opción

Revista de Antropología, Ciencias de la Comunicación y de la Información, Filosofía, Lingüística y Semiótica, Problemas del Desarrollo, la Ciencia y la Tecnología

Año 35, 2019, Especial N° 20
Revista de Ciencias Humanas y Sociales
ISSN 1012-1587/ ISSNe: 2477-9385
Depósito Legal pp 198402ZU45

Universidad del Zulia
Facultad Experimental de Ciencias
Departamento de Ciencias Humanas
Maracaibo - Venezuela

Opcion, Año 35, Nº Especial 20 (2019):*2899-2921*
ISSN 1012-1587/ISSNe: 2477-9385

A Study On Tools And Techniques For Business Models

Enita Rosmika[*1], Phong Thanh Nguyen[*2], Oksana M. Gushchina[3], E. Laxmi Lydia[4], K. Shankar[5]

[1]Universitas Amir Hamzah, Medan, Indonesia; shalihahilna@gmail.com
[2]Department of Project Management, Ho Chi Minh City Open University, Vietnam; phong.nt@ou.edu.vn
[3]Togliatti State University, Russia.
[4]Professor, Vignan's Institute of Information Technology(A), Department of Computer Science and Engineering, Visakhapatnam, Andhra Pradesh, India. E-mail: elaxmi2002@yahoo.com
[5]Department of Computer Applications, Alagappa University, India. E-mail: shankarcrypto@gmail.com

Abstract

In this new time of digitalization, cyber-attack are constrained by inventive, wise and profoundly expert people. Continuous synchronization enables an attacker to bit by bit get familiar with the objective system, adjust to any protective measures, and advance the attack after some time. On the off chance that we have not actualized any system security risk recognition benefits from our association, it will uncover the closure of our forthcoming overwhelming voyage. System security threat identification centers around individual stages, frameworks, systems, endpoints or practically some other IT asset. System security threats recognition is juvenile (and remarkable) in real digital security tasks. By and by digital protectors by and large rebate these methodologies for mark location and instinct. The progression for this is most likely special, including getting designs, chance hunger and choice focuses. We require a total comprehension of all parts of the information age process. Information science will deliver specialized information that takes into consideration "strategic"

revelation of a potential trade off on a framework that choose when to square and when to alert on something. This paper expects to actualize the idea of information science for system security risk identification.

Keywords: Data Science, Cyber Security, Threat Detection.

Ciencia De Datos Ecológicos En Ciberseguridad: Técnicas De Detección Y Prevención De Amenazas De Seguridad De Red

RESUMEN
En este nuevo tiempo de digitalización, los ciberataques están limitados por personas ingeniosas, sabias y profundamente expertas. La sincronización continua permite al atacante familiarizarse poco a poco con el sistema de objetivos, ajustarse a cualquier medida de protección y avanzar el ataque después de un tiempo. En caso de que no hayamos actualizado ningún beneficio de reconocimiento de riesgos de seguridad del sistema de nuestra asociación, descubrirá el cierre de nuestro próximo viaje abrumador. La identificación de amenazas de seguridad del sistema se centra en etapas individuales, marcos, sistemas, puntos finales o prácticamente algún otro activo de TI. El reconocimiento de amenazas de seguridad del sistema es juvenil (y notable) en tareas de seguridad digital reales. Poco a poco los protectores digitales en general reembolsan estas metodologías para la ubicación de la marca y el instinto. La progresión para esto es probablemente especial, incluyendo la obtención de diseños, el hambre de azar y los enfoques de elección. Requerimos una comprensión total de todas las partes del proceso de la era de la información. La ciencia de la información entregará información especializada que toma en consideración la revelación "estratégica" de una posible compensación en un marco que elige cuándo cuadrar y cuándo alertar sobre algo. Este documento espera actualizar la idea de la ciencia de la información para la identificación de riesgos de seguridad del sistema.
Palabras clave: ciencia de datos, ciberseguridad, detección de amenazas.

