IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

A Study of Cyber Security, Its Challenges and Its Emerging Trends on Latest Technologies

Dr. Sandeep

Assistant Professor, CSE, OM STERLING GLOBAL UNIVERSITY, HISAR, India

ABSTRACT:-In today's world driven by technology and network connections, knowing what cyber security is and being able to use it effectively is key. Systems, important files, data and other important virtual things are at risk if there is no security to protect them. Cyber security plays an important role in the field of information technology. Security of information has become one of the biggest challenges of today. Regardless of whether it is an IT company, every company must be protected in the same way. With the development of new technology in cyber security, attackers will not similarly collapse. They use better and improved hacking techniques and target the weak points of many businesses. Cybersecurity is critical as military, government, financial, medical and corporate organizations collect, practice and store unprecedented amounts of data on computers and other devices. An important quota of this data can be sensitive information, be it financial data, intellectual property, personal information or other various types of data where illegal access or exposure could cause negative concerns.

KEYWORDS: cyber security, cyber crime, cyber ethics, social media, cloud computing.

I. INTRODUCTION

An effective cybersecurity method has many layers of defense spread across networks, computers, programs, or information that aim to keep it non-toxic. In a company, processes, people and tools must accompany one alternative to create a real defense during or after cyber-attacks. A unified threat management system can mechanize additions across select Cisco Security products and accelerate key security process functions: detection, investigation, and remediation.

Users:
Users must appreciate and follow basic information security ethics, such as choosing strong passwords, keeping email attachments up-to-date, and backing up data. Learn more about the core values of cybersecurity

Processes
The government needs to keep track of how they follow up on joint attempts and popular cyber attacks. Some well-respected syllabus can accompany you. It clarifies how you can recognize attacks, protect organizations, alert and respond to threats, and improve from successful events.

Technology :-
Technology is essential to provide system security tools to individuals and organizations looking to protect themselves from cyber attacks. Essentially, three main objects are at risk: endpoint strategies such as computers, handheld devices and routers; systems; and a cloud. Shared technology designed to protect these objects includes next-generation firewalls, DNS filtering, anti-malware protection, anti-virus tools and email security scores. Cyber can be distinct as somewhat associated with a collection of workstations or networks. At the same time, security means a mechanism to protect anything. As a result, the concepts of Cyber and security that have been adopted define the way of defensive user information during or after malicious attacks that could be the key to a security breach. It's a time that was postponed for a while, after which the Internet developed like anything else. Through cybersecurity assets, any company or any user can protect their critical data from hackers. As much as hacking is feared at some point, it has actually used ethical hacking to create cyber security in any structure.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

2.Cyber Crime

Cybercrime is the term for any illegal activity that uses a computer as its primary means of committing and stealing.It could be defined as a procedure to mitigate security concerns in order to protect the reputational damage, business loss or financial loss of the whole group. Of course, the term cyber security requires that it is a fine-grained security that we propose to an organization that can often be contacted by users using the Internet or network. There are many tools and techniques that are used to deploy it. The most important fact about information security is that it is not a one-time procedure, but a continuous process. The organization owner must keep the products updated in the mandate to keep the risk low.

3.Cyber security

Data privacy and security will always be top security measures that any organization will take care of. We currently live in a world where all information is stored in digital or cyber form. Social networking sites provide a space where users feel safe to interact with friends and family. For home users, cybercriminals would continue to target social media sites to steal personal information.

Not only on social networks, but also during banking transactions, one must take all the required security measures.

II.TRENDS CHANGING CYBER SECURITY

Below are some of the trends that are having a huge impact on cybersecurity.

Cloud computing and its services:

Nowadays, all small, medium and large companies are slowly moving to cloud services.

In other words, the world is slowly moving towards the clouds. This latest trend poses a major challenge to cybersecurity as traffic can bypass traditional checkpoints. Plus like the number of appsavailability in the cloud grows, policy controls for web applications and cloud services will also need to evolve to prevent lossvaluable information. Although cloud services are developing their own models, there are still many security issues. The cloud can provide tremendous opportunities, but it should always be noted that as the cloud evolves, so do its security concerns.

Web servers:

The threat of attacks on web applicationsextract data or spread malicious codepersists. Cybercriminals distribute theirsmalicious code through legitimate web serverscompromised. But data theft attacks,many of which attract media attention arealso a big threat. Now we need a bigger oneemphasis on protecting web servers and the webapplications. Web servers are especially the bestplatform for these cybercriminals to steal fromdata. Therefore, you should always use the safer onebrowser especially during important transactionsto avoid becoming a victim of these crimes.

