THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-41-December-2019

A Research Paper on Social Engineering and Growing Challenges in Cyber Security

Shashikanth Kandukuri and Gangadhara Srikanth
Assistant Professor, CSE Department, VITS (N6), Karimnagar, Telangana

ABSTRACT
Social engineering is the art of manipulating people so they give confidential information. The types of information on these criminals can vary, but when individuals are targeted, criminals usually ignore you by giving them passwords or bank information, or to secretly install malicious software Access the computer - which will give them access to your password and bank information as well as give them control over their computer Right.

Integrating national economies with the global market, and enabling citizens or "netizens" to access more and more e-services. Safety of critical infrastructure operations has emerged as a major challenge. The reason for this is that billions of dollars go through the network every day, encompassing a wide range of activities including e-commerce, e-governance, travel, hospitality, health care, and general communications. Electricity distribution, water distribution and many other utility services are based on ICT infrastructure. The defense sector relies heavily on electronic systems.

INTRODUCTION

Social engineering, in the circumstances of state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this, by controlling the emotional state of people into performing actions or uncovering the sensitive information that is restricted to an individual or an Organization. A type of relying trick for the cause of information collecting, fraud, or system access, it differs from a traditional "dupe" in that it is often one of many steps in a more compound artifice scheme.

Criminals use social engineering tactics because it is usually easy to exploit their natural inclination to rely on which it is to discover ways to hack your software. For example, it's very easy to fool you into giving someone your password, because you try to hack their password (unless the password is really weak). Safety everyone knows who and what to trust. It is important to know when and what not to take a person at their word and when the person you are communicating with says who they are.

Cyberspace includes IT networks, computer resources and all fixed and mobile devices connected to the global Internet. A nation's cyberspace is part of global cyberspace; since cyberspace is borderless, it cannot be separated to define its boundaries. This is what makes cyberspace unique. Unlike the physical world, which is limited by geographic boundaries in space — land, sea, river water, and air — cyberspace can and continues to expand. Increased Internet access is leading to the development of cyberspace, as its size is proportional to the activities occurring through it.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

CHALLENGES OF CYBER SECURITY

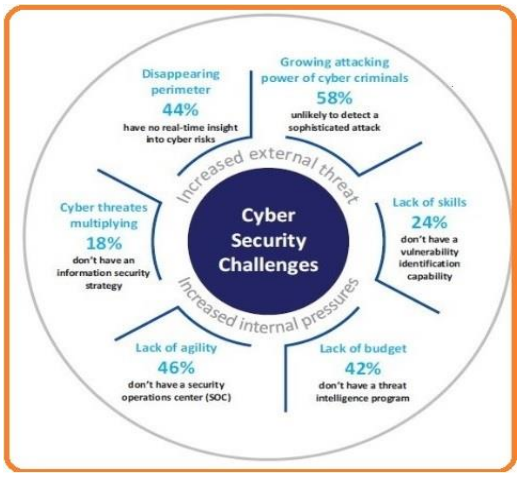

Figure: Challenges in Cyber Security

1. NETWORK SECURITY:

THREAT #1: UNKNOWN ASSETS ON THE NETWORK

There are many businesses that don't have a complete inventory of all of the IT assets that they have tied into their network. This is a *massive* problem. If you don't know what all of the assets are on your network, how can you be sure your network is secure?

The easiest fix for this is to conduct a review of all the devices on your network and identify all of the various platforms they run. By doing this, you can know what all of the different access points are on your network and which ones are most in need of security updates.

THREAT #2: ABUSE OF USER ACCOUNT PRIVILEGES

According to data cited by the Harvard Business Review, for the year of 2016, "60% of all attacks were carried out by insiders." Whether it's because of honest mistakes (accidentally sending info to the wrong email address or losing a work device), intentional leaks and misuse of account privileges, or identity theft arising from a phishing campaign or other social engineering attack that compromises their user account data, the people inside your business represent one of the biggest security problems you'll ever face.

