VOLUME 4 (2018) ▪ ISSUE 3

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments.

ISSN: 2450-21113

The ECJ is a quarterly journal, published in January, April, July and October.

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows:
"European Cybersecurity Journal",
Volume 4 (2018), Issue 3, page reference

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

www.ik.org.pl
www.cybersecforum.eu

Printed in Poland

OPINION

CAN A PUBLIC TENDER BE A THREAT TO IT INFRASTRUCTURES IN PUBLIC INSTITUTIONS?

PAWEŁ SAWICKI

is an expert in criminal cases involving IP rights and cybersecurity and has extensive experience in the prosecution of cybercrime. He has been appointed as anti-piracy counsel for the world's leading software producers (Microsoft, Autodesk and Adobe) and leads the criminal enforcement programme for BSA | The Software Alliance in Poland. He has represented clients from IT software and chemicals sectors before the authorities and courts in connection with violations of intellectual and industrial property rights; he has also assisted many clients in relation to internal investigations.

Paweł is a member of the Association of Certified Fraud Examiners (ACFE).

First, let your imagination run free.

Let's imagine that an intelligence agency of a foreign country wants to access personal computers of all Polish deputies and senators. And I do not mean the physical seizing of their computers, but undetected ongoing access to everything what is done on them. It would make it possible to trace the planning process for the legislative acts before they even go public or imperceptibly change a few words in them, why not? It would make it possible to get access to private conversations about what exactly the opposing parties think about the governing party and vice versa. It would enable them to search for proof of unethical behaviour or provoke one, or even place compromising materials and incite an international scandal. With unfettered access to somebody's computer, the only limitation is our imagination. Tempting? Unreal? Mission impossible? Because no one can install spyware on a deputy's computer, right?

If not the computers of the deputies and senators, then maybe somebody would be interested in hacking the database of the Polish Social Insurance Institution (ZUS) and stealing personal information of millions of Poles? How much would the data be worth on the black market? Let's try to assess that. On the Internet, the price for a regular database starts from PLN 0.10 for a record. The data available in ZUS are inevitably more valuable and thus worth at least PLN 1.00 for a record. It can be easily assessed that even a small data leakage – let's say of 2 million records – would be worth around several tens of millions Polish zloty on the black market, not to mention that such a database could be sold more than once.

In August 2016, there was an incident described initially as 'a leakage from the PESEL database'. PESEL means Universal Electronic System for Registration of the Population; it is a massive central database, currently managed by the minister in charge of computerisation. This register stores identities of all Polish citizens and foreigners residing in Poland. They are extremely sensitive and therefore access to the data is very restricted. The PESEL system is mainly used by the authorities responsible for the safety of the country: the police, the Internal Security Agency, the Central Anti-corruption Bureau, the Public Prosecutor's Offices, courts, but also tax offices and bailiffs. The latter were initially to be blame for the 'data leakage'. On 12 August 2016, the Ministry of Digital Affairs informed the law enforcement agencies about an extremely atypical behaviour of the entities which collect data from the PESEL database. In a relatively short period of time, at night, the ministry's servers received hundreds of thousands of requests, and data of more than 1.4 million people were downloaded. At first, it might have looked like a cyberattack. However, after the investigation by the Public Prosecutor's Office in Warsaw, it turned out that it was not a cyberattack, but an uncommon hyperactivity of bailiffs' offices. It seems that the data did not fall into unauthorised hands after all.

However, the case re-emerged after two years. In July 2018, the public learned that a private company GetBack S.A., until a recent big financial scandal one of the most rapidly growing entities in the debt collection sector, also had access to the PESEL database. The company had issued bonds for the total value of PLN 2.5 billion and was unable to redeem them. The management of the company was temporarily arrested. In 2015, the Ministry of Internal Affairs, which was responsible for managing the PESEL database at that time, set the precedent by granting consent to Kancelaria Prawna GetBack, which was related to GetBack S.A., to share address details from the PESEL register by using data telecommunication devices through verification. It was the first time in history when a private debt collection company had gained access to this database. Clearly, a completely unreliable entity was given an unusually high level of trust. In this situation, the question that arises is: who verifies the credibility and reliability of the entities that are given such extensive rights?

