Hacking the human element

Technical treachery often steals the headlines when data systems are breached by hackers. But Ilia Kolochenko, CEO of High-Tech Bridge, a leading web security company, says the human element is the hacker's most useful tool.

ILIA KOLOCHENKO
CEO, High-Tech Bridge

"People are easily deceived, and they are easily distracted," he observes. Then there are those who are simply out to make a quick buck. Combine the two, and it adds up to many open doors for hackers with a bit of insight into human nature.

It can start with technology investors looking to diversify with a minimum of risk: "They invest venture capital in startup security companies, but they have only limited knowledge of cyber security. The solutions they are presented with might be smart, but they are often impractical or too expensive to for the market. And when investors put pressure on their companies to make money, they seek out clients without the proper knowledge to recognise ineffective solutions."

> People are easily deceived, and they are easily distracted.

Enter the client – or the victim: "Many managers understand cyber security, but many more do not. Either they do not assess, or do not understand their risks," Kolochenko says. As proof of this, he cites examples where companies have been hacked almost weekly after installing expensive but inadequate cybersecurity solutions. "Instead of identifying and meeting their top ten security requirements, some security companies lead them into random priorities. They spend huge amounts of money on mitigating the wrong risks, while many of their key risks go unaddressed."

Holes in the wall

Kolochenko cites incomplete inventory of digital assets as one global weakness, whether it be assets represented by the hardware, software, the data, or the users. "With cloud computing, shared data, and connectivity, it can be really difficult to gain a comprehensive and up to date overview."

Armed with this knowledge, hackers seek out the weakest points in a company's data defence, often profiling associated parties and attacking through them, rather than going for the big companies head-on.

"Companies build their castle, and then they build a wall around the castle. But all around them are villagers and farmers and merchants with access to the castle, and they either forget or cannot keep track of all their connections. In this case, a wall, or a firewall, does not give much protection."

Any business can be of interest to hackers, and ransomware makes them all potential sources of income. But this is a human problem, not software problem, Kolochenko emphasises. "Now it's about using humans as entry points in to the castle."

Defend the choke points
The core business of High-Tech Bridge is machine learning and artificial intelligence in application security, and testing web and mobile applications for vulnerabilities. This is certainly a timely focus, at least according to the 2016 edition Gartner's Hype Cycle for Application Security, representing the gold standard in ICT consultancy:

Applications, not the infrastructure, represent the main attack vector for data exfiltration. As organisations lose more control over their infrastructure with trends like mobility and cloud, applications become one of the last control points for imposing the organisation's security policy.

—

With cloud computing, shared data, and connectivity, it can be really difficult to gain a comprehensive and up to date overview.

"We are doing what we know best, and where we can offer the most competitive price-to-quality ratio, thanks to our award-winning technology." Ilia confirms.

Kolochenko was nominated to the Forbes Technology Council last year, and has recently started on a Master's degree in Law. "Technical and human sciences will be intertwined in future," he believes. "I want to be informed as that happens." He also sees the challenge of bringing the legal system up to speed with developments in digital technology. "Today if a business gets hacked, they are on their own. The legal system cannot protect you," he states flatly.

Cyber surrender
One example of the legal community's belly-flop on hacking: When a machine with access to a company's mission-critical data is blocked, they are simply advised to pay a ransom fee to release the data. Investigation and prosecution are time consuming and complex, and it is much more practical to pay a small fee and keep the business running.

This practice has become so commonplace that data hijackers even operate multilingual call centres that advise on how to pay ransom, and even how to protect data from future attacks. "Now there is even ransomware as a service," Ilia says. "They sell the attack software and collect a flat fee, and the hacker simply plugs it in and goes to work."

Virtual capitulation is also becoming institutionalised: "Companies are budgeting with bitcoin to unblock devices, rather than using resources to fight hacking." While private citizens are more likely to balk on ransoms for monetary or ethical reasons, companies make better targets. "They need their data to keep functioning, and paying a small fee is not a problem. 50 dollars may be a lot for a private person, but it's cheap for a company. Also companies don't want to look vulnerable or unprofessional by admitting publically that they are being hacked."

But don't hackers ever get caught? "Beginners and those who are indiscrete get caught. If you get greedy and demand too much ransom, a company might go after you. Or if all of a sudden a Lamborghini is parked in the driveway of your new house, you are asking to get caught. But the real professionals can technically make hacking almost impossible to trace."

And how to keep from getting hacked? "Just keep all your systems and all installed software up to date," is Kolochenko's practical advice. "Enough to minimise the majority of vulnerabilities." Big companies will not change dramatically overnight, he points out. Bound as they are by legacy systems, contracts, and internal politics, they can only keep somewhat protected, and they will always have to live with weak points.

Everything is hackable – but why would you?
"We could also test cars or other hackable assets, but too much hype is generated around these risks in order to create business for security companies." That being said, Kolochenko readily admits that the Internet of Things and sensor saturation could cause problems: "90 per cent of manufacturers do not care about security when they imbed sensors in their products. Often the systems cannot even be updated." Still he believes the threat of virtually anything being hacked is exaggerated.

"Not everything needs to be connected. You don't need to connect your smart toilet to the Internet." For Kolochenko, it comes down to a simple rule of prevention: "Don't stick your finger in the light socket, and you won't get shocked. It may seem cool to connect to your car through the Internet, but then you are exposed, and you need to decide, is it worth it? Maybe you could just program your car to do what you want, and keep it offline."

—

Technical and human sciences will be intertwined in future.

Though he acknowledges that most people will allow themselves to be lured into excess connectivity, Ilia Kolochenko's insight into the practical nature of humans keeps him from fearing the worst. "If you want to take over a car, it's still easier just to break a window than to hack into the motherboard. If you want to wreck something, it is much easier to burn it than to hack it."

A very down-to-earth reminder that even as we ascend into cyber space, we are still only human.

04