E-Biuletyn 1(2)2023

NOWINY NAUKI O BEZPIECZEŃSTWIE

Bezpieczeństwo miejskie i cyberbezpieczeństwo w praktyce sektora publicznego i prywatnego

Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Nauk Politycznych i Dziennikarstwa
Zakład Studiów nad Bezpieczeństwem

Redakcja e-Biuletynu
„Nowiny Nauki o Bezpieczeństwie”

Zakład Studiów nad
Bezpieczeństwem
WNPiD UAM
ul. Uniwersytetu Poznaskiego 5 Poznań

Kontakt |
mikolaj.tomaszyk@amu.edu.pl

Redakcja nie zwraca tekstów niezamówionych i zastrzega sobie prawo do redagowania i skracania nadesłanych materiałów.
Śródtytuły pochodzą od redakcji.

Zespół redakcyjny:

Redaktor naczelny |
prof. UAM dr hab. Mikołaj Tomaszyk

Konsultacja naukowa |
prof. zw. dr hab. Jerzy Konieczny
prof. UW dr hab. Cezary Smuniewski

Projekt okładki i skład |
Oliwia Oleszak
oliwia.oleszak@gmail.com
instagram: o.leszak

Ilustracje | www.adobe.stock.com

Spis treści:

Szanowni Państwo,

mam nadzieję, że w Nowy Rok weszli Państwo z nutą optymizmu i powiewem świeżości wynikającej chociażby z tego, że wkraczamy w nieznane. Od stycznia 2022 roku wiele się zmieniło. Ogłoszona została data końca pandemii w Polsce. W drugiej połowie lutego wybuchła wojna Rosji z Ukrainą. Mamy głęboki kryzys gospodarczy, a kwestie bezpieczeństwa energetycznego państw nabierają nowego, innego znaczenia. Testowane są sojusze międzypaństwowe a słowa „wsparcie", „uchodźca", „sojusz" i „pomoc" nabierają nowego znaczenia. Ostatnie lata i historyczne już wydarzenia są dla wielu cezurą życia osobistego, społecznego i politycznego w wymiarze krajowym i międzynarodowym.

O skutkach wojny w Ukrainie, sprawności działań polskich władz samorządowych i rządowych pisaliśmy na łamach ostatnich numerów e-biuletynu. W pierwszym numerze w 2023 roku proponujemy temat dotyczący **bezpieczeństwa miejskiego** oraz **cyberbezpieczeństwa**. Taką nazwę noszą dwie, **nowe specjalności** na prowadzonych przez Wydział Nauk Politycznych i Dziennikarstwa UAM, studiach uzupełniających magisterskich. Korzystając z okazji zapraszamy do **zapoznania się i do skorzystania z tej oferty dydaktycznej**.

Oddajemy w ręce Czytelniczek i Czytelników pierwszy w 2023 roku numer e-biuletynu pt. Nowiny Nauki o Bezpieczeństwie. Wybierając temat przewodni tego numeru, kierowaliśmy się doświadczeniami płynącymi z obserwacji rynku pracy dla absolwentów studiów I i II stopnia oraz wagą tematyki bezpieczeństwa miejskiego i cyberbezpieczeństwa.

Doświadczenia pandemii SARS-CoV-2 pokazują nam, jak zmienia się perspektywa przestrzeni, w której żyjemy. Aprzestrzenność relacji – to pojęcie wprowadzone m. in. przez prof. Noworóla do polskiego dyskursu nt. zmian zachowań przestrzennych w okresie pandemii (1). Ich skutkiem jest zmiana mobilności codziennej, popularyzacja zdalnych form kontaktu oraz zdalnych form zaspokojenia wielu codziennych potrzeb. Zmiany te wpływają na poczucie bezpieczeństwa w świecie realnym, ale również w wirtualnym.

Badania nad poczuciem bezpieczeństwa w mieście to dynamicznie rozwijający się obszar o charakterze interdyscyplinarnym. Wiedza na ten temat jest wspierana danymi zbieranymi za pomocą urządzeń rejestrujących obraz, dźwięk, mierzących ruch, dokonujących różnych pomiarów. Umiejętność ich analizy powinna stanowić podstawowe źródło danych w pracy specjalistów ds. bezpieczeństwa lokalnego. Z kolei nasza obecność w sieci jest związana z różnymi ryzykami, które mogą się materializować. To od nas zależy co, komu, w jakim celu udostępniamy, o czym informujemy i przed czym się zabezpieczamy.

