SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 149

MANAGING A COMPANY'S WEBSITE IN THE FACE OF A CYBERATTACK – AN EXAMPLE OF PROACTIVE DETECTION BY GOOGLE

Artur STRZELECKI[1], Karol KRÓL[2*], Dariusz ZDONEK[3]

[1] University of Economics in Katowice, Department of Informatics; artur.strzelecki@ue.katowice.pl, ORCID: 0000-0003-3487-0971
[2] University of Agriculture in Krakow, Faculty of Environmental Engineering and Land Surveying; k.krol@onet.com.pl, ORCID: 0000-0003-0534-8471
[3] Silesian University of Technology in Gliwice, Faculty of Organization and Management; dariusz.zdonek@polsl.pl, ORCID: 0000-0002-6190-9643
* Correspondence author

Purpose: Proactive detection by Google is designed to protect users and website administrators from threats resulting from malware infections. The aim of the research is to analyse the threats resulting from the development and universality of the World Wide Web service in the world and the solutions offered by the Google consortium in the field of proactive protection of websites against cyberattacks.
Design/methodology/approach: The research covered processes informing users and website owners about the potential threat, carried out as part of proactive Google protection.
Findings: Management of a company's website in the face of a cyberattack boils down to the use of various security measures and monitoring implemented mostly by network system administrators.
Originality/value: Research has shown that the key to the security of the website is to have an up-to-date version of the content management system and continuous monitoring of the website.

Keywords: Security management, proactive protection, cyber security, search results.

Category of the paper: Research paper, case study.

1. Introduction

The World Wide Web concept was developed in response to the need for fast and automated data exchange between the academics and scientists around the globe. Its inventor is considered to be Tim Berners-Lee, a British scientist who developed a hypertext system design in 1989-1990 while working for CERN (*The European Organization for Nuclear Research*) (Benito-

Osorio et al., 2013). The first website was dedicated to the World Wide Web project and was hosted on a NeXTCube computer. On April 30, 1993, CERN made the World Wide Web available in the public domain, which contributed to the popularization of the web. The first web sites were static (Web 1.0 – the mostly read-only Web) and lacked interaction (Choudhury, 2014). Brian Merchant (2014) compared the exploration of the "early web" content to watching a classic black-and-white silent movie. Since then, the global network has grown rapidly and the Internet is now available to every second person on Earth.

The increase in the number of Internet users has resulted in a surge of content made available through the Internet. Content is published on websites and mobile applications, both by the users themselves and by the so-called content publishers. Specialised content is also available in databases, in the so-called deep web (Weimann, 2016). Content publishers operate websites that are mainly used for specific purposes, especially business.

Enterprises setting up webpages can use existing content management systems (CMS) to create and maintain websites. The most popular content management systems are created and made available under a free software license. In June 2019, around 61% of all websites worldwide were created based on a content management system, with Wordpress being the most popular among the users (W3Techs, 2019).

The great popularity of content management systems has made them the focus of attention of criminals who are looking for security gaps that are most often found in additional modules, such as graphic templates or functional add-ons. The most popular modules have many users around the world and that is why security gaps found there are often used for cyberattacks.

1.1. Purpose and goals of the research

ICT security is a complex issue involving, among others, the security of webpages which invariably fall victim to attacks from the outside. The aim of the study is to analyse the solutions offered by Google consortium in the field of proactive protection of websites against cyberattacks. The analysis covered processes informing users and website owners about the potential threat, carried out under the proactive Google protection procedures. It was assumed that proactive actions in the field of cyber security consist in Google taking over the initiative and taking responsibility for the websites presented in search results. These are preventive actions to protect users and website administrators from threats resulting from infection of websites with malicious software.

Two companies' websites classified as potentially dangerous by Google's web robots were analysed. They both were given an appropriate warning in the search results. This is particularly important in the case of sales websites as malware can lead to a significant decrease in traffic on the website, resulting in the drop or retention of sales records, i.e. an overall decrease in target conversion. Due to the reservations of the entities on which the research was conducted, the brand name and the scope of services provided by them remain undisclosed.

2. Cybernetic threats in enterprises

Cyberspace is a virtual space. This logically separated (physically non-existent) space is created by the collection of data, files, websites, applications and processes contained in data systems, which are accessed through ICT systems (Wasilewski, 2013).

