IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

Volume : 3
Number: 2
Year: 2019
Pages: 105 - 110

IT Security Trends for E-government Threats

Ahmet Efe[1*]

[1]*Internal Audit Executive, PhD, CISA, CRISC, PMP, Ankara Development Agency, Turkey*
[*]*Corresponding author: icsiacag@gmail.com*

Abstract – Information Security is the implementation of measures and systems designed to safeguard information using various systems and algorithms on different attributes and behaviors of data and information. Although many security products, projects and solutions have been developed to ensure confidentiality, integrity and availability of the information and systems in the e-government environment, there occurs many errors and control weaknesses in applications that new threats began to exploit. Because many other security problems have appeared in these applications, sometimes inappropriate or insufficient measures caused a waste of resources, time and money for e-services provided by local and central government organizations. Security trends have to keep up with the threats that always tend to use new methods according to latest innovative technology of both software and hardware. The content of this paper is consisting of some IT Security trends for e-government environment. We try to seek how security trends evolve over time according to new threats and innovative technology.

Keywords – IT security trends, Secure Software Development, Web Applications Security, E-government security

I. INTRODUCTION

The e-government term is defined by the Organization for Economic Co-operation and Development (OECD) as the use of new information and communication technologies (ICTs) that apply to all state functions of governments and municipalities. In particular, the networking potential is provided by the Internet and related technologies [11].

While local, regional and national governments use technology to improve the lives of their citizens, market-driven companies also use innovative technology to gain more and lower their costs. In automation, municipalities and businesses are exploring how to use technology to improve workplace productivity and improve citizens' lives in order to make intensive use of IoT to make cities smarter. This trend has brought about and brought about information security risks, weaknesses and measures.

Over the past 20 years, information technology has greatly improved. While it became a tool for facilitating office processes, it became a strategic tool for industry, administration and military. Before 9/11, the risks and security issues of cyber space were only discussed in small groups of experts. But after that day, it became clear that the cyber world posed serious risks to societies that became increasingly interdependent.

The world-wide-web (www), which was invented only twenty years ago, has evolved over time. But the threats also increased. Worms and viruses have evolved from annoying problems to serious security problems and excellent cyber espionage tools.

Distributed Service Inhibition (DDoS) attacks, to date only seen as the online form of “sitting actions“, have become a means of information warfare. In June 2010, malware called “Stuxnet”, which attacked Iran's nuclear program, appeared a digital version of the American-made “bunker buster” bomb that pierced the caves and exploded inside. With this incident, the warnings of experts since 2001 have come true, and have brought to mind the idea that the cyber dimension can sooner or later be used in serious attacks that result in death in the physical world.

Information and IT security require performing of various defense mechanisms against unauthorized access, exploitation, denial of service and interruption. As is known, information technology has many weak points regarding security and privacy. In recent years, companies and researchers have expanded more work in order to develop the state of the art for optimization of risks, benefits with security measures. Many new algorithms, protocols, frameworks and solutions are always appearing. But still stolen, corrupted or missing data are becoming common occurrence, it is heard that many cyber-attacks against social network companies (WhatsApp in October 2013), nuclear reactors (Stuxnet virus 2010), Websites an even antivirus and security Corporation (Norton 2013).[1]

There are three basic principles of information security; confidentiality, integrity and availability. Confidentiality includes applications for ensuring that information is made inaccessible to unauthorized persons. However, attackers can access information and violate the principle of confidentiality via new techniques that are being developed.

Integrity principle includes applications for ensuring that the information transmitted to the receiver does not change or corrupt the information delivered to the receiver. Accessibility or continuity policy includes applications that ensure that the system is used and maintained in-house and out-of-bounds without damage. [2]

Great number of research and development projects has been carried out and still being implemented by many organizations and countries in order to take precautions against computer malware and attacks. As a result of these projects, they developed antivirus software, firewalls, encryption techniques, VPN software / hardware, intrusion detection and prevention systems, content controllers, central management software

used in computer systems. This article has dealt with some information security trends that have come to the forefront in IT security research from both internal and external threats.

The threat no longer had a clear sender address. In addition to the territorial boundaries of the states, the rules of military space and time became meaningless. The use of civilian aircraft as a means of terrorist attack showed that almost anything could turn into weapons at any time. Suddenly, nothing turned out to be impossible or unthinkable.