Because these threats come from trusted users and systems, they're also among the hardest to identify and stop.

However, there are ways to minimize your risk in case of an insider attack. For example, if your company uses a policy of least privilege (POLP) when it comes to user access, you can limit the damage that a misused user account can do. In a POLP, every user's access to the various systems and databases on your network is restricted to just those things that they need to do their jobs.

THREAT #3: UNPATCHED SECURITY VULNERABILITIES

Many businesses are concerned with "zero day" exploits. These exploits are those unknown issues with security in programs and systems that have yet to be used against anyone. However, zero day vulnerabilities aren't the problem unpatched known vulneratbilites are the problem.

This is because when a "zero day" exploit is used it can be discovered—becoming a known issue that the software vendor can begin working on. The more often the exploit is used, the more likely it is to get discovered and patched. Also, it takes a lot of effort to independently discover a completely unknown vulnerability in a system.

THREAT #4: A LACK OF DEFENSE IN DEPTH

Eventually, despite all of your best efforts, there will be a day where an attacker succeeds in breaching your network security. However, just how much damage this attacker will be capable of depends on how the network is structured.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

The problem is that some businesses have an open network structure where once an attacker is in a trusted system, they have unfettered access to all systems on the network.

If the network is structured with strong segmentation to keep all of its discrete parts separate, then it's possible to slow down the attacker enough to keep them out of vital systems while your security team works to identify, contain, and eliminate the breach.

THREAT #5: NOT ENOUGH IT SECURITY MANAGEMENT

Another common issue for many companies is that even when they have all of the best cybersecurity solutions in place, they might not have enough people in place to properly manage those solutions.

When this happens, critical cybersecurity alerts may get missed, and successful attacks may not be eliminated in time to minimize damage.

However, finding a large enough internal IT security team to manage all of your needs can be an expensive and time-consuming process. Qualified professionals are in demand, and they know it.

To build up IT security staff quickly, many businesses use the services of a dedicated partner such as Compuquip Cybersecurity. This allows these businesses to access a full team of experienced cybersecurity professionals for a fraction of the cost of hiring them full-time internally.

Some businesses use these cybersecurity solutions partners to shore up their IT security departments in the short-term while they're preparing their own internal cybersecurity teams.

2. APPLICATION SECURITY:

This security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities.

Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security. But security measures at the application level are also typically built into the software, such as an application firewall that strictly defines what activities are allowed and prohibited. Procedures can entail things like an application security routine that includes protocols such as regular testing.

APPLICATION SECURITY DEFINITION:

Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

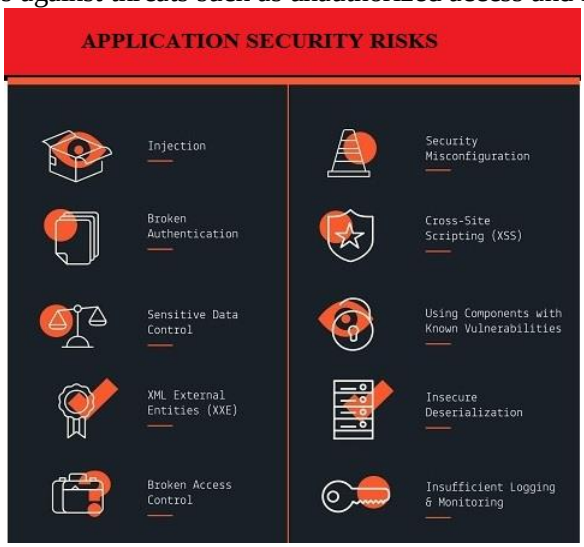

Figure 2.1: Application Security Risk in Cyber Security

ISSN:0971-1260

Vol-22-Issue-41-December-2019

IMPORTANCE OF APPLICATION SECURITY:

Application security is important because today's applications are often available over various networks and connected to the cloud, increasing vulnerabilities to security threats and breaches. There is increasing pressure and incentive to not only ensure security at the network level but also within applications themselves. One reason for this is because hackers are going after apps with their attacks more today than in the past. Application security testing can reveal weaknesses at the application level, helping to prevent these attacks.