The development of the Internet and online technologies has resulted in cyber criminals now having at their disposal a wide range of tools which they choose according to their objectives. Sublime techniques and advanced software to infiltrate and carry out targeted attacks are often used in cyberattacks on public administration or corporate computers. Most of cybercrime is aimed at acquiring sensitive data, with the number of attacks against mobile devices on the rise. Criminals also use the practice called *Bring Your Own Device*. However, the highest number of malware infections occurs during web browsing. Internet users are most vulnerable to attacks when they (unwittingly) use crafted websites that infect their PCs with malware. Many companies have not yet developed new, sufficiently flexible IT security procedures that would ensure their protection (Dwornik, 2013).

The weakest link in cyber-security system are, undeniably, people. Incidents compromising the security of the company are caused by the employees and typically result from the routine, recklessness, negligence, lack of understanding of technology and lack of awareness of threats (Grzybowska, 2018). Therefore, the number of targeted attacks is growing. Criminals try to break into corporate networks and government institutions most often via personalized e-mails with malware attachments sent directly to the employees (Dwornik, 2013). Research conducted in companies from various industries has shown that employees are prone to phishing passwords to company systems and are willing to make them available by e-mail (Król, 2015).

3. Examples of cyberattacks on companies

There is now a kind of organized 'hacking industry' that provides a wide range of software for theft and economic espionage. This type of software can be purchased for example in the so-called dark web (Dark Web). Experts point out that malware is most often used against companies and organizations. Cases of cyberespionage and cyberterrorism are becoming more and more common as well. An example of this was breaking into the network of the U.S. Department of Energy, or the editorial offices of popular magazines (Smaga, 2013). In 2014 alone, the economic losses resulting from cybercrime were estimated at about 52.9 billion dollars. In addition, highly damaging, targeted attacks by ransomware (data encryption), many of which were carried out by specialized and organised crime groups, are increasingly common, like in the example of an organized group called SamSam (SamSam ransomware).

In 2018 the Symantec company found evidence of 67 SamSam attacks targeting mainly US entities. The attacks generated considerable profits for the criminals, so more of them can be expected in the future (Symantec, 2019).

The number of cyberattacks keeps growing. Kaspersky Lab recorded around 758 million instances of cyberattacks worldwide in 2016. In 2018, cyberattacks using ransomware, like WannaCry and NotPetya, which temporarily paralyzed many large companies and organizations (Outpost, 2018) became very popular. According to Symantec's report (2019), the number of thefts of credit card data and other information from payment forms on e-commerce websites (formjacking) is growing. Intercepted data, e.g. on a single credit card, is then sold on illegal markets (Dark Web) (Chertoff and Simon, 2015).

In 2013, a break-in to Adobe's IT infrastructure was reported. Personal data was stolen from 2.9 million user accounts, including logins, passwords, names, credit card numbers and expiry dates. In addition, over 40GB of Adobe source code was stolen, including the entire source code of the ColdFusion product, as well as fragments of Acrobat Reader and Photoshop source code. Cyberattacks on Sony PlayStation Network were reported in April 2011. Sensitive data of tens of thousands of players leaked.

In 2017, security gaps in the data communications systems of the Marriott hotel chain were identified. Personal information of up to 300 million customers could have been seized illegally, including payment information, names, addresses, phone numbers, email addresses, passport numbers, and even Starwood Preferred Guest account details, i.e. a high-end card issued to travellers by American Express. About 500 million Yahoo! users also fell victim to a cyberattack. Users' names, dates of birth, phone numbers and passwords were stolen. Although the company assured users that their bank details were not compromised, it recommended caution (Outpost, 2018).

3.1. Cyberattacks on Polish companies

A common threat is posed by targeted phishing attacks in which the frauds pretend to be a contractor by sending a false invoice, fiscal control reminder, or a note about an alleged change of account number, whilst at the same time inducing the customer to transfer money to a false bank account (Grzybowska, 2018). Yet, however gloomy it actually is, many companies still do not see the need to take extra measures in order to protect their extensive IT infrastructure against cyberattacks. Meanwhile, the hard fact is that in 2017 about 82% of enterprises in Poland reported at least one breach of cyber security, and every fourth company observed at least 10 of them (Grzybowska, 2018). Research conducted by PwC in Poland showed that 44% of companies suffered financial losses due to cyberattacks, 62% reported disruptions and downtime, and 31% fell victim to disk encryption (ransomware). At the same time, 20% of medium- and large-size companies did not employ a cyber security specialist, and 46% of companies had no procedures to handle (cyber)incidents (PwC, 2018).