This is exactly how cyber threats can be defined.

II. Materials and Method

A general survey to the literature and related magazines on cyber security is done. Analysis and descriptions in the literature are harvested for a better understanding of the security trends.

In order to effectively define cyber security trends, risks, vectors and threats need to be analysed first. Therefore, we have provided general terms and definitions for these security paradigms and jargons.

III. TRIGGERS OF SECURITY TRENDS

Every year trends can change due to different technological advancements. As is shown in the Fig 1., according to new technology and possibilities to exploit, each year the trends for attack vectors and threats may change.

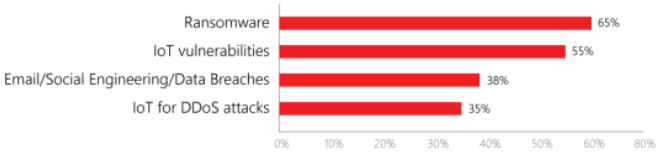

Figure 1. Top Cyber Security Trends

There are many factors that trigger new security measures, give indication of security culture of government organizations, and reflect security architecture. Among these factors, the biggest digital transformation trends that cause the government to fluctuate on security measure are as follows:

A. Connected Smart Cities and Critical Infrastructure

Connected household appliance IOT manufacturers and service providers will try to exceed their fine profit margins by collecting more personal data, with or without approval, transforming our home into an enterprise storefront. Enterprise marketers will gain strong incentives to monitor consumer behaviors in order to understand device owners' purchasing needs and preferences. This will pose serious risks of privacy and confidentiality.

Data and information are automatically collected, processed and distributed with the use of sensors installed in automobiles, street lamps, air traffic, traffic cameras and electric networks. Common to IoT, which is inevitable for smart cities, are smart meters that "talk" to public companies to save energy and road sensors that track and manage traffic patterns. All of these can provide hosts to weaknesses, as well as different approaches to packages of countermeasures and practices. In addition to major electronic infrastructure projects, IoT also works behind service efforts such as public transport, public safety and sustainability. Smaller, localized automation and municipality e-government projects are more difficult to implement due to lack of funding and technical support, but some countries use IoT for years without even realizing their information risks.

In 2017, cyber threats affecting critical infrastructure came at the forefront of important events. One of the most important of them was the "Industroyer", the malware that was held responsible for the attack on the Ukrainian electricity network in 2016. In the same year in Turkey were also expressed by the Minister that similar attacks. As attacks on critical infrastructure are made with political and terrorist motives, they can also affect much more than the electricity grid and can include defense and health sectors, municipal services, water, transportation, communications, and both critical production and food production. Governments and organizations are working hard on security, but constantly changing conditions mean that the threats continue until after 2018.

B. Internal Threats

Information security threats include internal threats that are defined as conscious or unconscious threats that may be created by those working in the organization. Conscious threats can be handled in two categories. The first category involves abusing the access rights granted to a malicious person in the organization intentionally. The second category involves the conduct of a malicious activity by obtaining the access information of another person. According to a survey conducted by CSI (Computer Security Institute), 44 percentages of participants had experienced internal abuse during 2008 [3]

Research on the identification of internal threats often involves artificial intelligence-based solutions. These studies are particularly successful in detecting malicious persons who gain access to someone else's knowledge. Even if access information is stolen in some way, it is not easy to know the access profile of the stolen person.

One of the most important methods used in determining the internal threat is to make definitions of information. This is sensitive or critical to the organization; control the flow of information and storage of such information under the definitions. Detection systems that do this are considered as data hiding prevention.

C. Decreasing Personal Privacy

Privacy has become one of the most important issues recently, due to wide usage of social media. Personal confidentiality is used to determine the identity of a person or group of people and their conditions under which they will access their information. Securing personal privacy should be done in two different situations.[4] The initial situation should be protected against all threats while personal data is in the person's information in the systems. In this case, the current precaution can be applied for the protection of any information. These precautions include issues such as access control, authorization, and provision of continuity.

The second case involves the security measures that will be applied to the need to share personal data with another system.

