IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 6, Ser. I (Nov. – Dec. 2022), PP 44-48
www.iosrjournals.org

Mitigation of Cyber Risk through Digital Forensics Tools

Viral Kumar Maurya[1], Dhwaniket Kamble[2], Dr. Mohan Awasthy[3], Hayrambh Rajesh Monga[4], Nikunj Rajendra Shetye[5], Anas Ahmed Shaikh[6], Vikrant Sankpal[7], Ashish Upendra Sharma [8], Hrishikesh Sunil More [9], Diksha M. Bhalerao[10], Poonam V. Kapse[11], Sumita Kumar[12]

[1] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[2] *Department of Computer Science and Engineering, Faculty of Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[3]*Department of Engineering and Technology, Principal of Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[4] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[5] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[6] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[7] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[8] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[9] *Department of Information Technology, Student in Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[10]*Department of Computer Science and Engineering, Faculty of Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[11] *Department of Computer Science Engineering and Artificial Intelligent and Machine Learning, Faculty of Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*
[12]*Department of Computer Science and Engineering, Faculty of Bharati Vidyapeeth Deemed University Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India*

Abstract: *Cyber-attacks are becoming more frequent and severe. When an attack occurs, the attacked enterprise responds with a series of predetermined actions. The use of digital forensics to help in the recovery and examination of data from networks and digital media is one of these acts. Cyber forensic investigation is gathering and analyzing digital data to prove or deny Internet-related theft. Previously, computers were only used to store enormous quantities of data and conduct several operations on it, but they have evolved and now play an important part in criminal investigation. The selection and use of forensic tools is critical to solve these cyber-related problems. The developers created it for better research and faster investigation.*

Key Word*: Mitigation; Digital Forensics; Cyber Risk; EnCase; Autopsy.*

Date of Submission: 15-12-2022 Date of Acceptance: 30-12-2022

I. Introduction

The digital era has undoubtedly changed people's lives and professions. However, a wave of cybercrime that puts end-user privacy and data at risk is eroding the allure of digital technology. Concern among cyber experts is at an all-time high due to the frightening increase in cybercrime. Digital forensics has emerged as a benefit for cyber professionals in this dire situation, proving to be a vital resource. efficient method of analysing cyber-attacks[1]. Cybercrime is the most critical issue that has a considerable influence on the economics of enterprises, particularly those that operate online[2]. This economic loss affects all sectors, including the government and traditional enterprises. Cybercrime, often known as computer crime, is the criminal use of computer equipment and networks to accomplish other goals, such as fraud. The internet is the primary source of all of these activities[3]. The development of software application tools/computer forensics

tools is the most promising technological breakthrough in digital forensics. Data storage platforms range from industrial machine controllers to standalonedevices,personalcomputers,mobiledevices, cloud-basedcomputernetworks,systems,andservers.TheTherearemanytypesofdigitalforensictoolsavailableinthemarket. Oneistokeeptheoriginalfilesordataevenafterthedatahasbeen recoveredfromthesedevicessoyoucancompareitwith originaldataandconfirmthattheextracteddateisincorrect. Contaminatedor manipulated. There are some basic concepts to keep in mind when using digital forensic tools. Data is collected and should not be changed. Individuals using digital forensic tools must comply. A detailed record of their activities. Additionally, access to the original document should be controlled avoid tampering with or tampering with evidence [4].

Digital forensics is a branch of forensic science concerned with the recovery and analysis of evidence located in digital devices, which is frequently related with computer crime. Cybercrime is another term for computer forensics. This entails using computer technologies for research and analysis to solve crimes and give evidence to back up a claim. This is the process of preserving, analysing, and presenting digital evidence in a legally acceptable format acceptable. Using cyber forensic tools, it is quite straightforward to investigate the evidence. [5].

