A REVIEW PAPER ON INFORMATION SECURITY AND CRYPTOGRAPHY

Y. Durga Tejaswi[1]
CSE department, VITS
Karimnagar, Telangana
yagnapudurgatejaswi4@gmail.com

T.Sahithi[2]
CSE department, VITS
Karimnagar, Telangana
sahithisriguptha@gmail.com

Firdous Fathima[3]
CSE department, VITS
Karimnagar, Telangana

ABSTRACT

Security is a state of being secure free from danger. Information security is a practice of defending digital information from unauthorized. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data while maintaining a focus on efficient policy implementation, all without hampering organization productivity. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types in order to keep information in all its locations and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and audit ability."

Keywords: *Information Security, Threats, cryptography, security, private key, public key.*

1. INTRODUCTION

The internet is a worldwide collection of loosely connected networks that are accessible to anyone with a computer and a network connection. Thus, individuals and organizations can reach any point on the internet without regard to national or geographic boundaries or time of day. Along with the convenience and easy access to information come risks. Among them are the risks that valuable information will be lost, stolen, changed, or misused. Intruders can steal or tamper with information without touching a piece of paper or a photocopier. They can also create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

Three basic security concepts important to information on the internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and no repudiation. This paper explains all of these concepts.

2. CHARACTERISTICS

The 3 key characteristics of information that must be protected by information security.

Confidentiality

Only authorized parties can view information. In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes."While similar to "privacy," the two words aren't interchangeable. Rather, confidentially is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

Information is correct and not alerted over its entire life-cycle. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

Data is accessible to authorized users whenever needed. For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Good policy has the following seven characteristics:

- Endorsed – The policy has the support of management.
- Relevant - The policy is applicable to the organization.
- Realistic – The policy makes sense.
- Attainable – The policy can be successfully implemented.
- Adaptable – The policy can accommodate change.
- Enforceable – The policy is statutory.
- Inclusive – The policy scope includes all relevant parties.

Endorsed

We have all heard the saying “Actions speak louder than words.” In order for an information security policy to be successful, leadership must not only believe in the policy, they must also act accordingly by demonstrating an active commitment to the policy by serving as role models. This requires visible participation and action, ongoing communication and championing, investment, and prioritization. Nothing will doom a policy quicker than having management ignore, or worse, disobey or circumvent it. Conversely, visible leadership and encouragement are two of the strongest motivators known to human kind.

Relevant

Strategically, the information security policy must support the guiding principles and goals of the organization. Tactically, it must be relevant to those who must comply. Introducing a policy to a group of people who find nothing recognizable in relation to their everyday experience is a recipe for disaster. Policy writing is a thoughtful process that must take into account the environment. If policies are not relevant, they will be ignored or worse, dismissed as unnecessary and management will be perceived as being out of touch.

Realistic

Think back to your childhood to a time you were forced to follow a rule you did not think made any sense. The most famous defense most of us were given by our parents in response to our protest was “Because I said so!” We can remember how frustrated we became whenever we heard that statement, and how it seemed unjust. We may also remember our desire to deliberately disobey our parents – to rebel against this perceived tyranny. In very much the same way, policies will be rejected if they are not realistic. Policies must reflect the reality of the environment in which they will be implemented.

Attainable

Information security policies and procedures should only require what is possible. If we assume that the objective of a policy is to advance the organization’s guiding principles, one can also assume that a positive outcome is desired. A policy should never set up constituents for failure; rather, it should provide a clear path for success. It is important to seek advice and input from key people in every job role in which the policies apply. If unattainable outcomes are expected, people will fail. This will have a profound effect on morale and will ultimately affect productivity. Know what is possible.

Adaptable

In order to thrive and grow, businesses must be open to changes in the market and willing to take measured risks. An adaptable information security policy recognizes that information security is not a static, point-in-time endeavor, but rather an ongoing process designed to support the organizational mission. The information security program should be designed in such a way that participants are encourage to challenge conventional wisdom, reassess the current policy requirements, and explore new options without losing sight of the fundamental objective. Organizations that are committed to secure products and services often discover it to be a sales enabler and competitive differentiator.

