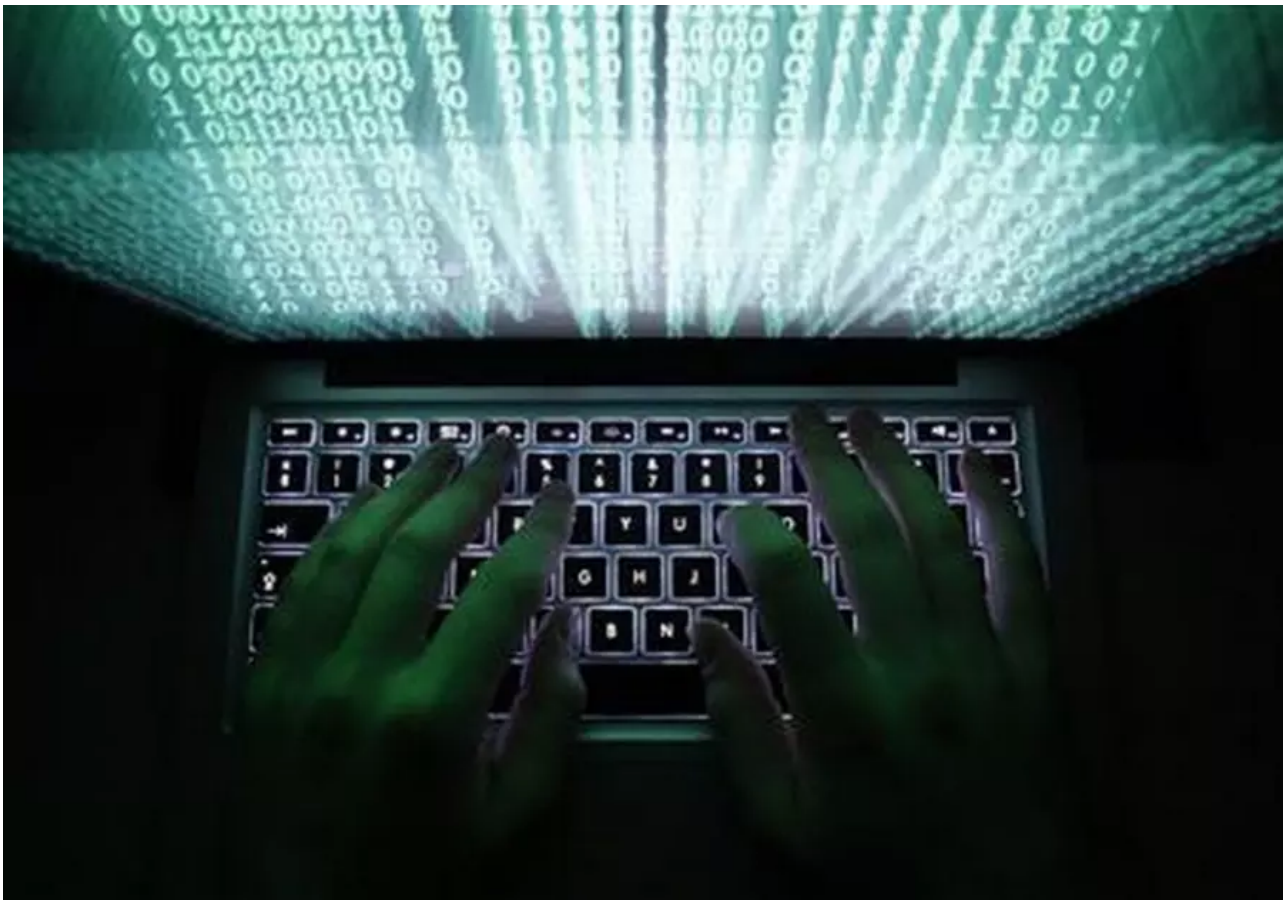
- > Defense Ministry working to turn high schoolers into cybersecurity wonks
- > The cyber security insurance industry must adapt and thrive in Israel

By Max Schindler
December 28, 2017 07:12

While it may sound cocky, the company has a track record that's hard to beat.

4 minute read.



Cyber hackers [illustrative]. (photo credit: REUTERS)

You wake up, go online to check your website and bank account, and suddenly you discover: "OMG, I've been hacked!" But this time it's different. The hack is meant to help you – to diagnose and treat your cybersecurity failings.