Cyberattacks are also targeted at public sector entities, including public administration units, hospitals and energy sector entities. A cyberattack on energy infrastructure may have disastrous consequences for property, health and life of employees, the natural environment, the whole economy or even the functioning of the state, as it can compromise the functioning of administration and even the military force. Research has shown that as many as 16% of cyberattacks target the energy sector, making it the second most frequently attacked sector after public administration (Ciglic, 2017).

4. Costs of cyberattacks and types of cyber crimes

Cybercrime generates measurable costs – direct, indirect, defence costs, also "hidden" costs. The traditional approach to calculating the financial impact of cyber incidents focuses mainly on the direct costs associated with the theft of personal data. While this can be helpful in certain cases, it does not take into account the increasing number and severity of incidents that do not necessarily involve the infringement of customer or employee personal files. Many security breaches involve the theft of intellectual property, disruption of operations or destruction of critical infrastructure. The focus on personal data is partly due to the availability of such data, but also due to the tendency to highlight visible and easy-to-estimate costs (Mossburg et al., 2016).

Anderson and the co-authors (2013) divided cybercrime into: (1) Traditional crimes that have now become "cybercrimes", as they are committed online (e.g. tax fraud); (2) Transitional crimes, where the way things work has changed considerably and which take place in cyberspace, e.g. credit card fraud; (3) Brand-new crimes that emerged together with the Internet; and (4) Platform crimes, such as those committed via computers infected with malware, known as botnets. According to Anderson and co-authors (2013), indirect and defence costs of cyberattacks are much higher for transitional and brand-new crimes than for other crime types due to the global nature of cybercrime.

5. Selected ways of taking control of a website

Unauthorized persons can access a site using password guessing techniques. Password guessing attacks may involve entering common passwords or random combinations of letters and numbers until the password is deciphered. Therefore, it is recommended to use different, the so-called strong passwords in different services. Unauthorized interference with the site code may also result from security gaps, particularly in outdated software. Cybercriminals

actively search for old and outdated software. Ignoring update notifications increases the risk of attack. Graphic themes and plugins can also be dangerous, although they are a valuable addition to the standard functions of a content management system. It is recommended for the users to update them and be cautious about free versions from unreliable websites, as they may contain malicious code.

An incident of cyberattack may at first look like a technological problem, but it usually goes far beyond the technology field. This is because social engineering is also used to gain illegal access to websites. This technique takes advantage of human nature to circumvent advanced security infrastructure. In such attacks, users are (deceitfully) persuaded to transfer confidential data. Google's research on social engineering shows that some of the most effective phishing campaigns are successful in as many as 45% of cases (Web, 2019).

5.1. Proactive detection by Google

Proactive (heuristic) methods of malware detection rely on automated analysis of website code and the analysis of the way in which the website "behaves". On the basis of a predefined set of rules, the algorithm of a network robot diagnoses whether a given website poses a potential threat.

Google has developed two mechanisms to inform users and website administrators about potential security threats. The first mechanism was introduced to the search engine in 2009 (Szymanski, 2009). It consists in detecting potentially dangerous websites and marking them with a notification message: *This site may harm your computer* (Fig. 1). Sites marked in this way were in fact "hacked" – which means illegal access to the website, and both the operator and the owner of the website may not even be aware of this. When a user clicks on a link to a website with a threat warning in the search results, they are not sent directly to a given site but instead to another site with a warning. It is likely that the website or web server has some security gap that was used to infect the website.

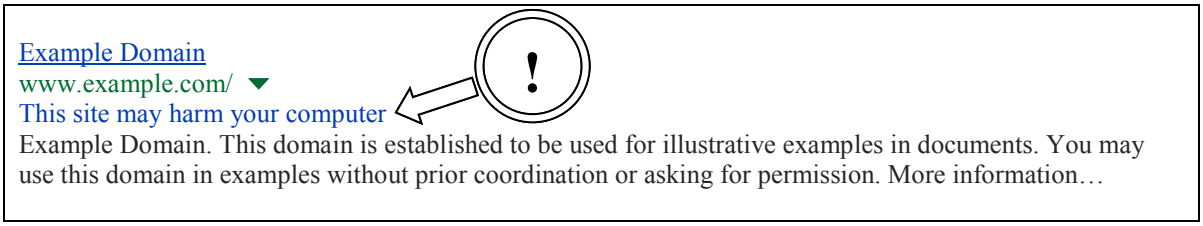

Figure 1. A message in Google's results about possible threats. Source: compiled on the basis of: (Szymanski, 2009).