1 Introduction

Digital security insinuates the collection of advancements, strategies, and

practices expected to guarantee frameworks, gadgets, ventures, and data from attack, damage, or unapproved get to. Digital security may in like manner be implied as information advancement security. It is moreover portrayed as the body that wraps techniques, developments &methodologies expressly educated in order to offer protection to the frameworks, structures from interference gets to.

2 Significance of Cyber Security

Digital security is critical in light of the fact that organization, military, corporate, cash related, and therapeutic affiliations assemble, strategy, and store excellent proportions of data on PCs and various gadgets. A vital piece of that data can be fragile information, paying little respect to whether that is ensured development, cash related data, singular information, or various types of data for which unapproved access or introduction could have negative outcomes. Affiliations transmit touchy data transversely over frameworks and to various gadgets all through doing associations, and digital security depict the control focused on guaranteeing that information and the structures used to process or store it. As the volume and headway of digital strikes create, associations and affiliations, especially those that are depended with protecting information relating to national security, prosperity, or cash related records, need to figure out how to guarantee their unstable business and staff information. As in front of calendar as March 2013, the nation's top knowledge experts admonished that digital ambushes and propelled spying are the top hazard to national security, dominating even dread based abuse.

Because of the fast and voluminous development of cyber assaults, steady center is a persistent necessity for the insurance of individual information that subjects to affectability &business purposes. So as to guarantee and guarantee we have the inescapable need of different cyber components like Information security, Application security, Disaster recuperation &Network security and User Education.

The disturbing spread of security dangers is a noteworthy testing issue before cyber security. A portion of the methodologies that are in real life since the customary period are as under: CTO open part (a security specialist organization to government offices including Defense Department organizations)&Adam Vincent have depicted the issue.

I. Purpose of Attack

Categories of attacks range from intellectual property theft, identity theft and critical infrastructure attacks, tofinancial frauds. It becomes tediouswhile judging the motivation behind the hackers for attacksTheft of

credit card information and cyber crimes involving government agencies and public properties has taken the shape of trending interests of hackers.

II. Types of Threats

As we know two types of attacks are Active and Passive. Active network attacks lookout decoded information so as to discover the significant and related data and then again uninvolved passive attack at decrypting the frail encoded data/information and gaining the applicable data by making in record of the risky network zones. A portion of the cyber security dangers are arranged as under:

• Phishing

Phishing is a strategy by which cybercriminals specialty messages to trick an objective into making some unsafe move. The beneficiary may be fooled into downloading malware that is veiled as a significant record, for example, or asked to tap on a connection that takes them to a phony site where they'll be requested sensitive data like bank usernames and passwords. Numerous phishing messages are moderately unrefined and messaged to a large number of potential unfortunate casualties, however some are explicitly made for profitable objective people to attempt to get them to part with valuable data.

• Distributed Denial of Service (DDoS)

A denial of service attack is a brute force method to try stop some online service from working properly. For example, attackers may send such a great amount of traffic to a site or such a significant number of solicitations to a database that it overpowers those frameworks capacity to work, making them inaccessible to anyone. A Distributed Denial of Service (DDoS) attack utilizes a multitude of PCs, more often than not undermined by malware and under the influence of cybercriminals, to channel the traffic towards the objectives.

• Trojan Attacks

A Trojan attack is one of the most unsafe PC attack which misinforms the PC or the client as a significant data and the client should introduce it. Trojans are commonly spread by web downloading and transferring and irregular structure fillings on web.

• Man in the center

A man in the middle attack (MITM) is a strategy by which attackers figure out how to intervene themselves furtively between the client and a web administration they're attempting to get to. For example, an attackers may set up a Wi-Fi connect with a login screen intended to impersonate an inn arrange; when a client signs in, the assailant can reap any data that client

sends, including banking passwords.

- Advanced Persistent Threats (APT)

The standard focuses of an APT are by and large associations or nation workplaces for business related data thefts. It is a gathering of a few systems of PC hacking that are guided by the programmers to focus upon the chose substances.

- Insider Data Theft

An insider risk is completely worried about the institutional data. It is the most harmful attack to any institutional association that is controlled by the ordinary individuals like temporary workers, business partners or representatives who straightforwardly approach the applicable sensitive data of that specific foundation. What's more, this danger targets taking that private data.

