International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 23 No. 1 October 2020, pp. 468-472

Cybersecurity - The Cloud and Government Intervention within Cyberspace

Bogdan Nedelcu[1], Andreea Nedelcu[2] and Alexandru Ioan Sgarciu[3]

[1]University Politehnica of Bucharest
Computer Science, Bucharest, Romania

[2]University Politehnica of Bucharest
Computer Science, Bucharest, Romania

[3]University Politehnica of Bucharest
Computer Science,Bucharest, Romania

Abstract – The aim of this article is to show the importance of cyber security and its growing influence on companies. We can also see how much companies are willing to invest in security. In this cyber security era, there is a fiercely competition between companies and the technologies they use to protect themselves against threats.

Keywords – Cybersecurity, Cloud, Spam, Malware

I. INTRODUCTION

The connectivity that the internet has provided between all of its users is one of the most useful tools for any field that requires even the most basic communication. Undoubtedly, the fastest way to share resources, including proprietary and sensitive data, both businesses and government have adopted it and become reliant on its capabilities. Services such as email, file sharing and data storage have proven to be most lucrative for any company, whether it is an administrative institution or a corporate entity. However, one cannot employ such an appliance without the confidence that it will handle the data it is given without fail, bearing in mind that vast amounts of public and private information are transferred over the web on a daily basis.

The need for trustworthy cyber security practices and policies is evident, as both businesses and their clients are affected by any kind of incident of this nature. The emergence of the internet into industrial and economic activities has opened a niche of exploitation, since any kind of vulnerability at this scale means the potential losses grow at an exponential rate. In order to fully understand the extent of what cybercriminals can achieve, one must consider their methods of attack: spreading spam and malware in order to infect as many computers as possible, ultimately, their goal is to obtain access to sensitive information such as passwords, credit card details, acquisition plans, financial data, etc.

However, on an organizational level, these threats must be either mitigated hastily or prevented altogether. The unauthorized entry into a system is usually achieved by exploiting its weakest link, in the case of cyber security, human error is the culprit, as it is the source of up to 95% of all security incidents [1]. Other points of entry exist as well, and these are covered by layers of firewalls, and anti-malware, antivirus and anti-spam software, that is not to say that these measures are impenetrable, but bypassing such defenses requires a large-scale coordinated attack.

The constant fast-paced expansion of the Internet entails the continuous growth of security threats; businesses must either take responsibility and handle the associated risks on their own, or find a trustworthy partner to provide such

Corresponding Author: Bogdan Nedelcu

services. Neither solution is fail-proof, as both require significant investments and cannot offer the certainty that one is absolutely safe. While it is difficult to achieve total safety, a series of preventive security practices consolidated by a healthy network of firewalls and most importantly strong antivirus, antimalware and anti-spam software provide an environment in which a company can operate without the constant fear of an attack disrupting its activity.

The maintenance of such a system is also crucial to its integrity, as constant patching and updating is expected for an optimal working capacity in keeping its users out of harm's way. Both banking and governmental institutions are supposed to be intrinsically trustworthy, which means that any kind of orientation toward an Internet-based model has to consider cyber security as a top priority. While guidelines and directives of this nature exist (e.g. ISO-2700x, the European NIS directive), the approach of the big administrative bodies, like the EU, is still in its infancy. As bureaucracy implies the slow movement of documentation, the growth of the Internet easily outpaces it, so it is hard to keep up with the ever-changing threats of this environment.

A company's security vulnerabilities can be limited through proper user administration, as risks exist inside its premises as well. Limiting access to cover only the needs of the employee eliminates the potential damage an insider attack might cause. Through proper use of existing tools such as Active Directory, IT administrators can restrict the permissions of end users and machines by linking them to Organizational Units, through which a high level of access control is obtained. While the employment process is supposed to eliminate any kind of insider threat, one must be aware of social engineering and the methods hackers use to gain entry in a system. As such it is the company's responsibility to establish secure channels of communication between its departments while also confirming, through the use of rigorous practices, the identity of all its users and machines.

The most widespread procedure is the use of digital certificates, electronic documents that bind users to cryptographic keys. Furthermore, these are part of a larger public key infrastructure (PKI), which is based on an asymmetric cryptographic system which authorizes and encrypts its users and the messages they send through it. They are entirely dependent on three bodies: the certificate authority (CA), the registration authority (RA), and the validation authority (VA).

Usually, the CA needs to act as a trusted third party (trusted by both the owner of the certificate and the customer relying on it), that issues, signs and stores the digital certificates, while the VA concerns itself with verifying the identities of those who attempt to use the CA, and the registration authority bears the responsibility of accepting requests and authenticating the users who perform these.

