World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

From keyboard to cloud-base network revamped data lifecycle cybersecurity

Amadi Chukwuemeka Augustine [1,*], Juliet Nnenna Odii [2] and Stanley A Okolie [2]

[1] *Audit & Investigation Department, IIRS, Owerri, Imo State, Nigeria.*
[2] *Department of Computer Science, FUTO, Owerri. Imo State, Nigeria.*

World Journal of Advanced Research and Reviews, 2021, 11(03), 226–233

Publication history: Received on 10 August 2021; revised on 17 September 2021; accepted on 19 September 2021

Article DOI: https://doi.org/10.30574/wjarr.2021.11.3.0442

Abstract

This paper review seeks to identify the need for a revamped data life cycle security in the era of pervasive threat from skill cyber criminals at this time of internet of things. The motivation is to fill the knowledge gap by presenting some of the ways of data leakages and the likely protection in the organization. The aim is to present a good practice that encourages data confidentiality, acceptable use policy, knowledge of personnel and physical security policy. The building blocks of information security infrastructure across the entire organization is implemented by Enterprise Security Architecture. Rather than focus on individual functional and non-functional components in an individual application, it focuses on a strategic design for a set of security services that can be leveraged by multiple applications, systems, or business processes.

Keywords: Cybersecurity; Cloud base network; Cyber-attack; Advanced persistent threat; Enterprise security architecture; Malware

1. Introduction

To be outstandingly operational, data protection has to be everywhere, from the server to the terminals (endpoints), notably at the office, at home, throughout the cloud and across the web. This data protection must be intelligent to detect threats from any vector, automatically prevents as many attacks as possible, and provide actionable information to enable ranking and response. At the same time, organizations need centralized visibility and control over their data wherever it may be. They need control that enables granular categorization and policy application depending on a variety of attributes, not just user credentials. Consideration must be given to the user's location, the application in use, the actions relative to the category of data, and the possibility of malicious code, among others. With the typical collection of discrete point products operating in isolation, this combination of pervasive protection and centralized control may be possible, but it is difficult to manage consistent policies across all environments. Even if they are "best of breed," there are too many manual interactions required from attack to detection to response for the overall result to be timely and effective. As a result, security defenses tend to be locked down too tightly and negatively impact business work flows, or they may be too open and consume too many resources remediating attacks and compromised systems. These types of security operations are often driven by regulatory compliance or operate in a continual fire-fighting mode in reaction to the latest breach. The more effective alternative is an integrated security solution that delivers interoperable data protection across all endpoint, network, and cloud environments.

1.1. From Keyboard to Cloud-Based System

There has been a significant evolution in the way in which we save, store and access data. And particularly, the scale with MySQL databases shows no signs of stopping expansion. You no longer need to save documents on one particular

* Corresponding author: Amadi Chukwuemeka Augustine
Audit & Investigation Department, IIRS, Owerri, Imo State, Nigeria.

device. Personal files and data can be accessed from anywhere with a solid Internet service connection, at all time. This is made possible by cloud technology. The numerous cloud service providers make choosing a cloud service vendor difficult. Many of these cloud vendors offer storage space for free. Having gone pass the days of saving files on storage devices and media like floppy disks, CDs and even USB flash drives, cloud storage vendors namely Dropbox, Box.com and Back blaze now trend in these days even with some cloud storage vendors like Cloud wards allowing users to vendors in one place. With the aid of an internet connection, cloud storage functions by authorizing users' access and data download on choice device such as personal computers (PCs), personal digital assistants (PDAs) and tablets. Users of cloud storage can simultaneously edit documents with other users. This feature makes it easier to work offsite (that is away from the work site). Price for cloud storage is with respect to the specific needs of the user from the cloud storage vendor.