TYPES OF APPLICATION SECURITY

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

i. Authentication

ii. Authorization

iii. Encryption

iii. Logging:

iv. Application security testing

3. END POINT SECURITY

Endpoint Security, Endpoint Protection refers to the approach of protecting a business network when accessed by remote devices like smartphones, laptops, tablets or other wireless devices. It includes monitoring status, software, and activities. The endpoint protection software is installed on all network servers and on all endpoint devices.

Endpoint security is about securing your enterprise endpoints (mobile devices like laptops, smartphones and more) – and, of course, the enterprise against the dangers posed by these endpoints as well – whereas network security is about taking security measures for protecting your entire network (the whole IT infrastructure) against various security threats.

The main difference between endpoint security and network security is that in the case of former, the focus in on securing endpoints, and in the case of latter, the focus is on securing the network. Both types of security are important. Ideally, it's best to start from securing the endpoints and building out. You wouldn't leave the doors to your home open, just because there's a security guard out there, would you? In the same sense, both are important and should be given equal importance, starting from the endpoints and slowly building out.

4. DATA SECURITY AND ITS IMPORTANTANCE:

All businesses today deal in data to a degree. From the banking giants dealing in massive volumes of personal and financial data to the one-man business storing the contact details of his customers on a mobile phone, data is at play in companies both large and small.

The primary aim of data security is to protect the data that an organization collects, stores, creates, receives or transmits. Compliance is also a major consideration. It doesn't matter which device, technology or process is used to manage, store or collect data, it must be protected. Data breaches can result in litigation cases and huge fines, not to mention damage to an organization's reputation. The importance of shielding data from security threats is more important today than it has ever been.

DIFFERENT DATA SECURITY TECHNOLOGIES:

Data security technology comes in many shapes and forms and protects data from a growing number of threats. Many of these threats are from external sources, but organizations should also focus their efforts on safeguarding their data from the inside, too. Ways of securing data include:

1. Data encryption

2. Data masking

ISSN:0971-1260

Vol-22-Issue-41-December-2019

3. Data erasure
4. Data resilience**:**
5. Data Security Compliance and Standards

THE FIRST STEPS TO A SOLID DATA SECURITY STRATEGY

It is entirely possible to enforce a solid data security strategy that protects your most vulnerable data without restricting employees or affecting productivity. Forcepoint's Data Loss Prevention (DLP) solution helps you to identify the data, identify your riskiest users in seconds and share data with third parties with confidence.

5. IDENTITY MANAGEMENT

Identity management (IdM), also known as identity and access management (IAM or IdAM), is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. IdM systems fall under the overarching umbrellas of IT security and Data Management . Identity and access management systems not only identify, authenticate and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access. Identity and Access Management solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

The terms "identity management" (IdM) and "identity and access management" are used interchangeably in the area of Identity access management.

Identity-management systems, products, applications and platforms manage identifying and ancillary data about entities that include individuals, computer-related hardware, and software applications.

IdM covers issues such as how users gain an identity, the roles and, sometimes, the permissions that identity grants, the protection of that identity and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.).

6. DATABASE AND INFRASTRUCTURE SECURITY

Database security covers and enforces security on all aspects and components of databases. This includes:

- Data stored in database
- Database server
- Database management system (DBMS)
- Other database workflow applications

Database security is generally planned, implemented and maintained by a database administrator and or other information security professional.

Some of the ways database security is analyzed and implemented include:

- Restricting unauthorized access and use by implementing strong and multifactor access and data management controls.
- Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload
- Physical security of the database server and backup equipment from theft and natural disasters
- Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

7. CLOUD SECURITY:

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

Why is cloud security important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

8. MOBILE SECURITY

Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security.

