BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
No. 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-002
Received: 20.06.2023
Accepted: 21.09.2023

Mirosław Laszczak
PhD, University of Economics and Humanities in Bielsko-Biała
https://orcid.org/0000-0001-6060-4285

A critical link in the cybersecurity system

Introduction

Cybersecurity is a huge business, and at the same time one of the biggest challenges of our time. Any negligence in this area limits the economic development of companies, states and societies. According to forecasts, the annual costs associated with cybercrime will grow at a rate of 15% and reach the value of USD 10 trillion in 2025. 85% of small and medium-sized enterprises, especially in recent years, have taken the issue of digital security seriously, admitting that they stop saving on digital security and increase spending on IT network protection from year to year.[1]

Data theft and information leakage are a fact. And although blame is usually seen on the side of program weakness, in reality the weakest, and at the same time the key component of security is always the human being.

There is a popular saying that a safe computer is a turned off computer. But that's only partially true. The art of extracting information is also the ability to persuade someone to go to the office, turn the device on to the network and transfer the information.[2] Socio-technical tricks, manipulation, knowledge of the psyche turn out to be effective tools for obtaining classified material. Hackers and spies are already favored by the process of upbringing, which values such features as trust, empathy and

[1] *Cybersecurity trends: Looking over the horizon*, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon#/ [accessed: 23.05.2023].

[2] K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, transl. by J. Dobrzański, Helion, Gliwice 2003, p. 19.

willingness to help. Hence, it is only a step to not deal with pushy requests or the inability to recognize signs of fraud. Computer scientists who perform penetration tests on behalf of companies reveal that hacking into security systems using social engineering tricks is almost one hundred percent effective.[3] Some character and personality dysfunctions push employees to commit crimes and reveal secrets.

The purpose of this article is to indicate which personality traits or which characterological dysfunctions are responsible for an employee's predilection to disclose secret data. What makes it so that, despite excellent security measures, phishing and leakage of important files still take place. In turn, the hypothesis that this text undertakes to verify is the conviction that the weakest, yet most important link in the cyber security system is the human being. At the same time, the article points to the development of security features and discusses how attempts are made to make it more difficult to conduct criminal activities inside an organization.

The study is based on an analytical and diagnostic approach. The primary research method to achieve the stated objectives is the method of analysis and critique of the literature on the subject and the analysis of review papers describing security breaches in cyberspace when the source of these breaches is the exploitation of human personality vulnerabilities.

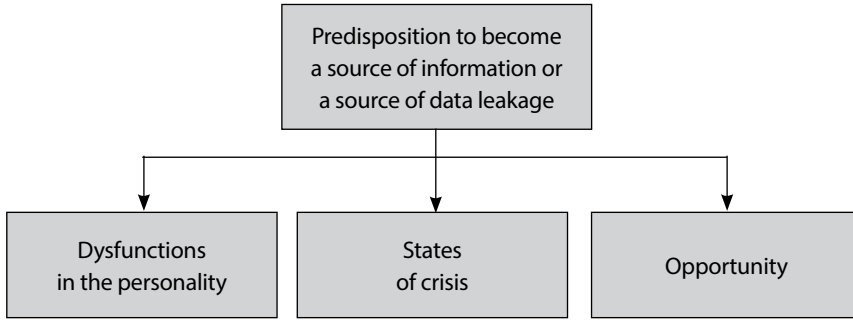
Whistleblower or traitor

Handling important and classified material is intriguing: it is combined with the illusion of being an insider, there is an impression of greater self-worth, one has access to knowledge that is guarded and therefore valuable, which in itself forces caution and self-control. Such people find themselves targeted by the intelligence services and are persuaded to cooperate in various ways. This is not always successful. A sense of patriotism, high morale, reluctance to get involved in dangerous situations, and fear of punishment stand in the way. At the same time, the inspiration to commit a crime turns out to be: the desire for excitement, the desire to experience adventure or the way to earn money. Bored with their previous jobs, the officials get involved in risky arrangements in which the stakes are really high. For some, maintaining a dual identity is an interesting and welcome adventure, for others it is exhausting and beyond stressful. There are prerequisites to help pick out the right person and make them a source of information.