II. Methods

The potential for loss or damage to an organization's information or communications technology is called cyber risk, also known as cyber security risk. Cyber-attacks and data breaches are his two examples of cyber risks. On the other hand, cybersecurity risks are not limited to data corruption or destruction, or financial loss, but also include intellectual property theft, productivity loss, reputational damage, etc.[6]. Cyber threats have both immediate and long-term effects. A short-term risk is anything that disrupts the day-to-day operations of a covered organization, government, business, or end-user. Examples include fraud, data breaches, and ATM cash withdrawals. Long-term threats include industrial and military espionage, civil unrest and unrest, and violations of national security. All of these have long-term effects and seek to shift the balance of nations and societies.

CYBER THREAT AND THEIR AFFECTS:

1. Malicious Software: Malicious software, such as Trojans, infections, keyboard listening, spyware, and spam email, is used to obtain, modify, or delete data. Malicious software is frequently regarded as the most damaging cyber-attack technique for governments, organizations, and end users, in terms of both simplicities of usage and speed of effects. Malicious apps can be both hardware- and software-intensive. Keyboard listening devices that process hardware are one example of this[7].
2. Unsafe Environment: Network security is determined by the safety of the network components that comprise the network. Using the product's security features, it is possible to attack systems and get information. One example is the Stuxnet virus. Index of PLC rootkits for a specific product brand This virus, which was intended to be beneficial, has halted the industrial system.
3. DOS attacks: These are direct attacks on the system that cause significant harm by halting or disrupting systems. DDOS attacks are attempts to put the system to a halt by sending more requests than the operating system, server, or application can handle, hence violating the information accessibility rule.
4. Password Handling Attacks: Social engineering assaults, dictionary attacks, and password prediction programs are the most common approaches utilized in these attacks, which are evaluated in the context of privacy breaches. Information on people is collected via social engineering assaults and social skills, and the population is attempted to be distributed.
5. Side Channel Attacks: Side channel attacks target power analysis, electromagnetic applications, and system scheduled operations. The main goal of these assaults is to insert a spy program onto the system to steal the encryption key[8].
6. HTML Injection: This vulnerability advantages faulty coding by programmers while coding. The absence of a control mechanism in the web program for data taken from the database or data from the database. The so-called XSS is used to create a session and a cookie play. It is reasonable in apps to respond to a request given to the page. The server evaluates the request provided to the page and returns a response. However, if your website is moved to a bad URL or dangerous programmers such as a Trojan horse are installed, your response will differ from what you intended. The goal of this form of assault is not to harm the online application, but rather to get access to users that visit it.
7. SQL Injection: SQL injection is a type of attack that targets database queries. The questioning language construct is used in this attack. SQL injection is one of the most significant online application vulnerabilities. It's a bit less frequent now, because to the popularity of extra database layers like frameworks and ORM (Object Relational Mapping), but they're still ubiquitous! Because of fatal mistakes, web application developers do not completely comprehend SQL Injection. As a result, there aren't many easy SQL Injection techniques known today, yet there are complex SQL Injection vulnerabilities ranging from huge corporations to ready systems[9].

8. Command Injection: Shell injection attacks, as opposed to SQL injection and XSS attacks, are a form of attack that directly targets servers. It seeks to get remote access to information on the operating system, database management system, and server via the web application's command line[10].

COMPUTER FORENSICS TOOLS:

