HealthManagement
Promoting Management and Leadership

Experts argue context matters in healthcare IT security

Protecting sensitive health data and patient records is a challenging task for infosec teams. In a large hospital, for example, multiple users have access to patient data in the electronic health records system (EHR). How do you tell if any of these users is accessing the system with some hidden agenda, such as trying to steal information?

It's important for the industry to move beyond "statistical anomaly detection" (i.e., the count of accesses to the system) and focus on "the context of the access," said Daniel Fabbri, assistant professor, biomedical informatics and computer science, at Vanderbilt University, and founder and CEO of Maize Analytics. “Moreover, there are tons of timing eccentricities to consider in healthcare that must be thought through. For example, a doctor sees a patient but does not write a note until 24 hours later.”

EHRs generally have an open environment so that employees can access any patient’s data after logging into the system. As such, role-based access controls are limited.

“Further, employees are mostly well behaved,” Prof. Fabbri said. “Thus, occasional inappropriate accesses, snooping or identity theft, for example, are buried among normal treatment operations. Unlike other environments that treat a user as exclusively bad or good, in healthcare the user can be both good and bad on a single day.”

With these factors in mind, security approaches that look at the access login isolation, without clinical context, can only detect a few types of threats, and may even miss breaches, the professor explained.

“Other statistical anomaly detection systems attempt to identify ‘normal’ access patterns, and then alert on outliers,” he said. “The major challenge here is defining what is normal given the extremely dynamic nature of patient care, consultation services and constantly rotating clinical staff.”

One well-defined way to capture normal or appropriate behaviour is to understand the clinical or operational reason why an access occurs. If there is a reason for the user to access a patient’s record, then the access is likely appropriate.

The clinical context necessary to make such a decision is already stored in the EHR and can be leveraged to infer why most EHR accesses occur. Accessing a patient’s record without a valid reason is suspicious.

“The importance of context-based methods is that they not only tell you if an access is good or bad, but also the reason why, with the evidence for the decision, thus providing transparency rather than a black box,” Prof. Fabbri explained.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Wed, 4 Oct 2017

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.