In order to obtain a whistleblower and make him/her own agent, there should be special circumstances, namely with a deficit of responsibility, the encouragement for betrayal could be the experienced state of solstice in personal and professional life, and also a chance for high earnings or hope for global publicity and fame (Figure 1).

[3] *Ibidem*, p. 267.

Figure 1. Basic factors for involvement in espionage activities



Source: Author's own elaboration based on: U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 20.

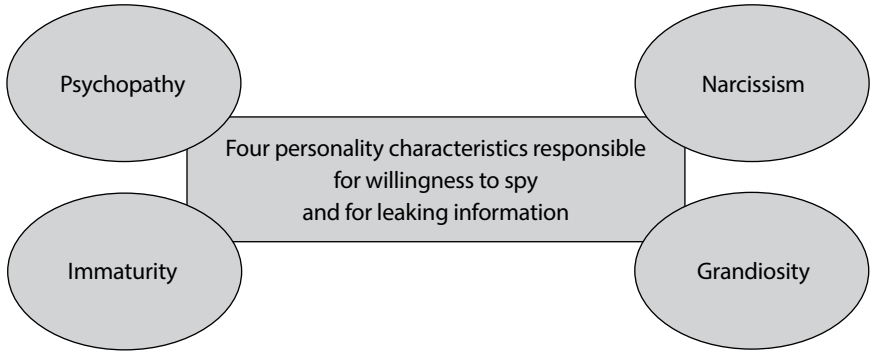
The dysfunctional personality takes many forms. Spies usually become thrill-seekers, struggling to hide their desire for power and seeking to take control of their surroundings. They are largely selfish, sometimes betraying a mania for greatness, in other cases trying to compensate for their own problems by taking revenge on the whole world.[4]

The domino principle works here: people with a dysfunctional personality fall into a state of crisis, look for a way out in activities associated with a higher risk and offering an effective escape from everyday troubles. Some emotions are covered by others, more expressive, stronger. Hence only a step to trading secrets; sometimes without thinking, sometimes out of desperation, which distorts the vision of the world and changes the understanding of the word "reason", sometimes in search of a particular thrill of emotions. Intelligence services are well aware of this, so they often initiate crisis situations themselves; there are no shortages of ways, it is enough to escalate debts, get involved in a risky sexual relationship or in a romantic relationship with a person controlled by the services. It is difficult to get out of such a system, and in addition, crises can easily be exacerbated, introducing an additional element of risk and exacerbating the state of mental enslavement.

There are at least four types of dysfunctional personality that are conducive to engaging in the activity of revealing secrets (Figure 2). Of course, it is impossible to say which of these personalities is most susceptible to being recruited by competing intelligence forces, but enumeration always begins with the psychopathic personality.

[4] U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 20.

Figure 2. The four personality components that lead people to steal information and espionage



Source: Author's own elaboration based on: U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 20–28.

Psychopaths by nature are predators forever chasing risks. They are strangers to remorse, and experience limited feelings of guilt, shame, or regret. They easily mislead others. At first contact, they make a good impression. They at the beginning easy make friends, create an atmosphere of honest conversation, and slowly take control of the other person. At the same time, they are born liars who take pleasure in cheating and seizing power over others.[5] Enchanted by their pretended kindness, their superiors allow them to do more and more. Their power expands, their subordinates fear them, and their co-workers see merciless persecutors who, without hesitation, will use every means at their disposal to take revenge for their superiority.

Seeing how easy it is for them to take control of others, they want more and more until they overdo it. Mainly because they don't learn from their mistakes, can't plan for the long term, don't understand other people. Immersed in the present, they seek short-term excitement.

Psychopaths are not the only group of potential intelligence sources. Equally good sources of intelligence are narcissistic personalities, i.e., employees convinced of their uniqueness, who see themselves almost as organizational superstars that no one appreciates. So they fantasize about themselves and look for people who would attest to their uniqueness.

