Identity is the New Attack Surface

In 1988 Robert Morris, a student at Cornell University, created the first computer worm. Nicknamed the 'Morris Worm', the origin of this computer virus was a simple curiosity – Morris wanted to get an idea of the size of the internet. This worm's attack vector (path of attack) was to exploit known vulnerabilities in computers at the time.

On 28 March 1994, the Rome Air Development Center – a US Air Force research facility – discovered that a password 'sniffer' had been installed onto their network. Many accounts were compromised. The vector of this attack was simply to hack into the Air Force's systems and plant the virus.

Both these attacks are key events in the history of cybersecurity. And both had attack paths that relied upon poor programming and weak firewalls.

Fast forward to late 2016. The personal information of 57 million Uber users and 600,000 drivers was exposed. The attack vector? Simple identity theft. The hackers accessed Uber's GitHub account, where they found access credentials to Uber's Amazon Web Services account. Github is a web-hosting service and Amazon Web Services (AWS) is an on-demand cloud-computing platform.

Identities are the true trojan horses of the cyber world. Instead of wasting time with researching vulnerabilities in target systems and creating complex programs to exploit them, hackers are now on cruise mode. They simply wait for people to write down one or more of their numerous passwords in a computer document or on a sticky note, pick it up, and enjoy anonymous access to confidential data for potentially infinite periods of time.

Because the source of the hack is not an infection that leads to unauthorized access, but instead seemingly legitimate access from a genuine identity, this kind of breach can take very long to detect and is exponentially more dangerous.

This challenge is largely solved by Single-Sign-On (SSO) and Multi-Factor Authentication (MFA) technologies. SSO enables users to log in to all their apps and systems with just a single password. This reduces the number of passwords required to be remembered and eliminates confusion that results in people noting down or saving their numerous passwords in a document on their machines. MFA protects identities further by forcing authentication on multiple levels. Here, credentials-based authentication is further protected by challenge-response questions, SMS or Email OTPs or even biometrics. Both these features form the base of most available IAM solutions.

Not only do IAM systems protect against unauthorized access, they typically offer solutions for managing user access rights and trends. You can use them to govern and even automate the different accesses that someone may have to different systems and apps used by your organization.

Protecting identities is of far more pressing importance than safeguarding apps and systems against unauthorized access. By securing an identity you protect the very root of the access mechanism. Shielding apps and systems from hackers only insulates the last barrier in the access vector. Using chess as a metaphor, identity management protects your king but firewalls and antiviruses only protect your pawns.

To conclude, gone are the times of hackers using their own technology to hack into your systems. Even the time piggybacking credential-sniffers through malicious emails and malware is at an end. Identity is the new attack surface. It is in your organization’s interest to protect against this threat with an IAM system that works for you.