1.2. Cloud Based Network

Network communication and the interconnectivity between IT resources and application within a cloud computing infrastructure is referred to cloud-based networking. Cloud-based networking as a form of cloud networking, exist and operates within a cloud environment and infrastructure. With cloud-based networking, cloud computing service and solution can interact and perform network connection with other resources on the cloud. In cloud-based networking, the network structure, resources, management and other administrative and effective processes are performed within, from and through the cloud.

The key initiative behind cloud-based networking is to make available network connectivity between applications and resources which are either present or deployed on a cloud. For example, interconnectivity between virtual machines formed or installed within a same cloud environment is achieved through cloud-based networking.

1.3. Revamped Data Lifecycle Cybersecurity

Cyber-attack can be tremendously costly and fatal to a business' survival; this is irrespective of the business size which could be micro, small, medium or large business. An example is the Arkansas-based telemarketing firm's ransomware attack that apparently had to shut down operations and dismiss 300 employees. In avoiding similar catastrophic experience, building a security that will help team mates to proactively identify and respond to cyber threats, is necessary. To do that, you can refer to the National Institute of Standards Technology (NIST) framework, which according to Gartner is used by 73% of organizations worldwide (full content available to clients only).

In this paper, we'll elucidate how to create a 5-phase cybersecurity maturation framework that can holistically advance your organization's security stance.

1.3.1. Identify: Assess the security risk

In protecting business from cyber criminals, there is need to first identify the valuable cyber assets and information that can be prime targets or that will become prime target. One will need to take inventory of assets and implement data classification policies, which will help in assessing the kind of threats a business face.

1.3.2. Protect: Implement security measures

Once the valuable cyber assets and information has been identified, security measures for protection of such cyber assets and information have to be adopted. Protecting businesses is a multi-pronged approach. The right mix of security solutions and employee training, can ensure that business data and IT assets receive layered protection.

1.3.3. Detect: Monitor threats proactively

Detecting threats proactively is a critical phase in the cybersecurity lifecycle framework as it enables your business to prevent hackers from accessing and assessing your systems and remaining undetected, which can sometimes be up to four years.

This requires you to continuously monitor the logs on your networks, devices, and applications for detecting any incidents or threats. It also involves steering security assessments to recognize vulnerabilities and fix them before they be converted into serious cybersecurity events.

1.3.4. Respond: Create a response plan

Security framework is not full-proof, hence a cyber attacker who is persistent may find chinks in your security armour. An incident response plan is needed to be prepared for any such event; when a persistent cyber attacker finds a way.

An incident response plan being readily available, empowers your organization to swiftly come up with rejoinders and resolutions in case of any cyber-attack.

1.3.5. Recover: Ensure business continuity

The absence of an effective business continuity plan, for instance a data backup strategy; an organization can suffer incredible financial losses. State of Data Security Report in 2020, indicates that 75% of businesses paid ransoms to get their data back from hackers, however, 30% of them didn't get their data back.

2. Data privacy and integrity

Ensuring that your data is kept private and secure from unauthorized users as well as free from malicious or unintentional modifications is no easy task. When managing these aspects of security one main issue is the lack of control a cloud user has over the actual server the data is stored on, [1]. Data stored in the cloud can be separated into two groups, IaaS environment data and data in PaaS or SaaS environments. IaaS data is data that is stored in the cloud instead of on a local hard drive; examples of this include services such as Amazon Simple Storage Service. PaaS and SaaS data differs from this since this data is primarily used in the applications processing the data, certainly not storing it long term, [1]. Data stored in an IaaS environment can simply be scrambled in order to decline the risk of private data becoming public. Access control is the way a service provider can ensure that only authorized users have access to applications and data storage. It is significant to have formal procedures in place when allocating access rights to users. Policies that dictate how and when a user can gain access privileges as well as deciding on what application level their access should be viable are an important step towards keeping access control secure, [2].