This example shows very clearly how valuable the data are of which public institutions keep custody of.

Databases collected by public institutions contain unique information about each of us and therefore there are many people who would like to acquire it.

The public sector in Poland includes a huge number of institutions, public offices and therefore – computers. It is enough to point out that every fifth Pole works in the public sector. Public administration, offices, uniformed services, health care institutions, and cultural institutions constitute thousands of entities, each of which uses IT technology. Regardless of whether it is a small school or the National Bank of Poland, they all create and collect massive amounts of data. Databases collected by public institutions contain unique information about each of us and therefore there are many people who would like to acquire it.

The public sector is one of the major investors when it comes to IT. Public institutions spend a considerable amount of public funds on technology and their expenses continue to rise. For instance, the public tenders for the supply of IT services announced and won in 2016 amount to PLN 4 billion. The amount increased to PLN 5.1 billion in 2017. New investments are driven by the EU funds, and the purchases are made by small offices as well as big ministries with thousands of computers in their infrastructure. Computerisation is required because of the changes in legislation, such as the GDPR which sets high standards regarding personal data protection safeguards and demands improvements in IT security.

Despite growing investments, the public sector is identified as the most threatened by cyberattacks. It seems obvious, taking into account the fact it has the information cybercriminals are looking for. In August 2014, a DDoS attack paralysed the websites of the Chancellery of the President and the Warsaw Stock Exchange. In November 2014, the IT systems of the Polish National Electoral Commission were attacked and as a result employee data were stolen. In February 2017, the website of the Polish Financial Supervision Authority was blocked, presumably by North Korean hackers whose aim was to target the

whole banking sector in Poland. Finally, in June 2018, numerous governmental IT systems, including CEPiK (Central Register of Vehicles and Drivers) or ePUAP (Electronic Platform of Public Administration Services) stopped working, most likely as a consequence of multiple DDoS attacks.

These are just a few examples of successful attacks. The ones that failed have never gained public attention. If we consider that each day in Poland there are 100,000 attempts of cyberattacks, we can be sure that sooner or later we will witness at least one successful and spectacular attack on an unprecedented scale.

Let's go back to the 'fantasy scenario'. Suppose that someone would like to keep track of cyber activity of Polish parliamentarians and have access to their IT resources. How can one accomplish that? To begin with, such a person should start a limited liability company (Sp. z o. o.) selling computers and other IT equipment and software. Then, the company should participate in a public tender for the supply of computers and software announced by the Sejm Chancellery. It should not be a problem to win the bidding since in the Polish reality of public tenders it would be sufficient to offer the lowest price. Next step would be to buy computers from a computer hardware reseller and install spyware with a cleverly disguised computer virus.

The last thing would be to deliver the computers to the contractor and wait until they connect to the IT infrastructure of the Sejm. It seems to be very easy but also extremely unreal. After all, the plan could never be successful because the attempt would undoubtedly be detected by the respective services. It appears, however, that it is not necessarily correct.

In April 2016, under the public service contract, the Sejm Chancellery received 15 personal computers with office software. The hardware was collected and was ready to be handed over for use. Unfortunately, it turned out that there was a problem activating office programs – the activation keys delivered by the supplier did not work and therefore the installation process and activation of the office programs could not be completed. Apart from that, everything seemed to be in order. The computers operated perfectly, the operating system worked as it should. The employees of the Sejm Chancellery asked the software manufacturer for support in establishing the sources of the problem with activation. It turned out that the provided keys were blocked because they had been abused – the keys had been previously used multiple times. Further explanatory proceedings led to the finding that illegal copies of a popular computer system had been installed on the delivered computers with affixed counterfeit certificates of authenticity.

