Inside this Issue Vol 3: Issue 1/19

Cyber Tips

How to stay safe on line.

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.Read more >>

Your Smartphone: Friend or Foe?

The fact of the matter is that a backdoor can be cleverly hidden in a picture you receive on your WhatsApp group chat. Since you most likely have auto download, you will execute the said backdoor unknowingly.>>

Institute Of Forensics & ICT Security www.forensicsinstitute.org

Forensics & **Cyber Security** Newsletter

Your source of forensics, security and fraud insights

Your Smartphone: Friend or Foe?

Your Smartphone: Friend or Foe?

How safe is your information and pictures? Have you ever paused to think what would happen in the event that your phone got hacked? Or lost and the information on it accessed? Those handheld gadgets that take up a big percentage of most peoples' lives providing access to entertainment, communication, health information, commercial services, among others are more of a threat to you than you can ever imagine.

Many individuals take time to set up security measures like pins, fingerprint locks, facial recognition locks and patterns to prevent other people from using their phones. After all this is done, one connects to an open wi-fi network to access the internet, download cracked apps, root or jailbreak the phones, thereby undoing all the good work.

There is also a widespread mindset that smartphones can't be attacked by viruses and malware. Many smartphone users thus don't bother to install anti-virus and anti-malware programs.

Security tips

01

Consequently organisations should invest in intrusion detection with alerts and automatic prevention systems in the event of an inadvertent hack. Segmented networking, data encryption, role-based security and two-factor authentication architecture should also be implemented.

02

Pen testing, otherwise known as penetration testing, is an authorized simulated attack performed to evaluate the security of the system and identify any vulnerabilities. It should also flag up the strengths of the system as well as weaknesses which will need to be addressed immediately.

From page 1

The incident is believed to be one of the largest data breaches in history, behind 2016 Yahoo hacking in which nearly 3 billion user accounts were stolen.

How easy is it to hack an android phone?

Kali Linux, a Debian-derived Linux distribution designed for digital forensics and penetration testing recently released a new version. This version was more important than the one released last year because it came with a new version of the Metasploit framework.

According to the makers of the Metasploit framework, "It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development."

Among the payloads that Metasploit has, there is one that is used to specifically built to exploit android devices by creating a fake app that opens a backdoor in your phone to an attacker once installed. Once this back door is open, anything, and everything that is on your phone can be accessed by an attacker.

One must think that if they don't download and use unknown apps, their phone is safe. But is it?

The fact of the matter is that a backdoor can be cleverly hidden in a picture you receive on your WhatsApp group chat. Since you most likely have auto download, you will execute the said backdoor unknowingly.

Corporate risks caused by individual Smartphones

When looking at the bigger picture, smartphones could be a greater cyber threat to corporate organizations as company cybersecurity policies do not take into consideration the fact that phones used by their employees are also access points for attackers.

Companies have tried to evolve regarding sharing confidential documents with employees. In the past, it was USB drives, but these spread viruses, so many companies decided to innovate and use platforms like Skype to share these documents. Applications like Skype download these documents to their local storage, thus leaving them exposed to attackers as explained above.

In addition, these same smartphones are carried around by employees. Reports on mobile security, have noted that mobile devices are breached largely because people lose them or don't practice good security habits (including not applying the latest security updates) — not because of inherently weak security in devices.

Simply put, most corporate mobile security incidents are due to humans failing to follow basic security procedures. Given that reality, mobile security needs to be part of the broader policy and procedure mix.

