Why is cybercrime rising?

Most businesses have had their systems hacked into among other forms of cybercrime. The rising cases that are currently understated, have also forced chief executive officers to invest up to a third of their investments in information security prevention and detection, **Eronie Kamukama** writes.

Someone hacks into a computer system. Findings from the 2018 annual crime report indicate that they were able to get passwords and user names for 92 per cent of the systems. INTERNET PHOTO

A Facebook page was created in the names of Martin Okoth Ochola, the Inspector General of Police (IGP), last year. The recently released 2018 Annual Crime Report reveals this transpired between March and June within Kampala and the eastern district of Tororo.

A case was opened and investigations show the social media page was used to solicit money from the public and members of the Uganda Police Force under the guise of helping them acquire better offices and promotions.

"The accused person Geofrey Kalele aged 27 years, Musoga by tribe, resident of Kalitumba, Magada sub-county, Namutumba District appeared at Buganda Road Court on two counts of electronic fraud, three counts of personation and two counts of obtaining money by false pretenses. He was subsequently remanded and later released on court bail on 22/08/2018 after presenting two substantial sureties. The accused consistently jumped bail but was re-arrested," the 2018 annual crime report reads.

Cases

In 2018, cybercrime cases rose by 40 according to the report. A total of 198 cases were reported in 2018 compared to 158 in 2017. Slightly over Shs600m was lost, with most of the crime committed over the internet. Earlier revelations by Police indicate numerous cybercrimes remain unreported or undetected, partly for purposes of protecting reputations.

Security services provider Summit Consulting Limited says an increase of 40 cases is too significant a number given that Police has not deliberately put a direct mechanism for any victim of cybercrime to report. On the other hand, government has prioritised investment in cyber security training and equipment at Police and Ministry of Information and Communication Technology.

"The more people go online, the more you expect a lot of mistakes because the attack vector increases so somebody has more people to attack. But also, there is generally no nationwide strategy for creating awareness to managing the cybercrime," Mr Mustapha Mugisa, chief executive officer Summit Consulting Limited, says.

The expectation now is that like in developed countries, information on targeted institutions and prevailing threats is provided at least on a weekly basis to anticipate and prevent cybercrimes.

"The increment of only 40 cases is completely understated in terms of the extent of the problem on ground. We get so many people asking for our help in terms of tracking passwords when someone hacks into emails, Facebook, identity changed, loss of money through payment of rogue companies because of an email instruction," Mr Mugisa says. "If they were capturing network attack cases at national level and in real time, you would find we have 100,000 attempts every day because we are talking about 10 million people online. That is too much," Mr Mugisa says.

Data obtained from Project Frontline 2018, a cyber security report based on 121 assessed organisations in 2016 and 2017 by Summit Consulting Limited, shows there is a general poor state of security hygiene in the country.

Findings indicate that it was possible to exploit internal critical production systems with one or more exploits at 68 per cent in all assessments. Exfiltration of data was achieved at 92 per cent of the time. It was easy to acquire credentials in at least 92 per cent of the cases using common credential exposure methods. It was possible to gain full control of the target organisation's infrastructure at 94 per cent of the time.

"68 per cent means for every 10 systems we tried to exploit, six were breached so they are below average in terms of security. Exfiltration is stealing confidential information. For credentials, this means that we were able to get passwords and user names for 92 per cent of the systems. For the organisations that gave us permission to assess their infrastructure, we were able to breach and found they were vulnerable and that means it is very important to test your security because if you rely only on IT, your department may be lying to you," Mr Mugisa explains.

94%

PERCENTAGE BY WHICH IT WAS POSSIBLE TO GAIN FULL CONTROL OF THE TARGET ORGANISATION'S INFRASTRUCTURE

Source: 2018 Annual Crime Report

Digital disruption

KPMG's 2019 East Africa Chief Executive Officer (CEO) outlook on redefining resilience casts light on concerns presented by the digital disruption facing major sectors today.

Of the East African CEOs who reported emerging technology as the greatest threat to their organisation's growth, four out of five cited cyber security risk as the primary source of this threat. Globally, two out of five CEOs agreed.

CEOs, cyber attacks

About 49 per cent of East African CEOs state that becoming a victim of cyber-attack is only a matter of when and not if. Despite the heightened sense of vulnerability, 46 per cent of East African CEOs report being prepared for a cyber-attack in 2019.

"Half of the CEO's time in our group is spent focusing on how to build strong cyber resilience in the business. Out of the total technology investment, up to a third goes towards information security in prevention, detection, monitoring and response," Mr Joshua Oigara, Group CEO, KCB bank says.

Project Frontline report reveals the extent of the impact of ongoing cybercrime on internet users ranges from disclosing confidential or private information, to making unauthorised modifications to data and making important company systems unavailable for use.

Companies and individuals are responsible for their online security. It takes a combination of complicated passwords, clicking only genuine emails, using safe internet spots and more.

"Companies must do ongoing security assessments from a hacker's perspective," Mr Mugisa says. "In this case, you test the threat from outsiders but every time we find fraud, we find insiders are involved. So you need to look into how they also get information they should not have."

Advice

Uganda Police offers simple advice for individuals through its website. Your gadget's antivirus and firewall must be good.

Posting personal information online must be limited as scammers use it to guess passwords and commit fraud.

Check how much information is available about you on the internet by typing your name into a search engine. Lastly, online friends may not be who they are and unexpected requests for money may not be genuine. Contact friends and family to verify the requests first.

TOP 10 CYBERCRIMES

CRIME	CASES
Electronic Fraud	76
Threatening violence	28
Defamation	25
Offensive communication	19
Personation	12
Unauthorised access	10
Obtaining money by false pretenses	8
Cyber harassment	7
Theft	3
Illegal modification of computer material	2

SOURCE: 2018 ANNUAL CRIME REPORT