Google software recognizes harmful (strange) code with the use of algorithms. If a website has a threat warning in its search results, it is very likely that it was hacked, even if it is owned by a reputable person or institution. Entering an infected site may result in running a hidden script or opening another site attempting to attack the device on which it is being viewed. The consequence of a successful attack may be the installation of malware on the recipient's

device. It can be used to steal passwords or credit card numbers; it can slow down the computer or alter search results.

The second proactive mechanism of Google is to detect potentially dangerous websites and to mark them with a message in search results: *This site may be hacked* (Fig. 2). This mechanism was introduced to the search engine in 2011 (Wald, 2011). The message is intended to alert users to websites that may have been modified by unauthorized persons, most often for criminal purposes. Clicking on the message takes the user to the content that explains the situation, while clicking on the link takes the user to the searched site.

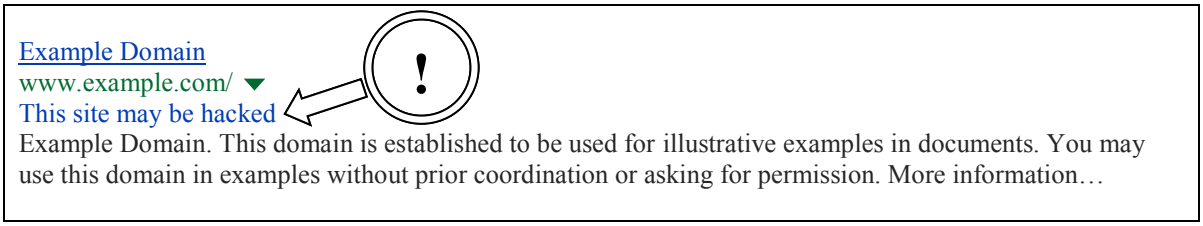

Figure 2. A warning in Google results. Source: compiled on the basis of: (Wald, 2011).

Google also uses various notifications. Warning like this one: *Visiting this site may harm your computer* appears in search results when algorithms indicate that a website may allow malware to be installed.

When Google's algorithm detects unusual or specific code sequences that are typical to malware, it publishes a warning in search results. When a communication is published, an attempt is made to contact the website operator via e-mail or Google Search Console.

6. Case studies

The websites of two companies were marked with an indication of possible threat. In the first case, the website was marked with the message *This site may be hacked*, which was confirmed after accessing the Search Console service (Fig. 3). This type of warning has a negative impact on the number of visitors directly from the search results. After accessing the Search Console service, the *Security issues* section checked the addresses of websites that may have been attacked. In this way sensitive sites were located and bugs that infected the site were removed. The content management system was updated, as were all its components. After closing the security gap and passing Google verification, the message was removed from the search results. Sometimes, however, the search results display a warning of potential threat, but there is no information about it in the Search Console panel.