2.1. Insider Accidental Policy Violation

When someone who is close to an organization, and who has authorized access, misuses that access to negatively impact the organization's critical information or systems, then an insider threat has occurred. Organizations globally are experiencing increasing count of insider threats; hence insider threat is becoming progressively rampant. According to Accenture, "69% of organizations have experienced an attempted or successful threat or corruption of data in the last 12 months". Insider threat is misinterpreted and many organizations have the misconception of insider threat; being the malicious insider, such as the disgruntled ex-employees, or current employees who have ulterior motives. There is always the looming threat that an employee, partner or vendor may go to boundless means to snip data on purpose. These are valid judgements but they aren't the only insider threat risk.

In fact, the accidental insider threat can be equally risky to the organization and is regrettably quite rampant, and in 2017, it accounted for 25% of data breaches. These are employees, vendors and partners with the best of intentions, but may by accident click a link, forgo company policy, or use an unapproved cloud storage service. Take, for instance, the data leaks resulting from misconfigured AWS S3 repositories that occurs almost weekly from Accenture to Tesla. For this reason, it is imperative to comprehend what accidental data misuse looks like and to put in place a plan to detect and prevent unintended insider threats before they by accident leak information outside the organization. Whenever an employee steps outside of company policy, cyber-attack risk is increased; be it intentional or as a result of forgetting or non-comprehension of the policy; it poses a threat to the organization. It's true that mean insiders may break policy, but it's equally true that an employee with no mean intent may break policy to simplify a task, or even without their knowledge.

Consistent and systematic appraisals of company policies are a given, but written policies can't be relied on to ensure prevention. You also need to have a proactive way of apprehending employees in the act of breaking policy, educating them on their mistake, and preventing them from taking further action outside policy.

2.2. Data Exfiltration through Database Access

Data exfiltration is sometimes referred to as data extrusion, data exportation, or data theft. All of these terms are used to describe the unauthorized transfer of data from a computer or other device. According to TechTarget data exfiltration can be conducted manually, by an individual with physical access to a computer, but it can also be an automated process conducted through malicious programming over a network. This second example is at the operational maturity level, and, while perhaps not as common as an accidental policy violation, it could still happen in most organizations. In this case, a user with malicious intent and privileged access to sensitive data accesses a database and attempts to send data to an external cloud service. The motivation could be financial, activism, or retaliation and will likely cause some financial and reputational damage if the thief is successful. The user engages their privileged credentials to access a delicate database and send the query result to an external cloud service.

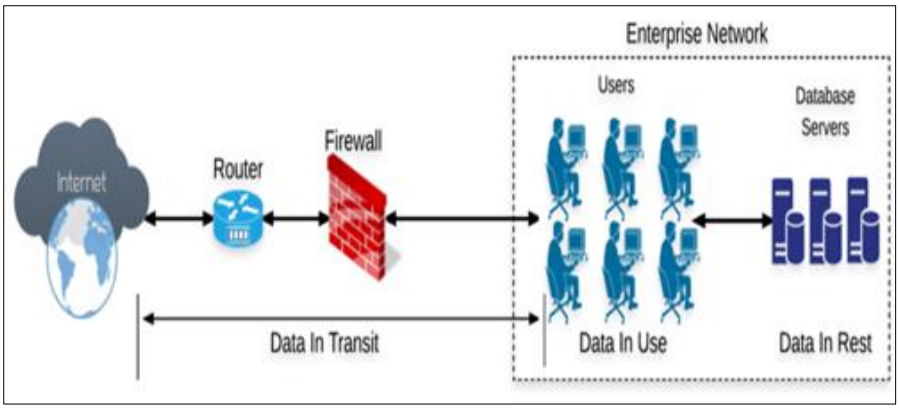

Figure 1 Data Analysis in an Enterprise Network [3]

2.3. Data Exfiltration with Malware

Advanced Persistent Threats (APTs) refer to a category of high-risk threats that pertain to computer intrusions by threat actors that aggressively pursue and compromise chosen target institutions or enterprises. Data exfiltration is the key goal of Advanced Persistent Threats (APTs). APTs attempt to go on undetected in the network in order to gain access to the company's crown jewels or treasured data. These treasured data include intellectual property, business secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret credentials from government or military institutions. APTs typically use social engineering techniques by fashioning email content that would be contextually relevant in order to transport exploits. These exploits are later on used to download more malware. Once threat actors infiltrate the network and establish persistent control, they can easily transmit the gathered company data. Once attackers acquire the stolen information, the impact to any organization or institution may include sabotage, data theft, and harm to brand image and reputation. When attackers have reached this stage, it is not a big issue for them to transfer data out.