Powyższe zagadnienia to tylko powierzchownie określony zbiór zagadnień, które rozwijają Autorki i Autorzy bieżącego numeru. Zachęcamy do przeczytania wywiadu z **Konradem Glejtem**, zapoznania się z najnowszą książką **Łukasza Olejnika**. Temat bezpieczeństwa dzieci w sieci podejmują **Piotr Świdziński** oraz **Zuzanna Czachorek**. Z kolei **Marcin Rachwał** i **Małgorzata Pilichowska-Woźniak** odnoszą się do teorii i praktyki funkcjonowania e-administracji oraz systemu ochrony informacji niejawnych. Ostatnie trzy opracowania są autorstwa seminarzystów **gen. dr Lecha Konopki**. Młodzi pasjonaci zagadnień dotyczących cyberbezpieczeństwa: **Radosław Tyl, Jonasz Żak** i **Krzysztof Łukaszewski** opisują rynek pracy dla specjalistów z tej dziedziny, system alertów RCB oraz zasady wyrażania zgody on-line. Dziękuję prof. UW dr hab. Cezaremu Smuniewskiemu oraz prof. dr hab. Jerzemu Koniecznemu za inspirujące i pozytywne recenzje nadesłanych tekstów i za dobre słowo kierowane pod adresem inicjatywy e-biuletynu.

Życzę dobrej lektury i zapraszam na łamy e-biuletynu.

Przypisy:

(1) Noworól A. (2021), Pandemia COVID-19 jako stymulator procesów despacjacji, w: Polityka przestrzenna w czasie kryzysu, red. M. Nowak, Wydawnictwo Naukowe Scholar, Warszawa.

prof. UAM dr hab. Mikołaj Tomaszyk
Redaktor naczelny
„Nowiny Nauki o Bezpieczeństwie"

Teksty zebrane pod wspólnym tytułem „Bezpieczeństwo miejskie i cyberbezpieczeństwo w praktyce sektora publicznego i prywatnego" inspirują do przemyśleń o sytuacji obecnej naszego społeczeństwa oraz o tym, co nadchodzi i już za chwilę będzie naszym zagrożeniem. Trzeba nam dobrze obserwować rzeczywistość, precyzyjnie identyfikować to, co może zaszkodzić, nazywać zagrożenia i szukać – odważnie – nowych rozwiązań. Z dużym przekonaniem rekomenduję lekturę tekstów składających się na kolejny numer „Nowiny Nauki o Bezpieczeństwie" e-biuletyn nr 1(2)2023.

prof. UW dr hab. Cezary Smuniewski
Uniwersytet Warszawski, Wydział Nauk Politycznych i Studiów Międzynarodowych, Katedra Bezpieczeństwa Wewnętrznego

Cyberbezpieczeństwo dziś to nie tylko kwestia bezpieczeństwa systemów informacyjnych, komputerowych – nowość na rynku wydawniczym!

Znaczenie szerokiej problematyki cyberbezpieczeństwa obszaru ewoluuje. Postępująca komputeryzacja i cyfryzacja, oznacza, że coraz więcej z naszej działalności w ten czy w inny sposób zależy od technologii. Często nawet się na nich opiera. Technologia i cyfryzacja to wielkie dobro społeczne. To jednak także ryzyka i zagrożenia. Trzeba sobie zdawać z tego sprawę. Co się stanie, gdy technologia będzie sterowała całym naszym światem, życiem, całymi krajami, kluczowymi dobrami, infrastrukturami? To ryzyko słabych punktów i podatności.

Cyberbezpieczeństwo to rzecz o bezpieczeństwie całego społeczeństwa. To dlatego warto uporządkować ten temat. Stąd pomysł na książkę. Książka pod tytułem Filozofia Cyberbezpieczeństwa ukaże się wkrótce nakładem Wydawnictwa PWN i obejmuje temat cyberbezpieczeństwa bardzo szeroko. Dlaczego „Filozofia”? Bo chodzi także o to, by wiedzieć jak myśleć o zagrożeniach i cyberbezpieczeństwie w dzisiejszym i przyszłym świecie. Książka ta to pewnego rodzaju niezbędny *ekwipunek* na dziś i jutro. Wyposaża w świadomość. Wskazuje na przykład, jakiego rodzaju treści lub doniesienia mają duże znaczenie, a jakie już niekoniecznie (albo takie, które wcale nie mają znaczenia, są szumem).

W Filozofii Cyberbezpieczeństwa mowa o perspektywie użytkownika (mnie, Ciebie), ale także kwestiach systemowych.

To książka dla każdego - szerokiego grona odbiorców. To jeden z głównych celów. By materiał ten, ta tematyka - by było to wszystko przystępne i zrozumiałe. Lecz jest to jednak przede wszystkim materiał ekspercki, odnoszący się do złożonego problemu. Hermetyczny, niewątpliwie. Zatem znajdą tam wiele ciekawych treści eksperci, także wykładowcy akademiccy, oczywiście i studenci . I to różni studenci.