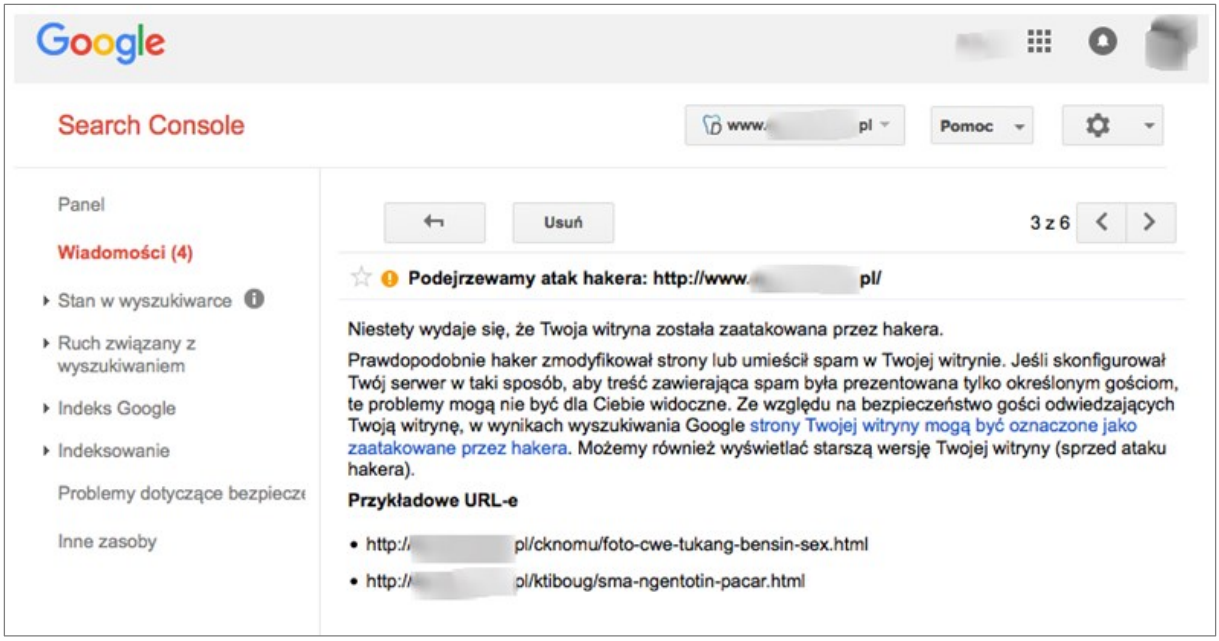

Figure 3. Proactive Google detection – Google Search Console view (screenshot). Source: Google Search Console.

In the case of the second site, a more complex attack was reported, resulting in the imposition of the so-called 'manual penalty' on the site. The website was tagged with a message: *This site may be hacked* in the search results. Some pages of the site had been attacked, resulting in spam and links to harmful content. Figure 4 shows the Google Search Console dialog box, which allows for "manual actions" in partial matching. If the user sees a penalty imposed by Google in the "Manual action" tab, they can appeal against it. To do so, an appeal with Google needs to be filed.

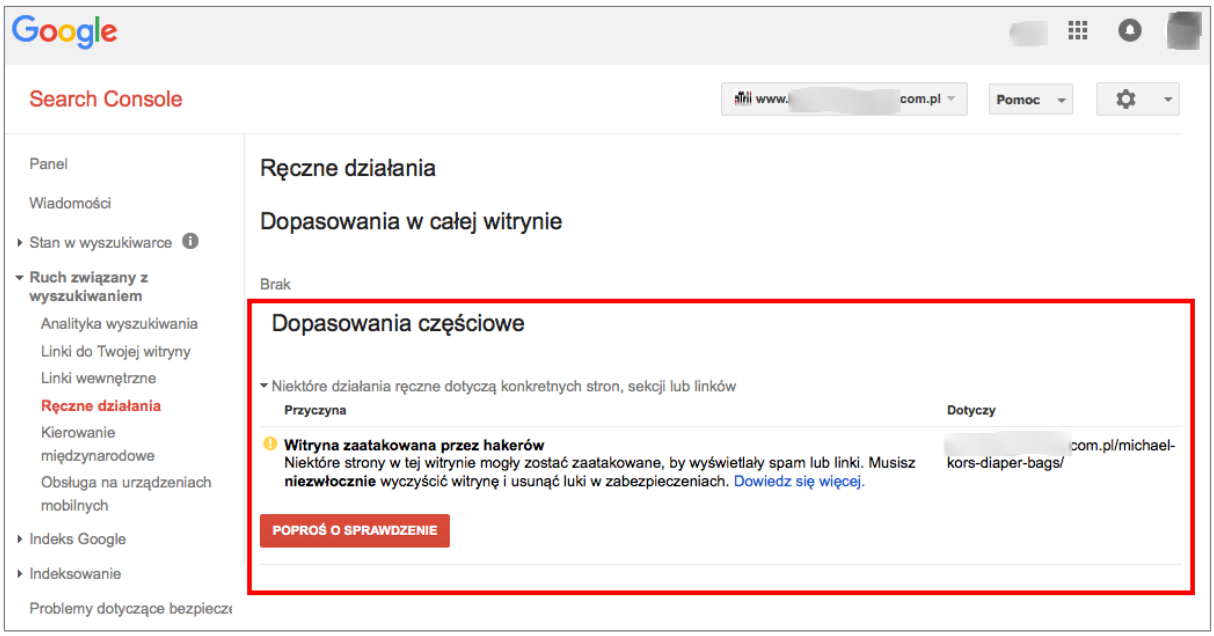

Figure 4. Corrective actions – view in Google Search Console (screenshot). Source: Google Search Console.

In order to restore the proper functioning of the website it was necessary to remove the security gap and send an electronic request to Google describing the corrective actions taken. In both cases, thanks to the quick response of the website administrator, the limitations in the availability of the websites lasted less than 24 hours.