1. EnCase: Encase is a commercial platform that includes a set of investigative tools and procedures. It investigates recovering lost files, sorting, and reviewing files, signature analysis, internet history review, Hash value analysis, timeline review, gallery review, and registry analysis in depth. EnCase provides a well-formatted report that explains crucial facts and organizes the content with the help of the bookmarking tool[11].
2. Autopsy: This is open-source software that works as a forensics suite on both Windows and UNIX operating systems. autopsy can be used for research purposes, Web artifact extraction, hash filtering, multimedia inspection, timeline analysis, keyword search, and file analysis for file formats such as NTFS, FAT, ExFAT, HFS+, Ext2/3/4 [12]. Autopsy is the leading open-source digital forensics platform that is easy to use, fast, and applicable to any computer-based test. Examine hard drives, smartphones, memory cards, and other devices. Designed primarily for Microsoft Windows, but also supports Linux and macOS. This white paper provides an autopsy overview, autopsy installation, and autopsy cases and data sources [13].
3. Forensic Toolkit (FTK): AccessData's Forensic Toolkit is a digital forensic program for Windows. This program supports data analysis, recovering lost files, MD5 and SHA hash verification, file analysis for FAT, NTFS, Ext2, and CDFS, and graphical file viewing. The FTK Imager application, which is included with the FTK Toolkit, is also used for disc imaging[14].
4. Volatility: Volatility is an open-source program that is mostly used for memory forensics, malware analysis, and incident response. This is compatible with Linux, Windows, Mac, and Android. Volatility examines raw dumps, VMware dumps (vmem), crash dumps, virtual box dumps, Firewire, LiME format, Expert witness HPAK format (rapid dump), and QEMU memory dumps in 32-bit and 64-bit systems[15].
5. NIST SP 800-30 Rev 1: It is a framework that gives guidelines on risk assessment, which is part of the planning process for cyber-risk management. To mitigate the effect of potential hazards, proper controls must be put in place. The NIST SP 800-53 Rev 5 and the Center for Internet Security (CIS) Controls v8 can be utilised for this. The Center for Internet Security created CIS controls v8 to assist companies and people in focusing on and initiating the most crucial activities to fight against cyber-attacks[16].

Cybersecurity risk mitigation strategies:

As the chance of a cyber-attack increases, proactive cybersecurity risk reduction is increasingly becoming the only choice for enterprises[17]. Herearesometechniquestoreducecybersecurityproblems inyourITecosystem:

1. Drivecybersecurityrisks Rating

Cybersecurityrisks assessment, which may assist reveal possible vulnerabilities in your organization's security policies, should be the first step in a cybersecurity risk reduction approach. A risk assessment can provide information on the assets that need to be secured as well as the security procedures that are presently in place. A cybersecurity risk analysis can also assist an institution's IT security department in identifying areas of concern. Determine which vulnerabilities are most likely to be exploited and should be addressed first. One safety rating is a fantastic way to obtain real-time understanding of the cybersecurity situation of your organization, as well as those of third- and fourth-party vendors[18].

2. Set up network access constraints

Following an assessment of your assets and the identification of highpriorityproblemareas.Thenextstepistolimitinsiderriskbyimplementingnetworkaccessrestrictions.

attack.Many firms rely on security solutions that evaluate trust and user access, such as Zero Trust. Credentials are required based on everyone’s work role. This decreases the severity of risks or assaults caused by employee irresponsibility or, at best, a lack of cybersecurity knowledge. Endpoint security has also become a significant problem as the number of networked devices increases.

3.Install firewalls and antivirus software

Introduction of security measures such as firewalls and antivirus software are another key cybersecurity risk reduction approach. These technical safeguards give another layer of protection to your computer or network. Firewalls act as a barrier between the outside world and your network, allowing your firm to have more control over incoming and outgoing traffic. Similarly, antivirus software searches for potentially harmful viruses on your device and/or network.[19].

4. Create a patch management strategy

A lot of software vendors constantly offer fixes, which fraudsters are aware of. Unpatched vulnerabilities can be swiftly exploited by threat actors. To develop a successful patch management plan that can assist your organization's IT security personnel in staying ahead of attackers, organisations should understand the average patch release schedule for their service or software suppliers[20].

5. Continuously monitor network traffic

One of the most effective ways for reducing cybersecurity risk is proactive action. With over 2,200 attempts each day, just one way to remain ahead of criminals is to constantly traffic on a network as well as your organization's cybersecurity stance. Consider solutions that provide you a complete picture of your whole IT environment at any moment, rather than simply a manual, static snapshot rather than just a manual, static point in time, to enable real-time threat detection and cybersecurity risk reduction. Monitoring allows your IT security team to actively discover new risks and choose the best approach to respond to them.