Dziedzin technicznych jak informatyka, ale także społecznych, chociażby w obszarach takich jak stosunki międzynarodowe, dyplomacja, strategia, nauki o bezpieczeństwie, nauki polityczne. To także pozycja dla samorządowców poruszonych tematów, dla funkcjonariuszy różnego rodzaju instytucji, urzędników. Również — dla polityków. Bo cyberbezpieczeństwo to także kwestia strategii i polityki państwa. I dla każdego, kto pragnie zrozumieć i móc docenić ewolucję cyberbezpieczeństwa w ostatnich dekadach. Lub nabyć, pozyskać świadomość zagrożeń i niezbędnych podstaw by tym przeciwdziałać (jak się zabezpieczyć).

Być może będzie to pierwsza książka o cyberbezpieczeństwie, którą zrozumiesz.

W książce tej mowa o takich podstawach szczegółowych jak np. to, czym jest dobre hasło, oraz dlaczego tak się dziś uważa. Bo to są kwestie techniczne, które muszą być na czymś oparte. Mało kto wie, że do niedawna zalecenia w tym obszarze były raczej uznaniowe. Dopiero od mniej-więcej 10 lat temat ten jest aktywnie badany. Mowa także o kwestiach systemowych. Takich jak cyberbezpieczeństwo opieki zdrowotnej (*wyzwania, dlaczego tak trudno zabezpieczyć, czy z powodów cyberataków mogli ginąć ludzie? Czy cyberatakiem można zabić?*), infrastruktury krytycznej (*czy cyberatakiem można wysadzić w powietrze elementy systemu elektroenergetycznego?*), państwa (*państwa już hakowano, w tym także i Polskę*).

Jest także o tym, że cyberprzestrzeń nie jest „szarą strefą" bez żadnych zasad. To pogląd nieprawidłowy, nieoparty na rozumowaniu merytorycznym. W książce jest bardzo logicznie wyłożone to, czym jest cyberwojna. Jak ją rozumieć. Czy nam grozi, oraz w jakich okolicznościach cyberataki mogłyby doprowadzić do wojny szerszej. Także o tym, jak taki początek mógłby wyglądać. Warto o tym pamiętać, bo z dzisiejszej perspektywy niektóre z cyberataków na Ukrainę w styczniu 2022 r. stanowiły preludium do późniejszej wojny. W książce oczywiście nie sposób pominąć kwestii specyficznych takich jak cyber wywiad. Bo nie tylko o „cyberprzestępczości" trzeba mówić... Ostatecznie, wyłożone są realistyczne (dobrze przemyślane, oparte o podstawy naukowo-techniczne, a może i coś więcej...) scenariusze cyber operacji wywołujących (1) fizycznie zniszczenia, (2) efekty śmiertelne, (3) rozpoczynające wojnę.

Ostatni punkt (cyberwojna) nabrał dużego znaczenia przy okazji wojny na Ukrainie. To najdłuższy rozdział. To także pierwsza książka, która analitycznie i ekspercko podchodzi do tego tematu. Wyjaśniona jest ranga i waga tych działań, także na tle szerszych działań wojskowych. To właśnie teraz toczy się ta dyskusja. Kiedy cyberatak można potraktować jako agresję zbrojną, a kiedy jedynie jako naruszenie suwerenności? W jaki sposób państwa mogą odpowiadać? Bo niektóre z państw zaznaczają, że odpowiedź może być cyberatakiem, ale może być także kinetyczna. Taką opinię ma właśnie, oficjalnie, Rzeczpospolita Polska. Albo Republika Francuska.

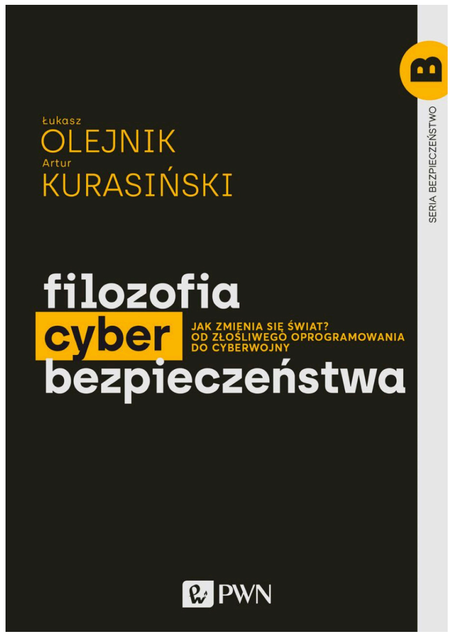
Filozofia Cyberbezpieczeństwa to książka pisana z dogłębnym zrozumieniem tematu nabytym w ostatnich 20 latach, obserwując szereg zmian zachodzących na świecie i pisana przy braniu aktywnego udziału w niektórych tych zmian. Wydawcą jest PWN, więc poziom ekspercko-naukowy zobowiązuje.
Dlaczego taka książka teraz? Jednym z powodów mógłby być specyficzny tryb pracy w trakcie pandemii. Ale to proza życia. Inny, bardziej bezpośredni i konkretny — to spotkanie prezydentów USA i Rosji (Biden, Putin) w Genewie, w 2021. To pewnego rodzaju punkt zwrotny dla cyberbezpieczeństwa. Już „wyżej" rozważać tego tematu nie sposób w ramach sporów międzypaństwowych. I nikt się takiego obrotu spraw nie spodziewał te 20-30 lat temu. Także dlatego powstała ta książka. I to właściwy na nią czas. Także dlatego, że właśnie powstaje polski potencjał, wojska ochrony cyberprzestrzeni, coraz więcej uczelni zaczyna prowadzić kursy, specjalności, kierunki w dziedzinie (choć bardzo często trudno tu o odpowiednią kadrę — na co nie mam wpływu; ale także o właściwy dobór bibliografii — na co mam wpływ choćby tą książką). Chciałem napisać taką książkę, zatem zrobiłem to.

