ANALYZING AND FIXING CYBER SECURITY THREATS FOR SUPPLY CHAIN MANAGEMENT

Anil Lamba[1], Satinderjeet Singh[2], Balvinder Singh[3], Natasha Dutta[4], Sivakumar Sai Rela Muni[5]
Department of Computer Science, Charisma University, Turks and Caicos Islands

Abstract: This research aims to investigate the current status and future direction of the use of information systems for supply chain management for companies with multicomponent production. Paper presents a qualitative research method for analyzing a supply chain processes and for identifying ways of its information support. Based on data collected from different enterprises, can be concluded that in order to identify the most effective strategies of information support of supply chain the attention should focus on the identification and management of the sources of uncertainties, risks and cyber security. To successfully integrate business processes between suppliers and customers, manufacturers must solve the complex problem of information security. The main practical results are: proposed a new approach to the identification and prediction of supply risk within uncertainties conditions; proposed a complex solution to secure data in information systems for supply chain management.

Keywords: Supply chain management; Cyber security; Web supply management, Anomaly based algorithm; Classification algorithms; Data communication; Denial of service attack; Intrusion detection; Cyber Security; Cloud Security; Network ; Cyber; Cyber Threats; Threat Analysis ; Information Security; Data security.

Citation: Anil Lamba, 2017."ANALYZING AND FIXING CYBER SECURITY THREATS FOR SUPPLY CHAIN MANAGEMENT", International Journal for Technological Research in Engineering, Volume 4 Issue 5, pp.5678-5681, 2347-4718.

I. INTRODUCTION

Supply Chain Management (SCM) is the arrangement, planning, control, and realization of the product flow, range from designing and purchasing through production and distribution to the final consumer in accordance with market requirements for cost-effectiveness [1]. Information systems are designed to automate and manage of all stages of the organization's supply maintenance and control the entire product distribution in the organization (see Fig.1).The term was introduced in 1988, when the founders of the US-based company i2, Sanjiv Sidhu and Ken Sharma discovered another unoccupied segment in the information system market. Since then, many suppliers offer a variety of solutions that are marketed as those intended for supply chain management. SCM modules are in all ERP systems [2].

Fig. 1. Stages of SCM.

The SCM system allows significantly better satisfy the demand for the company's products and significantly reduce the costs of logistics and purchasing. SCM covers the entire cycle of purchasing of raw materials, production and product distribution. Generally, researchers identify six main areas that supply chain management focuses on: production, supplies, location, warehouse inventory, transportation, and information (see Fig. 2).

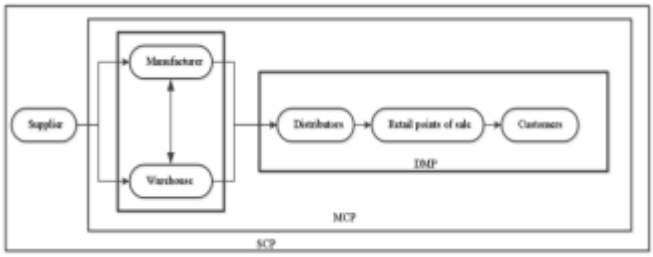

Fig. 2. Processes of SCM.

The following tasks are implemented:

- Improvement of service level
- Optimization of the production cycle Reducing of warehouse inventory
- Improvement of enterprise productivity Rise of profitability
- Control of the production process

SCM solutions create optimal plans for the use of existing technological lines detailing what, when and in what sequence should be made taking into account the limitations of capacity, raw materials and materials, batch sizes and the need to change equipment to produce a new product. This helps to achieve a high satisfaction of demand at minimum cost. According to AMR Research and Forrester Research, the implementation of SCM allows the companies gain such competitive advantages as reducing the cost and order processing time (by 20-40%), reducing purchasing costs (by 5-15%), reducing time to market (by 15% -30%), reducing the warehouse inventory (by 20-40%), reducing the production costs (by 5-15%), increase in profits by 5-15%.

A well-functioning supply chain helps to improve the

planning system, optimize warehouse inventory, make timely deliveries, ensure offer to demand conformity, reduce costs and, as a result, increase the company's market value.

