



## How Russia's biggest bank fights off its attackers - with a little help from a VC fund

**Summary: The head of IT strategy at Russia's biggest bank sees the cloud as a necessary evil and is investing in security startups to deal with hackers that want to get into its systems.**

By [David Shamah](#) for [Tel Aviv Tech](#) | December 2, 2013 -- 08:49 GMT (00:49 PST)

The rumor that Russian hackers never attack Russian banks is a canard, according to Mircea Mihaescu, the head of IT strategy at Russia's biggest bank Sberbank. "Not only do hackers attack my bank — they use us as a 'sandbox' to try out new and more powerful hacks before 'exporting' them to the West."

That 'export' business has been enhanced by the cloud, which gives wrongdoers new attack vectors, and extends the severity of headaches for people like him, whose job it is to mitigate the threat they present.

Russian banks are fighting off swarms of attacks, according to Mihaescu. "We appear on the top ten lists of numerous security companies that gauge the number of attacks on institutions," he said. "The hackers figure that if they can get through our defences, they can get through anyone's."



Mircea Mihaescu. Image: Sberbank

And those defenses are substantial, according to the IT chief. Sberbank (half private, half state-owned) has 80 million customers in Russia and Eastern Europe, while over 250,000 people work for the bank — 15,000 in IT alone. "We have a large staff dedicated to preventing hacks — it is one of the best teams in the world," he said.

Very often, Mihaescu said, Sberbank finds itself the victim of zero-day attacks — including some very weird ones, which he declined to describe, in order to not alert the malware writers to Sberbank's knowledge of their methods.

Sberbank takes security so seriously, in fact, that it runs a venture capital fund that invests in security tech companies. "We have invested in several companies, in Europe, Russia, and in Israel," Mihaescu said. The bank also hires white-hat hackers to fight back against its would-be attackers.

Mihaescu is in charge of IT strategy and tech innovation — so it's his job to stay on top of the tech news, and be aware of the latest in online security, an area Israel specialises in. In Israel for Go4Europe, an event geared towards cementing business ties between Israel and European countries, Mihaescu said that his bank has partnered with several Israeli tech security firms to eliminate some of the headaches involved in securing accounts.

### A change of cloud

The advent of the internet as a banking environment hasn't made his job any easier, he said. "Customers want the convenience of the cloud and they want banking apps to work the way other apps do, so if we are going to distribute an app that customers are going to want to use, it has to work in a manner that they are used to," Mihaescu said. "That means we have to do a lot more work on the back end in order to secure transactions."

One strategy Sberbank is using successfully is moving transactions from a public cloud to a rigidly-controlled internal cloud. Under that scheme, customers make a transaction request using an app or a browser, accessing Sberbank's website. As soon as a transaction enters the stage where private information is being processed, the transaction moves to a private-cloud-hosted system — which, according to Mihaescu, is on one of the most secure networks in Europe.

"To get access to data, hackers have to go through a lot of hoops, and chances are we will be able to catch them at some point," he said. For the user, there is a slight delay as those 'hoops' are managed, but that delay can save them from losing cash.

Mihasecu's department includes thousands of workers — but that number could be slashed in the coming years. Not because of budget cuts, but because of changes that are coming to the IT business.

"The cloud is changing not only banking and shopping, but IT as well," Mihasecu said. "Software as a service, with proper security, will provide what users need. There will be much less of a need for system administrators; already there are many tools available for automating just about everything.

"Even database programmers are being replaced by the cloud, with database development being automated," said Mihasecu. "The need for someone who knows SQL by heart will disappear." That said, he added, there will always be room for the best and brightest. "Software developers too are being replaced by automated cloud tools. There will be fewer of them, as there will be fewer sysadmins — but they will be more talented."