- Zero-day Attacks

Zero-days are vulnerabilities in programming that still can't seem to be fixed. The name emerges in light of the fact that once a fix is discharged, every day speaks to less and less PCs open to attack as clients download their security refreshes. Methods for abusing such vulnerabilities are frequently purchased and sold on the dim web and are some of the time found by government organizations that questionably may utilize them for their very own hacking purposes, as opposed to discharging data about them for the regular advantage.

- Physical attack

These attack fundamentally focus on the hardware components of a devices or a variety of devices. As IoT is a rising innovation that has been in far reaching utilization everywhere throughout the globe on account of its decentralized and conveyed condition. Henceforth, the devices become increasingly inclined to such physical conclusion and attacks

- Access attack

Physical Access &Remote Access are the two noteworthy classifications of access attack that are for the most part activated somewhere near the assailants. In a physical access, the intruder harms a physical device by acquiring unauthorised access to it physically whereas in a remote access, the major harm is done to the networked devices using the IP addresses.

- Supervisory Control and Data Securing (SCADA) Attacks

SCADA framework is most inclined to a few digital assaults. The different strategies where the framework can be assaulted upon are:

i. Utilizing Viruses or Trojans to totally take off the whole control of the PC/framework.

ii. Utilizing disavowal of-administration assaults for unapproved interruption.

• Cyber-crimes

Cyber-crimes include PCs both as a weapon and as an objective relying on the programmer's necessity. These crimes include data fraud, brand theft, intellectual property cheats, banking burglaries and so forth.

• Supervisory Control and Data Securing (SCADA) Attacks

SCADA framework is most inclined to a few cyber-attacks. The different strategies where the framework can be attacked upon are:

i. Utilizing Viruses or Trojans to totally take off the whole control of the PC/framework.

ii. Utilizing denial of service attacks for unapproved interruption.

3 Threat Impacts

The following is the depiction of what effects a risk leaves in the wake of attacking a network or a system:

• Corruption of Information:

Also called as data altering. As its name proposes, it harms the data by undermining the documents and furthermore that information which is on the move state on a specific system. Altering of data implies that the genuine data or information gets changed in both of the ways, memory can likewise get influenced.

• Destruction of information:

Best model can be given of is DOSs denial of service attack that purposefully plan on tearing the data.

• Disclosure of Information:

Dissemination of the data to the outside clients who are not authorized or part of the system or permitted to access is known as data spillage and exposure. Models: data presentation, caught data and so on.

• Theft of service:

Theft of uses programs, burglary of significant and classified records and security codes just as program codes and utilizing that data for illicit use is robbery of administration.

• Denial of service:

Network blockage or purposeful framework blockage

• Elevation of privilege:

The different hit and preliminary techniques like passwords speculating to get an interruption to the framework or any system to decode and get an unapproved get to.

• Illegal use:

Usage of the general framework capacities to get and accomplish the attackers activities for unlawful purposes.

4 Cyber Attack Detection

Detection of Cyber-attacks is described as "the issue of distinguishing proof of the people who seek after an authentic however unapproved access to an organized PC framework and are abusing the benefits that they are having which is additionally said as "Insider threat". It can likewise be expressed as the recognizable proof of each and every attempt that is being made to for an unlawful utilization into a PC framework without approval

- Host Intrusion Detection Systems (HIDS)

Host Intrusion Detection Systems intends to control or observe a specific host machine. That isit calls to a space of a few Intrusion Detection Systems that are the inhabitants over a single host machine and furthermore are checked by an individual host PC. So as to catch information utilizing a host machine displays the accompanying qualities as under:

File System – Any updates or changes on the host machine's record framework realize or shows the different activities performed on the host PC.

Network Events – Once the network stack appropriately procedures and works upon the different interchanges occurring over the system, at that point just the recognition framework can block the data for the different interruptions being made.

System Calls–System calls are likewise named as high priority interrupts. All the system calls can be followed and watched once when the host part gets adjusted and an appropriate identification framework gets situated in the opportune spot. This appropriate arrangement of the intrusion detection system will improve the extravagance of the data and will improve the procedure of location.