The current trends in the development of SCM technologies are defined by the enormous possibilities of the Internet. The chains of manufacturers, suppliers, contractors, transport and trading companies are intertwined in the most intimate way and are already real online networks. Companies merge into the business community, and the boundaries between them are disappeared. However, there is a transparency of joint activities, performers can quickly adapt to customer requirements, as well as quickly bring new products to the market using advanced methods of prediction and planning.

The Internet is the simplest, cheapest, and most efficient technological means to manage and control the partner networks. Companies usually start with combination of the simplest activities using emails and workflow automation systems, then moving on to virtual docking of the most important business processes, and then merging into one virtual corporation within which the entire network is synchronized. This is already a transition to global e-commerce, when all business transactions and payments are arranged through the Web without exception.

As a result, not only productivity significantly increases, but also all processes significantly accelerate which lead to qualitatively new effects. For example, such a network system can minimize the impact of almost any negative external influences and create new products much faster than competitors. One of the first corporations that successfully switched to the parallel design of their products (laser printers) by uniting development teams from different countries is Hewlett-Packard. A company like Adaptec saves $ 10 million annually using web-based design with partners from Japan.

Approximately as much save Boeing and TRW when conducting joint research. And General Motors, working through the CommerceOne TradeXchange e-platform and selecting suppliers in fact in real time, saves about $ 400 million annually on costs. [3]

However, in spite of the obvious advantages of Web Supply Management, there is a huge amount of uncertainty and cyber security risks. All these types of vulnerabilities and other weaknesses can leave users vulnerable to the threat being compromised or attacked. Inefficient security methods include, such as not sufficiently fast fixing of known vulnerabilities, unlimited privileged access to cloud systems, and unmanaged terminators and infrastructure.

We also consider the question: why the expansion of the Internet creates an even greater risk for organizations and their users, as well as for consumers, and what information security specialists must do now to eliminate these risks before it becomes impossible to control them.

II. TYPES OF VULNERABILITIES: WAYS TO CONDUCT WEB-ATTACKS

The use of proxy servers is often an integral part of the implementation and operation of Supply Chain Management. Proxy servers have existed since the Internet inception, and their functionality has developed directly with it. Today, information security specialists use proxy servers when scanning content to identify a potential threat that are search for vulnerable Internet infrastructures or network weaknesses that allow hackers to gain unauthorized access to Supply Chain Management, penetrate into them and conduct their campaigns. Among these threats are [4]:

- Potentially unwanted applications (PUA), such as malicious browser extensions Trojans (droppers and loaders)
- Links to web spam and fraudulent advertising
- Browser vulnerabilities, such as JavaScript and graphics rendering engines
- Browser redirection, clickjacking and other methods used to direct users to fraudulent web content

Table 1 shows the most common types of malicious software that hackers used from November 2016 to May 2017. The list given in Table 1 contains a number of the most reliable and cost-effective methods for compromising a large number of users of Supply Chain Management [5].

Table 1. The most common malware, November 2017 - May 2018.

Threat type	Trojan-droppers	Malware	Trojan redirected browser	Bootloader of Trojan redirected browsers	Trojan Bootloader	Heuristic algorithm of Trojan bootloader	PUA and suspect binary files	Trojan	Browser redirection	Packed	Virus
Number of malicious	32737	23479	23727	19822	17635	15148	12519	9079	8428	5616	2678

They include the following:

- "Primary loads", such as Trojans and utilities that facilitate the initial infection of a user's computer (a macro virus in a malicious Word document is an example of this type of tool)
- PUA, which include malicious browser extensions
- Suspicious Windows binaries that spread threats such as adware and spyware Facebook fraud which includes fake offers, media content and deception
- Malware includes ransomware programs and agents to steal data when typing from the keyboard that deliver the load on compromised nodes

2.1. Spyware

Most of modern online advertising software in the Internet is potentially unwanted application (PUA) and is spyware. Spyware providers advertise their software as legal tools that provide useful services and adhere to end-user license agreements. Spyware disguised as PUA is software that secretly collects information about a user's computer activity. It is usually installed on a computer without the user's knowledge. In this study, spyware is divided into three broad

categories: adware, system monitors and Trojans. In a corporate environment, spyware represents a number of potential security risks. For example, it may do the following:

