Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 14 (2020) Pp-227-230

BBRC
Bioscience Biotechnology Research Communications

Challenges and Innovations in Cybersecurity

Simran Baheti[1*], Nikhil Tiwari[2], Rushil Parikh[3], Paritosh Dandekar[4], Rajat Chandak[5] and Abhijeet R. Raipurkar[6*]

[1, 2, 3, 4, 5, 6]Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

ABSTRACT

The World Wide Web or the internet today is a vast space. It contains information about everything one wants and is accessible at the tip of the finger. Billions of people use the internet every day and most of them at the same time. When we think about the activities taking place on the web, we are bound to think about all the crimes that happen throughout the web. People are exposed to crimes like identity theft, crypto-jacking, cyber extortion, etc. Therefore, their security becomes a serious question and the topmost priority of the creators. Here comes the need for cybersecurity. This paper focuses mainly on the threats faced and the innovations in technology to encounter those threats.

KEY WORDS: CYBERSECURITY, CYBERCRIME, CLOUD SECURITY, AI AND ML, BLOCKCHAIN.

INTRODUCTION

In the age of analytics and intelligence, nearly 5 billion people and 31 billion devices have access to the internet. The digital world has seen a drastic expansion in the recent time of COVID-19. From MNCs to governments, schools to universities all are functioning online. Almost all organizations use the internet to transfer data and cloud services to store it. This increases the concern of several organizations toward the protection of data and communication. Cybersecurity helps in the protection of this sensitive information and the system used to store the information. With the sudden increase in cybercrimes and cyber-attacks, companies and research organizations are embracing technologies and innovations to tackle them.

There are existing technologies for cybersecurity although due to the variations in cyber-attacks, the organizations need better technology for early detection of the attacks. The advancements in technology that we are seeing are blisteringly fast as compared to the past, which increases the number of cyberattacks with new challenging threats. With every passing year, thousands of new threats are created which are getting more and more dynamic which results in hazardous and challenging threats to the organizations. The pandemic has brought a workplace shift to work from home which has resulted in more cyberattacks. Nowadays cybersecurity is not only about protecting the system from known attacks but also preventing the system from new threats. Everyday threat actors are conceiving new strategies for attacks, this evokes the need for innovation in security measures for the integrity of data.

Cybersecurity; For any individual or an organization, the most important concern while working online is the safety of their data. Cybercriminals work with the exact opposite motif to hack into a system for financial gains or simply to create chaos. Here comes the need for cybersecurity to stop such people from achieving their goals. Cybersecurity is the practice of defending an electronic device from any kind of an external, malicious attack that breaches the safety software and can cause harm to the system or the person at whom the attack is aimed. Various security

ARTICLE INFORMATION

*Corresponding Author: bahetism@rknec.edu
Received 15th Oct 2020 Accepted after revision 29th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

Clarivate Analytics

crossref

NAAS Journal Score 2020 (4.31)

Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.14/53

measures include protecting networks, applications, information, operations, disaster-related and business continuity and end-user education.

- Currently, over 98% of corporations have cybersecurity resources and over 50% of those are allotted for online privacy in Malaysia itself.
- It was predicted in 2017 that nearly 50% of the company's budget will go into cybersecurity by 2020
- The cost of a post-data breach is around 1.56 Million USD in the USA.
- Therefore, cybersecurity should be the topmost priority of every individual and organization.

Cybercrime or Computer Oriented Crime: Cybercrime is done by individuals who aim to get recognized or to spread fear. It is a type of crime that uses a computer as a source or target or both, meaning that cybercrime can be carried out through a computer, carried out on a computer, or both. These attacks are tough to identify but when identified, the punishments are extreme.

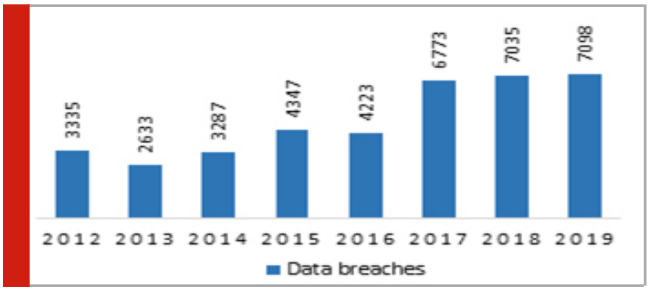
Different types of computer-oriented crimes include:

1. Cybercrime: - Aimed at an individual or an organization.
2. Cyberattack: - Crime with a political motive.
3. Cyber Terrorism: - Conducting violent acts resulting in damage, loss of life, or any kind of bodily harm.

