International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206130

Survey on Cyber Security and Defensive Measures

Prof. Hemlata. R. Kosare, Prof. Kiran V. Likhar, Prof. Pranali Manapure
Assistant Professor, Department of Computer Science and Engineering, G.H.R.I.E.T, Nagpur, Maharashtra, India

ABSTRACT

The progression of advanced data is developing a regular routine making it gradually hard to oversee and structure it or even to isolate what is significant based on what is pointless. Looked with this test, new encouraging achievement advancements are being created to bring 'information examination's to the following developmental level. Man-made reasoning (AI), specifically, is required to wind up huge in numerous fields. A few types of AI empower AI like profound learning can be utilized to perform prescient scrutiny. Their possible for the defense domain is huge as AI solutions are expected to develop in serious fields such as cyber defense, decision-support systems, risk management, pattern recognition, cyber situation awareness, projection, malware detection and data relationship to name but a few. One of the potential uses of AI in digital protection might be to empower the setting up of self-designing systems. It would imply that AI agendas could recognize vulnerabilities (programming bugs) and perform reaction activities such as self-fixing. This opens better approaches to fortifying correspondences and data frameworks security by giving system strength, avoidance and insurance against digital dangers.

Keywords : Data Analytics, Artificial Intelligence, Cyber Defense, Cyber Threats

I. INTRODUCTION

Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber security and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

The purpose of cyber security is to help prevent cyber-attacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate cyber-attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

1) Types of cybersecurity threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it's necessary in order to protect information and other assets from cyber threats, which take many forms.

- Ransomware is a type of malware that involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.

- Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
- Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

2) Elements of cybersecurity

Ensuring cyber security requires the coordination of efforts throughout an information system, which includes:

- Application security
- Information security
- Network security
- Disaster recovery/business continuity planning
- Operational security
- End-user education

Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: **a)** Input parameter validation, **b)** User/Role Authentication & Authorization, **c)** Session management, parameter manipulation & exception management, and **d)** Auditing and logging.

Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: **a)** Identification, authentication & authorization of user, **b)** Cryptography.

Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include: **a)** Anti-virus and anti-spyware, **b)** Firewall, to block unauthorized access to your network, **c)** Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks, and **d)** Virtual Private Networks (VPNs), to provide secure remote access.

3) Benefits of cybersecurity

Benefits of utilizing cybersecurity include:

- Business protection against malware, ransomware, phishing and social engineering.
- Protection for data and networks.
- Prevention of unauthorized users.
- Improves recovery time after a breach.
- Protection for end-users.
- Improved confidence in the product for both developers and customers.

II. Applications for Artificial Intelligence in Cyber Security

In cybersecurity solutions, AI is either already being applied to, or being heavily considered for, some of the following fields:

- Spam filter applications: Gmail uses AI to detect and block unwanted spam and fraudulent emails. Gmail's AI was trained by the billions of active Gmail users – whenever you click "Spam" or "Not Spam" on an email, you are actually helping train

the AI recognize spam in the future. Thus, the AI has become so developed, it can detect even the sneakiest of spam mails that try to go undetected as "regular" emails.

- Fraud detection: MasterCard implemented Decision Intelligence, an AI-based fraud detection that uses algorithms based on predictable customer behavior. It assesses customer's typical spending habits, the vendor, location of the purchase, and a variety of other sophisticated algorithms, to assess whether a purchase is out of the ordinary.
- Botnet Detection: An extremely complex field, botnet detection typically relies on recognizing patterns and timings in network requests. Because botnets are typically controlled by a master script of commands, a large-scale botnet attack will typically involve many "users" performing the same, or similar, requests on a website. This could be failed logins (a botnet bruteforce attack), scanning for networkvulnerabilities, and other exploits. It's quite difficult to summarize the extraordinarily complex role AI plays in botnet detection in only a few sentences, but here is an excellent research paper on the topic.

III. LATEST TECHNOLOGIES USED IN CYBER SECURITIES

1. Context-Aware Behavioral Analytics:

- **Problem**: Companies are being overwhelmed by meaningless security alerts.
- **Solution:** Use sophisticated behavioral analytics to monitor and identify suspicious behavior/transactions.

Context-aware behavioral analytics is founded on the premise that unusual behavior = nefarious doings. Snowden achieving super root privilege and downloading 1.7 million files to a USB stick after hours? That's unusual behavior. Abnormal file movement and activity across Target's point-of-sale infrastructure? That's unusual behavior.