- Steal user and company information, including personal data and other proprietary or confidential information
- Reduce the effectiveness of security devices by changing their configurations and settings, installing additional software and providing access to third parties. Spyware can also potentially remotely execute arbitrary code on devices, allowing hackers to completely control the device
- Increase the number of infections. Once users are infected with PUA, such as by spyware or adware, they are vulnerable to even more malware infections

2.2. Spyware business email compromise

Recently, in the field of security, much attention has been paid to extortion programs. Nevertheless, another threat, by no means of such a high level, which gives its creators much more than ransomware, is the compromise of corporate e-mail. Today, this is currently the most profitable way to get a lot of money from a business. This is a deceptively light attack vector that uses social engineering to initiate theft. In the simplest version, the campaign to compromise business email includes the delivery of email to employees of financial departments (sometimes using fake data from other employees), who can send funds via bank transfer.

Hackers usually carry out some researches in hierarchy of the companies and its employees, for example, using profiles in social networks, and build management vertical. This may be a letter from the CEO or another top manager asking him to transfer a non-cash payment to a prospective business partner or supplier. The messageshould motivate the recipient to send money, which as a result will usually end up in foreign or regional bank accounts owned by cybercriminals.

Since messages aimed to compromise the business email do not contain malicious or suspicious links, they can usually avoid almost all the most sophisticated threat defenses.

III. TYPES OF VULNERABILITIES: WAYS TO CONDUCT SERVICE-ATTACKS

3.1. DevOps services

Despite the fact that SCM in their own way are proprietary IC, they are based on free or shareware DevOps services. By this concept is meant such technologies as Docker, MySQL, MariaDB and other popular DevOps components [6].

In January 2017, hackers began to encrypt publicly- available instances of MongoDB and demand a ransom for decryption. Later, hackers began to encrypt other types of databases, such as CouchDB and Elasticsearch. Services like DevOps services are often vulnerable because they are improperly deployed or intentionally left open to facilitate access by legitimate users. About 75% of CouchDB servers can be classified as maximally open (accessible via the Internet and do not require authentication). Only less than one quarter of them require authentication (at least entering some accounting information). As in the case of CouchDB, over 75% of Elasticsearch servers can be classified as maximally open. Unlike CouchDB, only an extremely small part of these servers may contain personal data. Docker is a software platform, whose operators from the very beginning paid great attention to security. However, despite these efforts, over 1,000 Docker instances are maximally open. Most Docker instances were found in the USA or China.

3.2. Cloud technologies

The cloud is a new area for hackers who are actively exploring it in order to gain new potential for their attacks. Hackers realize that cloud systems are vital for many Web Supply Management. They also realize that they can break into corporate systems faster if they can break into a cloud system.

Modern dynamic networks provide more opportunities for attack creating new security risks and reducing the possibility of control. The main source of such risks is the cloud. In addition, unauthorized and so -called shadow IT devices and applications create problems. End-companies underestimate the risk (and number) of loopholes in their corporate network, cloud and end-device infrastructure. The lack of simple control leads to the fact that, on the average, from 20 to 40% of the network infrastructure and infrastructure of end-devices becomes inaccessible for analysis or management of an organization [7].

It is a problem that affects organizations working in the public, healthcare, and financial and technology sectors. Unmanaged network infrastructure and end devices can be easily attacked by hackers who need a base to integrate into the organization’s infrastructure and compromise specific objects. They can also be used to extract data or send unauthorized Tor traffic, or they can be part of a botnet. Even a simple router, firewall, or incorrect segmentation setting can allow a hacker to break into the infrastructure and gain access to confidential data.

3.3. IoT

The Internet of Things (Internet of Things, IoT) is the interconnection of physical devices, vehicles, buildings and other items (often called “connected devices” or “smart devices”) that have built-in electronics, software, sensors, actuators and are capable to connect to the network, allowing them to collect data and share it. IoT includes three main elements: information technology (IT), operational technology (OT) and consumer technology (CT).