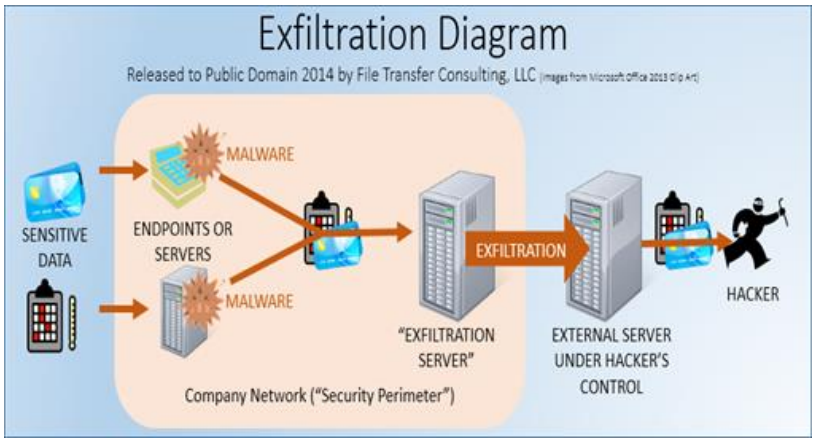

Figure 2 Data Exfiltration with Malware [3]

2.4. Data Exfiltration with SSL

SSL encryption is critical to shielding data in transit during web transactions, email communications and the use of mobile apps. Data encrypted with this common method can sometimes pass without inspection through almost all the mechanisms of your security framework, both inbound and outbound. As such, SSL encryption has become a pervasive tool for the enemy to conceal sensitive data transfers and to complicate their command and control communications. For example, suppose a user has yielded to one of the many phishing emails received daily, and has followed a bad URL link and involuntarily downloaded encrypted Zeus malware to the financial officer's computer used for bank transfers. Under the cover of encryption, Zeus sends that password information and other sensitive data to an external user, constructing a channel for the remote attacker to capture a login session, and using the transmitted password and deposit the organization's money in an offshore account. With all commands and traffic transmitted into and out of the network via SSL, the company's security tools were blind to these activities.

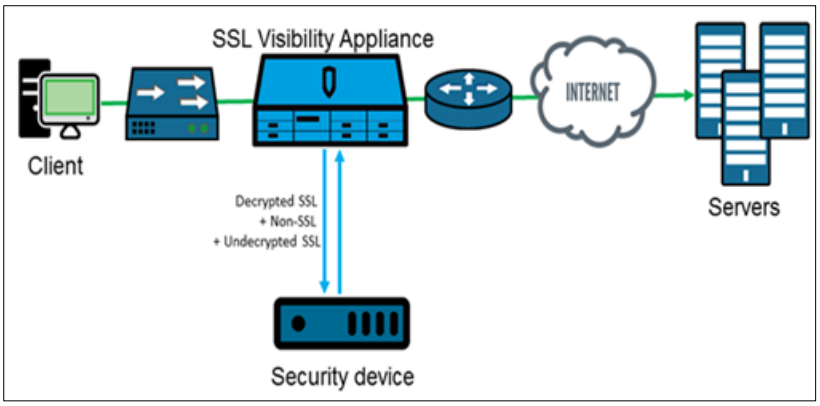

Figure 3 Data Exfiltration with SSL [4]

Five threats hiding in SSL traffic

2.4.1. Malware sent as attachments in email and instant messaging apps

Web and mobile applications such as Skype, WhatsApp, and Snap chat have default encryption on all incoming and outgoing messages. Similarly, most web-based email programs like Gmail and Yahoo Mail automatically encrypt traffic with the intention of protecting user privacy and data transfer between servers. However, this inescapably creates a blind spot in the corporate defenses when security applications fail to notice malware disguised as secured packets.

