Securing Online Learning Systems (Oct 07)

By Brian Summerfield

Information security probably doesn't cross the minds of learning leaders very often, if it ever does. Yet, given the increasing number of Web-based development offerings — not to mention a frequent lack of understanding of online threats on the part of employees — this should be a concern for the people in charge of the learning function.

Martin Rico, CEO of Inspired eLearning Inc., a provider of security awareness training, custom e-learning development and learning management system (LMS) software, said this problem should be a "very high priority."

Because he is a former information security consultant, that view isn't too surprising coming from someone like Rico. But in a business environment that includes issues such as compliance and zero-day threats, one can hardly deny his point.

"If you're hosting sensitive information, then you obviously don't want anyone accessing it," he said. "If there's a hole in any of the underlying technology, it could affect it. Data integrity is also very important because you need the records to accurate. The thing about LMSs and e-learning in general is that they're great things to outsource. A lot of companies do it that way, and the LMS is hosted, meaning it's not on their network. Because of that, it becomes a whole new category of risk."

In regard to security for online learning solutions, the threats are the same as the ones for any Web-based system, Rico said.

"The fundamental technology is a learning management system's server-side software — it can be written with ASP.NET, PHP, JSP and so on," he explained. "I don't know if there's anything particular to e-learning because a learning management system is really a database application and subject to the same vulnerabilities as any other system. It's all Web technology, so it's really subject to the same threats that all Web technologies are: viruses, worms, phishers and that kind of thing."

Because they're essentially no different from any other Internet application, Web-based learning systems can be defended with the standard tools of the trade. These include anti-virus and anti-spyware software, data encryption and firewalls.

"The minimal thing you should do is have a Cisco firewall on the network and also an onboard firewall on the system itself," Rico said. "You want a layered-defense architecture."

He added that most of his customers were aware of these issues to some extent, and some actually have him explain how his solutions are secured. A few of his clients have even urged IT professionals at their company to conduct "ethical hacking" exercises on the system.

For the time being, most of the "black hat" hackers don't seem to be too interested in — or even aware of — online learning solutions. But they are attacking tangential systems, and they eventually might find their way to the corporate LMS.

"It's probably off their radar screen," Rico said. "I think a knowledge base would be a more likely target for them, that is, a place where everyone's contributing information or a document repository. That would obviously be a gold mine for a black hat. Sometimes, they're the same system, but oftentimes they're not, or they're an add-on component."

Along with the technical tools, an effective way to defend against these online threats is with end-user education on best practices for using Web-based systems

"It's not particularly for an LMS, but in general, it's important for them to understand what's encrypted and what's not, what's on the Internet and what's not and why that's important," Rico said. "Everyone has a driver's license because if you just let anyone behind the wheel of a car, they could hurt somebody. "It's the same thing for letting someone on your corporate network — they could really hurt the company if they use that system in the wrong way. You have to train them on all of the best practices. When you train them on how to use Web applications in general in a secure way, then they'll also learn how to do it with an LMS."

CIomedia, ©2007 Media Tec Publishing Inc