



<http://www.techday.co.nz/itbrief/news/exclusive-interview-with-palo-alto-cto-nir-zu/21679/5/>

Exclusive: interview with Palo Alto CTO Nir Zuk

By Sean Mitchell, Wednesday, 7th December, 2011



With high-profile attacks on targets like the PlayStation Network placing an incredible amount of attention on network security this year, it's no surprise that businesses are upping their defences in the cyber battleground.

However, modern protection isn't about spending millions securing data with firewalls, but instead demands a more targeted approach, according to Nir Zuk, founder and CTO of Palo Alto Networks.

Zuk says the time when hackers were mostly bored geeks testing their skills for fun is well and truly over.

Now, attacks are more likely to come from nation states and organised crime syndicates willing to devote a lot of time and resources to infiltrate large targets. Once inside, the criminals will hit hard and cause significant losses.

The shift brings with it a fresh challenge for network security. Rather than issuing thousands of attacks and relying on scale to sneak through organisations' defences, the new hackers are more likely to choose a specific target, from a low-level employee to a CEO, and use social engineering to tailor an attack to their interests.

For example, if a chief executive's Facebook page lists golf among his or her interests, a skilled hacker can find out which club he or she belongs to, then send a message from the club president that includes an attachment offering five ways to improve his or her swing.

All the CEO has to do is open the attachment for the hacker to infiltrate their computer, and from there the rest of the organisation.

Zuk says this kind of attack, labelled 'spear phishing', is perfect for bypassing traditional firewalls, which are built to recognise large-scale attacks.

"If it happens once, to one company, with one employee, it will not be a trend worth investigating for the rest of the industry," Zuk says.

So, besides employee training, how can organisations protect themselves from spear phishing? Zuk says Palo Alto has a new solution, WildFire, which examines each attachment by opening it in a virtual machine to see what it does. Any machine WildFire suspects has been infected is blocked from the network, a process that initially took up to 24 hours, but that Palo Alto is hoping to cut to under 60 minutes.

The challenge is to automate the analysis process, Zuk says, rather than having individual engineers analysing every attachment.

"There simply aren't enough researchers in the world to get this granular."

Check out our recent story listing eight things you probably don't know about Palo Alto Networks [here](#), or go [here](#) for the Palo Alto website.