Forbes.com

Web Security: Xtreme Exostar

10.07.02

If you think a padlock in the corner of your browser is enough to keep your company's data safe, read on. In August, a 23-year old hacker nicknamed RaFa broke into a highly secure NASA database, and stole 43 megabytes of sensitive design data about planned space vehicles. The documents were created during a collaborative effort by Boeing, Aerojet and Pratt & Whitney.

Members of the defense business bristle at the thought of security breaches. So when companies such as **Boeing** (nyse: BA - news - people), Rolls Royce, **Lockheed Martin** (nyse: LMT - news - people), BAE Systems and **Raytheon** (nyse: RTN - news - people) invested $100 million to create online aerospace marketplace Exostar two years ago, they decided that they needed to implement no fewer than 87 security requirements. Among them: the highest level of data encryption not only while data is in transit but even while it is stored in the database. Exostar also maintains detailed background information on each user and a 12-month record of every file being accessed, what changes were made, by who and allows no one person or company (even at Exostar) to have complete access to all the data.

To create this highly secure environment in real time, Exostar's Herndon, VA.-based staff turned to Needham, Mass.-based PTC for its collaboration system?the underpinnings of the site. It hired @stake, a security company to incorporate additional security. Exostar also licensed security software from a number of vendors including Netegrity, which authenticates who the participants are; Webex, which offers Web conference systems based on secure socket layer; and eVincible, which encrypts data as it travels between networks and while it is stored on a server. It turned to Symantec to protect its network from viruses and it enlisted the services of Maven, a company which continually fakes hacker attacks into the system looking for weak points.

Rolls Royce, which won the contract to build the Trent 900 engine for Airbus's new 550-person A380 jet liner, recently put Exostar to the test. It used Exostar's electronic collaboration service so that its engineers could share CAD patterns and project management systems with other design engineers at Fiat-Avio, Goodrich Corporation, Hamilton Sundstrand, Honeywell, and Volvo.

When the project began, Rolls Royce appointed a manager who logged onto the system to start a session. Then Verisign verified the project manager's identity and authority to work on the project. Verisign gave the project manager a password and a digital certificate?a type of cyber passport to verify online identity. The certificate resided on the manager's computer so it was only possible to access the system from that computer. The manager then invited others to join the project and he specified the level of access to which each user was entitled.

Once that was completed the partners were ready to share information. While the engineers?located from Derby, England to Chandler, Arizona?worked on the same document using their personal digital certificates for verification, the file itself was encrypted with a 128-bit key.

After the session ended, the file was then sent to Exostar's data center, which provides high levels of physical and network security. Then, when another project member wanted to access the file for revisions, it was encrypted again before traveling over the Internet to his desktop, where it remained encrypted until the engineer with the authorized key opens it.

Overkill? Probably not if you are in the defense business. Indeed, today Exostar has over 11,000 members who think it's worth it. RRob Savidge, the chief engineer for the Rolls-Royce Trent 900, estimates that by collaborating over the Web, Rolls Royce saved as much as 60% on its travel budget, reduced project management errors by up to 50% and cut the product development cycle time by up to 40%. And so far, no break-ins.?Niall McKay

Back to article.