enterprise networking

JANUARY-2016

enterprisenetworkingmag.com

IN MY OPINION
By Kenny Gilbert,
CIO, InvenSense

CIO INSIGHTS
Ramon Padilla,
CIO & CISO,
Minnesota State Colleges & Universities

Ruckus Wireless:

Unleashing Smart Wireless Technologies for a Mobile World

Selina Lo,
President and CEO

$10

Enterprise Network Mag
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

The Three Largest Cyber Security Risks of the Decade Converge: Cloud Computing, BYOD, and IoT

By Jerry Irvine, CIO & EVP, Prescient Solutions

With technology comes risk. **Cloud computing** has increased cyber risks as a result of moving enterprise level resources and data outside the protected network perimeter. These risks are associated with the distributed resources and services of the cloud. Additionally, identity management, access controls and rights management have become much more complex across multiple providers and systems in the cloud. Still, new technologies, including single sign-on and cloud-based security solutions, provide organizations with the ability to develop and maintain a secure cloud-based solution.

BYOD (Bring Your Own Device) not only allows end users to access enterprise resources and data remotely but also permits them to use their own personal consumer grade devices. BYOD security solutions remain rather immature, primarily because consumer devices are designed for personal use, which limits the controls that can be implemented. While Mobile Device Management (MDM) solutions are available and provide many more security options than initial consumer grade solutions, they have to allow end users to continue to use their devices for personal use.

IoT (Internet of Things) devices are designed to allow remote connectivity, management and data acquisition to anyone, anywhere, to and from all kinds of devices. IoT devices are, for the most part, a reimplementation of Industrial Control Systems technology, which was designed initially in the 1950s. Small computer chips are designed to perform a specific function, such as remote management or alerting, and placed within mechanical devices. Unfortunately, these chips and their technology were not designed to communicate in a public network. They were designed to be on their own network away from any potential security threat. Due to this as well as their compact size, little, if any, security protocols or controls were designed within these devices. The vulnerabilities of these devices leaves facilities and organizations at risk of loss or corruption of data, eavesdropping, man-in-the-middle attacks, denial of service attacks and complete remote control of devices on the network.

While the vulnerabilities and risks stemming from the cloud, BYOD and IoT individually are dangerous, the combination of all three creates threats which are difficult, if not impossible, to mitigate.

Understanding the threats and how the malicious actors perform their job is important in mitigating the possibility of loss. A hacker's first step is to target end users via phishing/spam emails, web attacks and or malware in order to gain information. In fact, industry statistics show that more than 90 percent of hacks are a result of a phishing attack. Once malware is in place, hackers search the end user device for device information, names and addresses, financial and other personally identifiable information. The next step is then to perform network discovery or malware transmission from the device they were able to breach. The malware will attempt to discover all devices on the end users home network, the attached business network and the attached cloud network as well as perform cursory IP addressing queries,

packet capture and retransmission and OS discovery. It is in the discovery process when hackers obtain information on the device type, devices accessible and even the applications that are communicating on the network. Servers, workstations, peripheral devices and IoT devices are easily detected and in many cases automatically attacked placing malware on them in order to gain control of these devices as well. The discovery and information gathering steps can last seconds in an automated virus and malware introduction state, or as long as months or years in and Advanced Persistent Threat (APT). Each device breached "calls home", transmitting their information back to the hacker's collection and management devices.

Traditional IT security measures are no longer sufficient in securing the enterprise network. Protection against phishing, viruses and malware is provided through a combination of antivirus, endpoint security tools, spam filters and firewalls. Nevertheless antivirus solutions protect against less than 30 percent of known viruses and malware; new versions of spam and malware are created daily to avoid detection from spam filters and firewalls are configured to allow communications from end user devices directly to the internal network. So, hackers continue to outsmart typical IT security solutions allowing malicious applications and email content to make it to the end user and the networks to which they are attached.

Access controls for IoT devices should be implemented limiting the specific users and devices allowed to communicate to or control the devices

To help mitigate the risk of a hack in this evolving environment, enterprises can take a few steps:

• Increased real time security monitoring and alerting, including Intrusion Detection/Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) solutions, must be implemented to notify security professionals of communications to and from the Internet, even thosethat appear to be authorized.

• Firewalls should be configured to only allow encrypted communications from the external publicly accessible network to internal devices. Access controls within the firewall should be configured to allow remote users accessto only necessary information to perform their job.

• IoT devices should be segmented from direct public access from the Internet and only allowed via encrypted communications. Access controls for IoT devices should be implemented limiting the specific users and devices allowed to communicate to or control the devices. IoT management applications should be configured with unique user ID and complex password.

• Mobile devices, end user owned or enterprise owned, should have MDM and endpoint security solutions installed, be encrypted, and require a unique user ID and complex password for access.

• Cloud services should be configured so all users have a unique user ID and complex password.

• The enterprise should define security requirements and regulatory compliance requirements within the engagement contract and complete or have a third party complete a periodic security assessment of the cloud service provider to assure their compliance. One such security requirement should be a detailed systems update and patch management process to assure all applications, operating systems and firmware are maintained and kept current.

IT professionals continue to be challenged to provide network security to the enterprise in spite of the known vulnerabilities, threats and risks of technologies. As a result, organizations need to periodically perform detailed risk analysis and continually review, test and update their IT security policies, processes and standards.en