International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Fundamental Areas of Cyber Security on Latest Technology

Aye Mya Sandar[1], Ya Min[2], Khin Myat Nwe Win[3]

[1]Lecturer, Information Technology Supporting and Maintenance Department, University of Computer Studies (Mandalay)
[2]Lecturer, Faculty of Computer Science Department, University of Computer Studies (Lashio), Shan State, Myanmar
[3]Lecturer, Faculty of Computer Science Department, University of Computer Studies (Mandalay), Mandalay, Myanmar

How to cite this paper: Aye Mya Sandar | Ya Min | Khin Myat Nwe Win "Fundamental Areas of Cyber Security on Latest Technology" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.981-983, **https://doi.org/10.31142/ijtsrd26550**

IJTSRD26550

ABSTRACT

Cyber Security has developed one of the biggest challenges of information technology in the present day. Cyber security consists of controlling physical access of the hardware, application, networks and protecting against harm that may come via networks. It is a mixture of processes, technologies and practices. The objective of cyber Security is to protect programs, application, networks, computers and data from attack. Moreover, various measures of cyber security is quite a very huge concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on the latest about cyber security techniques, ethics and the trends changing the face of cyber security. This paper mainly focuses on cyber Security and its fundamental elements on latest technologies.

KEYWORDS: *cyber security, cybercrime, Security Attacks*

I. INTRODUCTION

Every day, new data threats are emerging that well-resourced companies are getting hacked despite the best efforts from cyber security specialists on a daily basis. This indicates the essential for new technology advancements because the existing technologies may be limited or not working. The attackers have been continually devising new strategies for launching attacks, which reminds the need for the innovation and evolution of defense capabilities to ensure data integrity in organizations Cyber security specialists now have to deal with the threats from the cloud, mobile, wireless, and wearable technology. Data that was once stored in systems are now being transmitted through a variety of data centers, routers, and hosts. [1].

The latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. also need a high level of security. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic safety. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes. The fight against cybercrime needs a comprehensive and safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts. [2]

In today's Internet-connected world where technologies support almost every feature of our society, cyber security and forensic specialists are increasingly dealing with wide-ranging cyber threats in almost real-time conditions. The capability to detect, analyze, and defend against such threats in near real-time conditions is not possible without the employment of threat intelligence, big data, and machine learning techniques. [3]

II. CYBER SECURITY

In [5]**, Cyber security** is the techniques of protecting computers, networks, programs and data from unauthorized access or cyber attacks that are aimed for exploitation. Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

In today's connected world, everyone benefits from advanced cyber defense programs. At an individual level, a cyber security attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructures like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning. [5]

Implementing actual cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. A safe and secure Internet is a global Internet governance priority. There are many threats that can undermine the security and stability of cyberspace, impacting governments, business, civil society groups and individual users. Cyber-attacks, or cybercrime, can come in many forms, resulting in loss of services or loss of control over services, stolen personal information (such as credit card details), fraud and identity theft and receiving a high volume of spam messages. A range

of actors execute cyber-attacks, including national governments, criminals, business, hacker groups or individual hackers. Attacks can be carried out by spreading computer viruses, denial of service attacks (DDoS), phishing, or hacking. [6]

With the increasing use of digital technologies such as the cloud, big data, mobile, IoT (The Internet of Things) and Artificial Intelligence (AI) in ever more areas of business and society and the growing connectivity of everything come greater challenges on the level of security, compliance and data protection and regulations such as the GDPR (The General Data Protection Regulation) that want to make sure organizations effectively tackle them. Cyber security has developed a key strategic priority for digital business and is a topic we need to be open about if we want to succeed in digital transformation. Moreover, in order to be able to update and realize their digital potential in regards to any given business and customer goal, organizations want security approaches that enable them to focus on their business, a phenomenon which is changing the face of the cyber security industry. [8]

III. FUNDAMENTAL AREAS OF CYBERSECURITY

One of the most challenging elements of cyber security is the constantly evolving nature of security risks. The traditional method has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks. In [4], the researchers studied the major areas which are included in cyber securities are as follows:

A. Application security

Application security is the expenditure of software, hardware, and procedural methods to protect applications from external threats. In software design, security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data**.** Application security embraces steps taken through an information application's lifecycle to thwart any attempts to transgress the authorization limits set by the security policies of the underlying system. In the context of application security, an asset refers to a resource of value like information within a database or in the file system or system resource. The challenge is to identify the vulnerabilities within the parent system which when becomes exposed to the cyber attacker can be exploited to provide valuable insights into the functioning of the application. The risk can be mitigated by weaving security within the application. [4]

B. Information security

Information security (InfoSec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. Information security includes safeguarding sensitive information from illegitimate access, usage, revelation, disruption, alteration, reading, inspection, damage or recording. This is an assurance that critical data is not lost when any issue like natural disasters, malfunction of system, theft or other potentially damaging situation arises. [4]

C. Network security

Network security refers to comprehensive security policies and provisions adopted in an adaptive and proactive manner by the network administrator for thwarting and monitoring unauthorized access, deliberate misuse, alteration, denial of service for a computer host and other network-accessible and interaction related resources. It involves checking the privilege rights of users to validate the legitimacy of users and grant them access to the network's data or allow for the exchange of information. Network security extends coverage over diverse computer networks, encompassing private and public that is used for transacting and communicating among organizations. The communication occurring among network hosts can be encrypted to avoid eavesdropping. Deployment of decoy network-accessible resources will serve as surveillance and early warning measures. Techniques employed by attackers for compromising the decoy resources can be studied post-attack to understand their logic behind the development of new exploitation means. [4]

