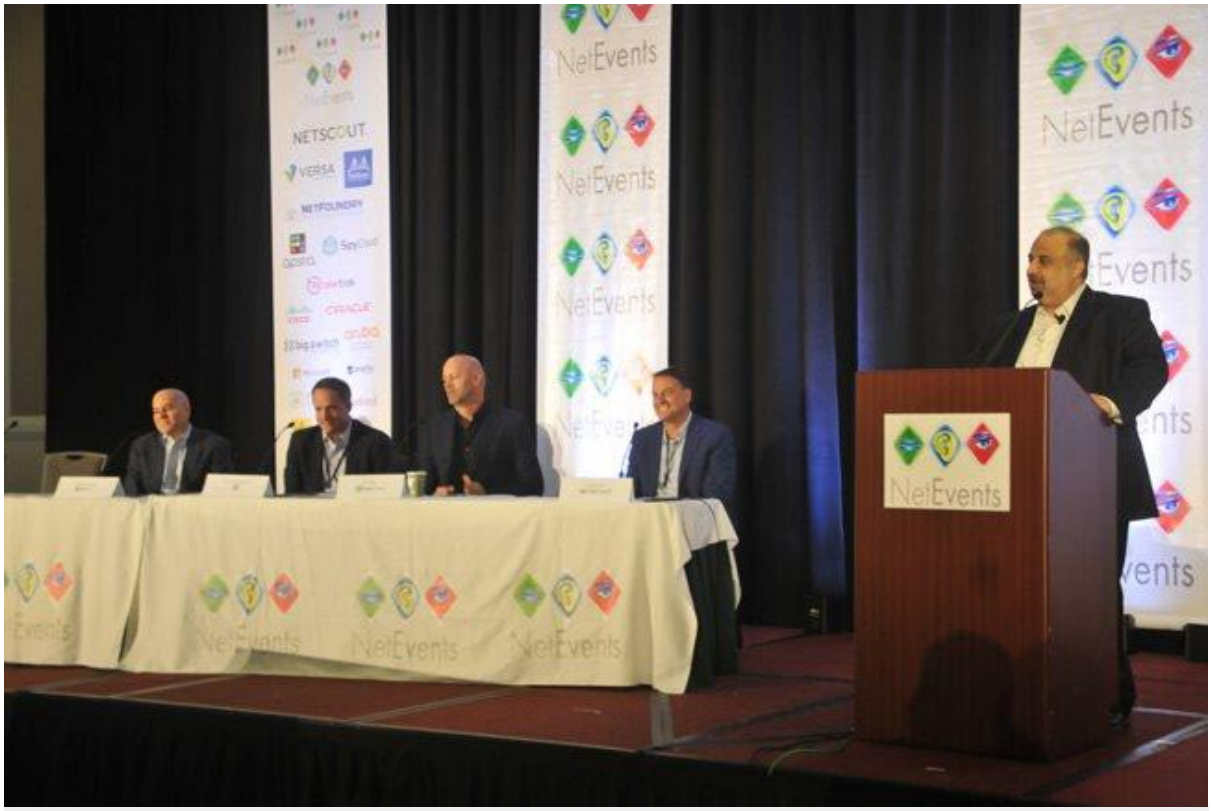
The Saigon Times

https://en.thesaigontimes.vn/tinbaichitiet/71991/

Technology application vs. cyber security

Saturday, 10/12/2019, 18:36

By Nhan Tam



Delegates discuss issues at the NetEvents 2019 Global IT Summit taking place at Hayes Mansion in Silicon Valley, San Jose City, California State, the United States, from October 2 to 4 - PHOTO: NHAN TAM

SAN JOSE – Ensuring security is critical in the age of digitalization as Internet users are now more vulnerable to hacking attacks.

Cyber security: the more advanced, the more risky

Ted Ross, CEO and co-founder of SpyCloud, a U.S.-based company, said a customer has an account on Fantasy Football (a game app) but the Fantasy Football game is breached, and the customer's password is stolen. Unfortunately, the customer uses the same password on their Gmail account. So the hacker can use the stolen password to enter the customer's Gmail account, find their bank account password and ultimately steal their money.