Examples of this behavior-based analytics approach include:

- **Bioprinting –** How firm workers type, how they utilize a mouse – these are bioprint markers. Organizations are additionally utilizing telephone printing, which is examining acoustic data to distinguish parody guest IDs.
- **Mobile Location Tracking –** Geo-area is a significant pointer of conduct. Is a cell phone signing into a few records from a new city? Risk, Will Robinson.
- **Behavioral Profiles** – Since people are animals of propensity, organizations are currently making conduct profiles of clients, accounts, customers, contractual workers – even gadgets and companion gatherings. At that point they are observing how that conduct changes from month to month and gadget to gadget. On the off chance that past conduct contrasts from continuous conduct, the organization could have a security issue.
- **Third-Party Big Data** – Say a criminal is setting up a phony center with counterfeit specialists so as to get their hands on persistent protection IDs and bill for hoax methods. Large information investigation can caution organizations to the way that these purported facilities are situated in remote office shopping centers with low populaces.
- **External Threat Intelligence** – Are contractual workers and contenders being focused on? Are sure records related with misrepresentation? Are programmers utilizing a similar IP hinders over numerous assaults? Insight gathering is a key piece of understanding criminal conduct.

2. Next Generation Breach Detection

- **Problem :** Hackers are utilizing "zero-day" misuses that enable them to build up a solid footing and mine information in systems and frameworks for quite a long time (for example Target's taken Mastercard numbers).

- **Solution :** Develop innovations that join AI and conduct investigation to recognize breaks and follow them to the source.

In the previous not many years, programmers have been utilizing bespoke assaults on frameworks. Rather than propelling a legion at a divider, they cautiously investigate a framework's safeguards and afterward, Odysseus-like, send in the Trojan Horse. Because of the volume, speed and assortment of large information, most organizations are not by any means mindful that their frameworks have been broken.

- Instead of concentrating on the primary line of safeguard, cutting edge break identification centers around what happens once the criminal is inside the framework. It takes conduct examination and adds much more devices to recognize the breadcrumbs that a programmer deserts.
- As the writers of a 2014 TechCrunch article clarify:
- "Rather than depending on recognizing known marks, these organizations wed enormous information methods, for example, AI, with profound digital security ability to profile and get client and machine standards of conduct, empowering them to identify this new type of assaults. What's more, to abstain from flooding security experts in an ocean of pointless cautions, these organizations attempt to limit the quantity of alarms and give rich UIs that empower intelligent investigation and examination."
- In different words, break discovery instruments can choose unusual developments and changes in an ocean of information and confirm that something is extremely, wrong.

3. Virtual Dispersive Networking (VDN)

- **Problem:** MiM assaults are breaking conventional encryption advances and focusing on moderate hubs.
- **Solution:** Split the message into various parts, scramble those parts and course them over various conventions on autonomous ways.

Man-in-the-Middle assaults (MiM) – times when a programmer can screen, modify or infuse messages into a correspondence channel – are turning into a prickly issue for organizations. Information that was once safely encoded would now be able to be broken by parallel handling power. SSL and Virtual Private Networks (VPNs) can't generally secure messages as they traverse delegate pathways. That is the place Virtual Dispersive Networking (VDN) from Dispersive Technologies comes in.

According to a 2014 article in Forbes:

"[VDN] removes a page from now-customary military radio spread-range security draws near, where radios turn frequencies arbitrarily or split up correspondences traffic into numerous streams, with the goal that lone the getting radio can reassemble them appropriately. With Dispersive, be that as it may, the Internet (or any system) is presently the fundamental correspondences stage."

VDN parts a message into different parts, scrambles every segment independently and courses them over servers, PCs and even cell phones. Conventional bottlenecks can be totally maintained a strategic distance from:

"The information likewise 'move' powerfully to ideal ways – both randomizing the ways the messages consider while at the same time taking clog or other system issues."

Programmers are left scrambling to discover information parts as they whip through server farms, the Cloud, the Internet, etc. To anticipate digital hoodlums from assaulting the frail purpose of the innovation – the spot "where the two endpoints must associate with a switch so as to start their protected correspondences" – Dispersive has a shrouded switch that additionally influences VDN. This does the switch hard to discover.

4. Smart Grid Technologies

- **Problem:** Smart meters and field gadgets have left basic foundations helpless against assault.
- **Solution:** Tackle the issue with a scope of new safety efforts and guidelines.