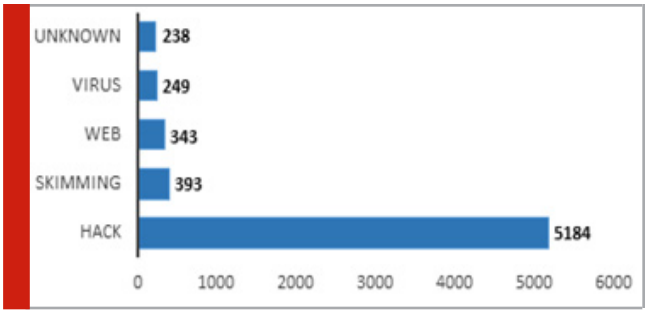
Email and internet fraud, Identity fraud/theft, Cyber Extortion (demanding money to stop the threatened attack), Cryptojacking (when hackers mine cryptocurrency using resources that they do not have any right on) are some common types of cybercrime.

Some statistics related to data breaches:

- In 2019, over 15.1 billion records were compromised with 7098 breaches reported.
- The chart below shows a comparison between data breaches in different years.



- The web itself contributed to 13.5 billion records while 1.5 billion records were hacked.
- In 2019 alone the % increase in records exposed was 284% as compared to 2018 and 91% as compared to 2017.
- The number of breaches per economic sector is topped by the Information Technology industry by 614. It is closely followed by the Healthcare industry at 512. Finance and Insurance come third at 435.
- The below chart shows breaches by breach type in 2019



Emerging Threats:

Cloud Vulnerabilities: Cloud computing is a way to offer storage services over the internet. The shortage of physical storage has led us to seek storage in virtual cloud domains thus cloud services are rapidly taking over the traditional physical storage. Many organizations find public cloud services to be safer than on-site data centres. With the COVID-19 pandemic on hand, the use of cloud-based services has seen an unprecedented demand. Due to this surge, it has led to the development of a hybrid cloud structure where enterprises combine their private cloud service with the public cloud service. This increased complexity in the cloud structure has made it prone to cyber-attacks.

Cloud security has been a major concern for a long time. Data breaches and leaks in the cloud have cost billions of dollars to the economy. They can lead to some sensitive data such as personal, financial, or health records in the wrong hands. Public cloud being used by millions of users has given attackers a sea of victims. Ransomware injection to one of the victim's local computers may get uploaded into the cloud thus corrupting the whole cloud. A major issue is the lack of awareness in the organizations regarding cloud security which may lead to a leak of credentials, system vulnerability, third-party misuse, distributed denial of service attacks, insider threats, etc.

The AI-based cyber attacks: Artificial intelligence (AI) has been there for more than a decade and there's still a ton of potential yet to be explored in this field. AI has been brought to use at numerous good places from traffic signals to cancer detection. But that unexplored potential is also being used for malicious purposes. There are various ways in which artificially intelligent cyber-attacks are helping attackers creating chaos. AI can help cybercriminals in blending their malware into the computer system and thus making detection harder which will lead to the creation of enhanced and intelligent malware. They can use AI to find their victims from social media or other platforms.

Cybercriminals can use machine learning to bypass CAPTCHA and can also create very convincing spam messages. IBM's Deeplocker is one of the examples where AI is being used to conceal in an unsuspicious application until it reaches a specific target. AI can be used to detect and exploit vulnerabilities before they are fixed in a patch. AI botnets scan the target systems for vulnerabilities and then inject the malware which steals data and remains undetected until the target has been attacked. Data poisoning is also an emerging threat and could cause significant damage to many organizations and businesses using AI systems. This happens when the data fed to machine learning or deep learning algorithms is corrupted thus misleading the algorithm. Though AI-based attacks have not made the news yet, they sure are a big threat if not looked after.