- Network Intrusion Detection Systems (NIDS)

A network cyber-attack detection system (NCADS) works by the correct putting of the network interface into a particular wanton mode, with the goal that the whole network can be effectively observed. Observing of the system is a basic prerequisite since checking will yield the network packets which thus will examine the whole network connection and correspondence interface. Checking of attacks isn't just vital regarding its tending to with the host machine but at the same time is significant in view of the "ping-of-death" attack of which the system gets inclined in light of the fact that that kill a host without even HCADS trigger.

- Signature-based Malware Detection

It is likewise called as an example coordinating methodology as business

antivirus is a case of mark based malware discovery where an arrangement of byte is checked by a scanner inside the whole program code with a reason to acutely distinguish and revealing of an unsafe savage code. Syntactic investigation phase of a run of the mill compiler is pursued upon so as to recognize such a malware by linguistically examining a flood of code of directions while he time of aggregation. Albeit semantic examination isn't played out, this thus turns into an impediment that can likewise come up as malware muddling during the program run period.

5 Tools and Techniques Used in Cyber Security

Cyber security is picking up conspicuousness in the light of expanding number of unauthorized attempts to jump into private information with the unequivocal point of taking the equivalent to scare or constrain clients into data extorting. The tools and methods utilized to handle cyber security concerns are:

•Authentication:

This basic cyber security strategy plans to check the identity of client dependent on the accreditations put away in the security space of the system. The most widely recognized method of administration is secret word innovation, anyway there are various different usage like the SIM card embedded in anybody's wireless. SIM cards are furnished with remarkable ID numbers which are ignored a protected correspondence line for distinguishing proof of a specific PDA. The principle challenge experienced in confirming procedure is upsetting endeavors of unapproved individuals to listen stealthily on the verifying message. The secret word transmitted over an uncertain medium is at risk to be captured by deceptive individuals who can utilize it to camouflage as the first client. This issue is countered by encryption.

•Encryption:

Encryption renders information undecipherable without utilization of an appropriate key to open the equivalent. To battle an encryption, one would be required to attempt taking care of muddled numerical issues like considering enormous primes that would expend galactic measure of processing assets and time. Symmetric encryption uses a similar key with the end goal of message encoding and decoding, and the security level is like that of the key. The appropriation of the key will be joined by potential security dangers. Unbalanced encryption uses an open key to encode the message and a private key to decode the equivalent. A dominant part of present day security conventions are utilizing awry encryption for conveyance of keys.

• Cyber-marks:

Cyber-marks can be raised out of the equivalent numerical calculations that are utilized in asymmetric encryption. A client is allowed to test that he has a private key by getting some data encoded with it. Anybody can get the equivalent decoded by having the open key that will check the individual's credentials. This procedure is basically the definite complementary of open key encryption and in like manner works on the supposition that the approved client just has the private key.

- Anti-virus:

The dangers of PC viruses or unfortunate short projects that trigger undesirable directions without the express assent of client have accepted enormous extents. Anti-virus software completes two functions; it prevents the installation of virus in a system and scans the systems for viruses that are already installed. Most viruses have been developed to target Windows OS working framework as it is the most favored processing stage of masses. Apple and Linux clients can likewise go under the attack of viruses only worked for such working Operating system.

- Firewall:

Firewalls adequately impedes any endeavor of unapproved access to a PC when it is associated on the web by programmers legitimately or by means of other system associations. Firewalls come packaged up with most working frameworks and are turned on as a matter of course. The assistance of business firewalls can be looked for if the security level of the default firewall isn't sufficient or on the off chance that it is presenting obstruction to genuine system exercises.

- Access control and Password Security

We should guarantee that we utilize diverse access components like OTPs, message verification, outsider security procedures so as to give a tied down access to our framework. And designing a complex password which is not easy to guess or crack and regular updating or changing of the passwords to get a hold back from getting hacked.

- Malware Scanners

Malware scanners are only the product programs that target filtering the malware that have gone into the framework using any and all means or passages. Malwares are not all that much yet the gathering of certain virus like worms, wormholes, Trojans, rationale bombs and so on. Malwarebasicallydo the checking of all the present records and data that might be harm.