The complex architecture of this asymmetric cryptographic algorithm is precisely what makes it a good line of defense, as a hacker cannot directly decrypt any message sent, as he needs both keys and proper authentication in order to do so.

II. The Cloud

The emergence of cloud technologies, meaning outsourced storage and processing of data through software-as-a-service and platform-as-a-service capabilities, are thought to bring about the renaissance of the IT world. However, such a revolutionary step forward does not come about devoid of risks and challenges, especially since a transitional period implies a myriad of potential vulnerabilities and exploits waiting to be taken advantage of by cybercriminals.

It is clear that thriving in this ever-changing environment requires a high degree of adaptability from the big business involved in this field, which is why a cloud solution is appealing, buying a platform on which to run day-to-day operations is significantly easier and less costly than building one from the ground up. Providers of cloud services are concerned with efficiently streamlining operations, so instead of tediously maintaining hundreds of machines (regular patching, backups, etc.), users can access network storage and remote processing via terminals/consoles on their machines.

Determining what cloud computing actually refers to can be achieved by listing its defining attributes, and analyzing what each one means: "multi-tenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources" [2]. Multi-tenancy can be understood as a consequence of the paradigm shift achieved though the change of the business model these systems are based on, rather than orienting dedicated resources toward the individual user, the computing facilities are shared among multiple users. Massive scalability refers to the ability to adjust bandwidth and storage capacities for businesses with increasingly larger user bases. Elasticity indicates the user capability of easily tailoring their computing resources as they see fit, however this poses an issue as it is difficult to accurately predict what the potential needs of the consumer might be. Finally, the business model relies on a pay as you go system, meaning that users only pay for what resources they use, as long as they use them for, and self-provisioning of resources is self-explanatory, as users can self-supply resources, such as additional systems like additional processing power or software. The growing interest in cloud computing solutions must be evident by now, as these "provide users with access to supercomputer-like power at a fraction of the cost of buying such a solution outright." [2]

Although it may be true that cloud computing is a useful and powerful tool for any business, it does not come without its limitations and vulnerabilities. Before diving head first into deploying all sensitive information to a third party, one should be aware of the risks involved. The first concern that needs to be addressed is the lack of privacy; public clouds are a potential hazard for companies that need to store sensitive data, as this information becomes available publicly over the

Internet.

Another issue that needs analyzing is the employer's lack of control over its information, by adopting such a solution, one becomes increasingly dependent on the provider, giving up some degree of flexibility over data processing. Since interoperability between multiple providers is not guaranteed, transferring one's assets to a new one (should the need arise) can be impossible because of vendor lock-in [3].

The occurrence of this phenomenon is attributed to the attempt of integrating two cloud services from different vendors, which most probably use distinct hardware architecture and software. Service availability is the last significant limitation of cloud computing, considering that even a small period of downtime can lead to meaningful customer dissatisfaction; widespread network connectivity must be a priority for the provider, while having a response team for any connection disturbance in order to limit the any potential server outage [4]. While these are not the only problems that can be posed to either the vendor or the client of a cloud solution, these are the noteworthy ones for the purposes of this article.

III. Cloud Security

Finally, the most important issue to address is the cloud's security, by accessing the computational capabilities enabled by the cloud, the users enter the virtual environment; this requires them to transfer their data, and seeing as both small and large businesses employ such services, vast amounts of data must be handled. Usually, customers cannot know the precise location of their data, or whose data it is that they share a storage space with, this leaves the security concerns as the responsibility of the storage provider.

The preservation of the CIA triad: confidentiality, integrity, and availability, is paramount to data security, therefore, policies and practices must be undertaken in order to facilitate the conservation of this triangle. As minimum requirements of data protection, a provider must include: "a tested encryption schema to ensure that the shared storage environment safeguards all data; stringent access control to prevent unauthorized access to the data; and scheduled data backup and safe storage of the backup media" [5].

Furthermore, in a shared environment more security concerns can arise, as the provider cannot claim total responsibility for its users, they must also be careful with password management, and even insider threats, in the event of a legitimate user uploading a corrupted file that jeopardizes the whole cloud, the business that enabled the attacker must surely be held responsible. Difficult situations with hazy circumstances cannot be allowed to become a common occurrence; therefore, both the provider and the client must cooperate and enable rigorous authorization controls while also being thorough with permission controls.