Deepfake: Deepfake is an emerging threat that could change our social life drastically. It is used to create fake still images, audio and videos that look and sound real. It uses Generative Adversarial Networks (GANs), which is widely available and could facilitate social engineering attacks. A user doesn't require any special skills to use deepfake. Also, free and paid software are available online that create deepfake content. This could be used for political agenda, blackmailing, defamation and frauds against politicians, celebrities, even the general public can be targeted. A rising concern is that the advancement in AI technologies is resulting in more and more undistinguishable fake content. Another potential threat deepfake could possess is deepfake ransomware. A threat actor could create deepfake videos and demand a ransom which failing to pay will lead to making the video public.

Smart Contract Hacking: Blockchain is an innovative technology that uses the concept of distributive and decentralized ledger. It helps in digitalization of the information being recorded and distributed but not edited. Though Blockchain is considered almost impossible to hack, the same cannot be said about smart contracts. A smart contract is nothing but a block of code as a part of a blockchain that defines a set of rules agreed by both the parties and are executed if both the parties follow these rules. If anyone of the parties fails to meet the defined rules, the output is not generated. This line of codes helps in automating the verification and enforcing of the agreement between both the parties. The concept of a smart contract is very new and thus it makes it very lucrative for cybercriminals to exploit bugs and vulnerabilities. These hacks can be converted into money very rapidly and there is no one to give a halt to these hacks. So, this field of the smart contract still requires research in its security and quality.

Fake news: Fake news has been a severe problem for a long time now since the advent of social media and has alarming concerns. The recent coronavirus pandemic has only exacerbated the situation. As people are becoming more dependent on social media for news, it is becoming more and more difficult to differentiate authenticated news from the fake ones. This makes it quite easy for agenda peddlers to spread misinformation about a political party and influence people's opinion in the wrong direction. This brainwashing may instigate violence or create differences among groups. Controlling fake news, hate speech and misinformation has become an obstacle for regulatory agencies.

Innovations in Cyber Security:

Cloud Security: Cloud Computing has become a necessity of every organization irrespective of its size. Cloud Security also known as Cloud Computing Security which involves some policies and technology which helps in securing the cloud computing data, environment and infrastructure from theft, deletion, alter and leakage. Predictive security in the cloud collects and examines the customer's data with the help of Machine Learning algorithms and AI which studies the pattern and determines the probability of future outcomes. Distributed Cloud provides more secure operations on the cloud. It is the distribution of cloud services to different geographical locations and each cloud service is autonomous in its governance, evolution and updates. Cloud services like Microsoft Azure, Amazon Web Services (AWS) and IBM Cloud are adopting Blockchain-as-a-Service (BaaS) which is the third-party cloud-based infrastructure for creating, maintaining and configuring cloud-based apps.

User Behaviour Analytics: User Behaviour Analytics is a process of tracking and assessing user data and then looking at the pattern of user's behaviour. It uses Big Data and Machine Learning algorithms to detect these abnormalities and when there is a deviation from a particular pattern then it might be a real threat to the organization. By using this on a large scale, organizations can find malignant movement and traded off endpoints. User Behaviour Analytics doesn't report all abnormalities as baleful, if it contains less sensitive data then it is given less impact score and if it contains risky information then it is given a high impact score. So that the predictions can be prioritized according to impact score. In this way, the organization can reach the illegitimate source before it can reach the organization.

Next Generation Breach Detection: From a security perspective, data breach is one of the critical problems in the past couple of decades in various industries. With an increase in cases of data breaches, companies need to have better detection systems for early detection and alerts. This problem is solved by next-generation Intrusion Detection Systems (IDS). In earlier times, signature-based IDS were used, they were only capable of

responding to breach once the has occurred. Signature-based IDS uses raw data and manual investigation. Whereas in current times, companies use next-generation breach detection systems like Legacy IDS technology. In this technology, activity or policy violations on a network is monitored by a device or software application. Unlike previous IDS, next-generation IDS uses intelligent data and Machine Learning features to implement full Network Traffic Analysis (NTA). A Security Information and Event Management (SIEM) system collects any malicious activity or security violation. SIEM generates alerts regarding malicious activity or security violation by combining all the inputs from all the security sources. Hence, next-generation breach detection systems will be helpful for early alerts and prevention of firms.