Research on personal privacy is usually focused on the second topic. Studies in this context are called as privacy preserving data publishing. These methods ensure that the data is never transmitted in a way that does not match the owner's critical information.

Personal security and confidentiality should be paid attention especially in the field of internet. In this regard, it can

offer the following to users; it should be checked that the websites (shopping, communication, commerce, file downloads, etc.) have been a valid certificate and https linked, take action with known and secure sites and do not share self-descriptive information on the Internet and social networks. Giving too much location information, address and other contact information away pose serious risks both for people and entities.

In the coming years, companies that are in search of "stickiness" in aggregate for personal data as a user application will become more aggressive in activating and aggregating user-generated content by the younger users. Parents will be aware of the apparent institutional misuse of digital content created by children and will consider the potential of long-term effects of these practices on their children. This may also pose special risks for those who are inclined to collective data altogether.

D. New Types of Malware

Malware is a general naming for malicious software designed to harm or exploit electronic devices or information. Malware can steal sensitive and critical information from the user's computer, slow down to the computer step-by-step or even send fake e-mails from the user's e-mail accounts.

Nowadays, internet users are exposed to many malware, such as viruses, worms, trojans, and adware. Malicious software has become dangerous. Computers that do not have any antivirus programs installed are now infected with viruses that connect to the Internet. Even some new types of malware cannot be detected by signature based antivirus software. In addition to suggesting various security mechanisms, researchers have done a lot of work to identify, intervene and prevent malicious software. Various hardware such as graphics cards and next generation processors have been used to block malware.

E-mails are sent to Internet users through various current communication channels, which consequently encrypt the data of the users. Many of these attacks are delivered to users via email channels in the form of various telecommunication, gas, electricity or similar corporate bills.

An emerging trend exists in ransom types of malwares. The profitability of traditional ransom software campaigns, dealer defenses, user education and industry strategies will continue to diminish as they evolve to tackle them. However, since weaknesses cannot be overcome, weaker ring attacks on the global scale will take over. Attackers will target less traditional, less profitable Ransomware targets, including high net worth individuals, connected devices and businesses. It also appears that the ransom will continue to be the target of the attack because e-government applications have strategic priorities. The outbreak of the traditional approach will see that it is applied beyond the purposes of extortion, sabotage and corruption of freemasonry. This journey between the threats of greater damage, deterioration and greater financial impact threatens not only to reveal new types of "business models" that are motivated by cybercrime, but also to seriously lead to the expansion of the cyber insurance market [13].

E. Serverless apps

Non-server applications will provide deeper details such as faster billing for services. However, privilege escalation and vulnerability to attacks those take advantage of application dependencies. These practices are generally defenseless against attack against a transit passing through a network. They are potentially vulnerable to unsuccessful service denials that an unsupervised architect cannot scale and suffer. In addition, they must include security processes that absolutely require functional development and deployment processes, scalability features should be used and protected with VPN tunnels or encryption. Otherwise, risks arising from usage of serverless apps will not be mitigated.

F. Blockchain and data security

An emerging approach and trend to reduce the growing number and complexity of cyber threats may be to use block-chain principles to strengthen security. It is given by block chain technology, and it is tried to be stored in decentralized and distributed manner. Rather than being stored in a single location, the data is stored in many different places in the open source code. The mass makes the data much more difficult to intervene or change the data. Because all participants in the block network immediately notice that the data has changed in some way. Blockchain has a significant leap potential to secure sensitive information, especially in highly regulated industries such as finance, government, healthcare and law, and can be used in virtual money and notary areas.

While every organization has personal security risks that require different defense methods to reduce attacks from inside and outside, or to keep losses at a reasonable level, some common technology trends emerge as trends. While security analysts and vendors benefit from the latest technology developments to produce more customized and better targeted solutions, businesses must adopt more consistent and reasonable protection strategies. These strategies should undoubtedly be predictive of future and risk trends.

G. Secure Software Development

The main reason for security vulnerabilities in software is seen as not considering security at every step in the software development cycle. Standards such as CMMI (Capability Maturity Model Integration) have been put forward in order to develop software in quality. But there is no assurance about the security of software developed by following these standards. Standards for creating a secure software development cycle are being developed. The Microsoft Security Development Lifecycle (SDL) method [5] and OpenSAMM [6] methodology are examples of such standard work. Important points in software security are the following; protection of the data, authentication, ethical commitment, authorization, accessibility, system monitoring and control, other security measures.