Not to mention, there is a distinct lack of legislature concerning the IT world and cybercrime, and whatever laws there might be in place, they differ from country to country, which complicates any investigation even further, considering the way the Internet works. It is particularly difficult for governments to keep up with the growth of technology, which is why a common approach to this persistent problem has come in the form of coalitions, international bodies that aim to combat cybercrime through cooperation between nations. Most notably, the ITU – International Telecommunications Union, is a body within the UN that specializes in the development of legislation and standards regarding telecommunications and cybersecurity [6].

Unfortunately, adoption and evolution of the treaties is still in its infancy, keeping in mind that investments are required and governments have to ration the country's budget according to their most stringent needs, and it is rarely the case that they consider cybersecurity a priority. As such, business small and large can contribute to the effort of strengthening the Internet through diligent implementation of policies and practices that protect them as well as their clients. The industry can facilitate law-making through self-regulation of enterprise cybersecurity solutions, as more and more companies adopt the same policies that follow a secure standard that significantly reduces risk, the legislative branches of governments all over the world can build on what is already in place. Cooperation between lawgivers and their counterparts in multiple countries can not only solidify cyberspace but also build a network of trust between nations for better responses to any kind of attack or breach.

IV. Transition to Practice Program

While black-hat hackers are continuously working on new ways of breaking into existing systems, governments and businesses are leading an effort to reinforce present defenses through the development of cutting-edge security technologies. The United States' Department of Homeland Security plays a leading role in the pioneering of solutions to the most pervasive of threats through their Cyber Security Division (CSD), in the hopes of cooperating with enterprise towards a safer cyberspace. The CSD identifies eight "critical vulnerabilities in the cyber security landscape": Internet Infrastructure Security – the development of more powerful internet protocols such that users are not directed to unsafe websites through malicious pathways, Critical Infrastructure/ Key Resources – reinforcing the information systems that govern energy framework (i.e. electrical grid, oil and gas refineries), National Research Infrastructure – enabling research facilities in order to develop and test new tools to deal with cyber security risks(e.g. botnets, malware, worms, DDoS attacks, etc.), Cyber Security Education – one of the most efficient methods of prevention is awareness of the subject, targeting students would make for a more secure future of cyberspace, Identity Management – manufacturing proof of concept solutions, and piloting trails for identity and access control architectures, Software Assurance – designing software, tools, and techniques for the evaluation of the flaws and vulnerabilities of software, such that proper analysis can be conducted [7].

While the US government invests over 1 billion dollars into cybersecurity research, an insignificant margin is ever integrated into the marketplace, which is why agencies like CSD attempt to bridge the gap between research and practice. What makes this transition so difficult is the limited communication between researchers and the private sector, and a lack of understanding on all ends of the progression (i.e. researchers, the commercialization community, and end-users). This is where the Transition to Practice (TTP) program comes into play, struggling to be the catalyst that concretely links R&D and the marketplace, by establishing clearer lines of communication, fund-raising events, and the active involvement of the research community in the commercialization process.

The aim of TTP is not only the short-term integration of various technologies within the private sector, but to also build a long-lasting, self-sustaining relationship between the two bodies, such that government intervention is no longer necessary. A self-regulating marketplace that has state-of-the-art cybersecurity technology would not only bolster the credibility of the Internet economy, but also improve customer satisfaction by achieving an actual feeling of safety. Extensive research was undertaken in order to develop and publish the following technologies, the US government updates the Cyber Security Division Transition to Practice Technology Guide annually by including promising new technologies, for the purposes of this article I will present some of the most relevant ones for the state of the cyberspace today.

The Department of Homeland Security has worked closely with four research laboratories, each presenting two products as a result of their collaboration. Johns Hopkins Applied Physics Laboratory, whose roots began in 1942 as a government entity designed to aid the war effort through their science and engineering expertise, is in a continuous collaboration with the DHS since the days of World War II [8].

Their contribution to the TTP Technology Guide consists in REnigma, a tool for reverse engineering malware, and Socrates, a graphical analysis kit for finding patterns or relationships in large data sets. REnigma uses virtual machine record and replay technology in order to map step-by-step the execution of the malicious code, what makes this software unique is the ability to rewind to any particular state so that an analyst can easily understand the inner workings of the malware.

As Big Data is becoming an increasingly prevalent problem, Socrates makes use of extensive and complex data sets in order to enable rigorous analysis through the use of a flexible graphics model, its analytic capabilities are built on a probabilistic representation of data for a condensed expression of knowledge. The Los Alamos National Laboratory in New Mexico, which is famous for the Manhattan Project (the Allied project to develop nuclear weapons [9]), produced PcapDB, optimized packet capture for quick retrieval, and GUIDED, a tool for the discovery of malware similarities. PcapDB takes advantage of the existent abundant CPU cycles and memory within modern servers in order to index and store the packets before they would be written on disk, while organizing them by flow rather than individually.