6. Make an incident response strategy

It is simpler to maintain resources on standby if everyone, even IT security professionals and non-technical workers, is aware of their obligations in the case of a data breach or attack. One of the most important components for mitigating cyber risk in an organization's evolving network environment is an incident response strategy. Threats can come from anywhere, and their complexity is improving all the time, making it increasingly impossible to totally avoid data breaches. An incident response plan assists your business in doing all necessary to be proactively prepared so that your staff is capable of responding promptly and effectively to any problem[21].

7. Examine your organization's physical security

Many firms believe that merely managing the digital component of cybersecurity threats is sufficient. However, the actual location of your firm is just as crucial. A cybersecurity risk assessment may assist you in determining if your critical data and infrastructure are secure against data breaches, as well as whether backup and protection plans are in place and up to date.[22].

8. Reduce your attack surface.

A vulnerability or entry point via which hackers can access sensitive information and data is represented as an attack surface. Employees, online apps, and software are all examples of this. Assessing the following factors is part of reducing your attack surface:

- A physical attack exposes all firm assets that hackers can exploit if they obtain physical access to company buildings, facilities, and so on.
- Any assets that are accessible via the internet or from the outside world of a firewall constitute the digital attack surface. This might range from known assets like corporate servers to unknown assets like programmes that spoof your company.
- A social engineering attack surface includes a cybercriminal manipulating your staff to divulge critical information and data about your firm.

Additionally, keeping software consistently up to date across all assets is critical to reducing the attack surface. Good attack surface intelligence will assist firms in understanding their security posture and threat landscape, allowing them to detect and mitigate vulnerabilities throughout their operations.

III. Result

The study of all these works in the domain of non-control and control data attack demonstrates that there is no ultimate security and trustworthy application to avoid all types of modification data assaults. Recent research and study in this field[23]. This section investigates the tools' availability and if they are maintained. Developing new tools has the potential to be profitable. Valuable to the digital forensics' community as tools improve, created, they promote the development of close-knit communities of developers who provide regularly updated and patched or maintained code, bug patches, and extensive documentation[24].

IV. Discussion

We grouped the tool search results under the attributes of availability, maintainability of code, documentation, and licencing. Cybercriminals are becoming more skilled in their use of technology that enable them to conceal their activities better than ever before. Large enterprises' continuous financial losses have prompted them to either engage a computer forensic agency or computer forensic investigators to safeguard them from assaults and solve cases by executing competent and complete investigations in a short period of time. The investigators must follow the investigative process while adhering to local laws and set standards, guaranteeing the integrity of evidence, and establishing a case in court[25].

V. Conclusion

The study in this report shows that digital forensics in cybersecurity necessitates more broad and rigorous research, both academic and industry-focused. Because digital forensics is a very broad and broad topic in and of itself, international authorities must stimulate study in this sector as well as hardware development in order to detect and mitigate technological and functional concerns and obstacles.To begin with, digital forensics are often Including tool development. After scrutinizing whether these tools were maintained after development, I found that many were not. when you refer toQuality of comments in the source code found. The problem lies

with the factthat in most cases, tool development is not the focus of theresearch, but rather a by-product. With a combined lack ofcoding standards, limited testing, disparate repository locationsand poor documentation, it is unlikely these tools will ever bewidely adopted by the digital forensic community.