APT's and targeted attacks:-

APT (Advanced Persistent Threat) is a wholea new level of cybercrime. For yearsnetwork security features such as webfiltering or IPS play a key roleidentification of such targeted attacks (mostly afterinitial compromise). As attackers growbolder and use more vague techniques,network security must integrate with otherssecurity services to detect attacks.Therefore, we need to improve our security techniquesto prevent further threats coming infuture.

5.How does cyber security make work so easy?

There is no doubt that the cyber security tool makes our job very easy by ensuring that limited capitals are reachable in any network. A business or company could look like a huge shame if they are not honest about the security of their online presence. In today's connected world, everyone benefits from advanced cyber defense programs. On a separate level, a cyber-security breach can result in everything from identity theft to blackmail attempts to the corruption of vital data such as family photos. Everyone relies on dangerous structures like power plants, dispensaries and money services businesses. The security of these and other societies is necessary for us to trust our civilizing agents. One and all also rewards the work of cyber threat investigators, much like Talos' team of 250 risk investigators who research new and evolving cyber conflict concerns and policies. They uncover new vulnerabilities, educate the community about the state of cybersecurity, and strengthen open source tools. Their work will make the internet harmless for everyone.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

6.Types of cybercrime:-

Phishing:-

Phishing messages ask recipients to send sensitive information such as a person's name, date of birth, social security number, account passwords, personal identification numbers, and anything else a criminal can use to commit identity theft. The ultimate goal of these phishing scams is to obtain information that the criminal can use to open fraudulent accounts in the victim's name or otherwise fraudulently access or exploit the victim's identity for financial gain.

Identity theft:-

Identity theft is the crime of obtaining another person's personal or financial information in order to use that person's identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways, and victims are usually left with damage to their credit, finances and reputation.

Malware or malicious software:-

Malware or malicious software is any program or file that intentionally harms a computer, network or server.Types of malware include computer viruses, worms, trojans, ransomware, and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack basic computing functions and monitor the computer activity of end users.

Ransomware:-Itis a type of malware. It is considered to extract currency by blocking contact to records or the PC system until the deal is paid. Paying the ransom does not assurance that the records will be recuperated or the system returned.

Trojan horse:-A computer program that appears to have a useful function but also has a hidden and potentially harmful function that evades security mechanisms, sometimes by exploiting the legitimate authority of the system entity that invokes the program.

Cyberbullying:-Cyberbullying is a type of bullying where one or more individuals use computer and technology to intentionally and repeatedly harm another person.

Cyberstalking:-Cyberstalking is defined as using email, instant messaging, or other electronic means to harass, intimidate, or threaten someone with physical harm. Cyberstalking can take many forms such as bullying, sexual harassment or other unwelcome attention around your life and activitiescyberstalking differentiates between cyberstalking and cyberbullying based in part on the age of the victim. The term cyberstalking is used more often when the victim is an adult. And the term cyberbullying is usually used when the victim is a child, teen or teenager.
In some cases, the term cyberstalking can be used to refer to online activities and communications that cause the victim to fear for their physical safety. And the term cyberbullying can be used to refer to communications that may cause emotional harm or distress to the victim.

7.Goals of Cyber Security?

The definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this we aspect at 3 important goals of cybersecurity.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only to approved users

These objectives practice the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation. This model is similarly mentioned to in place of the AIC (Availability, Integrity, and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency. The rudiments of the triad are reflected the three greatest vital mechanisms of safety. The CIA standards are one that greatest of the societies and businesses practice once they have connected a new request, makes a record or when assuring access to approximately information. On behalf of data to be totally safe, all of these safe keeping areas must originate into result. These are safe keeping strategies that all effort together, and hence it can be incorrect to supervise one policy. CIA triad is the greatest collective standard to measure, choice and appliance the proper safety panels to condense risk.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

Confidentiality:-
Confidentiality Making guaranteed that your complex statistics is reachable to accredited users and safeguarding no information is revealed to unintended ones. In case, your key is private and will not be shared who power adventure it which ultimately hampers Confidentiality.

Methods to safeguard Confidentiality:
•Two or Multifactor verification
• Data encryption
• Confirming Biometrics

Integrity:-
Integrity make sure all your data is precise; dependable and it must not be changed in the show from one fact to another. Integrity ensure methods: • No illegal shall have entrance to delete the records, which breaks privacy also. So, there shall be • Operator Contact Controls. • Appropriate backups need to be obtainable to return proximately. • Version supervisory must be nearby to check the log who has changed.