H. Increasing Web Applications

Since the HTTP protocol is not designed with security in the beginning, many security vulnerabilities have emerged especially within the scope of the protocol and solutions have been produced to close these holes. Since web applications are the basis of critical systems on the Internet and the http protocol is not secure, the attackers are getting lot of web applications. BM's 2008 Risk Report, 55 percentage of security vulnerabilities in 2008 are related to web applications [7].

A significant portion of web application vulnerabilities are cross-site scripting, SQL-injection, and file inclusion.

İ. IT Security of Industrial Systems

The integration of utility systems and energy management to e-government platforms will pose serious risks. Modern industrial systems such as power plants, nuclear power plants, dams, gas stations are large complex distributed systems. During operation, it is desirable that operators monitor and control different parts of these systems. Network technologies enable these monitoring and control operations with SCADA (Controller Control and Data Exchange).

SCADA systems can connect to corporate networks and internets. While this connection facilitates the production and distribution process, the system faces security problems of the Internet. A configuration attack on the SCADA system can affect the entire system [8]. As a result of this attack, besides physical and economic losses, people can suffer more lives and environment. Therefore, the safety of SCADA systems must be the primary priority [9].

With the advent of new paradigm such as IoT, smart cities, industry 4.0 and e- governance that require devices that communicate via internet pose serious risks that cannot be assured by existed security infrastructure and ability of people and organizations. More and more costs need to be covered by victims and information & systems owners.

Access to the SCADA network is required to be deceived by the defense-in-depth principle as much as possible. It is also necessary to consider not building unmanageable infrastructures by moving from defense in-depth principle. Improperly managed complex structures will cause false security perception. It is proposed that the security layers be regulated only to provide access to the required permissions and to restrict all accesses that are not needed.

J. Advanced analytics and tailor made security

Organizations that are sensitive to information security risks and threats use a combination of security products that are used to mitigate data corruption and confidentiality risk, from virus protection software and data loss prevention (DLP) tools to complete security, information and event management (SIEM) software. However, it can be said that the e-government is relatively backward in the field of security. In particular, SIEM is recommended for e-government units due to its large data generation capacity, which makes it difficult to find information that requires urgent attention. Advanced data analysis tools help organizations to better understand the risks and vulnerabilities. Adoption of technologies such as user and asset behavior analysis (UEBA) should be ensured by public institutions. Public institutions can improve security vulnerabilities before a data breach, providing e-service better control over IT infrastructures and better understanding of vulnerabilities.

While the global cyber security market is constantly evolving, it is too threatening for the e-government. Security providers are rapidly expanding the solution spectrum to enable their customers to solve similar problems differently depending on their infrastructure. With strong data protection applications on demand, security vendors will start to offer a more personalized approach taking into account factors such as IT infrastructure size and complexity, industry and budget. A more specific approach and trend to IT security will increase the search for solutions tailored to their needs.

IV. CYBER PROJECTIONS FOR TRENDS

Cyber security is still an issue that every business leader has in mind. So, what can be expected to see in 2019 and beyond? Here are the things from latest cyber security reports (bga.org in particular) to consider as part of basic needs against new cyber security trends:

A. Improving cyber security regulations

Legislation that is too slow and inadequate to benefit cannot capture the dynamic and fast-moving nature of cyber security due to hyper speed of innovative technology that produce new threats alongside its benefits. This weakens security by creating a culture of compliance with regulations and a false sense of security against agile, motivated and intelligent enemies. Trainings to lawyers and judges are of crucial importance to provide an effective law mechanism.

B. Transformation of data theft into data manipulation

It is highly anticipated that attackers can transform their methodology from data theft and website hacking to data integrity attacking. People may not understand that their data has been changed. Such an attack would cause long-term, reputation-related damages to institutions by causing people to question the integrity of the data, compared to a direct data theft.

C. Demands for security skills will continue to increase

The scarcity of cyber security skills in workplaces globally makes organizations suitable for attack. Demand for expertise will increase as companies notice this. Furthermore, all of the managerial positions will ask for a certain level of cyber security literacy.