Skills, charisma, beauty, wisdom, prospects for the future – these features make up the inner image of a narcissistic person, it is enough that they find someone who will convince them that they are exactly like that, and they will be happy to share their opinion about co-workers and the uniqueness of the work they do. When a co-worker does not share their opinion, narcissists become malicious and vindictive. The possibilities of taking revenge on the organization, on superiors, even on the whole country

[5] J. Gibas, *Psychopata w pracy, w rodzinie i wśród znajomych*, Helion, Gliwice 2021, pp. 41–42.

are found primarily in the network.[6] Access to important information builds in them a conviction of superiority over others, which is dangerous insofar as they, sometimes experiencing Promethean illusions, want to save the world, to introduce a new fantastic order. It is among them that the sources of information leaks are recruited. All it takes is for top-secret documents to be made available online, secret services to be disseminated, governments will be shaken, international relations will crumble and the heads of superiors who failed to see to their duties will be sprinkled. They, in turn, will quickly find supporters shouting paeans to their courage, praising their uncompromisingness and affirming any uniqueness they can think of. Those eager for affirmation become easy objects to be controlled by the services and by all those whose approval and admiration they seek.

In the case of the April 2023 leak of classified documents, the reason was to impress members of an online OG group that publishes confidential documents. While Snowden was a Russian agent, here vanity came into play. "I had the impression that I was at the top of Mount Everest. I was special person and above everyone else. [...] I knew things that others had no idea about" – said one of the members of the group responsible for the data leak.[7]

The third group of people used in intelligence activities are people with immature personalities, treating the world as a great sandbox, life for them is the accumulation of adventures. They don't take their responsibilities seriously. They treat the entrusted secrets as toys that shine in front of the other participants of the game. Immaturity manifests itself in the inability to reliably assess the consequences of actions. They want to have fun and have an adventure, to see what it's like, regardless of the fact that the fun of being a spy is like riding on a slide. With each second you gain speed and even if you initially considered resignation, it turns out quite quickly that it is impossible to leave the game. People with an immature personality do not cope with difficult situations, difficulties at work, disagreements in personal life are enough to start looking for new activities, most often marked by an emotion similar to that remembered from the preschool game of policemen and thieves. Rapid boredom with routine work, leads to the search for stimulation and at the end lead to betrayal of secrets. Thanks to this, they are again in the center of attention, like a child who needs attention from adults.

Perhaps the most characteristic feature of the immature personality in adults is excessive fantasy, it seems to them that the world is to fulfill their desires.

The fourth group includes people with grandiosity, men with exaggerated ego. Having access to kept secrets, they gain the power to influence the future of their own organization, sometimes of the entire country, which gives them a sense of importance, which – it happens – they want to verify. When looking for a way to be at

---

6 U.M. Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, *op. cit.*, s. 4.

7 M. Budzisz, *Wyciek tajnych dokumentów*, „Sieci" 2023, nr 16, pp. 45–47.

the center of events, they agree to break the law and share information they have access to.[8]

Internet – tool and tube

Cyberspace is an environment in which people with low self-esteem, low morale or poorly tolerating crisis situations feel especially good. Here they fall into uncontrollable gambling, break away from everyday affairs, play computer games, find an outlet for their addictions or compulsions. It is not for nothing that we talk about a global network, because it is actually a network into which psychologically sensitive and weaker individuals fall like insects into a trap set by a spider.

The Internet additionally suggests how to anonymously cause a data leak, it also promises to publicize the crime, global dissemination of stolen secrets and promises fame. Information that goes to the Internet is immediately reproduced and sent to other Internet users. The more sensational, the more legally protected information in them, the greater the chance that the stollen dates will gain a wider reach.

A study conducted in Canada found that online trolls are "prototype daily sadists" and there is a connection between "trolling" and those what psychologists call a "dark tetrad" of personality traits: narcissism, a tendency to manipulate others, psychopathy, and sadism.[9]

In assessing attitudes, the researchers used a Likert scale, allowing respondents to mark answers along the lines of: "The more beautiful and pure a thing is, the more satisfying it is to corrupt it," and "Hurting people is exciting".[10]

It is worth noting, however, that not all trolls are pathological characters, only some part shows signs of pathology and sadism,[11] most are ordinary people giving vent to anger, their daily frustrations and jealousies. The Internet additionally provides arguments convincing that betrayal or data leakage is no great wickedness. After all, one need only visit the Dark Web to see things far worse and more horrific. In view of the violations of decency on the Dark Web – data theft seem to be a trivial crime.[12]

---

8 U.M. Wilder, *The Psychology of Espionage*, *op. cit.*, p. 28.

9 Eadem, *The Psychology of Espionage and Leaking in the Digital Age*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 4.