"We bypass everything," explained Sharon Nimirovski, head of White Hat cybersecurity firm in Tel Aviv. "We bypass every piece of security solution and design you've implemented. I'm saying that because we're doing that today. And if we bypass you, the bad guys can do it too."

While it may sound cocky, the company has a track record that's hard to beat, counting among its 50 clients several elite financial institutions, governments, health-care firms and blue-chip companies.

Meeting at White Hat's offices near Rothschild Boulevard in the heart of Tel Aviv, employees whizzed by on electric scooters.

Photographing any of the 50 employees, aside from the CEO, was out of the question. Many hail from prestigious army intelligence branches such as Unit 8200, and in their cat-and-mouse game to thwart hackers, they prefer to keep as low a profile as possible. The White Hat guys are strolling the far reaches of the darknet, appearing incognito as they chat and cajole bad hackers.

As recently as five years ago, it could suffice to build a cybersecurity strategy off installing antivirus software and scanning for bugs. Since then, threats have grown exponentially and money is pouring into the world of black market hacking, with new attackers ready to pounce on the latest coding mistake.

While companies like Google and Apple pay for "good" hackers who discover coding faults and weaknesses, they offer rates that are around a 50th of what you can make on the black market, Nimirovski added.

Despite the known threats, most companies still lack a proactive and offensive cybersecurity game, playing only defense against hackers and waiting to be attacked before responding.

"You may buy everything – the best firewall, the best sandbox – you may even have disconnected your Internet from the network, but still, you allow emails to pass through," he said. "That's enough for us to get access to the data and control you."

The huge Equifax leak earlier in 2017 – which jeopardized personal information of millions of people – showed the limits of being reactive, as they spent millions on security and probably had procured the best technology.

What White Hat does is not risk management, Nimirovski insisted, because profiling all your weaknesses and risks doesn't secure the company. Instead, if White Hat can hack your company every week and systematically close one hole after the next, that may help.

"We gather intelligence; we build and simulate the attack around the first piece," he said. "And at the end, we provide you as the client a full picture of what can the bad guys do to you. We tell you what the bad guys see, what can they do, and we tell you what they can do before they do it. We actually walk the path of the bad guys... It's a continuous advanced-persistent-threat test."
In the process of hacking companies, White Hat guys often stumble upon "nasty stuff," Nimirovski said, including pedophilia, gun and drug trafficking. The company then reports that to the police.

For clients that have been hacked and their files encrypted for a ransom, White Hat succeeds in decrypting the files without paying 50% of the time in. If that doesn't work, they try to locate a backup that's good enough for recovering the data. Sometimes, the companies have to pony up and pay exorbitant fees.

The Israeli cybersecurity success story has opened offices in Greece, in Cyprus, and are in the process of setting up shop in New York sometime in early-to-mid 2018. Only three women are currently employed by White Hat, and its CEO pledged to do more to diversify its staff.

The company is also setting up a VIP service called "Black List," which monitors the client's website, IP addresses for hostile threats, along with personalizing a home-and-office cybersecurity plan for the client's family and home devices. If suspicious activity arises, the client gets notified on their mobile device.

If you're a small businessman or someone who can't afford White Hat's hefty fees, there's still a lot you can do, Nimirovski said.

"Assume that you're not going to be hacked but that you're already hacked. There's a 99% chance that you're already hacked and you have some piece of malware sending data out of your PC."

White Hat recommends users put all sensitive information on a cloud computing server, like Google Drive, and not on a personal computer. (It's much harder to hack a cloud than your personal device.)

"All personal accounts should require two-factor authentication, or requiring a text from your phone in order to log in. And every time you're finished working on data, log out," it advised.

Also, it's safer to use Apply pay, Google Pay, PayPal, anything other than typing in your credit card number directly, according to Nimirovski.

On the company's advisory board sits a list of well-known Israeli security experts. Executives recently appointed to the board include, Ilan Mizrahi, Mossad deputy head and National Security Council head; Eyal Fisher head of the cyber division and second in command of Unit 8200, the IDF's largest unit; and Ronen Zaretsky, former vice president of technologies at Isracard.

Tags:
- israel tech
- start up nation
- startapp israel
- high tech