References

[1]. Abhishek Kumar Pandey, Ashutosh Kumar Tripathi, Gayatri Kapil, Virendra Singh, "Current Challenges of Digital Forensics in Cyber Security", January 2020.
[2]. Prashant Saurabh, Amrit Jay Kumar Roy, "Role of Cyber Forensics in Investigation of Cyber Crimes", IJLMH, vol. 4, 2021.
[3]. Muthu Dayalan, "Cyber Risk, The Growing Threat", IJNRD, vol. 2, November 2017.
[4]. K. Ghazinour, D. M. Vakharia, K. C. Kannaji and R. Satyakumar, "A study on digital forensic tools," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 3136-3142, doi: 10.1109/ICPCSI.2017.8392304.
[5]. B.V. Prasanthi, "Cyber Forensic Tools: A Review", IJETT, November 2016.
[6]. Nikita Sura Sheth, GRC 101: What is Cyber Risk? [Internet], October 2020: Available From: https://www.logicgate.com/blog/grc-101-what-is-cyber-risk/#:~:text=Examples%20of%20Cyber%20Risk,-Cyber%20risk%20can&text=An%20example%20of%20malicious%2C%20internal,out%2Dof%2Ddate%20software.
[7]. Şükrü Okul, Orhan Muratoglu, M. Ali Aydin, H. Sakir Bilge, "A Review on Cyber Risk Management", June 2019.
[8]. Loai Tawalbeh, Hilal Houssain, Turki F. Al-Somani, "Review of Side Channel Attacks and Countermeasures on ECC, RSA, and AES Cryptosystems", April 2017.
[9]. Mohd Amin Bin Mohd Yunus, Muhammad Zainulariff Brohan, Nazri Mohd Nawi, Ely Salwana, "Review of SQL Injection: Problems and Prevention", June 2018.
[10]. S. Chakrabarty and B. Sikdar, "Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems," in IEEE Transactions on Power Systems, vol. 36, no. 1, pp. 271-280, Jan. 2021, doi: 10.1109/TPWRS.2020.3008184.
[11]. V. Fernando, "Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges," 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2021, pp. 1-7, doi: 10.1109/NTMS49979.2021.9432641.
[12]. Fahdiaz Alief, Yohan Suryanto, Linda Rosselina, Tofan Hermawan, "Analysis of Autopsy Mobile Forensic Tools against Unsent Messages on WhatsApp Messaging Application", November 2020.
[13]. Balakrishnan Subramanian, "An Overview of Autopsy: Open-Source Digital Forensic Platform, May 2020", https://datascience.foundation/sciencewhitepaper/an-overview-of-autopsy-open-source-digital-forensic-platform-1
[14]. Sakshi Singh, Suresh Kumar, "Qualitative Assessment of Digital Forensic Tools", AJES, vol. 9, 2020.
[15]. Htar Htar Lwin, Wai Phyo Aung, Kyaw Kyaw Lin, "Comparative Analysis of Android Mobile Forensics Tools", ICETA, March 2020.
[16]. Amiruddin Amiruddin, Hafizh Ghozie Afiansyah, Hernowo Adi Nugroho, "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8", ICIMCIS,2021.
[17]. SecurityScorecard [Online]. Available: https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation
[18]. Cynthia Brumfield; Brian Haugli, "Cybersecurity Risk Planning and Management," in Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, Wiley, 2022, pp.1-22, doi: 10.1002/9781119816348.ch1.
[19]. Ali Sadiqui, "Studying Advanced Firewalls," in Computer Network Security, Wiley, 2020, pp.189-242, doi: 10.1002/9781119706762.ch10.
[20]. Nadean H. Tanner, "Patch and Configuration Management," in Cybersecurity Blue Team Toolkit, Wiley, 2019, pp.165-185, doi: 10.1002/9781119552963.ch12.
[21]. Andrew Gorecki, "Crafting an Incident Response Plan," in Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk, Wiley, 2020, pp.143-194, doi: 10.1002/9781119679349.ch4.
[22]. Y. M. Tukur, "Mobile Information Security Risk Calculator," 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2019, pp. 104-110, doi: 10.1109/FiCloudW.2019.00031.
[23]. Vahid Kaviani J, Parvin Ahmadi Doval Amiri, Farsad Zamani Brujeni, Nima Akhlaghi, Modification data attack inside computer systems: a critical review, IAESPrime, November 2020.
[24]. Tina Wu, Frank Breitinger, Stephen O'Shaughnessy, Digital forensic tools: Recent advances and enhancing the status quo, Forensic Science International: Digital Investigation, Volume 34, 2020, 300999, ISSN 2666-2817.
[25]. A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," in IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

Viral Kumar Maurya, et. al. "Mitigation of Cyber Risk through Digital Forensics Tools." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 24(6), 2022, pp. 44-48.