Enforceable

Enforceable means that administrative, physical, or technical controls can be put in place to support the policy, that compliance can be measured and, if necessary, appropriate sanctions applied. If a rule is broken and there is no consequence, then the rule is in effect meaningless. However, there must be a fair way to determine if a policy is violated, which includes evaluating the organization support of the policy. Sanctions should be clearly defined and commensurate with the associated risk.

Inclusive

It is important to include external parties in our policy thought process. It used to be that organizations only had to be concerned about information and systems housed within their walls. An information security policy must take into account organization objectives; international law; the cultural norms of its employees, business partners, suppliers, and customers; environmental impacts and global cyber threats. The hallmark of a great information security policy is that it positively affects the organization, its shareholders, employees, and customers, as well as the global community.

3. OBJECTIVES

The objective of an information security policy and corresponding program is to:

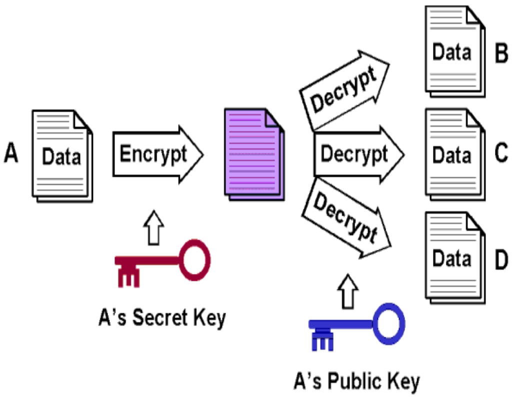
- Protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information;
- Protect the integrity of the information; and
- Ensure the availability of information systems.

Successful information security policies establish what must be done and why it must be done, but not how to do it.

4. CRYPTOGRAPHY

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted can be transformed back into its original usable form by an authorized user who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage.

Cryptography provides information security with other useful applications as well, including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry-accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure solutions address many of the problems that surround key management.



5. THREATS

Security threat: any action/inaction that could cause disclosure, alteration, loss, damage or

There are three components of threat:

Targets: organization's asset that might be attacked
Information (its confidentiality, integrity, availability), software, hardware, network service, system resource, etc.

Agents: people or organizations originating the threat – intentional or non-intentional
Employees, ex-employees, hackers, commercial rivals, terrorists, criminals, general public, customers.

Events: type of action that poses the threat
Misuse of authorized information, malicious / accidental alteration of information, malicious / accidental destruction of information, etc.

6. CONCLUSION

Information security should not be taking lightly when considering the repercussions offailure.With the institution of any new program or information system, the level of safety and responsibility is required to ensure business continuity and safety for the information that is derived from the data used in the system. The information in this report presented the proposedKudler fine foods customer loyalty program and a look at the possible safety issues that the program may represent. A look at top threats was identified as user authentication, network vulnerabilities, system backups, malicious intrusion attempts, and data access restrictions. Recommendation for security access procedures with regular data backup to the system was suggested to maintain system integrity.

7. REFERENCES

1. https://en.wikipedia.org/wiki/Information_security#Definitions
2. https://www.sciencedirect.com/science/article/pii/S0167404808001168
3. https://www.emeraldinsight.com/doi/abs/10.1108/09685229810227649
4. https://www.sagedatasecurity.com/blog/seven-characteristics-of-a-successful-information-security-policy
5. https://www.eecs.yorku.ca/course_archive/2013-14/F/4482/CSE4482_01_Introduction_2013_posted.pdf
6. Anderson, D., Reimers, K. and Barretto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge.publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)
7. Security notification laws National Conference of State Legislatures. 12 April 2017. Retrieved 25 January 2018.