10 C. Mooney, *Internet Trolls Really Are Horrible People: Narcissistic, Machiavellian, psychopathic, and sadistic*, Slate, 14.02.2014, http://www.slate.com/articles/health_and_science/climate_desk/2014/02/internet_troll_personality_study_machiavellianism_narcissism_psychopathy.html [accessed: 20.05.2023].

11 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, transl. by S. Baranowski, Vis-á-vis Etiuda, Kraków 2019, p. 212.

12 K. Finklea, *Dark Web*, Congressional Research Service Report R44101, 10.03.2017, National Security Archive, https://nsarchive.gwu.edu/media/22737/ocr [accessed: 26.05.2023].

Growing danger

The development of IT networks takes place in a geometric progression. In highly developed countries, employees work on-line three to five days a week. They are relentlessly downloading information and uploading new information. It is assumed that the hosting industry will grow from $108.54 billion in 2023 to nearly $400 billion in 2030,[13] and there are perhaps no other industry that will grow at such a rate. Online service networks are expanding and the types of online activity and mobile platforms are multiplying. Demand for wider and more convenient access to online resources is emerging, while at the same time confidential data sets are swelling and natural security gaps are appearing. In 2020, each person generated an average of 1.7 megabytes of data per second.[14] All this information was aggregated, analyzed, passed through various filters, and then synthesized into conclusions of interest to everyone from large corporations to government agencies and foreign intelligence, to commercial organizations and small businesses. A hacker is no longer an introverted computer science student struggling with existential problems. Cybercrime is a multi-billion-dollar industry, with an elaborate organizational structure and massive research and development budgets. The attack cycle: from reconnaissance to data extraction is accelerating, no longer measured in weeks, but in days or even hours. The number of ransomware attacks doubles every year, starting in 2019. Phishing attacks saw an increase of 510% from January to February 2020.[15]

These numbers alone make it clear how much the information stored in the cloud is at risk. This is partly because risk management in the digital space has not kept pace with the multitude of transactions taking place. It is also not very clear what standard of protection should be set for data protection, so as not to block some services on the one hand, and on the other not to expose them to criminal activity. It is a constant maneuvering between the Scylla of convenience and the Charybdis of caution.

When constructing security, newer and newer technological solutions are used. Integrated programs to fight Internet espionage are being created, which combine artificial intelligence and machine learning. However, they also do not guarantee that human error will be noticed or predicted and that it will preventively block access to important data in time.

That is why multi-layer security is emerging (Figure 3).

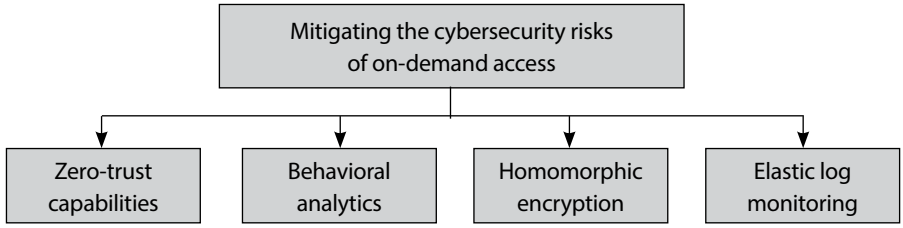
---

[13] *Web Hosting Services Market Size, Share, Growth Report, 2030*, https://www.fortunebusinessinsights.com/industry-reports/web-hosting-services-market-100863 [accessed: 26.05.2023].

[14] *Data Takes a Quantum Leap*, https://quantium.com/wp-content/uploads/2016/08/BFM_Quantium.pdf [accessed: 26.05.2023].

[15] *Cybersecurity trends: Looking over the horizon*, *op. cit.*

Figure 3. Contemporary trends of mitigating the cybersecurity risks



Source: Author's own elaboration based on *Cybersecurity trends: Looking over the horizon*, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon# [accessed: 23.05.2023].

