioural analytics can continually analyse user activity to detect actions that are out of role, suspicious, or in violation of the formal insider threat programme. And live session response allows healthcare administrators to receive real-time alerts when an unauthorised or suspicious activity takes place.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 14 Aug 2018