2.4.2. Malware distributed via social media

Facebook, Twitter, and LinkedIn all uses SSL but have lately fallen victim to emerging threats such as like jacking, malware propagation, data leakage, and spam. Koob face is one example of a Facebook based malware campaign. The network worm was notorious for the speed at which it was able to spread malware amongst multiple users, by using social engineering techniques on Face book messages.

2.4.3. Web application and DDoS attacks

Since the mainstream of websites support encryption for compliance purposes, attackers can now use SSL to bypass controls and intrude into the corporate network. Progressively, DDoS attacks are leveraging SSL vulnerabilities to overwhelm servers by performing HTTPS flood or SSL renegotiation attacks to take down the web server.

2.4.4. Insider abuse for data exfiltration hidden in SSL

Email on the web services and file sharing services have default encryption settings, which means that insiders can unnoticeably send sensitive data and files outside of the organization without being noticed by data loss prevention products. Ironically, while employees are the greatest asset in any organization, they can also be the biggest threat.

2.4.5. C&C communications and malware-based data theft

Malware-infected machines communicate to command and control servers via SSL. Recent examples include China's APT1, Zeus, Shylock, KINS and Crypto Wall, which all use SSL traffic to spread malicious malware. As malware becomes more advanced, hackers can now use social media, file sharing and email websites to exfiltrate data. By the time organizations detect a data leak, the damage is already done.

3. Organization Applications

3.1. Segregation of Networks

Once information has been classified and the critical information identified, organizations will want to ensure that they are preventing inappropriate access to that information. A common issue with many organizations is a lack of effective segregation of networks. This means that once an attacker has a toehold in the organization, their movements are likely to be poorly restrained. In fact, many organizations have an entirely flat network where even business units in different countries have full network access to the full resources of a business. As well as a lack of effective network segregation, it is rare to find organizations with effective information segregation, as organizations will typically have large

repositories of information (such as file shares, SharePoint or wikis) with few access restrictions. The outcome is that attackers have few boundaries to overcome in locating, accessing and aggregating information that will be of use to them. To increase the difficulty for the attacker, and also increase the number of opportunities to detect malicious activities, internal networks need to be segregated and hardened. Access to both networks and information is best based on the principle of 'need to know' and 'least privilege', whereby users are only allowed access to information (and indeed the servers where the information is stored) if they need that access for their job.

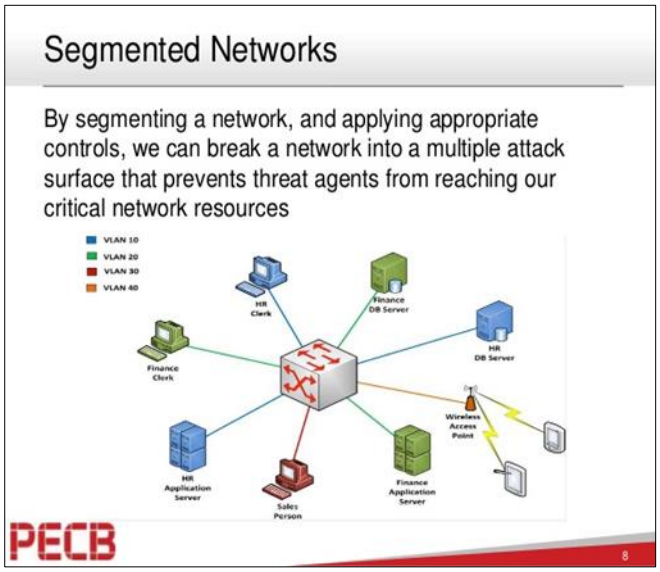

Figure 4 Network Segregation [5]