D. Cyber Security and Internet of Things (IoT)

the new generation of artificial intelligence-based attacks will be skilled enough to trick even qualified security personnel by mimicking certain user behavior. This could include the ability to create complex and bespoke phishing campaigns that will successfully trick even dangerous people. IoT producers will invest more on the security aspects of their products in the market.

E. Attackers will continue to target consumer devices

Ransomware is a recognized problem for companies of all shapes and sizes, as evidenced by the massive WannaCry attack that affected Britain's National Health System and organizations around the world.

Will we start to see that consumers are targeted through a series of linked objects in 2019 and beyond? Considering examples from child hunters targeting IoT devices in toys designed for children, this is a possible scenario. Attackers can even target smart TV in home, drones in the space and unmanned vehicles.

F. Attackers will be more courageous, more commercial and less traceable

Hackers will pay attention to becoming more organized and more commercialized - they can even create their own call

centers; this is something we've already seen with cheat dating sites.

Attackers; they will attach importance to working in countries outside the jurisdiction of judicial authorities in countries where cybercrime is not considered a criminal offense.

G. *Attackers will become smarter*

They will continue to exploit the Dark Web, a small part of the Deep Web, to successfully hide and communicate with other criminals. Crypto currency will provide a very fertile cyber areas for easy earnings.

H. *Violations will be more complex and difficult to handle*

Cyber criminals will try to expand their malicious activity by using malicious codes in more surprising ways.

If the victim transmits the malware via a link and two or more people upload and pay for this file, the first victim will decrypt the files for free.

APT attacks that can numb a whole structure will be major concern for big companies, government and military units.

İ. *Cyber risk insurance will become more common*

This type of insurance will increasingly become part of the operational risk strategy, but the insurance industry needs to adapt products tailored to customer needs and go beyond expanding existing insurance coverage.

As the industry develops; loss of reputation and trust, loss of revenue from negative news, and development costs for security infrastructure or system improvements.

V. CONCLUSION

Cyber security is an important issue. Every company, every organization is a potential target. The cost of cybercrime worldwide is estimated to reach $ 2 trillion by 2019. IBM CEO Ginni Rometty believes this is the biggest risk for any company in the world [14]. Nevertheless, despite international awareness campaigns , many organizations remain insufficient to understand and take action against this growing threat [15].

Important ones are often large-scale external attacks. However, most of the daily cyber risks come from within your company [16]. This may include employees who intentionally or accidentally leak passwords and sensitive information, or malicious people within the company that is the employees or known partners who use access and information to damage or use the company's networks for their own benefit.

External attacks are, of course, a growing threat - they're looking for 24/7 vulnerabilities to infiltrate your systems or trying to damage your online presence from the outside. For a logical and sound step to cyber security, it is necessary to be aware of and fight against both internal and external threats.

Every business is at risk. Because of the interconnected nature of the modern business world, hackers often target smaller businesses to reach larger partners, customers, or suppliers. Larger businesses are now demanding that all suppliers and partners, regardless of how small they are, have their cyber security regularly checked.

Machine learning , a technology that evolves with large amounts of useful data(ML) has also become a mainstay of cyber security trends. ML algorithms can save cyber-defenders from repetitive jobs, especially confusion about suspicious files' sharing priorities, which can ultimately help them identify real threats more efficiently. On the other hand, the ML can be a boon for malicious people who are aware of their potential in automating labor-intensive tasks and researching vulnerable targets.

Special security measures such as firewalls, intrusion detection and prevention software, encryption and secure networks should be designed and implemented by government agencies and municipalities to ensure appropriate levels of security of electronic public services provided through e-government applications. However, information security, innovative technologies that are constantly evolving, people who trust systems, hackers and out-of-date processes must also count. Employees with day-to-day access to e-government systems should be trained in cyber security and this aspect should become part of their own work. An exemplary research by the Department of Computer Science at Columbia University [12] shows how the human factor affects cyber security policies and how this work will train government employees to improve the security situation of government departments and institutions.