Securing mobile devices has become increasingly important in recent years as the numbers of the devices in operation and the uses to which they are put have expanded dramatically. The problem is compounded within the enterprise as the ongoing trend toward IT consumerization is resulting in more and more employee-owned devices connecting to the corporate network.

9. DISASTER RECOVERY/BUSINESS CONTINUITY PLANNING

In order to prosper in today's business marketplace, Cyber Security, Disaster Recovery planning and Business Continuity must stay top of mind for business leaders. One of an organization's objectives is to take strategic steps positioning itself in the best position to prosper in a very competitive marketplace. By not focusing enough resources on Cyber Security, Disaster Recovery or Business Continuity planning, an organization leaves itself vulnerable. Its existence could be threatened by any one of these significant factors.

10. END-USER EDUCATION

10.1: END-USER EDUCATION – THE BEST LINE OF CYBERSECURITY DEFENSE

Not educating your end-users in cybersecurity initiatives is like trying to keep a flood at bay using a screen door. Your end-users are the first line of defense against cybersecurity attacks (like phishing scams). So, how do you educate your user? What needs to happen?

Here are three steps you can take to make cybersecurity top of mind in your organization:

1. Implement a cybersecurity policy and procedure document.
2. Use a tool that creates a fake phishing email and see how many of your end-users open it.
3. Deploy a cybersecurity awareness certification program as a part of your continuing education process.

11. CONCLUSION:

The above challenges can be under surveillance and methodical steps can be taken to avoid such malpractices. To solve data theft problem, online space must regulate the use of data and clearly indicate when information will be shared provided by the users. The user can then choose to opt out, leaving personal information restricted to the space for which it was deliberated. When software online contains bugs or viruses, it is fairly easy for cyber criminals to gain personal information. Large technology firms should collaborate and create solutions that to increase security for their customers. Security controls need to move

ISSN:0971-1260

Vol-22-Issue-41-December-2019

outward, beginning at the application level where such frauds can be caught easily. When there are no unified monitoring methods, firms become vulnerable. However, when every network has monitoring that detects changes, data can be protected.

REFERENCES:

[1] https://www.compuquip.com/blog/5-common-network-security-problems-and-solutions

[2] https://www.vmware.com/topics/glossary/content/application-security
https://www.forcepoint.com/cyber-edu/data-security

[3] https://en.wikipedia.org/wiki/Identity_management

[4] https://www.techopedia.com/definition/29841/database-security

[5] https://www.forcepoint.com/cyber-edu/cloud-security

[6] https://whatis.techtarget.com/definition/mobile-security

[7] https://efprgroup.com/news/article-publication/it-consulting/importance-cyber-security-disaster-recovery-business-continuity-ever-changing-world/

[8] https://www.proserveit.com/blog/end-user-education-best-cybersecurity-defense

[9] "Social Engineering Defined - Security Through Education". Security Through Education. Retrieved 3 October 2018.

[10] Knowing Your Data to Protect Your Data Archived 2017-09-28 at the Wayback Machine.

[11] *Lee, Sung-Min; Suh, Sang-bum; Jeong, Bokdeuk; Mo, Sangdok (January 2008).* A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization. *5th IEEE Consumer Communications and Networking Conference,2008.CCNC2008.* doi*:10.1109/ccnc08.2007.63.* ISBN 978-1-4244-1456-7. *Archived from* the original *on May 16, 2013.*

[12] *Inc, Gartner.* "Endpoint Security and Protection Software Reviews". *Gartner*. Retrieved December 24, 2019.

[13] *Gross, Ralph; Acquisti, Alessandro; Heinz, J. H. (2005). "Information revelation and privacy in online social networks". Workshop On Privacy In The Electronic Society; Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 71–80.* doi*:*10.1145/1102199.1102214. ISBN 978-1595932280.

[14] *"Disaster Recovery & Business Continuity Plans". Stone Crossing Solutions. 2012. Archived from* the original *on 23 August 2012.* Retrieved 9 August 2012.

[15] IISFA Italian Chapter – International Information Systems Forensics Association