At the forefront is the principle of zero trust. Access to confidential data must be particularly strictly protected, and since it is well known how eager employees are to share confidential data with others, behavioural analysis is another layer of security, aimed at identifying and 'screening' employee behaviour. Each access request, the state and type of devices used are assessed for possible crime and, in the case of suspicious movements on the network or unusual forms of behaviour, deviating from the habits of a person using IT resources on a daily basis, access protection tools prevent such a person from logging in and enforce new authorisation methods.

Another form of security is login monitoring based on several open-source platforms. Each connection is analysed in real time, thus identifying potential threats.

Finally, homomorphic encryption comes to the rescue. With this technology, users can work with encrypted data without decrypting it first. In this way, strict data privacy requirements can be maintained and the significant increase in computing power allows this form of security to be used more widely.

Machine learning technologies, in conjunction with artificial intelligence, can further identify extraneous patterns and the impact of incompatible systems. They can automatically patch the holes in the system and detect an attack. It is just that cyber security services cannot keep up with the creativity of hackers. Even the best-organised and most secure system will not be able to withstand the bad will of a person who suddenly wants to make amends for imaginary grievances or who, with a Herostrates complex, longs for fame. Then the system's safeguards won't even have a chance to work and data leakage will become a reality.

Control

The fact that a person has become the source of a leak, and that after all it was easy to foresee, is usually known after the incident. However, the possibility of singling out a potentially dangerous person is no so difficult as earlier. In organisations

handling confidential data, there is continuous monitoring of employees. Machine learning and cognitive programmes conduct continuous digital surveillance. Network users are assessed, their personality is profiled and future activity is predicted based on current behaviour. Anything can be important, which is why cognitive technologies analyse the footprints, which are used to refer to as digital exhaust, i.e. the digital fumes left by employees during normal on- and off-duty activities. This huge body of information is analysed first by artificial intelligence and then by the organisation's safety officers. Of course, therein lies the danger of intruding into the intimate sphere of the lives of those being observed, but this is the price that is paid for protecting confidential and valuable information. There are other disadvantages of this type of employee surveillance.

Working in an atmosphere of constant suspicion, the awareness that one is being observed, and on different levels: from the general to the very intimate, affect the atmosphere at work. This manifests itself in employee behaviour such as:[16]

- resentment towards the employer and implicit contestation of work,
- deterioration of morale among employees,
- reduced productivity,
- erosion of loyalty to the organisation,
- and last but not the east the undermining of creativity cannot be forgotten either.

Constant supervision is always a burden. It becomes a clear signal sent in the direction of the employees, informing them of limited trust. For some, suspicion and scrutiny is an understandable part of the organisational culture, typical when dealing with valuable information, but for others, it is something unbearable that hinders the performance of professional duties. In the first instance, it discourages creative individuals – who usually have a strong need for autonomy – from continuing to work and staying with the company. The most prominent ones leave, leaving the teams they previously worked in without substantive support and without interesting ideas.

And what after a data leak?

Just as the weak part of security is the human being, with all character weaknesses and biases, so too he is the strong part of dealing with crisis situations after a data leak. What counts above all is creativity, which no artificial intelligence can currently afford.

The modus operandi does not resemble typical crisis management – no apologies, no abasing in front of the media and explaining everything to the public. Instead, a game resembling a hare and hounds in the house of mirrors begins. There are contradictory reports in the media and on the web, either that the leak was

[16] U.M. Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, *op. cit.*, s. 9.

controlled, or that the information leaked is false and intended to mislead or target the hacker network, or that only what was supposed to see the light of day was leaked and instead much more valuable information was obtained. In addition, explanations and contradictory suggestions come from a variety of sources, most often unrelated to the site of the data leak. The public is misled and conspiracy theories are circulated by the mass media and coloured by social media.

