Tech Center: Database Security

E-mail this page | Print this page | BOOKMARK

Shell Employee Directory Leaked, Allegedly By Activist Workers

Oil company acknowledges leak, but says it isn't sure current employees did the deed

Feb 12, 2010 | 02:31 PM

By Tim Wilson
DarkReading

The names and phone numbers of more than 170,000 employees and contractors at Royal Dutch Shell have been emailed to environmental and human rights campaign groups, the oil company acknowledged today.

The database, from Shell's internal directory, gives names and telephone numbers for all of the company's workforce worldwide, including some home numbers, according to a story in the *Financial Times*. The e-mail was ostensibly sent by disaffected staff calling for a "peaceful corporate revolution" at the company.

The database was emailed with a 170-page cover note, explaining that it was being circulated by "116 concerned employees of Shell Oil dispersed throughout the USA, the UK, and the Netherlands" to highlight the harm allegedly done by the company's operations in Nigeria, according to the Financial Times.

Shell confirmed the database was genuine, but said it did not pose a security risk because it did not include home addresses, according to the news report. The company said it was investigating the security breach, but did not believe the claim it had been leaked by disaffected staff. So far, no Shell employee has admitted playing a role in the data theft.

The leaked information is about 6 months old, suggesting it could have been taken by a former employee, Financial Times said. Shell cut 5,000 jobs last year and recently announced a further 1,000 job losses for this year.

The e-mail was sent to a handful of campaign groups, including Greenpeace, and to www.royaldutchshellplc.com, a Website used to air grievances about Shell, the report said.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's *editors directly, send us a message.*

Discuss This

Add Your Comment:

Please login or register here for a free Techweb account to post

XML Subscribe to RSS

» Write To Editor
» Reprint This Article
» Download Top Reports

Learn best practices and specific tips for effectively securing Oracle, SQL Server, DB2, MySQL and Sybase environments, including tracking security vulnerabilities, the anatomy of buffer overflow vulnerabilities and database auditing.

Databases at Risk: Current State of Database Security (ESG Research)
This recently published ESG report analyzes the current state of database security -- concluding it depends upon too many manual processes -- and also offers concrete steps to improve database security across the enterprise.

Database Security Newsfeed

- PacketMotion Simplifies PCI DSS Compliance With New Virtual Segmentation Solution
- Dataguise Announces Dgmasker Application Templates
- Study: Server Virtualization Still Growing
- Secerno Debuts Data Protection At 230,000 Transactions Per Second
- Facebook Automates Sensitive Data Discovery
- Oracle Announces Latest Release Of Oracle Audit Vault

MORE NEWSFEED >>

Web 2.0 Blog
Wolfe's Den

About TechWeb | Advertising Contacts | Become a Member / Membership Benefits | Contact Us
Feedback | Reprints | Technology Marketing Solutions | TechWeb Digital Library / White Papers | TechWeb.com

Dark Reading Home Attacks and breaches Vunerabilities Application Security Client Security Perimeter Security Security Management
Storage Security Encryption NAC Antivirus Privacy Blogs Security discussions

Newsletters Video Webcasts Live events TechWeb Digital Library Registration/membership About us
Sales and marketing contacts Send us a tip or comments Site map Technology Marketing Solutions