6 Conclusion and Future Work

The detection systems of cyber-attacks are different in the way in which

they gather and mine the information from the various sources and storehouses and furthermore in the distinctive plentiful procedures theutilize and use to apply different adjustments and perceptions on a particular information thing. The slanting and evacuating advances, alongside the new cyber strategies and threat that are up fronting, are only the associations that need the new systems and instruments to play out their errands just as they look for smart techniques to give help to their verified foundations. The point by point investigation of discovery system of cyber-attacks is very new as looked at to the different spaces of research zones and this zone has been experiencing a ton of future investigations promotion much research work to go.

Acknowledgement
The authors acknowledge Ho Chi Minh City Open University, Vietnam, for helping this research.

References

Adams, N., Heard, N., Adams, N. and Heard, N., 2014. Data analysis for network cyber-security. World Scientific Publishing Co., Inc..

Alnasser, A., Sun, H. and Jiang, J., 2019. Cyber security challenges and solutions for V2X communications: A survey. Computer Networks, 151, pp.52-67.

Bilal, K., Malik, S.U.R., Khalid, O., Hameed, A., Alvarez, E., Wijaysekara, V., Irfan, R., Shrestha, S., Dwivedy, D., Ali, M. and Khan, U.S., 2014. A taxonomy and survey on green data center networks. Future Generation Computer Systems, 36, pp.189-208.

Buczak, A.L. and Guven, E., 2015. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), pp.1153-1176.

Di, M., 2019, February. Design of the Network Security Intrusion Detection System Based on the Cloud Computing. In The International Conference on Cyber Security Intelligence and Analytics (pp. 68-73). Springer, Cham.

Kantarcioglu, M., 2019, May. Securing Big Data: New Access Control Challenges and Approaches. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (pp. 1-2). ACM.

Mahmood, T. and Afzal, U., 2013, December. Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In 2013 2nd national conference on Information assurance (ncia) (pp. 129-134). IEEE.

Mäurer, N. and Schmitt, C., 2019, April. Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat-and Risk Analysis. In 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS) (pp. 1-13). IEEE.

Sani, A.S., Yuan, D., Jin, J., Gao, L., Yu, S. and Dong, Z.Y., 2019. Cyber security framework for Internet of Things-based Energy Internet. Future Generation Computer Systems, 93, pp.849-859.

Srinivas, J., Das, A.K. and Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, pp.178-188.

Verma, A., Khanna, A., Agrawal, A., Darwish, A. and Hassanien, A.E., 2019. Security and Privacy in Smart City Applications and Services: Opportunities and Challenges. In Cybersecurity and Secure Information Systems (pp. 1-15). Springer, Cham.

Wu, J., Guo, S., Li, J. and Zeng, D., 2016. Big data meet green challenges: Greening big data. IEEE Systems Journal, 10(3), pp.873-887.

Xu, G., Yu, W., Chen, Z., Zhang, H., Moulema, P., Fu, X. and Lu, C., 2015. A cloud computing based system for cyber security management. International Journal of Parallel, Emergent and Distributed Systems, 30(1), pp.29-45.

Zhao, R., Liu, Y., Zhang, N. and Huang, T., 2017. An optimization model for green supply chain management by using a big data analytic approach. Journal of Cleaner Production, 142, pp.1085-1097.

Zhong, S., Zhong, H., Huang, X., Yang, P., Shi, J., Xie, L. and Wang, K., 2019. Networking Cyber-Physical Systems: Algorithm Fundamentals of Security and Privacy for Next-Generation Wireless Networks. In Security and Privacy for Next-Generation Wireless Networks (pp. 33-48). Springer, Cham.

UNIVERSIDAD
DEL ZULIA

opción
Revista de Ciencias Humanas y Sociales

Año 35, N° 20, (2019)

Esta revista fue editada en formato digital por el personal de la Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia.
Maracaibo - Venezuela

www.luz.edu.ve

www.serbi.luz.edu.ve

produccioncientifica.luz.edu.ve