7. Summary

As the number of websites grows, so does the number of attacks against users' security. In most cases, attacks on websites are executed in an automated way, using various scripts and programs. They scan thousands of websites whose addresses are taken from search results or public databases to find the most common security gaps. Once they are found, the sites are infected with malicious code. A large part of attacks are automated "bruteforce" type actions, which are designed to additionally burden the server infrastructure.

Management of a company's website in the face of a cyberattack boils down to the use of various security measures and monitoring implemented mostly by network system administrators. Research has shown that the key to the security of the website is to have an up-to-date version of the content management system and continuous monitoring of the website.

Over the last few years, the number of websites created on the basis of a content management system has grown dynamically. The more websites are based on widely known and accessible scripts, the more threats are bound to be created by manipulating the source code for criminal purposes. This is why it is crucial for the users to monitor their website, use a secure password and store it properly, as well as update the software on regular basis. All these precautions will optimize the overall security of the website.

References

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T., Savage, S. (2013). *Measuring the cost of cybercrime*. In: The economics of information security and privacy (pp. 265-300). Berlin-Heidelberg: Springer, https://doi.org/10.1007/978-3-642-39498-0_12.
2. Benito-Osorio, D., Peris-Ortiz, M., Armengot, C.R., Colino, A. (2013). Web 5.0: the future of emotional competences in higher education. *Global Business Perspectives, 1(3),* 274-287. https://doi.org/10.1007/s40196-013-0016-5.

3. Chertoff, M., Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance Paper Series, No. 6.*
4. Choudhury, N. (2014). World wide web and its journey from web 1.0 to web 4.0. *International Journal of Computer Science and Information Technologies, 5(6),* 8096-8100.
5. Ciglic, K., Jurczyk, M., Konkel, A., Lewandowska-Wiśniewska, I., Mikołajczyk, D., Podwiński, K., Rozenblum, L., Sordyl, J., Spychała, M., Vager, Y., Żelechowski. R. (2017). *Cyberbezpieczeństwo polskiego przemysłu*. Sektor energetyczny. Kraków: Instytut Kościuszki.
6. Dwornik, B. (2013). *Sieć pełna zagrożeń, ale które jest największe? To zależy od ciebie!* Raporty interaktywnie.com – Bezpieczeństwo w internecie, 5-15.
7. Grzybowska, K. (2018). *Cyberbezpieczeństwo. Co grozi firmom i jak duży jest to problem.* Raporty interaktywnie.com – Cyberbezpieczeństwo, 6-39.
8. Król, K. (2015). Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu. *Organizacja i Zarządzanie, 2(30),* 19-32.
9. Merchant, B. (2014). *What It Was Like to Surf the Web in 1989*. Motherboard Blog, http://bit.ly/2Wibwg1.
10. Mossburg, E., Gelinne, J., Calzada, H. (2016). *Beneath the surface of a cyberattack. A deeper look at business impacts.* Deloitte Development LLC. http://bit.ly/2KHYEZF.
11. Outpost (2018). TOP 10 of the world's largest cyberattacks. Outpost24, http://bit.ly/2X2Flkx.
12. PwC (2018). *Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście*. Badania Stanu Bezpieczeństwa Informacji. PwC Polska.
13. Smaga, M. (2013). *Internetowa grypa – nowe obszary i metody cyberprzestępców*. Raporty interaktywnie.com – Bezpieczeństwo w internecie, 32-39.
14. Symantec (2019). *Symantec 2019 Internet Security Threat Report*. Symantec Corporation.
15. Szymanski, K. (2009). *Wyniki wyszukiwania z ostrzeżeniem*, Blog Google, http://bit.ly/2Kgq1Ka.
16. W3Techs (2019). *Usage of content management systems*. W3Techs. Web Technology Surveys. Q-Success, http://bit.ly/2HOGwf6.
17. Wald, G. (2011). *Nowe powiadomienia w wynikach wyszukiwania dotyczące witryn zaatakowanych przez hakerów*, Blog Google, http://bit.ly/30WGVTX.
18. Wasilewski, J. (2013). Zarys definicji cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego, 5(9),* 225-234.
19. Web (2019). *Top ways websites get hacked by spammers*. Web Fundamentals. Google Developers, http://bit.ly/2XGzMW2.
20. Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism, 39(3),* 195-206. https://doi.org/10.1080/1057610X.2015.1119546.