Availability :-
Availability Every time an operator requests a resource for a piece of statistics, no notifications such as Denial of Service (DoS) must occur. All evidence must be available. For example, a website is in the hands of an attacker result in a DoS, thus preventing its reachability.
Here are some steps to maintain these goals
1. Categorize assets based on their position and priority. The most important ones are always kept safe.
2. Containment of possible threats.
3. Determining the security method for each threat
4. Monitoring potential breaches and managing data at rest and data in motion.
5. Iterative maintenance and response to any related issues.
6. Update of risk management policies based on previous assessments.

8.Advantages:-
It consists of many plus points. As the term itself suggests, it offers network or system security, and we all know that securing anything has a lot of benefits. A few benefits are listed below. Company security – Cyber security is about protecting the organization's network from outside attacks.
This means that the company should achieve a decent and secure feeling around its important information.
-Complex data protection – Highly private data such as student data, patient data and transaction data must be protected from illegal access so that it cannot be altered. This is what we can achieve with cyber security.
-Prevent illegal access helps us defend the system after it has been acquired by someone who is not authorized to contact it. The data is reserved highly protected and can only be created with valid users.
Cybersecurity provides protection in addition to information theft, protects workstations from theft, reduces PC freezes, provides operator privacy, suggests strict guidelines, and is problematic to try with non-technical people. It is the only income of computer protection, protecting them compared to worms, viruses and redundant unwanted programming. It deals with protecting against hateful attacks on the system, erasing and/or preserving hateful bases in a pre-existing network, stopping illegal access to the network, eliminating programming on or after other bases that might cooperate, and also securing complex data. . Cyber security offers enhanced internet security, increases cyber flexibility, accelerates system data and information protection for industries. It guards individuals' private data, protects networks and capitals, and tackles computer hackers and identity theft. It protects against data theft because malicious operators cannot disrupt the network construction by using a highly secure procedure. Secure the hacking technique. Ensure data privacy and organization. This can be achieved by good application of security rules and system protocols.

9.Disadvantage:
Firewalls can be difficult to configure correctly, misconfigured firewalls can prevent operators from doing anything on the Internet until the firewall is properly connected, and you will continue to upgrade the latest software to remember the current defense current, cyber protection can be expensive. In addition, cyber security has cost a significant number of operators. Firewall rules are difficult to configure properly. The security of a weekly or occasional scheme is too high. Normal is expensive.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

The operator cannot have the right to use different network devices through incorrect firewall instructions.
More Pandemic Phishing Cybercriminals will continue to use the COVID-19 pandemic as a theme for their phishing campaigns.
Attacks often coincide with significant events, such as an increase in new cases or the announcement of a new drug or vaccine. Their unbiasedness is to acquire unsuspected fatalities to check a harmful link or accessory or give up complex data. **New "Nigerian Prince" Fiddle Plots**
In a classic Nigerian Prince scam, employees playing on distant royal potentials to stretch you big if you hand over your bank account details. Currently, phishing hackers pretend to be with a government agency that sends out economic stimulus payments. Otherwise, the scam works the same.
Ransomware Attacks Accelerating Cybersecurity Speculations beat past cybercrime data and predicted that ad will fall victim to ransomware every 11 seconds in 2021. This is reduced every 14 seconds in 2019. The total cost of ransomware will exceed $20 billion worldwide.
Growing number of cloud breaches While cloud infrastructure is very secure, customers are responsible for implementing cybersecurity features and configuring them properly. Cloud misconfigurations are common sources of data breaches and are expected to grow as more companies adopt cloud services to support remote workers.
Growing threats targeting user devices:-
Employees working from home consume systems that are not patched, completed and protected by the business IT department. It increases the company's attack space and allows hackers to enter the system bypassing border security. The existence of critical business data to be stored on these systems further compounds the risk of data leakage.
Attacks Occurring in Internet of Things (IoT) Systems
More and more organizations are implementing IoT devices and applications to capture data, remotely control and manage infrastructure, improve customer service, and more. Many IoT devices lack robust security, making them vulnerable to attack. Hackers can increase the mechanism of strategies to practice in botnets and influence IoT weakness to gain access to the network.