3.2. Host Hardening

Modern, advanced threat actors are highly capable when it comes to gaining access to machines through activities such as spear phishing and obtaining valid credentials. Despite the fact that organizations need to assume an attacker with sufficient skill and motivation will be able to succeed in these endeavors, host hardening is nevertheless a useful tactic, as it will make it far more difficult for the attacker to locate critical data or to penetrate further into the network. A number of hardening measures can be applied to standard desktops and servers that will impede attackers without a negative effect on normal business activities. Meanwhile, more restrictive measures are recommended for machines that will be used for the storage of highly sensitive data.

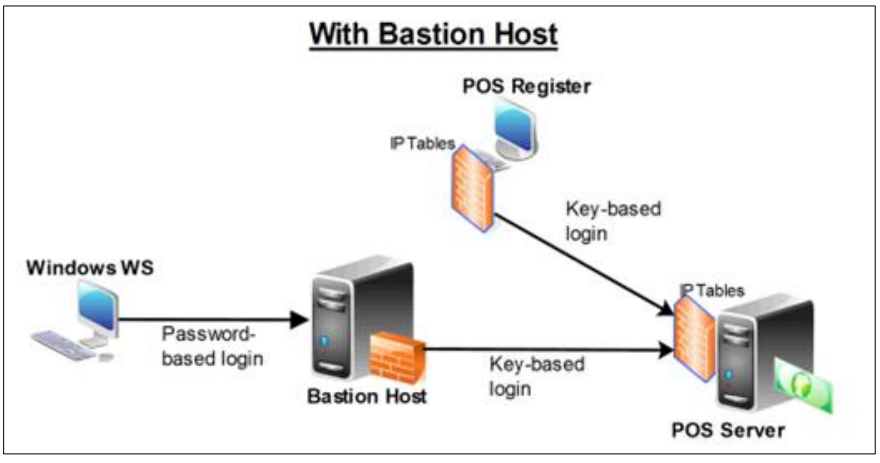

Figure 5 Host Hardening with Bastion Host [6]

3.3. Honey pots

Monitoring the access or use of sensitive resources can prove difficult, because of the legitimate use of the same resources throughout the working day. Hence staff involved in monitoring can find themselves spending large amounts

of time sorting legitimate from illegitimate access. This often results in attempts to identify specific patterns representing 'bad accesses, as opposed to 'good accesses, and alerting on the former. However, an attacker then needs only to remain within a 'good' pattern to escape detection. Honey pots avoid this problem by creating resources that appear to be sensitive but in fact have no legitimate use. This addresses the problem of monitoring, as any attempt to access the resource is highly likely to be an indicator of compromise. Different definitions of 'honey pot' exist, including a full computer, or a file on a computer, but for the purposes of this document it will be assumed that honey pots can be created within any resource that an organization might wish to monitor.

3.4. Emails

The mailboxes of senior members of staff are common targets for attackers, since they will typically contain highly actionable information, from attachments incorporating sensitive data to informal reports of project status or defensive plans. Organizations might therefore wish to consider creating an email account for a fictional high-level employee. Considerations will include the extent to which the fictional employee is publicized; for example, adding them to public webpages might cause legal difficulties, particularly in the case of executives, and yet their absence could alert attackers to the honey pot. The mailbox can initially be populated with real emails, or it could simply be a clone of a similar high-level employee's mailbox. The address can then be added to related groups, so that new emails flow into the account and an attacker identifying individuals through their membership of groups will find the honey potted account. Organizations might wish to develop the project by ensuring the fake individual appears in locations such as SharePoint, the organizational chart, and other places an attacker might look to identify a suitable individual. Mail servers or networking equipment can be set up to trigger an alert at any attempt to access the honey potted mailbox. This should then be treated as an active breach, as other executive mailboxes are likely to be attacked at the same time.