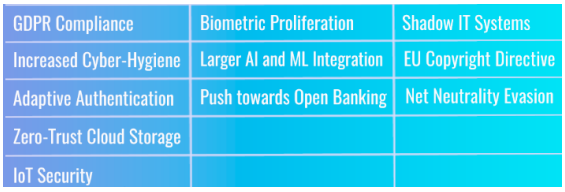

Figure 2. Top Cyber Security Trends in 2019

Source: https://www.le-vpn.com/cybersecurity-trends-2019/

Malware research has proven that legal regulations in fighting cybercrime are very useful for security applications. Collaboration between Microsoft, ESET, NSA and law enforcement agencies, including the FBI and Interpol, is an important example in this sense and they are working together to stop an important botnet operation known as Gamarue. This information demonstrates the need to establish global platforms for security governance. With the development of practices based on the NATO Talinn Guidelines, co-operation in the face of cyber terrorism will become a trend in the future. Increased co-operation will lead to the emergence of fewer active cybercrimes as more deterrence is a deterrent effect. Government officials continue to gain experience to work with private cyber security experts, showing that we can look after more successful research and potentially safer after 2018.

Researches and projects on information systems security have pick up speed, while the internet has become widely used all over the world in such fields as military, e-government, industry, e-health, e-commerce, e-learning. Today, while the information technology develops day by day for individuals, companies, institutions and governments, security problems are also increasing alongside with innovation. As we have seen in the examples for security of information technologies, information security is not just technology and information security. Information technology is a system that requires people, processes and technology to work together.

The number of services offered on electronic platforms (internet banking, e-bill, e-ticket, e-commerce, e-government etc.) is increasing day by day and the number of users using these platforms is increasing. As a result of various natural disasters, human error, fire, flood, earthquake, terror attacks,

etc., information security can be damaged. Electronic applications developed with information technology, on the one hand, facilitate the functioning of our lives while bringing new security threats and new types of crime.

REFERENCES

[1] Salah-ddine Krit and Elbachir Haimoud, "Review on the IT security: Attack and defense", IEEE, 2016

[2] Temiz Semanur, Yilmaz Bülent, "Awareness of Information Security in Information Centers: Sample of Academic Libraries in Ankara", 2013

[3] Richardson R.,"CSI Computer Crime and Security Survey" 2008, http://www.kwell.net/doc/FBI2008.pdf

[4] Spiekermann S., Lorrie Faith Cranor, "Engineering Privacy," IEEE Transactions on Software Engineering, pp. 67-82, 2009

[5] Microsoft Security Lifecycle (SDL) Version 3.2

[6] Software Assurance Maturity Model, "A Guide to Building Security into Software Development Version. 1.0",

[7] IBM Internet Security Systems, X-Force 2008 Trend and Risk Report, January 2009

[8] Christos G. Panayiotou, Georgios Ellinas, Elias Kyriakides, Marios M. Polycarpou, "Critical Information Infrastructures Security", 9th International Conference, CRITIS 2014, Limassol, Cyprus, October 13-15, 2014.

[9] Igure V., Laughter S., Williams R., "Security Issues in SCADA Networks", Computer and Security, p496-506, Elsevier, 2009

[10] Madhavi Dhingra, Manisha Jain, Rakesh Singh Jadon, "Role of Artifical Intelligence in Enterprise Information Security: A Review ", IEEE, 2016

[11] Organisation for Economic Co-operation and Development, Public Management Service, PUMA 16/ANN/Rev1 (2001). "*E-Government: analysis framework and methodology"* http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=PUMA(2001)16/ANN/REV1&docLanguage=En (Link at 21-October-2017)

[12] Brian M. Bowen, Ramaswamy Devarajan, Salvatore Stolf (2012). "Measuring the Human Factor of Cyber Security". Homeland Security Affairs, Supplement 5, article .http://academiccommons.columbia.edu/catalog/ac%3A142664

[13] Ismail. N., "Uber hack affects 2.7M UK customers" Information Age, http://www.information-age.com/uber-hack-affects-2-7m-uk-customers-123469804/ 2017

[14] Morgan, S., "Cyber Crime Costs Projected To Reach $2 Trillion by 2019" https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4e4a3c903a91

[15] GFCE, "Global Campaign to Raise Cybersecurity Awareness", https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness

[16] Zadelhof, M.V., "The Biggest Cybersecurity Threats Are Inside Your Company" https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company