PTA CERT for Telecom Sector

Security Advisory-No: Ext:163-29

11, Dec 2018

Introduction: In the last decade, the use of smart TV has increased immensely. Recently, Security researchers have disclosed that along with advanced features and services like reading emails, installing applications, surfing web etc, it is presenting a new attack vector to hackers for compromising and stealing sensitive info.

Threat Posed by Usage of Smart TV:

Multiple studies dealing with security and Privacy issues in smart TVs indicate following threats:

a. A malware can easily find its way into smart TVs that could convert them into bugging devices.

b. User profiling can be done by viewing logs, browsing history etc.

c. Access to sensitive files, photos and other data on storage devices connected to your smart TV.

d. Smart TV may become part of a botnet that can be used to attack corporate or government websites.

e. Hackers can access the apps installed on the TV by user and steal personal/ account information.

f. These devices also come with a variety of out dated firmware's and vulnerable applications.

g. Smart TVs equipped with remote controls for voice commands and cameras for video conferencing making them the perfect tool for espionage. Hackers may lock the TV and demand a ransom.

h. Continuous pop-ups with targeted advertisements.

Best Practices for Safe Usage of Smart TV:

Following best practices may be employed for safe usage of smart TV:

a. Only purchase smart TVs from reputable vendors that have a track record of Regularly fixing bugs and releasing security updates.

b. Keep all operating systems, firmware and software up to date.

c. All smart TV users are strongly advised to keep these devices off the network and ensure that the USB ports are not exposed.

d. Users are advised to regularly install updates on the home TV as these updates may contain critical security fixes.

e. For foolproof security of webcam and/or microphone, cover them with opaque tape or a sticky note.

f. Limit online activity on smart TV, if required to log into banking websites, never use TV instead use your phone or personal computer.

g. Be cautious when installing new apps and only install apps from known sources.

h. Set up a separate Wi-Fi account for your smart TV as hackers may reach your laptop or computer via your smart TV.

i. It is advised to use wired connections over wireless because they are more difficult to compromise.

j. Avoid connecting USB sticks to your TV because they might contain malware.

k. Make sure you clearly understand the terms, conditions, and privacy policies before activating any service on your smart TV.

l. It is also suggested to avoid using generic browsers on smart TVs because they do not have built-in security controls to protect against malicious web attacks.

m. The old Wired Equivalent Privacy (WEP) protocol is still widely used, but it is weak and easily compromised. Make sure the home wireless network is protected by Wi-Fi Protected Access II (WPA2) protocol and a, complex password.

n. Disable guest network access entirely.

o. Good password management is essential. Neither network equivalent (such as routers and switches) nor gadgets (such as smart TVs) should use default factory-set administrator passwords.

p. Permanently disable remote-management access and other network tools.

Recommendations

a. Smart TVs are relatively new to the security field, as long as manufacturers step up their cyber security and offer effective security features and strong

firewalls; t is strongly advised to follow the guidelines outlined at para3.

b. Only purchase smart TVs from reputable vendors that have a track record of regularly fixing bugs and releasing security updates.

c. Keep all operating systems, firmware's and software's up to date.

d. In case of any incident, please report to this office.