2. "Current technology advancements and information security threat's"

Dr. Biju Nathan
Pune, India
bijunathan@yahoo.com

Abstract— *with advancement in technology there are information security across all industry. New technologies are developed and new threats keep coming. More over with social networking becoming very popular and a basic necessity, there is no surprise that there has been breach of security across various sites. With over millions of members combined it takes a single person or a group to cause a major damage. This paper focuses on learning from the various Information Security threats and how to deal with the threats.*

Keywords—Breach, Networking, Security, Privacy, Anti Virus

I. Current world Scenario

In current world scenario there is lot of technology advancement. The use of technology is primarily to make our work and life easier. The other side of technology is bringing the people closer. This has been achieved where technology is a key contributor in our life. Networking sites have brought people closer. It is much easier to connect with each now as compared to earlier years. However the technology advancement has also brought in privacy and security issues. There is private data available in the networking site and it is vulnerable to breaches.

One of the resent security threat was WannaCry ransomware attack was a worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system. Recently Yahoo accounts were compromised as hackers were able to get access to password of a billion Yahoo users. In 2016 the founder of Facebook, Mark Zuckerberg's Facebook book account was breached. There are some of the security threats in current world.

II. Key contributors

Fig. 1. Privacy threats

A security issue occurs when there is a unauthorized access to a site's. An unwarranted access of private information could also be unintentional or intentional. Someone can gain access to confidential information by simply watching you type your password. And use this information for their own benefit. On social networks ssecurity lapses necessarily involve the exploitation of a user's private information.

III. The reason

The reason social network security and privacy lapses happen simply from large amounts of information the sites process each and every day that contributes to making it that much easier to exploit a single flaw in the system.

The data put in by various users in the networking sites are not protected. It is available to public. The credential used to login to their accounts are not secured. With algorithms easily available it can be easily cracked.

Problems also occur due to the lack of security software's in the devices used to access the networking devices. In cases where public computers are used, a hidden program in many a case captures all details and passes on to a hacker.

Another reasons can be:-

- Phishing
- Security issues on the network
- Application breach
- Negligence

IV. The Solution

Fig. 2. The Key to threats

With the growth of social networks, it's becoming harder to effectively monitor and protect site becoming harder to effectively monitor and protect site users and their activity. Even though there are problems with privacy and social network security which also seems to continue in future as world is moving towards a digital age. By taking some careful approach a lot can be secured.

Few of the ways in which it can be tackled are

1. PDP - Personal Data Protection

Protection of Personal data on the internet is most critical. All the application need personal data to create an account. As such the personal data is already there in the internet with a third party. This also means there is risk to the data if there is a data leakage from the application or if a person has not enabled the settings to protect personal data. There is a need to know this and enable data protection mechanisms available in the applications.

2. Accessing Data over a network

It has become a necessity to be online most of the time, this also imposes to use any available network. Many a time when the network is accessed over a public network like a public wifi there is a risk that the personal data can be breached by a hacker.So it a need to avoid such network or use it using a private VPN.

3. Complex password

An individual has access to multiple application. Each application also needs its own login credential. It is difficult to remember all of them. Hence individual use some generic or common credentials. Example date of birth, name of individual etc. This also creates threat as it can be easily cracked by a hacker as most of the data is already available online. There is a need of creating a strong passwords to enable security.

4. Awareness on Phishing

Phishing is a form of fraud. It is basically a attempt to obtain sensitive information such as user names, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Emails are used as a primary source for phishing. Before opening any email or responding to them a check on the authenticity can help prevent such attack.

5. Securing the device

Laptops and Mobile have become primary device to surf the net. However the reach of mobile is very high due to competitiveness and ease to handle. It is the most primary source.

It has become a priority to secure the device by having the latest OS, anti virus applications in place, enabling security settings and having lock protection on data and application. Hackers can take advantage of vulnerabilities in operating systems (OS) and applications if they are not properly patched or updated. This puts all of the data on those system and other connected systems at risk.

This could be some common steps for security. Genuine application must be used. In both the devices the applications also needs to be upgraded with the latest releases, so that the threats are prevented.

V. SUMMARY

In the current digital age, there is a threat to data. However there is away to over come security issues, this is possible by taking steps which are already built in to the applications and devices being used. This can be the initial step towards security.

References

[1] http://en.wikipedia.org/wiki/Information_security
[2] https://www.pcisecuritystandards.org
[3] https://www.owasp.org/