This is well illustrated by the case of the leaked US intelligence documents, which became notorious after April 6th 2023. First, it was reported that the documents had previously been altered and differed from the originals. In the United States, serious losses of the secret service were written about, while on Russian news platforms the view was propagated that the whole leak was an intelligence operation prepared in fine detail and planned.[17]

Hair of the dog that bit you. Once a leak becomes a fact, the Internet proves to be a convenient tool for diluting the importance of the information revealed. Two patterns in particular prove helpful. The first is that anger is the emotion that travels fastest and reaches furthest on the web;[18] the second is that made-up stories spread six times faster on the internet than real ones.[19] Thus, an emotionally wrapped lie with the presentation of a new narrative is likely to re-format the thinking of Internet users. All the more so because anger is exciting and addictive at the same time.[20]

Along with disinformation activities, the source of the leak is identified and forms of security are modified. Additional knowledge about the characteristics and behaviour of those responsible for the disclosure of data is emerging, new safeguards are arriving, including methods of behavioural analysis to more effectively identify the personality traits of the perpetrator of the leak. Only that all these activities resemble a cat-and-mouse game and seem to have no end.

Conclusions

The risks associated with the disclosure of confidential and classified information are increasing year by year. Network intrusions are on the rise, data leaks are occurring, information trafficking is intensifying. But the data collected is also becoming more valuable every year. Everything is there: shopping behaviour, political and religious preferences, illnesses and treatments, new discoveries, ideas, business strategies, citizens' savings – everything is of interest to market players. And, of course, anything directly related to security – this is of particular interest to intelligence

[17] M. Budzisz, *op. cit.*
[18] P.W. Singer, E.T. Brooking, *op. cit.*, p. 209.
[19] *Ibidem*, p. 178.
[20] *Ibidem*, p. 213.

services. And since there are always weaknesses in the system, endless attempts are made to penetrate the security.

The opportunities for penetration are numerous. One that springs to mind is underdeveloped software, but more often than not, the main weakness is in the employees, whose carelessness, perhaps overload of duties and fatigue, but above all character flaws, provide a gateway through which important data leaks out.

According to the ancient Romans, whenever one wants to solve a difficult case, one must find the woman in it and understand her will.[21] Nowadays, when trying to find the place of the leak, the first place to look at is the people using the network. Second place is bugs in the programme itself and faulty system design. Attention is drawn to personality flaws: egotism, narcissism, psychopathic behaviour. Behavioural analysis looks for deviations from the usual behaviour of each employee, because perhaps behind such deviation lies a personality crisis.

The peculiarities of the Internet are capable of making a breach even in the case of healthy personalities, creating many opportunities for pathological traits to emerge.

Today, it is already known that the impulse to break the law, to spy and to take important data outside the organisation comes out of the human psyche and will never disappear, just as the personal tragedies experienced or the desire to improve one's own ego by showing the world how important information one has dealt with will never disappear. Of course, behavioural analysis attempts to detect human weaknesses, and machine learning and artificial intelligence also come into the picture. However, they are at least one step behind the cleverness of a human thinking about committing a crime. Thus, there is a never-ending procession of betrayals, leaks and new security features, and this will continue at least as long as humans are in charge of the most important secrets and have access to information so valuable that it already seems to have no upper bound.

In addition to security systems, the educational layer cannot, of course, be overlooked. Employees not only need to be monitored and their behaviour analysed, they should also be taught to distrust and be cautious. They need to know what sociological trickery will be used to penetrate beyond the security barrier.

References

Budzisz M., *Wyciek tajnych dokumentów*, „Sieci" 2023, nr 16, pp. 45–47.

Cybersecurity trends: Looking over the horizon, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon# [accessed: 23.05.2023].

[21] W. Suworow, *Szpieg, czyli podstawy szpiegowskiego fachu*, transl. by A. Pawłowska, Dom Wydawniczy REBIS, Poznań 2017, p. 116.

Data Takes a Quantum Leap, https://quantium.com/wp-content/uploads/2016/08/BFM_Quantium.pdf [accessed: 26.05.2023].

Finklea K., *Dark Web*, Congressional Research Service Report R44101, 10.03.2017, National Security Archive, https://nsarchive.gwu.edu/media/22737/ocr [accessed: 26.05.2023].

Gibas J., *Psychopata w pracy, w rodzinie i wśród znajomych*, Helion, Gliwice 2021.