Ujęcie tematu w taki unikalny i szeroki sposób jest odpowiednie i właściwe. Wobec tego Filozofia Cyberbezpieczeństwa traktuje cyberbezpieczeństwo bardzo szeroko. Od technologii, poprzez prawo, także europejskie i międzynarodowe, dyplomację, wojskowość, sprawy bezpieczeństwa, nawet w kwestii konfliktów. Międzypaństwowych i zbrojnych, geopolityki, nauk politycznych, o stosunkach międzynarodowych. Bo takie właśnie mamy czasy i potrzeby. Tematy te w książce ze sobą współgrają w taki sposób, że to wszystko jest ze sobą powiązane. Jako ciekawostkę, dodam, że książka ta zawiera tzw. drabinę eskalacyjną uwzględniającą cyber operacje. Ale pomyślaną w sposób realistyczny, tj. jak w praktyce mógłby wyglądać konflikt międzypaństwowy przechodzący w konflikt zbrojny. Zatem od niskiej skali cyberataków, poprzez naruszenie suwerenności, do użycia siły, rozpoznania itd.

To pierwsza tego rodzaju książka, nie tylko zresztą w j. polskim. Choć, co naturalne, odnośniki, bibliografia, cytowania są w większości do materiałów jakościowych, anglojęzycznych. Czasem w innych językach, jak np. jest w przypadku rosyjskiej doktryny bezpieczeństwa państwa, albo doktryny wojskowej, lub dokumentów Republiki Francuskiej. Książka ta napisana jest z dogłębną znajomością tematu. Także dlatego mnadzieję, że gdy wezmę do rąk Filozofię Cyberbezpieczeństwa za, powiedzmy, 10 lat, to uznam, że wciąż się ona dobrze trzyma. W tym sensie jest to podręcznik.

Słowem, solidna pozycja. Nad tą książką spędziłem bardzo wiele czasu, włożyłem bardzo dużo pracy. Przełożyłem swoje doświadczenie nabywane podczas ostatnich 20 lat. To zatem użycie mojej wiedzy także z poprzednich lat. Wszystko napisane w taki sposób, by było ciekawe i zrozumiałe.

Zaszczytem dla tej książki są pozytywne opinie (“blurby”), które do tej książki napisały wspaniałe osoby. To prof. Koziej, prof. Zybertowicz, gen. bryg Karol Molenda, Frank Bajak (Associated Press), Edward Lucas (b. starszy edytor „The Economist”, dobrze znany w naszym regionie Europy brytyjski analityk), oraz Michał Zalewski (b. CISO Snap; były najlepszy polski haker).

