TECHWORLD
The UK's infrastructure & network knowledge centre

08 October 2004

SANS unveils Top 20 security threats

Instant Messaging and P2P software jump into 2004 charts.

By Scarlet Pruitt, IDG News Service

The SANS Institute has released its annual Top 20 list of Internet security vulnerabilities.

Listing the top 10 problems for Windows and for Unix, the list aims to point companies in the right direction by flagging up the most common and most significant holes in people's system and provide advice on how to plug them.

"When you tell your systems people to test for thousands of vulnerabilities, your enterprise comes to a stop. What the Top 20 does is give you a place to start your remediation each year," said SANS director Alan Paller.

The SANS list is compiled from recommendations by leading security researchers and companies around the world, from institutes such as the National Infrastructure Protection Center and the UK's National Infrastructure Security Coordination Centre.

Topping the Windows list is Web servers and services, while the Unix list leads with BIND domain name systems. While each entry represents a sometimes broad category, the 100+page SANS document goes into specific security holes in the categories, and instructions for correcting them.

Many of the vulnerabilities have made the list before, but there were some surprises this year, according Ross Patel, director of the Top 20 list. Vulnerabilities in file sharing applications and instant messaging (IM), which ranked seven and 10 on the Windows list, respectively, represent a fairly new categories of risk, Patel said.

"There was almost unanimous concern among experts around file sharing and peer-to-peer," Patel said. As with IM, file sharing applications are simple and operational in nature and security concerns are often overlooked, Patel said. Web browsers, at number six on the Windows list, were another hot topic. "Hands down Web browsers for Windows were the topic that caused most of the harm, pain and passionate debate for experts from every continent," Patel said.

With the number of vulnerabilities in Microsoft's Internet Explorer browser prompting some security experts to suggest earlier this year that users switch to other browsers, list contributors were left wondering if they should recommend the same, Patel said.

However, they finally decided that the move was too much to ask, and that they should endorse securing whatever platform a user chooses. In fact, this year for the first time this list gives instructions on how to deal with flaws on various software platforms. "We tried to make the list as relevant as possible this year," Patel said.

According to Gerhard Eschelbeck, chief technology officer at network security firm Qualys, and list contributor, the Top 20 is widely used by organisations as a security benchmark. "There is a consensus among people from the industry and academia that this is the list of the most critical vulnerabilities," Eschelbeck said. "With 50 new vulnerabilities announced a week, or about 2,500 a year, the challenge is for companies to decide which ones they should be looking at. It helps them prioritise," he said.

The full list can be found on SANS's site at www.sans.org/top20/.

---

previous Top of Page Security » News next