If we consider that each day in Poland there are 100,000 attempts of cyberattacks, we can be sure that sooner or later we will witness at least one successful and spectacular attack on an unprecedented scale.

The fraud scheme was very simple: a small company, without a physical office, infrastructure, a warehouse or employees, was buying PCs of well-known brands. The computers either had already been equipped by the manufacturer with a free operating system or did not have an operating system at all. The ordering party demanded computers with a leading commercial operating system that required a fee-based license. The company which won the tender installed the commercial operating system on its own. In order to increase its credibility and make the illicit activity appear legal, the company affixed counterfeit labels imitating the certificates of authenticity purporting to originate from the leading manufacturer of the computer programs. The computers operated properly; however, the operating system on the equipment was unauthorised. In that way, the company could save approx. PLN 400 – 500 on one computer. It was sufficient to be competitive.

At some point, the scale of the phenomenon increased to the extent that the same companies – previously not recognised in the market – started winning the majority of the tenders. These companies began eliminating companies which had been associated with the IT services for the public sector for many years. In some cases, these well-known companies also started to look for 'alternative' solutions to lower the costs of the offered equipment.

Therefore, since it was possible to install a 'pirated copy' of the software and deliver such computers to a public institution, what could preclude someone from installing on computers other 'extra' programs with various specifications?

The Sejm Chancellery organised a tender, chose an offer, collected their order and used computers with illegal copies of the operating system. Imagine the consequences the incident would have had if the computers had been integrated into an internal infrastructure of an institution and had had additionally installed spyware or other custom-written viruses?

The moment the fraud was revealed (let me remind you that it could have not been discovered at all if the activation keys to other programs had worked or the ordering party had requested computers with the operating system only), the investigation proceedings conducted by the police and the Public Prosecutor's Office were initiated. It turned out that the scale of this type of offences is enormous, with dozens of public institutions becoming unaware victims of fraudulent suppliers of IT products.

It is worth noting that the first revealed and defeated attempt to deliver personal computers with illegal copies of the operating system took place in a big tender organised by... the Polish Police Headquarters in 2015. Obviously, it was not the first tender in which the fraudulent practice had occurred; however, it was the first time when the law enforcement agencies had realised its extent. The fact that unfair tenderers decided to supply the police with illegal software demonstrates their certainty of their impunity. Thus, the conclusion is they must have successfully conducted similar deliveries in the past. In this case, this happens to be true.

It turned out that the scale of this type of offences is enormous, with dozens of public institutions becoming unaware victims of fraudulent suppliers of IT products.

In November 2015, after disclosing a number of attempts (failed and successful) to deliver computers with illegal copies to several ministries, the Public Procurement Office published on its website a letter to the President of Lewiatan – the Polish Confederation of Private Employers in the Digital Technology Industry (Polski Związek Pracodawców Technologii Cyfrowych Lewiatan) regarding the identified risks related to offering unlicensed software in public procurement procedures. The letter pointed out for the first time the scale of the problem and drew attention to the way the perpetrators act and how to avoid similar events.[1]

However, back then, the problem failed to raise any greater awareness.

On 13 January, 2017, the Ministry of Family, Labour and Social Policy published an official statement on its

1 The text of the letter was published on the website: https://www.uzp.gov.pl/__data/assets/pdf_file/0007/31012/Nielegalne_oprogramowanie_w_zamowieniach_publicznych.pdf

website as a response to the then current press reports. The statement confirmed that in May 2015, the Ministry of Labour and Social Policy purchased computers with illegal software. The computers were purchased by the office to carry out tasks arising from the Act on the Big Family Card. The number of computers was 2,500 and the value of the tender was estimated at PLN 10.5 million. The computers were delivered to the municipalities throughout the country.

