

Computer Security: Stop Playing With Hackers

February 26, 2007

By [Deborah Gage](#)

The Problem: An online gaming company, K2 Network, is threatened by hackers who attack Web sites to extort money from players or steal their gaming assets.

The Details: K2 licenses games from developers in Korea and builds online gaming communities in the Western Hemisphere. Its four games—medieval fantasy, war, golf and a dragon-battling contest—are designed to accommodate millions of players at once and are played simultaneously by people all over the world. Players can enter the game for free, but they have to buy assets from K2—five extra swords to fight dragons, for instance—if they want to get deeply involved. Players may spend years accumulating assets, which are traded on eBay and on gaming auction sites. K2 also runs discussion forums for players, hosts gaming events and processes payments.

K2's Web sites have never been breached, according to vice president of infrastructure David Lee. But the company loses money if the sites are down, and it does not want its database exposed to the type of attacks that plagued another multiplayer game, Second Life, which warned in September that information on its customers was compromised. K2 also wants to improve its own software development process so its applications are more secure.

The Solution: Two products—a firewall appliance, the NC-2000 AG from NetContinuum, to protect K2's Web applications against attacks; and the ClickToSecure managed service from Cenzic to minimize flaws in the applications that hackers can exploit.

Nobody thought about [security](#) in the early stages of K2, Lee says. (The company was founded in 2001.) But by the time K2 launched its first game in North America in 2003, hackers were becoming a force in the industry. What Lee describes as "traditional I.T. security"—Secure Sockets Layer certificates to encrypt communications with players buying assets, for instance—while necessary, did not offer enough protection. K2's network was still open to people who knew how to exploit flaws in Web applications using techniques such as SQL injection, where a hacker types commands into a browser that fool a database into revealing its contents. These techniques work on many sites because they are poorly coded. In addition to games, K2 has the usual set of back-office business applications.

"Even with the best engineers, we always have vulnerabilities in coding," Lee says. "Code is so complicated."

K2 uses the two security products in concert to detect flaws in its software, make sure those flaws are not reintroduced during development, and to protect its

software against attacks. CenZic's product remotely probes applications the way a hacker would and reports any vulnerabilities it finds, along with suggestions for fixing them. CenZic has a team that tracks hacker activity and flaws so its products stay current. NetContinuum's product is a box that sits in front of a [Web server](#) to intercept and examine traffic. Suspicious traffic is blocked. "It does everything CenZic tests for and makes sure it does not happen again," Lee says.

The Result: K2 spent close to \$250,000 on security in 2006 and expects to spend the same this year. But the company saves the cost of three people doing development and quality assurance on its software applications—at \$45,000 to \$60,000 each, plus benefits—and can focus those resources on other projects. Right now, Lee is working with CenZic to get audits of K2's software on demand rather than on CenZic's schedule. He expects that feature to be addressed in a new product.

Copyright (c) 2007 Ziff Davis Media Inc. All Rights Reserved.