Industrial Internet of Things (Industrial Internet of Things, IIoT) means only connected devices within a production control network as opposed to a corporate IT network or datacenter. IoT offers great possibilities for cooperation and innovation in the business field. However, as it grows, there is the increasing of security risk of organizations and users.

One of the problems is the complexity of monitoring. Most information security specialists do not know which

IoT devices are connected to their network. Security, as a rule, doesn’t have top priority when creating IoT devices

(and these are all devices, starting with cameras and ending with thermostats and intelligent measuring instruments). Many of these devices are far behind in terms of security from desktop systems and have vulnerabilities fixing of which can take months or even years. In addition, they are characterized by [8]:

- Vulnerability and risk reporting and updates are almost or completely missing The launch is made on a specialized architecture
- The presence of non-updated or deprecated applications that have vulnerabilities, for example, Windows XP Fixing is rarely used

The difficulty in the security issue of IoT devices is added by the fact that information security specialists may not comprehend the nature of the alarms coming from these devices. In addition, it is not always clear who among the employees in the company is responsible in case of attacks on IoT. The teams responsible for implementing of these technologies, as a rule, leave the organization after the project is implemented.

IV. CONCLUSION

Organizations need real-time security context analysis to ensure easy control. In the absence of solutions that provide real-time monitoring and leak path detection, attackers can move around in the network without being noticed. In addition, organizations must test their segmentation policies and implement robust tools to verify the effectiveness of such policies. Organizations must also take the inventory devices and systems that are connected to the network. If security teams can only check with snapshots or old lists of managed devices, they can skip at least 20% of devices physically connected to the network via a wired connection. Such inventories should be regular and automatic, as the corporate network, cloud infrastructure and end-device infrastructure are constantly changing and cannot be effectively monitored by staff manually.

The situation is further complicated by the fact that Supply Chain Management is on the boundary of the transport and IT industries. The technological infrastructure of the transport industry has traditionally been based on closed, proprietary systems. Today, the industry is moving to modern network connections. It is necessary to move to connected IP systems because existing systems require expensive maintenance and are complex. In addition, consumers are waiting for new secure and mobile services that the existing communication infrastructure cannot offer.

For example, consumers want to be able to interact with airports, airlines, passenger and cargo rail traffic, highways or connected fleets and public transport departments on social networks using mobile devices or use mobile applications in vehicles.

REFERENCES

[1] Dubey, R., A. Gunasekaran, T. Papadopoulos, S. J. Childe, K. T. Shibin, and S. F. Wamba. (2017) “Sustainable supply chain management: framework and further research directions.” Journal of Cleaner Production, 142: 1119–1130.

[2] Ovacik, I. M. (2011). Advanced planning and scheduling systems: the quest to leverage ERP for better planning. In Planning Production and Inventories in the Extended Enterprise(pp. 33-43). Springer, Boston, MA.

[3] Baskerville, R., F. Rowe, and F. C. Wolff. (2018) “Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective.” ACM SIGMIS Database: the DATABASE for Advances in Information Systems49 (1): 33–52.

[4] Polatidis, N., M. Pavlidis, and H. Mouratidis. (2018) “Cyber-attack path discovery in a dynamic supply chain maritime risk management system.” Computer Standards & Interfaces56: 74-82.

[5] Cisco 2018 Annual Cybersecurity Report. (2018).Available:https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf. [Accessed: October 18, 2018].

[6] Boiko, A., V. Shendryk. (2017) ”System Integration and Security of Information Systems.” Procedia Computer Science104: 35–42.

[7] Gaudenzi, B., and G. Siciliano. (2017). “Managing IT and Cyber Risks in Supply Chains.” Supply Chain Risk Management, 85-96. doi: 10.1007/978-981-10-4106-8_5

[8] Khojasteh-Ghamari, Z., and T. Irohara. (2017). Supply Chain Risk Management: A Comprehensive Review. Supply Chain Risk Management,3-22. doi: 10.1007/978-981-10-4106-8_1.