This is precisely what incident responders need in order to execute their jobs more effectively, allowing them swift access in the longest, logically ordered history, such an application enables rapid investigation of any sort of network events. GUIDED makes for a powerful appliance in the dissection of malware, using a statistical approach to perform in-depth analysis by referencing an existing collection of samples and finding similar or distinctive segments of code inside the malicious software.

The MIT Lincoln Laboratory is a US Department of Defense R&D center that deals with problems related to national security. Their entries are Dynamic Flow Isolation (DFN), adaptive access control for the protection of networks, and TRACER (Timely Randomization Applied to Commodity Executables at Runtime). DFN achieves better network security through dynamic access control responsive to the current operational state, through the use of SDN (Software-Defined Networking) it applies policies to any users or machines it sees fit on an enterprise network.

Aiming to enforce the principle of least privilege automatically, DFN provides a means of invoking granular connectivity changes in response to user activity, reconfiguring network permissions and resource allocation, this allows for incident response teams to limit damage done by an attacker. TRACER secures closed-source Windows applications from complex attacks by automatically randomizing the sensitive internal data and layout, meaning stack cookies and heap metadata that protect static and dynamic memory, and the addresses of DLLs (Dynamically Linked Libraries). This is the usual target of an attacker, as it gives them remote access to the application; TRACER re-randomizes the encryption at every output making whatever information a hacker poached is stale and virtually useless.

The last laboratory to aid the TTP program is Pacific Northwest National Laboratory, a research facility that focuses mainly on energy, national security, and the environment. They contributed with FLOWER, a network flow analyzer that executes packet header inspection in real time in order to gather bi-directional network conversations between machines, and SilentAlarm, an interference-based technology which aims to identify abnormal activity like zero-day attacks and polymorphic malware without prior expertise of their specific traits. FLOWER empowers cyber defenders with understanding about traffic patterns, abnormal data flows, and forensic data for insight into future breaches or even lurking insider threats, through the parsing and aggregation of “up to 1 million IPv4/IPv6 packet headers per second”. SilentAlarm operates with dynamic behavioral analysis to detect suspicious network traffic as a byproduct of

malicious software and intervenes to address the code that spawned such abnormalities.

V. Conclusions

The current state of cybersecurity makes for some interesting developments from both the offensive and defensive, with innovation being the driving force behind the advancement of this field, be it in the form of more aggressive and stealthy malware, or harder to penetrate security measures. Aside from all the specialized software like anti-spam and antivirus, a key aspect of protection is the proper enterprise administration of machines and users, careful access and permission management can prevent insider threats or even limit the damage an unauthorized entry might achieve.

With the rising popularity of cloud solutions, security concerns have to be addressed quickly and efficiently so that businesses can employ these services without having to worry about losing their sensitive data.

By granting companies tremendous computational power at a fraction of the cost, the cloud is a tempting investment for both small and large businesses, as such providers have to build a secure and trustworthy environment in order for them and their customers to thrive.

Finally, governments are attempting to catch up with the advancements of the IT world, legislation is being made to combat cyber-crime and resources are allocated toward the development of tools to prevent, block, and analyze attacks, through programs such as TTP.

Through cooperation between states, countries are working to building a safer cyberspace which would make the Internet economy more reliable, so that we take full advantage of the unprecedented power of the telecommunications enabled by modern computing.

Acknowledgment

The work has been funded by the Operational Programme Human Capital of the Ministry of European Funds through the Financial Agreement 51675/09.07.2019, SMIS code 125125.

References

[1] Symantec Internet Security Threat Report, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[2] T. Mather, S. Kumaraswamy, S. Latif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”

[3] Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud, http://www.wseas.us/e-library/conferences/2013/Morioka/DSAC/DSAC-16.pdf

[4] S. Morshed, P. Goswami, ”Cloud Computing: A Survey on its limitations and Potential Solutions ”

[5] B. Potter, L. M. Kaufman, J. Harauz, “Data Security in the World of Cloud Computing”

[6] “About ITU”, http://www.itu.int/net/about/index.aspx

[7] “Cyber Security Division Transition to Practice Technology Guide ”, https://www.dhs.gov/sites/default/files/publications/CSD%20TTP%20FY16%20Tech%20Guide.pdf

[8] “Our History”, http://www.jhuapl.edu/aboutapl/heritage/default.asp

[9] “Fact Sheet”, http://www.lanl.gov/about/facts-figures/fact-sheet.php