In March 2018, the Central Anti-Corruption Bureau informed about the arrests of owners of the companies that participated in tenders for the supply of IT equipment and delivered computers with 'pirated' software. At that time, the law enforcement agencies had evidence which confirmed that unlicensed software was found on 3,256 computer units worth PLN 9.5 million that had been delivered to public institutions throughout the country. Among the affected institutions were the Sejm Chancellery, the Office of the Marshal of Warmińsko-Mazurskie Voivodeship in Olsztyn, the City Halls of Poznań, Radom, Kraków and Tychy, and a university. This fraud scheme took place between 2012 and 2016.

What is the real scale of the problem? Nobody knows. The law enforcement agencies are tracking the sources and find computers which were bought by public institutions years ago and which have functioned within the infrastructure of a given institution until now. Many entities are surprised when they discover anomalies; in their view, if everything is in order because, i.e. their computers work as they should and there are no problems with the equipment or software functionality, they do not have reasons to think otherwise. On the other hand, it sometimes happens that an institution discovers anomalies years after the purchase. They usually find out something is wrong when they need to reinstall the software and use the activation key again. It turns out that the activation is not successful because the key was blocked due to a multiple abuse of the key by other users who received exactly the same activation key.

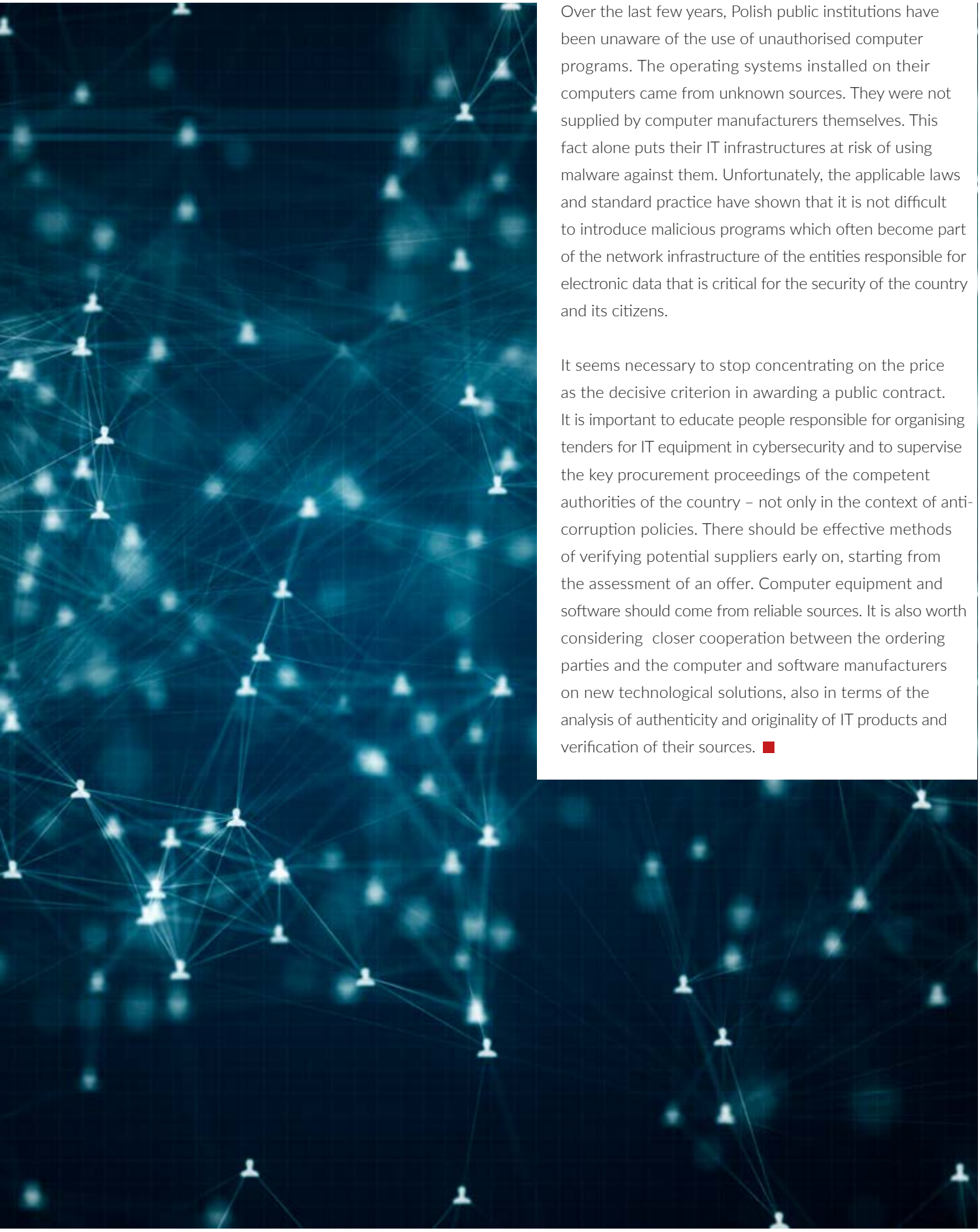
It is a well-known fact that public tenders are exposed to great risk, both actual and legal. The problems arise already at the stage of preparing the specifications and the terms and conditions of the tender where potential modifications of the conditions with regard to the service may affect the result of the tender, i.e. the selection of the tenderer. It is potentially a fertile ground for any corrupt activities.