Mitnick K., Simon W., *Sztuka podstępu. Łamałem ludzi, nie hasła*, transl. by J. Dobrzański, Helion, Gliwice 2003.

Mooney C., *Internet Trolls Really Are Horrible People: Narcissistic, Machiavellian, psychopathic, and sadistic*, Slate, 14.02.2014, http://www.slate.com/articles/health_and_science/climate_desk/2014/02/internet_troll_personality_study_machiavellianism_narcissism_psychopathy.html [accessed: 20.05.2023].

Piekałkiewicz J., *Dzieje szpiegostwa*, Czytelnik, Warszawa 1999.

Singer P.W., Brooking E.T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, transl. by S. Baranowski, Vis-á-vis Etiuda, *Kraków 2019*.

Suworow W., *Szpieg, czyli podstawy szpiegowskiego fachu*, transl. by A. Pawłowska, Dom Wydawniczy REBIS, Poznań 2017.

Web Hosting Services Market Size, Share, Growth Report, 2030, https://www.fortunebusinessinsights.com/industry-reports/web-hosting-services-market-100863 [accessed: 26.05.2023].

Wilder U.M., *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 19–36.

Wilder U.M., *The Psychology of Espionage and Leaking in the Digital Age*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 1–17.

A critical link in the cybersecurity system

Abstract

The aim of this article is to identify human traits that are responsible for the propensity to betray and take secrets outside the organisation. For this purpose, an analytical-diagnostic approach has been used. The primary research method to achieve the stated objectives is the method of analysis and critique of the literature on the subject and the analysis of review papers describing security breaches in cyberspace, when the source of these breaches is the exploitation of human personality weaknesses.

First of all, personality and character traits leading to taking information outside the organisation or selling important data are identified. Psychopathic tendencies are identified, in addition to the immature, narcissistic and egotistical personality. The reasons for disclosing sensitive data are discussed. In this way, the article shows a different side of the problem of information system security and helps to understand the mechanism of theft or leakage of important information.

Since security weaknesses are attributed to personality traits, the article points to the possibility of anticipatory threat recognition and security enhancement. This is achieved through the use of machine learning, artificial intelligence and behavioural analysis. This succeeds in identifying potentially dangerous individuals who are not coping with their own problems.

Keywords: cyber security, personality, dysfunction, behavioural learning, artificial intelligence, data leakage

Kluczowe ogniwo w systemie cyberbezpieczeństwa
Streszczenie

Artykuł omawia rolę człowieka w systemie zapewnienia bezpieczeństwa cyfrowego. Podjęte na potrzeby artykułu badania wynikają z podejścia analityczno-diagnostycznego. Podstawową metodą badawczą służącą osiągnięciu wyznaczonych celów jest metoda analizy i krytyki literatury przedmiotu oraz analizy prac przeglądowych opisujących naruszenia bezpieczeństwa w cyberprzestrzeni wykorzystujące słabości ludzkiej osobowości.

Przede wszystkim identyfikowane są cechy osobowościowe i charakterologiczne prowadzące do wynoszenia informacji poza organizację lub sprzedawanie ważnych danych. Wskazano na skłonności psychopatyczne, a prócz nich wyróżniono jeszcze osobowość niedojrzałą, narcystyczną i egotyczną. Omówione zostały przyczyny ujawniania danych wrażliwych. W ten sposób artykuł ukazuje problem zabezpieczeń systemów informatycznych od innej strony oraz pomaga zrozumieć mechanizm kradzieży lub wycieku ważnych informacji.

Skoro słabości zabezpieczeń upatruje się w cechach osobowościowych – artykuł wskazuje na możliwość uprzedzającego rozpoznania zagrożeń i wzmocnienia bezpieczeństwa. Droga do niego wiedzie przez zastosowanie maszynowego uczenia się, wykorzystanie sztucznej inteligencji i analizy behawioralnej. Dzięki temu udaje się zidentyfikować potencjalnie niebezpieczne osoby, nie radzące sobie z własnymi problemami.

Słowa kluczowe: cyberbezpieczeństwo, osobowość, dysfunkcje, uczenie behawioralne, sztuczna inteligencja, wyciek danych