Getty Images

SECURITY > THREAT MANAGEMENT

How Boston Hospital Changed Its Approach to Protecting Data

After discovering how exposed its sensitive information was, Beth Israel Deaconess Medical Center decided it needed external help in protecting data.

Karen D. Schwartz | Apr 20, 2020

One day in early 2017, the payroll department at Beth Israel Deaconess Medical Center in Boston noticed irregularities in three direct deposits. Thanks to a major miscalculation on the part of the attackers — they wired three direct deposits to the because it meant that bad actors inside the system had access to everything inside PeopleSoft, the hospital's system of record. That included a lot of p identifiable information (PII), from names and addresses to Social Security numbers.

Soon afterward, other problems came to light. Some employees who opted for paper paychecks instead of direct deposit, for example, found that their accounts had been changed to an offshore account.

When investigating further, it became clear that there was yet another problem: People could easily see sensitive information on monitors in nursing stations simply by looking when they were unattended. While clinicians and nurses who used workstations are supposed to clear the screen when finished, they would often neglect to do so because they would be called away suddenly. In addition, about 7,000 of the hospital's 12,000 employees use shared workstations, which exacerbates the problem of "over the shoulder" vulnerabilities.

"We realized that if we're worried about people who are in Africa looking, we should also be concerned about people who are actually looking over the shoulder of our employees engaged in active sessions," said Bennett Walker, manager of PeopleSoft development and administration at BIDMC.

At the time, employees accessing the PeopleSoft system entered through a portal, supplying a username and password. But it clearly wasn't enough for protecting data. Walker's team wanted to provide higher levels of protection for everyone entering the network, both internally and externally.

The first attempt was to add two-factor authentication throughout the organization. However, it didn't work with PeopleSoft because employees couldn't get access to the applications they needed. Today, PeopleSoft provides some level of data masking, but at the time, it could not address the issue.

Clearly, it was time to look for some external help. The team set out to look for a solution that was as flexible and configurable as possible without i user experience. Appsian's ERP Data Security Platform, which focuses on securing enterprise resource planning (ERP) systems, was the winner.

The Appsian security platform allows BIDMC to mask sensitive data for both employees and dependents along with direct deposit information. That solved both problems: external hackers attempting to infiltrate the system and "over the shoulder" data sensitivities.

As the team began to get comfortable with the platform, the IT staff began to notice additional features they hadn't focused on at first. For example, the system produces logs that detail performance time of online access, as well as greater detail about where users are logging in and what they are accessing while logged in.

While users may not be doing anything wrong, the information can be useful in directing people away from dangerous activities, as well as blocking access by location.

"In the past, we may have suspected that a user was looking at something they shouldn't have been looking at, but this gave us the proof because we could see it in the log," Walker said. "So we don't end up chasing our tails to try to find something based on what the user says. We can now look at the data and confirm it."

The team also has extended the use of the security platform to non-production environments, for things like compensation data and paycheck information. With this capability, the team can enable access, disable it or override it for privileged users.

As time goes on, the IT team began thinking about other security measures they could put in place. One of the first was focusing on multifactor authentication some transactions inside the organization.

0 COMMENTS

RECOMMENDED READING

looking through a magnifying

McAfee Reworks Enterprise Security Manager for the Cloud

JUL 14, 2020

hands typing on a laptop

How to Get the Most Out of Your Penetration Tests

JUL 13, 2020

Cybersecurity

As Offices Reopen, Hardware from Home Threatens Security

JUL 10, 2020

security alert on laptop

Proofpoint Insider Threat Platform Detects, Prevents Risks

JUL 04, 2020