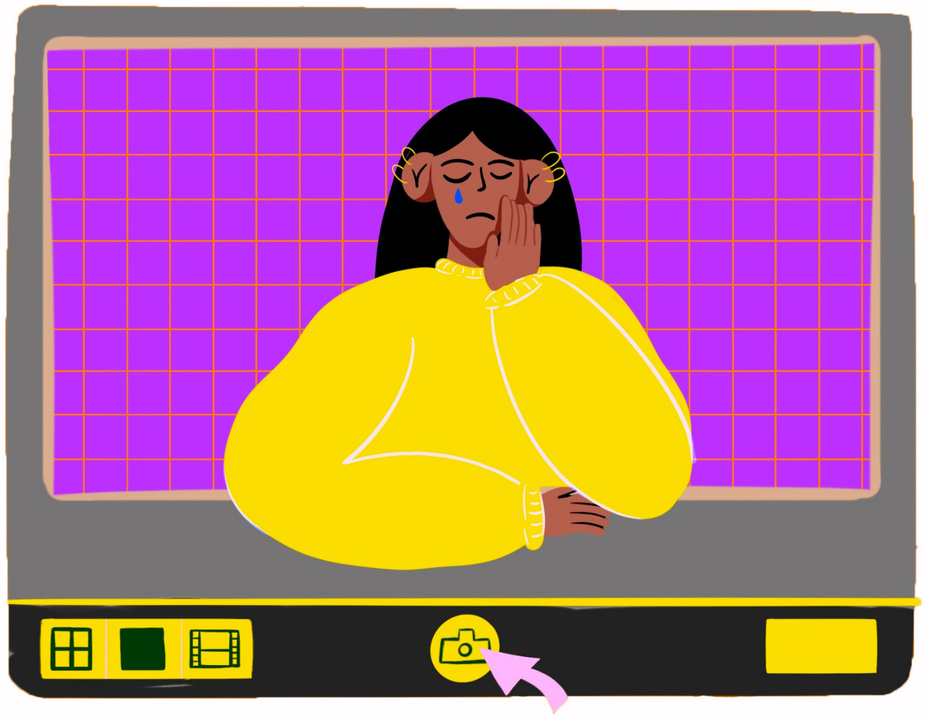


dr Łukasz Olejnik
niezależny badacz i konsultant cyberbezpieczeństwa i prywatności, zajmuje się kwestiami technologii i polityki technologii, czasem zwanej „cyfryzacją”. Doktorat we francuskim instytucie informatyki i automatyki INRIA. Pracował w CERN (Europejskiej Organizacji Badań Jądrowych). Research associate w University College London. Był związany z Princeton’s Center for Information Technology Policy i z Oxford’s Center for Technology and Global Affairs, Genewską Akademią Międzynarodowego Prawa Humanitarnego i Praw Człowieka. W 2018-2020 w Technical Architecture Group, World Wide Web Consortium (W3C). Był doradcą ds. cyberwojny w Międzynarodowym Komitecie Czerwonego Krzyża w Genewie, gdzie pracował nad humanitarnymi konsekwencjami cyberataków. Doradzał w kwestii nauki i nowych technologii w Europejskim Inspektoracie Ochrony Danych Osobowych, a także dla różnego rodzaju firm i organizacji.

Jest członkiem Komitetu Sterującego Narodowego Centrum Badań i Rozwoju CyberSecIdent (projekty R&D cyberbezpieczeństwa). W 2016/2017 członek zespołu eksperckiego ds. bezpieczeństwa cyberprzestrzeni w ramach BBN. Na tematy technologii, cyberbezpieczeństwa i prywatności zabierał głos w prasie polskiej i zagranicznej (Financial Times, Washington Post, New York Times, Wall Street Journal, Sueddeutsche Zeitung, El Pais, Le Monde, Telegraph, Guardian, Politico, Associated Press, Reuters, Bloomberg, Le Figaro, BBC, Wired, Dziennik Gazeta Prawna, Gazeta Wyborcza, itp.). Jego artykuły i analizy ukazały się m.in. w Foreign Affairs, Wired, Dzienniku Gazecie Prawnej, Gazecie Wyborczej. Na Twitterze @prywatnik, jego strona to https://prywatnik.pl. Lubi pomidory, ale tylko sezonowe. W Dzienniku Gazecie Prawnej ma cykl artykułów eksperckich “Cyberpolityka”

Bezpieczeństwo dzieci i młodzieży w sieci

Internet towarzyszy nam już od dziesiątków lat i pomimo wielu informacji na temat niebezpieczeństw, jakie na nas wszystkich czyhają, temat ten jest i będzie aktualny w przyszłości. Jako dorośli nie przywiązujemy niestety wagi do tego, jak korzystamy z sieci. Wynika to w dużej mierze z niewiedzy, braku czasu czy roztargnienia. Stąd już tylko jeden krok, na który czekają cyberprzestępcy.



Możemy w prosty sposób paść ofiarą oszustwa, stracić dane. Wydaje się, że szkoda może być niewielka, gdy utracimy konto do jakiegoś sklepu czy portalu. Jednak okazuje się, że zagrożenie może być bardzo duże. Wyobraźmy sobie, że konto, które stracimy, będzie miało podpiętą kartę płatniczą? Albo na naszej skrzynce pocztowej będziemy mieli zapisane dane wrażliwe, hasła do innych portali, prywatne zdjęcia itp.
Zastanówmy się więc, czy nasze działania, które przecież podejmujemy (m.in. w szkole), są wystarczające? Mimo coraz poważniejszych problemów z zapewnieniem bezpieczeństwa w sieci, nie radzimy sobie z tym zagadnieniem dość dobrze.

Czy kolejne pokolenia (dzieci i młodzieży) potrafią skutecznie obronić się przed zagrożeniami w sieci? Czy rola szkoły w tym zakresie powinna być większa? Czy mamy odpowiednią wiedzę i narzędzia, aby skutecznie działać w zakresie cyberbezpieczeństwa w sieci? Na te i inne pytania postaram się odpowiedzieć w poniższym tekście.