A couple of focuses from the DOE's 2014 Smart Grid System Report to bite over:

- By 2015, an expected 65 million keen meters will be introduced across the country – mutiple/3 of power clients.
- Customer-based advancements (for example programmable imparting indoor regulators, building vitality the executives frameworks, web-based interface, in-home showcases, and so on.) are turning into the new standard.
- Modernization inside the dispersion framework incorporates the organization of sensor, correspondences and control innovations – these are coordinated with field gadgets to improve lattice activities.

Every last one of these innovations propels makes a feeble point in computerized security. It is an obvious fact that digital assailants couldn't want anything more than to bring down the foundations that supply the country's power, oil or gas.

In response, the DOE is working on a number of tools and strategies to protect the energy sector. Some of these include:

- **Padlock** – Developed by Schweitzer Engineering Laboratories, Padlock is a digital security entryway that sets up scrambled correspondences between focal stations and field gadgets. It's intended to distinguish physical and computerized altering. Accomplices incorporate the Tennessee Valley Authority and Sandia National Laboratories..
- **Watchdog**– Watchdog is another Schweitzer creation. It's a Managed Switch that performs profound parcel examination for the control framework neighborhood (LAN). It utilizes a white rundown design way to deal with decide a lot of known and permitted correspondences.
- **SIEGate** – SIEGate represents Secure Information Exchange Gateway. It's a data convention that gives digital security assurances to data sent over synchrophasor arranges on transmission frameworks. It's being created by Grid Protection Alliance in association with the University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA and T&D.
- **NetAPT**– NetAPT is the University of Illinois' infant. It's a product apparatus that empowers utilities to outline control framework correspondence ways. Defenselessness appraisals and consistence reviews can be finished in minutes.

DOE National Laboratories (for example Idaho, Oak Ridge, Pacific Northwest) have additionally been working diligently. They've been working on undertakings, for example, mechanized defenselessness identification, an instrument suite for situational mindfulness, cutting edge secure and versatile correspondence systems and bio-roused innovations.

5. SAML & The Cloud

- **Problem:** Cloud-based applications and BYODs are past the domain of firewalls and conventional safety efforts/approaches.

- **Solution:** Combine SAML with encryption and interruption discovery advancements to recover control of corporate traffic.

Security Assertion Markup Language (SAML) is a XML-based open standard information design utilized for trading verification and approval information between parties. In spite of the fact that it is anything but a proportion of insurance all alone, various organizations are joining it with SSO, encryption and interruption discovery advancements to secure information in the Cloud.

One of these organizations is BitGlass. It investigated the ascent of the BYOD (Bring Your Own Device) development and the blast of utilizations like Google Apps, Salesforce, and so forth and chose to think of an answer. As Frank Ohlhorst of Enterprise Networking Planet clarifies:

"With SAML in the image, BitGlass planned an intermediary based framework to divert traffic to cloud specialist co-ops through BitGlass innovation, which verifies access and traffic, logs action, and even "watermarks" records and data for additional assurance by implanting security labels into reports and different documents to follow their development. Incredibly, all that occurs without affecting the end client. No product to stack on endpoints, no progressions to be made to end client arrangements."

Along these lines, information in the Cloud is corralled. A ready framework informs organizations of occasions like fizzled or unforeseen log-ins, suspicious action and such. On the off chance that a representative's gadget is taken, security directors can promptly wipe all the corporate data without influencing the client's close to home information.

6. Active Defense Measures

- **Problem :** Cyber lawbreakers are getting aggressive
- **Solution:** Fight fire with proverbial fire – use techniques that can track, or even attack, hackers.

Dynamic guard measures are a questionable theme in digital security. The thought is truly straightforward. Rather than kicking back and trusting that the hacker will come and get you, you take proactive measures to thwart them.

Examples of active defense measures include:

- **Counterintelligence Gathering** – This requires a digital master to go "covert" to look for data about programmers and their apparatuses and systems. It may be as straightforward as switch malware investigation; it may be as secret as shrouding your personality and going into Internet malware retail facades.
- **Sinkholing** – Designed to mimic the genuine article, a sinkhole is a standard DNS server that hands out non-routeable locations for all spaces inside the sinkhole. The objective is to catch and square pernicious or undesirable traffic so it very well may be caught and broke down by specialists. Peruse more in Brian Krebs' posts on sinkholes.
- **Honeypots** – Honeypots adopt the snare and trap strategy. A honeypot is a segregated PC, information or a system site that is set up to pull in programmers. Digital security investigators use honeypots to explore Black Hat strategies, forestall assaults, get spammers, etc. The idea has been around since 1999, however applications keep on developing in refinement.
- **Retaliatory Hacking** – This might be the most risky of safety efforts (and generally thought to be unlawful). Hacking back brings up a wide range of moral issues – will you bring down blameless outsider foundations in your main goal? Will your programmers fight back ten times in retribution for your activities? Indeed, even with every one of

the dangers, the thought is picking up footing in specific circles.