Virtual Dispersive Network (VDN): Virtual Dispersive Network (VDN) is a technology invented by Robert Twitchell Jr. and introduced by Dispersive Networks Inc. In this COVID-19 time, most of the companies are working on the public network rather than the private. This increases the chances of cyberattacks on any company as in any standard network the data sent from one device to another device using a single route or path. This single route data transmission increases the chances of Man-in-the-Middle (MitM) attack. The MitM attack is one of the major threats for several firms whose three-quarters of the employees are working from home. VDN is the technology that provides one of the finest solutions to this threat by protecting the network from MitM attacks. VDN takes the data from a sender, separates it into multiple smaller packets or pieces and adds encryption data to each packet. The encryption varies for each packet and depends on the transmission route of the packet. VDN compels those packets to take independent routes to the receiver. When data packets reach the receiver side, they are authenticated and then reassembled for use. If there is any MitM attack between transfers, the hacker will only access single packet of original data and that will be useless and unproductive for a hacker. VDN is a centenary software solution that can be installed on any firm's existing network.

Quantum Computing: Irrespective of any industry from Health to IT, all organizations focus on security of their digital data by encrypting them. Every encryption nowadays is done using the traditional Public Key Infrastructure (PKI) system. This PKI system can easily be deciphered using quantum machines in hours, certain minutes or even instantly while it takes several years to decrypt using classic machines. In this changing world, if this machine comes into the hands of cybercriminals, it might be a threat to the world. To overcome this threat, many companies and research institutions are working on the development of a new encryption system called "Quantum safe" which is based on quantum concepts. This encryption is done using Quantum Key Distribution (QKD). Rather than using hard mathematics, QKD uses quantum physics to build keys. QKD distributes and shares secret keys between the communicating parties. This is important for ensuring that their communication remains private and it is also necessary for cryptographic protocols.

CONCLUSION

Cyber threats are a global issue that needs to be given higher priority in any organization. With the rise in cyber threats, there has also been an emergence of new technologies to counter the threats. Cybersecurity should be practiced not only by organizations but also by every individual. Everyone needs to understand the prevailing threats and learn how to defend themselves from threats. The pandemic has opened a gate for a new era of cybersecurity as it has provided opportunities and also added more responsibilities to IT security professionals. They can enhance their existing technology and protect their data and system in which the data is stored from upcoming heightened cyber-attacks. It is high time that cybersecurity professionals look down the kaleidoscope of time and focus on developing more secure cyberspace. Cyber threats are incessant, so we need our cybersecurity techniques to be continuously evolving. Last but not least, the question isn't whether cyberattacks will happen or not, but how organizations can respond and recover faster when it happens.

REFERENCES

Corey Nachreiner, "Why Ransomware Will Soon Target the Cloud".

Eric O'Neill, "Why the future of cybersecurity is in the cloud".

Gaurav Belani, "5 Cybersecurity Threats to Be Aware of in 2020".

"IBM's 2017 Global CODB Report Final 3", pp 23.

Jay Dosanjh, "What is next-gen intrusion detection? Don't be the next data breach victim".

Jignasa Sinha, "5 Artificial Intelligence-Based Attacks That Shocked The World In 2018".

John P. Mello Jr, "Top 5 emerging information security technologies".

Jovi Umawing, "The face of tomorrow's cybercrime: Deepfake ransomware explained".

Luke Conway, " Blockchain: Everything You Need to Know".

Marc Ph. Stoecklin, Jiyong Jang, Dhilung Kirat, "IBM Research DeepLocker".

"Oracle and KPMG Cloud threat report 2020" pp 11.

Risk-Based security's 2019 Year end data breach quickview, pp 4-17.

Shyam Oza, "Deepfake: The AI Endangering Your Cybersecurity".

Susan Moore, Emma Keen, "Gartner Forecasts Worldwide Information Security Spending to exceed $124 Billion in 2019".

Vijay Teja, "Virtual Dispersive Networking".