Zagrożenia

Nie sposób w jednym miejscu poruszyć wyczerpująco wszystkich zagadnień dotyczących bezpieczeństwa w sieci. Spróbujmy ograniczyć się do kilku - moim zdaniem najważniejszych. Jednym z głównych zagrożeń jest czas, które dzieci i młodzież poświęcają na przebywanie w świecie cyfrowym.

Równie istotne jest to, że coraz młodsze osoby korzystają z sieci dość regularnie. Rodzice nie mają kontroli nad tym, jak długo ich dzieci przebywają w Internecie. Nie są również ich przewodnikami w przestrzeni wirtualnej.

Cyber(nie)bezpieczeństwo

Jednym z głównych zagrożeń jest przede wszystkim agresja w sieci (poniżanie, ośmieszanie, straszenie czy szantażowanie). Wg badań z raportu Nastolatki 3.0 - dotyczy to od 9,2% do mniej więcej 22% respondentów. Największym problemem jest jednak wyzywanie, co wg badań z 2020 roku stanowi 29,7% respondentów badań ankietowych i zwiększyło się o 2,9% w porównaniu z badaniem z roku 2018 (1).

Zauważalne jest również to, iż rodzice coraz bardziej zdają sobie sprawę z zagrożeń cyfrowych (wzrost świadomości o kilka % w porównaniu z badaniami w roku 2018 i 2020), jednak nadal ich świadomość jest mniejsza niż faktyczne zagrożenia, o których informują w ankietach dzieci i młodzież. Dość optymistyczne wyniki ankiet wśród rodziców, gdy zapytani zostali: “Czy Pana/Pani dziecko doświadczyło w Internecie: ...?”: poniżania 9%, ośmieszania 12,5%, straszenia 4,5%, szantażowania 2,5%, wyzywania 13,5%; nie pokrywają się w żaden sposób z oceną samych dzieci i nastolatków.

Niepokojące może być to, że różnica w odpowiedziach rodziców i dzieci jest dość duża. W tej sytuacji działania profilaktyczne, które są i powinny być prowadzone w szkole, nabierają istotnego znaczenia. Własną opinię na temat celu ataków doświadczanych w świecie cyfrowym wyrażały dzieci i rodzice. I niestety zauważalne jest to, że są znów znaczne różnice w odpowiedziach. Nastolatki zdają sobie sprawę, że są przedmiotem ataków w Internecie i potrafią o tym mówić. Dorośli natomiast nie zawsze są włączani w problemy swoich dzieci i jak widać w badaniu, nie mają wiedzy na temat trudnych doświadczeń swoich podopiecznych. Trudno powiedzieć, co sprawia, że dzieci nie mówią o tym swoim rodzicom. Zauważalne jednak jest to, że to nadal duży problem (1).

Warto podkreślić, że blisko 70% dorosłych jest przekonana, że najlepszym sposobem radzenia sobie z problemem przemocy w sieci, jest szukanie wsparcia u rodziców i opiekunów. Podczas gdy w rzeczywistości taką aktywność deklaruje tylko nieco ponad 24% dzieci, czyli co czwarty nastolatek. Jasno wskazuje to na pewien duży dysonans - my dorośli żyjemy w błogiej nieświadomości i jesteśmy przekonani, że nasze dzieci przyjdą po pomoc w sytuacji zagrożenia cyberprzemocą (1).

Warto podkreślić, że blisko 70% dorosłych jest przekonana, że najlepszym sposobem radzenia sobie z problemem przemocy w sieci, jest szukanie wsparcia u rodziców i opiekunów. Podczas gdy w rzeczywistości taką aktywność deklaruje tylko nieco ponad 24% dzieci

Rzeczywistość okazuje się jednak zdecydowanie inna i znaczna część osób małoletnich tego nie robi. Problemem może tu być obawa, brak zaufania, ale również strach czy nieumiejętność rozmowy z rodzicami na tematy cyfrowego bezpieczeństwa. Dzieci i młodzież zdają sobie sprawę, że wiedza dorosłych jest często ograniczona i nie mają oni wystarczających kompetencji do tego, aby im w jakikolwiek sposób pomóc. Nie zawsze jest to prawda, a często pewne wyobrażenie.

Technikalia

Jak uświadamiać młodzież i dzieci i uczyć bezpiecznych zachowań w sieci? Jedną z najprostszych odpowiedzi będzie taka: uczmy ich aspektów technicznych. Niebezpieczeństwa w sieci to nie tylko cyberprzemoc czy hejt, ale również obawa utraty danych, kradzież tożsamości czy wirusy komputerowe. Bez podstawowej wiedzy technicznej dzieci i młodzież nie będą potrafiły obronić się przed zagrożeniami, a to może skutkować problemami w życiu już dorosłym. Gdy utrata konta mailowego może doprowadzić do przejęcia przez cyberprzestępcę danych wrażliwych takich jak PESEL czy dostęp do usług finansowych, w tym m.in. bankowych.