And afterward there's MonsterMind. As per Edward Snowden, the NSA has been chipping away at a computerized program that would utilize calculations to look through storehouses of metadata and recognize and square malevolent system traffic. It could likewise possibly strike back at the server propelling the assaults.

Dynamic safeguard measures can lead you into risky waters. For example, state you need to penetrate a programmer network. Like the crowd, the gathering may need confirmation of your accreditations. You may need to construct a hacking notoriety, take part in illicit activities and incessant unlawful locales (for example ones that hawk kid sex entertainment). None of these things are lawful.

7. Early Warning Systems

- **Problem:** Vulnerable websites and servers are increasingly being hacked.
- **Solution:** Create an algorithm to determine which sites and servers will be hacked in the future.

In spite of the fact that this thought is still in the beginning periods, we thought it important. Utilizing AI and information mining strategies, analysts at Carnegie Mellon have made a "classifier" calculation that predicts which web servers are probably going to get vindictive later on.

To test their instrument, Kyle Soska and Nicolas Christin applied the classifier to 444,519 chronicled sites in the Way Back Machine. Over a one-year time frame, their calculation had the option to foresee 66% of future hacks with a bogus positive pace of 17%.

The thought is based on the reason that defenseless sites share comparable qualities. For instance, the calculation considers a website's:

- Software
- Traffic statistics
- Filesystem structure
- Webpage structure

Plus, a variety of other “signature features” to determine if it shares common denominators with known hacked and malicious websites. If it does, then steps can be taken to prevent an attack. Website operators can be notified. Search engines can exclude results.

What’s especially cool is that the classifier is designed to adapt to emerging threats. Although it doesn’t include vectors like bad passwords, it is growing in scope. As it absorbs more and more data, it should be able to improve its accuracy.

IV. CONCLUSION

Digital Defense is a PC organize guard system that spotlights on avoiding, distinguishing and giving opportune reactions to assaults or dangers to framework and Data. This opens better approaches to reinforcing correspondences and data frameworks security by giving system flexibility, avoidance and assurance against digital dangers. Digital specialists concur that the human framework reconciliation is a key component that must be available in an AI digital security framework. In the event that we consider the rapid required to play out any digital activity, clearly just machines are equipped for responding productively in the beginning periods of genuine digital assaults. Man-made intelligence would thus be able to conquer the deficiencies of conventional digital security instruments. It is likewise an amazing system ready to improve malware recognition rates utilizing a pattern of digital insight information. Artificial

intelligence digital security frameworks can gain from markers of bargain and might have the option to coordinate the attributes of little pieces of information regardless of whether they are dispersed all through the system.

V. REFERENCES

[1]. Dr. Sunil Bhutada,PreetiBhutada," Applications of Artificial Intelligence in Cyber Security," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, ISSN (Online) 2394-2320April 2018

[2]. Saeed S.Basamh,HaniA.Qudaih,et.all,"AnOverviewon CyberSecurityAwarenessinMuslimCountries".InternationalJournalofInformationandCommunicationTechnologyResearch,Volume4No.1,January2014, ISSN2223-4985

[3]. Jitendra Jain, Dr. Parashu Ram Pal,"A Recent Study over Cyber Security and its Elements,"International Journal of Advanced Research in Computer Sciencel, Volume 8, No. 3, March – April 2017, ISSN No. 0976-5697

[4]. Rajesh Kumar Goutam,"Importance of Cyber Security," International Journal of Computer Applications (0975 –8887) Volume 111 –No 7, February 2015

[5]. Eric A. Fischer," Cybersecurity Issues and Challenges: In Brief,"Congressional Research Service,August 12, 2016

Cite this article as :

Prof. Hemlata. R. Kosare, Prof. Kiran V. Likhar, Prof. Pranali Manapure, "Survey on Cyber Security and Defensive Measures", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 1, pp. 144-151, January-February 2020. Available at doi : https://doi.org/10.32628/CSEIT206130
Journal URL : http://ijsrcseit.com/CSEIT206130