1. Cyber ethics:
Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:
-Don’t be a bully on the Internet. Do not call people names, lie about them, sendembarrassing pictures of them, or do anything else to try to hurt them.
-USE the internet to communicate and interact with other people. By emailand instant messaging make it easy to stay in touch with friends and familymembers, communicate with work colleagues and share ideas andinformation with people from across town or halfway around the world.
-When you’re online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble

III. CONCLUSION

The advent of cybersecurity will be one intelligence like today's: hard to describe and potentially limitless as digital skills interact with humanoids in virtually every aspect of politics, society, family and beyond. We have built this project on the proposition that together the "cyber" and "security" mechanisms defining the idea of "cyber security" will be rapidly signed during the second half of 2010. This gesture will speed up rather than slow down, but its manner varies greatly in different situations. This is not an article of our investigation procedure; that is the basic point of the endeavor. We imagine that sometime in the not-too-distant future (if not actually right now), addressing cybersecurity will be widely recognized as the "major problem" of the Internet era. This ranks it among the highest of all difficulties facing civilization, alongside near-existential suffering like weather change, rather than the labor concerns that tech firms need to succeed. This gratitude will also bring great variations to how humanoid and digital machines work together. The purpose of these five situations is to give an idea of some of the ups and downs that can occur. In this effort, we have left on the cross influences related to direct armed to military "cyberwarfare". It was in the sense of a demonstrative choice to tie up trouble. It is indisputable that a cyber war or at least a cyber battle will (continue to) take place when hostile actions materialize and the Internet is a problem field, much like sea, land, space, air, and more, and we have already expended an incredible amount of effort to deal with the situations in cyber warfare, which can be combined with this paper to complete our set of market, user, technology and social driven scenarios. We realize that a major war between influential conditions waged significantly or even predominantly in cyberspace would be a tipping point that could significantly send approximately the driving forces we highlight. Then we decided to put this kind of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204286 |

opportunity as an exogenous surprise or "wild card" rather than an underlying trend - at least designed for the present. We must try to expand our imaginations to see glimpses beyond the horizon, how the set of problems will change and what new opportunities will emerge. The target for these situations, 2020, is similar to the current one in the near future. Our familiarity with situational thinking as a demonstration tool offers two significant explanations for this circumstance. The first is that adjustments generally happen faster than companies expect. While we can all experience a moment of internet hype-fatigue, especially when it comes to the rights to exponential duty of change, the truth remains that the scenery may look extra different than we imagine, sooner than we imagine. Another idea is that it is easier to imagine negative dangers than benefits. These types of senses in an evolutionary, natural mix-determined environment where it is beneficial to avoid potential harmful risk while protecting persistence, but it may not be as beneficial in a modified environment where humanoids have a better degree of switching. The Internet is among the most composite environments that humans have created, but it is a static (for now) modified environment composed of numerical machines that are constructed and programmed by companies. Acceptance in this context is as dysfunctional as satisfaction. We believe that these situations stimulate broad thinking and conversation, which they bring more questions than answers, extra bold ideas for inquiry and original policy proposals rather than safe, forceful announcements of what must or must not be done. With that in mind, we offer at a very high level the instant points and aggravation that came from this effort. Of course, the greatest increase in understanding is at what time specific actors and governments use similar situations to derive more detailed and targeted propositions applicable to their own advantages, capabilities, risk-taking and location. So we expect readers to ask themselves the following question: what do I think cyber security will mean, exposed to the scene of upcoming potentials highlighted by entities highlighting these scenarios – and what would I or the associations I am a part of do next? After basic research and strategy, just as importantly, what will be critical to achieving the best cyber security results I can forecast?

REFERENCES

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
2. Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole
3. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy
6. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
7. CIO Asia, September 3rd , H1 2013: Cyber security in malasia by Avanthi Kumar.
8. https://www.getgds.com/resources/blog/cybersecurity/6-cybersecurity-threats-to-watch-out-for-in-*2021*
•https://cltc.berkeley.edu/scenario-back-matter/
•https://www.bitdegree.org/tutorials/what-is-cyber-security/
•https://cltc.berkeley.edu/scenario-back-matter/
•https://www.bitdegree.org/tutorials/what-is-cyber-security/
•https://cltc.berkeley.edu/scenario-back-matter/
•https://www.bitdegree.org/tutorials/what-is-cyber-security/
•https://cltc.berkeley.edu/scenario-back-matter/
•https://www.bitdegree.org/tutorials/what-is-cyber-security/
9. https://cltc.berkeley.edu/scenario-back-matter/
10. https://www.bitdegree.org/tutorials/what-is-cyber-security/
https://www.google.com/search?q=advantages+of+cyber+security+in+2021&sxsrf=ALeKk02H69_Fh
11. https://www.google.com/search?q=advantages+of+cyber+security+in+2021&sxsrf=ALeKk02H69
https://www.google.com/search?q=goals+of+cyber+security+in+2021&sxsrf=ALeKk02Di8kocShVdB

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details