This story was told at the NetEvents 2019 Global IT Summit held on October 3 and 4 in San Jose, California in the United States. He noted that this case is not rare as 59% of Internet users use the same password for at least two of their accounts.

"Passwords and their reuse across personal and work accounts are the leading cause of ATO [account takeover], one of the most imminent threats to businesses of all sizes," said Ross. "As criminals use more complex, scalable methods to collect and weaponize compromised passwords, organizations need to take proactive measures to prevent, detect and remediate exposure."

The network is the business, so these cases are common, said Ravi Chandrasekaran from Silicon Valley-headquartered Cisco, adding that the network is growing massively, with 127 new devices connected to the Internet every second. There will be 26 billion devices connected by 2020. "The challenge is that changes to the network are still mostly manual, resulting in policy errors caused by human error. The consequent costs are high."

Meanwhile, Vikram Phatak, founder of NSS Labs (Texas, the United States), cited World Economic Council data as saying that cybercrime cost US$600 billion in 2018 and will rise to US$3 trillion by 2020. Spending on security was US$124 billion in 2019, and the figure is projected to rise to US$188.4 billion by 2023. "As for the state of cyber security, there is a major skill shortage. We need trained experts, but new attack vectors get people to expose themselves," stressed Phatak. "Security is harder than people think."

Michael Segal, area vice president of Strategic Alliances, Netscout, said: "As we place growing importance on the delivery of cloud-based services, it should come as no surprise that attackers are increasingly targeting these services with attacks. If it's important to you (network operators), it's important to them (attackers)."

What is the solution?

Artificial Intelligence (AI) is part of the solution, Chandrasekaran said. There is a parallel with the industrial revolution, which enables people to go beyond our physical capabilities; AI does the same for mental capabilities, he stated. "More traffic can be enabled at particular times of the day, using previous trends as a guideline."

Jeremiah Caron, global head of Research & Analysis, Technology Group, GlobalData (the United Kingdom), pointed out that new research on AI showed that only 47% of businesses see AI as being part of the future of their companies. However, he acknowledged seeing many AI/ML intelligence cycles, expert systems and neural networks over the years. Nick McMenemy, CEO of Renewtrak (Australia), agreed that AI is a catch-all term.

"I'm also a bit of a skeptic, but it can free up humans to do what we prefer to do, what we're better at," he said, adding that customers were 100% skeptical but did not fully understand the technology. But now, they know they have to predict what IT systems can do.

Michael Levin, CEO and founder, Center for Information Security Awareness (the United States), said that the challenge is in creating a culture of security within the

organization. He said: "We are doing a terrible job. Corporate executives are doing nothing or checking boxes. We know phishing testing will reduce risk, but hackers mostly just need to find open windows such as admin passwords on servers. That's human error and laziness due to no training or not enough training. Education can be very effective, as well as processes such as two-factor authentication."

Ross agreed, pointing out that people forget about the human element when installing equipment and software. People need training on zero-trust. Meanwhile, Paul Kraus, vice president of Engineering, NetScout Systems Inc. (Massachusetts, the United States), suggested visibility was the main issue. "You need to know what assets you have, what they touch, look at changes and monitor (the situation). Put a value on each asset. But physical monitoring doesn't scale," he explained.

NetEvents 2019 Global IT Summit connects businesses and press for 23 years

Themed "Innovators in Cloud/Data Center, AI, Cybersecurity, IoT, 5G & Mobile Technologies," NetEvents 2019 Global IT Summit took place at Hayes Mansion in Silicon Valley, San Jose City, California, the United States, from October 2 to 4, attracting press and analysts representing more than 100 publications from all over the world, as well as more than 100 business representatives and industry speakers.

Since 1996, NetEvents has provided a key communication channel for the networking and telecoms marketplaces. It fosters creative and profitable relationships between press, analysts, equipment manufacturers, software companies, telecoms operators, datacenter/hosting companies, system integrators, IT channel partners, business angels and leading industry associations.