Ta tematyka jest równie ważna jak pozostałe zagrożenia. W perspektywie czasu wydaje się, iż będziemy narażeni na coraz intensywniejsze ataki i próby wykradnięcia danych. Przedstawmy tu więc kilka najważniejszych porad, aby bezpiecznie korzystać z sieci:

- Używaj oprogramowania antywirusowego - chroń swój komputer programem antywirusowym.
- Pamiętaj, żeby po zakończeniu korzystania z danej aplikacji, wylogować się.
- Używaj różnych haseł do różnych

usług i stale je aktualizuj.
- Zwracaj uwagę na to, jakie informacje umieszczasz w sieci; zawsze zostaje po nich ślad. Z chwilą umieszczenia zdjęcia/nagrania, tracisz nad nim kontrolę.
- Staraj się nie poddawać presji otoczenia, jeśli nie jesteś do tego przekonany. Gdy klikniesz “wyślij’ może być już za późno.
- Nie krzywdź innych osób - nie rób zdjęć i nie nagrywaj nikogo bez jego zgody. Zastanów się, jakbyś się czuł w podobnej sytuacji.

Porady te wydają się nam znane, tak jak i dzieciom, nastolatkom, mimo to okazują się często niewystarczające. Szczególnie ważne będzie więc przedstawienie i omówienie technicznych aspektów i zabezpieczenie naszego komputera, telefonu, tabletu, dlatego w tym miejscu zwrócę uwagę na kilka ważnych aspektów:
- Wybierz bezpiecznego dostawcę usług pocztowych. Nie chodzi tu o reklamę, ale o możliwości technologiczne danej firmy - ma ona większe możliwości, doświadczenie itp. zdecydowanie lepiej filtruje SPAM, skutecznie powstrzymuje ataki phishingowe, dobrze skanuje wiadomości pod względem zagrożenia wirusowego.
- Uruchom weryfikację dwuetapową - oczywiście, może ona być pewnym utrudnieniem (jeśli np. potwierdzenie przychodzi na telefon, a nie mamy go pod ręką), ale zabezpiecza bardzo dobrze przed utratą naszego konta, szczególnie gdy korzystamy z niego w miejscu publicznym, w pracy czy szkole.
- Szyfruj ważne dla ciebie pliki (np. przy wykorzystaniu darmowego programu 7zip, w którym możesz zaszyfrować plik i bez podania hasła nie będzie możliwości jego otworzenia). Wystarczy, że odbiorcy wyślesz hasło SMS, a wiadomość z plikiem wyślesz mailem.
- Okresowo weryfikuj, jakie urządzenia mają dostęp do twojej poczty (można to sprawdzić w ustawieniach w wielu czołowych firmach).
- Używajmy managera haseł - jest to bardzo bezpieczne rozwiązanie, które zabezpieczy nam dostęp do naszych kont.

Inne zagrożenia

Poza wymienionymi zagrożeniami jest również szereg innych, o których tylko wspomnę, jednak na potrzeby tej publikacji nie będę tej tematyki szerzej omawiał. Jest to między innymi dostęp do materiałów o charakterze seksualnym, pornograficznym. Zainteresowanie nastolatków tą tematyką nie może dziwić. Wynika to z jednej strony z ciekawości poznawczej, typowej dla ich wieku, a z drugiej strony łatwość dostępu do takich stron powoduje chęć poznania. W ciągu ostatnich dziesięcioleci badań wykazano, że szeroki kontakt z pornografią ma negatywny wpływ i powoduje niezliczone szkody psychiczne.

Młodzież i dzieci deklarują dużo większy kontakt z pornografią niż wynika to z wiedzy rodziców. Rozbieżności te są bardzo duże, np. w szkole ponadpodstawowej ponad 62% chłopców i 33% dziewcząt przyznaje, że zdarza im się oglądać jakieś treści pornograficzne w Internecie, natomiast tylko 11,5% rodziców przyznaje, że ich dziecko mogło mieć kontakt z pornografią (w szkole średniej); prawie 60% jest przeciwnego zdania, a pozostała część czyli 28,6%, nie potrafi odpowiedzieć na to pytanie (trudno powiedzieć).