D. Disaster recovery/business continuity planning

Business continuity is the process of summoning into action planned and managed procedures which enable an organization to carry out the operation of its critical business units, while a planned or unintentional disruption hampering regular business operations is in effect. Once a cyber-attack has brought the business to a standstill by crippling the information systems, this disaster recovery planning plays a vital role in keeping critical parts ticking to make the business survive. The planning assists in bringing down the recovery cost and operational overheads. [4]

E. Operational security

Operational security (OPSEC) is an analytical process that classifies information assets and determines the controls required to protect these assets. OPSEC originated as a military term that described strategies to prevent potential adversaries from discovering critical operations-related data. As information management and protection has become important to success in the private sector, OPSEC processes are now common in business operations. [4]

F. End-user education

The human element in cyber security is the weakest link that has to be sufficiently trained to make less vulnerable. Comprehensive security policies, procedures and protocols have to be understood in depth by users who regularly interact with the highly secure system and accessing classified information. Periodic end-user education and reviews are imperative to highlight the organizational weaknesses, system vulnerabilities and security loopholes to the user. Sound security behavior of users should take precedence over other aspects. Better human element protocols in the security chain can be established by gaining insights into the viewpoints of users regarding technology and response to security threats. Training sessions will lead to further research in the region of human-machine

interactions. Cybercrimes are increasingly becoming social engineering, wherein perpetrators of the crime invest resources to gain knowledge about organizational stakeholders. Training will allow senior management to familiarize themselves with system users that will help to better nurture awareness regarding user-specific access privileges and internal sources capable of providing access to confidential information. User training will help eliminate resistance to change and lead to closer user scrutiny. [4]

IV. CYBER SECURITY ON LATEST TECHNOLOGIES

The link of [8], Freelance writer of John P. Mello Jr proposed emerging technologies include a variety of technologies such as educational technology, information technology, nanotechnology, biotechnology, cognitive science, psych technology, robotics, and artificial intelligence. Here are five emerging security technologies that may be able to do that.

1. Hardware authentication

The shortages of usernames and passwords are well known. Clearly, a more secure form of authentication is needed. One method is to bake authentication into a user's hardware. Intel is moving in that direction with the Authenticate solution in its new, sixth-generation Core v Pro processor. It can combine a variety of hardware-enhanced factors at the same time to validate a user's identity Hardware authentication can be particularly important for the Internet of Things (IoT) where a network wants to ensure that the thing trying to gain access to it is something that should have access to it.[8]

2. User-behavior analytics

Once someone's username and password are compromised, whoever has them can waltz onto a network and engage in all kinds of malicious behavior. That behavior can trigger a red flag to system defenders if they're employing user behavior analytics (UBA). The technology uses big data analytics to identify anomalous behavior by a user. Visibility into an activity that does not fit the norm of the legitimate user can close a blind spot in the middle of the attack chain. If the think of the attack chain as initial penetration, lateral movement, and then compromise, theft, and exfiltration of sensitive data, the middle links in that attack chain have not been very visible to enterprise security pros, and that's why the interest in user behavior analytics today.[8]

3. Data loss prevention

A key to data loss prevention is technologies such as encryption and tokenization. They can protect data down to field and subfield level, which can benefit an enterprise in a number of ways:

- Cyber-attackers cannot monetize data in the event of a successful breach.
- Data can be securely moved and used across the extended enterprise business processes and analytics can be performed on the data in its protected form, dramatically reducing exposure and risk.
- The enterprise can be greatly aided in compliance with data privacy and security regulations for the protection of payment card information (PCI), personally identifiable information (PII) and protected health information (PHI).[8]

4. Deep learning

Deep learning encompasses a number of technologies, such as artificial intelligence and machine learning. Regardless of what it's called, there a great deal of interest in it for security purposes, the user behavior analytics, deep learning focuses on anomalous behavior where malicious behavior deviates from legitimate or acceptable behavior in terms of security.[8]

5. The cloud

The cloud is going to have a transformative impact on the security technology industry generally. More organizations use the cloud for what has traditionally been the domain of on-premises IT, more approaches to security that are born in and for the cloud will appear. On-premises techniques will be transitioned to the cloud. Things such as virtualized security hardware, virtualized firewalls, and virtualized intrusion detection and prevention systems. But that will be an intermediate stage of the infrastructure as a service provider can do on a very large scale for all of its customers, there may not be the need to pull out all the defenses of need and also will build that into their platform, which will relieve the need to do that for the individual cloud customer.[8]

V. CONCLUSION

Computer security topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. The latest technologies, the new cyber tools and threats that come to light each day, are challenging organizations with not only secure their infrastructure but also require new platforms and intelligence to do so. Nowadays, many countries and governments are stately strict laws on cyber securities in order to prevent the loss of some important information.

REFERENCES

[1] https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field

[2] G. Nikhita Reddy, G. J. Ugander Reddy (2014)."A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES".

[3] Krzysztof Cabaj, Zbigniew Kotulski, Bogdan Księżopolski and Wojciech Mazurczyk. (2018) "Cyber security: trends, issues, and challenges", EURASIP Journal on Information Security; New York Vol. 2018, Iss. 1.

[4] Jitendra Jain, Dr. Parashu Ram Pal (2017)."A Recent Study over Cyber Security and its Elements, ISSN No. 0976-5697.

[5] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[6] https://www.myanmar-responsible business.org/pdf/SWIA/ICT/Chapter-04.05-Cyber-Security.pdf

[7] https://www.i-scoop.eu/cyber-security-cyber-risks-dx/,

[8] https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield