January 2014
Volume 9, Issue 1

2014 Cyber Security Outlook

Town of Wareham

!

!

From the Office of Information Management Technology

As we look ahead toward the cyber threats facing us this year, some key challenges will result from the advancements in technology that are becoming part of our daily lives. Ranging from the Internet of Things to online currencies, devices and systems have never been more interconnected. Before we adopt these new technologies, we need to ensure we understand the security implications, and have appropriate layers of defense in place.

Below are highlights of several of these new advancements and how they may affect us.

The Internet of Things

What is the Internet of Things? Put simply, the Internet enables connectivity from virtually any end-user device or thing. The latest trend is connecting things such as small appliances, refrigerators, personal medical devices, wearable health trackers and many other items.

One of the most common examples of how the Internet of Things impacts our daily lives is the automobile, which has become a sophisticated computer device. Researchers have demonstrated the ability to hack an automobile's systems to control the brakes, steering wheel, and even shut down the engine. Numerous discussion forums focus on the use of vehicle-to-vehicle (or V2V) technology, which will allow vehicles to talk to each other via wireless connectivity.

Bluetooth, which is a standard feature in many automobiles with options to include a personal hotspot, can allow a modern smartphone to connect to the automobile's stereo system to receive continuous Twitter feeds, or a system that may allow a technician to provide assistance in case of emergencies. Researchers have discovered ways to inject malicious codes/programs through CD players or iPod connectors. So theoretically, an infected song on your iPod or CD, when played in your automobile, potentially can spread malicious code from the automobile's entertainment network to other components of the automobile without many restrictions.

In another example of how the Internet of Things can impact us is from a recent news story, which suggested electric teakettles and other small appliances were able to exploit unencrypted WiFi and send data back to foreign servers[1].

Internet-connected devices that are able to process sensitive personal information tend to be high priority targets for cyber criminals. It will become increasingly critical in 2014 to protect these devices from unintended or unauthorized connectivity.

Bitcoins

A Bitcoin is a digital currency stored in a downloadable wallet on a user's personal computer or with an online wallet service provider. Each wallet has a unique identifier that allows users to transfer bitcoins to other users' wallets. Bitcoin is a decentralized, peer-to-peer payment

[1] http://www.businessinsider.com/russia-claims-china-bugged-tea-kettles-2013-10#ixzz2nM6vxMX8

system, currently with no regulatory authority. It is gaining popularity, with mainstream businesses adopting it as an alternative form of payment or investment.

While the long-term use of Bitcoin is uncertain, for at least the near term in 2014, the increasing adoption and publicity will continue to draw the interest of cyber criminals who target Bitcoin users' wallets for theft, or compromise systems to generate bitcoins via malware infection.

Mobile Transaction Risks

Every new smart phone, tablet or other mobile device provides an opportunity for a potential cyber attack. New features such as Near Field Communications (NFC), as well as AirDrop and Passbook for Apple, will continue to expand in 2014, increasing the opportunities for cyber criminals to exploit weaknesses. NFC and AirDrop allow for similarly configured smartphones to communicate with each other by simply touching another smart phone, or being in proximity to another smartphone. This technology is being used for credit card purchases, boarding passes, and file sharing, and will most likely be incorporated into other uses in 2014.

Risks of these technologies could include eavesdropping (through which the cyber criminal can intercept data transmission such as credit card numbers) and transferring viruses or other malware from one NFC/AirDrop-enabled device to another.

Summary

Before adopting any of the myriad new technologies that are rapidly being deployed, it's important to understand the implications and risks. While interconnectivity can yield many benefits, the risk could outweigh the benefit if the devices, systems and technologies are not properly secured.

For More Information

Georgia Tech: Emerging Cyber Threats Report
http://www.gtsecuritysummit.com/2014Report.pdf
Sophos: Security Threat Report 2014
http://www.sophos.com/en-us/threat-center/security-threat-report.aspx
Websense: 2014 Security Predictions
http://www.websense.com/2014predictions?cmpid=prnr11.14.13
Symantec: 2014 Predications
http://www.symantec.com/connect/blogs/2014-predictions-symantec-0

Provided By:

CENTER FOR INTERNET SECURITY
William F. Pelgrin, President and CEO
www.cisecurity.org
contact@cisecurity.org

STOP | THINK | CONNECT