3.5. Files

Once file stores and other repositories of sensitive information have been identified, organizations might choose to place files within them that would appear tempting to an attacker. These files could contain terms related to projects, organizational plans, defensive strategies or other keywords likely to be sought by an attacker. A range of honey pot files can be created to cover differing ranges of words that attackers might seek. Files should be placed in locations where attackers are likely to find them. An example is where project updates for executives are stored; a 'strategic project plan' or similarly enticing file can be added to the same store. The same principle can be applied to database records, with records that need not be accessed during normal business functions placed within sensitive data sets. The hosting file system or server can then be configured, potentially at the OS level, to alert when the file is accessed. An alert should likewise be triggered by an attacker who copies the entire data set.

4. Conclusion

The contrasts between reactive and optimized security processes are substantial, especially when it comes to preventing infections and data loss, instead of merely detecting them after the damage has been done.

In reactive mode, security operations teams are typically investigating incidents days or even weeks after they have happened, often focused more on the need to comply with privacy and security regulations than effectively managing the risks. Security technologies operate in silos, and analysis and correlation of events is largely manual and time consuming. Compensating for this with restrictive policies results in delays and disruption of standard business processes. In proactive mode, investigations happen more quickly, perhaps within hours of an incident being

Prioritized. Security operations armed with threat intelligence can identify some attacks as or before they happen and contain many accidental incidents and basic malware infections. Regrettably, the speed and erudition of cyber-attacks means organizations are still consenting data to slip out.

In optimized mode, integrated security technologies, automated analysis, and intelligence sharing can prevent and detect sophisticated multistage attacks within minutes. Analytics-driven security operations aided by single-pane management views can quickly identify internal or external threat indicators and unauthorized access attempts. Orchestrated management of policy control and data storage locations secures data wherever it goes, resulting in fewer disruptions to business processes. Pervasive data protection enables organizations to rapidly move their security operations from reactive or proactive to optimize. Common data classifications, rules, and policies allow organizations to effectively control their data, maintain compliance, and demonstrate data sovereignty.

Compliance with ethical standards

Disclosure of conflict of interest

The authors agreed to publish this article with this journal. There is no conflict of interest.

References

[1] Faheem Ullah, Edward Matthew. Data exfiltration: A review of external attack vectors and countermeasures. 2018.

[2] Tim Callan. Equifax Data Breach Revealed to Be Due to Unknown Certificate Expiration. 2018.

[3] Carter, Kim. “Network: Lack of Segmentation". Holistic Info-Sec for Web Developers. Leanpub. 2019.

[4] Scott, Stuart. "Effective security requires close control over your data and resources. 2017.

[5] Verizon. Data Breach Investigation Report”. 2013.

[6] Mandiant. “M-Trends – Attack the Security Gap”, Threat Report. 2013.

[7] IBM, “IBM Security Services Cyber Security Intelligence Index (2013): Analysis of cyber security attack and incident data from IBM’s worldwide security operations”, IBM Global Technology Services. 2013.

[8] Joe Pletcher, Hannah Pruse, Masoud Valafar, Kevin Butler, Adam Bates, Benjamin Mood. On detecting co-resident cloud instances using network flow watermarking techniques. International Journal of Information Security. 2013.

[9] G Al-Bataineh A. White. Analysis and detection of malicious data exfiltration in web traffic. Malicious and Unwanted Software (MALWARE), 7th International Conference. 2012.

[10] Jason Andress and Steve Winterfeld. Chapter 6 - Logical Weapons. 2014.

[11] Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, Kevin Butler. Detecting co-residency with active traffic analysis techniques. In Proceedings of the 2012 ACM Workshop on Cloud Computing Security. 2012.

[12] Sutherland I. Benham. Network attack analysis and the behavior engine. Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference. 2013.

[13] Mike Mckee. https://www.infosecurity-magazine.com/opinions/accidental-insiders-serious-threat/.