

Kaspersky Offering New Secure Industrial Operating System

By [The Moscow Times](#)

October 16, 2012



Eugene Kaspersky, pictured, said that his Moscow-based company is in talks with government institutions about installing the new operating system.

DUBAI — Antivirus-software company Kaspersky is developing a secure operating system to run computers inside nuclear power plants and other vital infrastructure and industrial plants, its founder and chief executive said.

Eugene Kaspersky, a Russian computer scientist who became a multimillionaire cybersecurity expert, said at a news conference in Dubai that the system was at the prototype stage and that his Moscow-based company is in talks with government institutions about installing the new operating system.

He declined to identify any, saying the talks were confidential.

Energy and water plants, factories and transportation systems are typically run with

supervisory control and data acquisition, or SCADA, systems accessible via conventional computer networks, making them vulnerable to hackers, Kaspersky said.

SCADA software is sometimes left unaltered for decades, which means that it does not get updates to protect against security bugs as they are discovered.

"It's not possible to design SCADA in a secure way, so the most obvious solution is to have a secure envelope that monitors what's going on within SCADA," Kaspersky said Tuesday. "Engineers travel with laptops, USBs, so even if the system is disconnected from the Internet, there is traffic."

Hacking was once seen as the preserve of rogue programmers working alone or in small groups. They usually targeted company websites and caused little long-term damage.

But the rise of "hacktivist" collectives and suspected state-sponsored cyberattacks has shifted the threat toward government-run institutions and energy, transportation and telecommunications networks.

Many such plants use firewalls designed to protect SCADA systems from being infiltrated by malicious bugs. But Kaspersky said he was developing an entire security-focused operating system to beef up their security further.

Some 30,000 computers at Saudi Arabian state oil producer Saudi Aramco were infected in August, although there is no evidence that the virus got into its industrial control systems. But the Stuxnet worm, which penetrated Iran's nuclear enrichment facility, is now freely available on the Internet.

"After Stuxnet, the attacks on Aramco and other incidents, governments and enterprises are listening," Kaspersky said.

Earlier this month, U.S. lawmakers said China's top telecom-equipment makers should be shut out of the U.S. market because they pose a potential security threat, but Kaspersky was unconcerned that his new operating system might attract similar concerns.

"This system is quite compact," he said. "It's easy to check; it doesn't have extra functionality. You own it."

Related articles:

- [Internet Business Expands While Restrictions Grow](#)
- [IT Sector Suffers from Brain Drain](#)
- [5 Reasons Why St. Pete Is a Leading Tech Hub](#)

Original url:

<https://www.themoscowtimes.com/2012/10/16/kaspersky-offering-new-secure-industrial-operating-system-a18642>