The fact that persons who perform public procurement proceedings lack specialisation constitutes another problem. It often happens that within one institution there is only one person who is responsible for the purchase of cleaning products and IT technology. It is impossible to possess expert knowledge in every field. Obviously, the persons are supported by individual departments for which the purchase is made. However, in some situations, it is not sufficient. No officials in a small municipality can be blamed for not having sufficient expertise in recognising counterfeit certificate of authenticity for a computer program.

And finally, we come to the most important issue. Since the price is practically the only criterion that determines who wins the bid, it is very common that the awarding process is done at the expense of the quality of products or services. It can be seen in almost every sector: from stationery supplies to construction works.

Since the price is practically the only criterion that determines who wins the bid, it is very common that the awarding process is done at the expense of the quality of products or services.

In some of the above-mentioned tenders for the supply of computers with software, as a result of which unauthorised copies of software were delivered, there were only two criteria that were taken into account when selecting the offer: the price and the warranty period. The price has always represented over 90% of the total points in the offer evaluation criteria. In practice, the company which gives the lowest price usually wins the tender. Neither the quality of the equipment nor the credibility of the supplier is significant. In those particular tenders, the ordering party did not verify or assess the tenderers. It was of no significance whether the supplier enjoyed a good reputation and had a track record as a supplier in the IT market or, by contrast, was a rather unknown company with a minimum share capital and a virtual office. As a consequence, the equipment delivered to the institutions did not only have unauthorised software installed (which constituted a risk in itself) and it was either defective and of poor quality, or previously used and refurbished.



Over the last few years, Polish public institutions have been unaware of the use of unauthorised computer programs. The operating systems installed on their computers came from unknown sources. They were not supplied by computer manufacturers themselves. This fact alone puts their IT infrastructures at risk of using malware against them. Unfortunately, the applicable laws and standard practice have shown that it is not difficult to introduce malicious programs which often become part of the network infrastructure of the entities responsible for electronic data that is critical for the security of the country and its citizens.

It seems necessary to stop concentrating on the price as the decisive criterion in awarding a public contract. It is important to educate people responsible for organising tenders for IT equipment in cybersecurity and to supervise the key procurement proceedings of the competent authorities of the country – not only in the context of anti-corruption policies. There should be effective methods of verifying potential suppliers early on, starting from the assessment of an offer. Computer equipment and software should come from reliable sources. It is also worth considering closer cooperation between the ordering parties and the computer and software manufacturers on new technological solutions, also in terms of the analysis of authenticity and originality of IT products and verification of their sources. ■