How to keep your information safe

a) For Organizations

i. Continuous user education. People need to learn how their actions can have consequences. Training sessions on protecting corporate data and thwarting social engineering efforts should be done. Educating upper management is a different task for information technology executives. The education job here is to make sure upper management know how dire security

ii. Data encryption. Organizations should continue to invest in systems to encrypt data, protect networks and various endpoints — internet of things sensors, point of sale terminals, mobile devices, etc.

iii. Hire a digital forensics specialist. These specialists are critical to investigating security issues on all fronts, including mobile.

b) For individuals

i. Back up information to cloud services, and store as little as possible on the device.

ii. Use basic security common sense, such as ignoring spam email and avoiding downloads that don't come from an approved app marketplace (Apple's App Store, Google Play, or a company-specific area).

iii. Use two-factor authentication whenever possible.

iv. (iv)If device is lost or stolen, notify your employer right away for remote wiping procedures. For a personal device, Android and Apple's iOS offer remote wiping features.

v. Avoid unsecure Wi-Fi connections. Resist the temptation to enjoy free data.

vi. Keep Bluetooth out of discovery mode when not in use.

vii. Encrypt corporate data using the security software your company provides.

viii. Connect your smartphone to Wi-Fi networks via VPN connections.

Security tips

01

Always switch off your wireless connection when it's not in use. It ensures that people can't connect to a device without your knowledge. It's also worth checking your phone's network security settings as it might be configured to automatically connect to a network when in range without you knowing.

02

Unfortunately the increase in malware relating to smartphones has increased the need to be cautious when downloading applications, and to pay attention to the requirements that any software requires when you install. It can be very easy not to read anything in an effort to get the app up and running, but be careful of any demands to access various features of your phone, particularly if the app isn't well known.

Reconsider your Business Continuity Strategy

Kenya recently suffered a terrible terrorist attack at the DusitD2 complex on Riverside Drive. This complex houses many businesses and among them, a bank. It goes without saying that business operations of this bank were disrupted in one way or another. One needs to pause and reflect on how the financial institution with which they transact suffered such a tragedy.

In the finance industry, disasters are especially dangerous as disruptions to a single branch's operations have the power to tarnish the entire brand and disrupt the entire institution's operations. For example, a survey conducted in July 2012 following the Tohoku earthquake, which inflicted mayhem in Japan in 2011, 11.4% of firms indicated that, following the earthquake, firms complained that the bank that was their most important source of lending could not operate the branch with which they transacted, and 4.8% of firms replied that they were adversely affected by the fact that the bank with which they transacted suffered damage as a result of the earthquake.

As seen in the above examples, despite the substantial indirect effects of disasters, more focus is put solely on disaster preparedness rather than business continuity. It is therefore very important for financial institutions to invest in developing robust Business Continuity Plans (BCP).

New business practices, changes in technology, and increased terrorism fears have focused even greater attention on the need for effective BCP and have changed the traditional thinking about an effective plan. The crucial element to any BCP is an impact analysis differentiating between critical and non-critical functions. Crucial functions may include the data of the business, physical cash at the premises, loss of crucial staff and systems among others.

As financial institutions spend more resources to protect the physical assets of the bank, critical controls to manage data protection and prevent cyber attacks may be completely ignored. In the last three weeks alone there have been data breaches of catastrophic impact all over the world. One is left to wonder what a financial institution can do to protect their reputation incase such disasters happens to them.

From a different perspective, institutions need to think of business continuity processes to prevent emergencies from turning into disasters. Let us take a look at the following scenarios:

Visit https://www.forensicsinstitute.org/11941-2/ to read more

IFIS
Institute of Forensics & ICT Security
Forensics. Security. Training

Transform Your Career with a

DIPLOMA in INFORMATION SECURITY & COMPUTER FORENSICS

Attain the skills in high demand by every employer

contact us on 4th Foor, Block B, Ntinda Complex
Plot 33, Ntinda Road Opp St Luke Church,
P.O. Box 40292, Kampala, Uganda
M: 256(414) 231136
E:admissions@forensicsinstitute.org

Visit >> www.forensics**institute**.org to enroll

This **Diploma in Information Security & Computer Forensics (DISCoF)** will give you the requisite skillsets to design, deploy and manage security architecture for your organization.

Get the skills in demand today. Become a DISCoF today

DIPLOMA in INFORMATION SECURITY & COMPUTER FORENSICS

With Practical Skills, You Succeed