Przeciwdziałanie

Jak wspominałem już wcześniej, z racji tego, że rodzice i opiekunowie dzieci często nie są do końca świadomi skali niebezpiecznych sytuacji i zachowań w sieci, w których uczestniczą ich podopieczni, olbrzymią rolę spełnia tu szkoła. Oczywiście, powinna ona współpracować w tej kwestii z rodzicami (i tak się dzieje w zdecydowanej większości sytuacji ujawnionych zagrożeń). Profilaktyka w placówkach oświatowych wydaje się jednak być na niewystarczającym poziomie. Choć nauczyciele są zdecydowanie bardziej świadomi zagrożeń w sieci (m.in. dot. cyberprzemocy), to jednak nadal odczuwają potrzebę szkoleń z zakresu bezpieczeństwa w sieci. Tematyka ta jest najczęściej poruszana na lekcjach informatyki lub na lekcjach wychowawczych jednak jak wynika z badań, brakuje spotkań ze specjalistami i zbyt mały nacisk na realizację tych zagadnień powoduje duże braki wiedzy wśród dzieci i młodzieży. Nauczyciele badani w raporcie “Cyber-

nauci - diagnoza wiedzy, umiejętności i kompetencji...", byli również pytani o szereg działań i zachowań związanych z bezpiecznym korzystaniem z internetu. Większość badanych twierdzi, że poziom ich wiedzy jest wysoki. Jednak należy zwrócić uwagę, że zagrożenia nieustannie się zmieniają. Sieć internetowa różni się diametralnie od tej, która istniała jeszcze kilka lat temu. Również szereg zagrożeń jest inny i należy się spodziewać dalszej jego eskalacji. Cyberprzestępcy są coraz bardziej wyrafinowani i ze względu na rozwój technologiczny ich ataki są również skuteczniejsze i niebezpieczniejsze dla użytkownika. W tej sytuacji wzrasta również zagrożenie dla dzieci i młodzieży.

Warto zauważyć, że kwestie techniczne dot. użytkowania Internetu nie są poruszane w szkole wcale lub bardzo rzadko i w niewielkim wymiarze. Oczywiście uczniowie dowiadują się o braku anonimowości, ale raczej rzadko informuje się ich o kwestiach zabezpieczeń, używania narzędziami do szyfrowania połączenia czy innych zabezpieczeń technicznych (1).

Przypisy:

NASTOLATKI 3.0 Raport z ogólnopolskiego badania uczniów, NASK, Państwowy Instytut Badawczy Warszawa 202, s. 80

Piotr Świdziński
nauczyciel informatyki w Zespole Szkół im. Kryptologów Poznańskich w Luboniu, pasjonat nowych technologii i programowania, trener i szkoleniowiec z zakresu nowych technologii w edukacji, bezpieczeństwa w sieci. Zainteresowania: film amatorski, pszczelarstwo, siatkówka i wiele innych.

Dzieci sieci. Znaczenie bezpieczeństwa w Internecie dla współczesnych nastolatków

W styczniu 2022 roku liczba internautów na świecie wyniosła 4,95 miliarda, co stanowi prawie 70% populacji świata. To o 4% więcej użytkowników Internetu niż w roku poprzednim. Wraz z powiększaniem się tej liczby, wzrasta także popularność mediów społecznościowych (zaobserwowano tu wzrost o 10% w porównaniu do zeszłego roku, co daje liczbę 4,62 miliarda użytkowników). Dziś z social mediów korzysta zatem 58,4% całkowitej populacji świata i prawie 94% wszystkich osób korzystających z Internetu. Wśród nich są oczywiście także najmłodsi, którzy Internetu używają coraz wcześniej i coraz częściej (1).

Według badań przeprowadzonych w Polsce w 2021 roku średni wiek inicjacji internetowej uczniów szkoły podstawowej wynosił 6 lat i 8 miesięcy (2). Jednak z raportu „Brzdąc w sieci – zjawisko korzystania z urządzeń mobilnych przez dzieci w wieku 0-6 lat" wynika, że ten wiek jest już nieaktualny i dziś co trzeci dwulatek i co drugi trzy- i czterolatek używa urządzeń mobilnych (3).

Urodzeni ze smartfonem

Osoby, które nie pamiętają czasów sprzed Internetu, dorastają z telefonem komórkowym i mają konto na Instagramie przed pójściem do liceum, Jean M. Twenge, autorka książki „iGen. Dlaczego dzieciaki dorastające w sieci są mniej zbuntowane, bardziej tolerancyjne, mniej szczęśliwe – i zupełnie nieprzygotowane do dorosłości – i co to oznacza dla nas wszystkich", nazywa przedstawicielami pokolenia iGen. Nastolatki z iGenu dorastają ze smartfonem oraz nieograniczonym dostępem do Internetu. Cechuje ich postawa tolerancyjna, otwartość, wrażliwość, unikanie agresji, a także duża troska o bezpieczeństwo (4).

Kwestie dotyczące bezpieczeństwa były poruszane w ramach wywiadów pogłębionych prowadzonych na potrzeby badań nad translokacyjnymi i nietranslokacyjnymi zachowaniami komunikacyjnymi młodzieży szkolnej, które przeprowadzaliśmy wraz z dr. Jakubem Jakubowskim w 2021 i 2022 roku. Podczas szesnastu rozmów z uczniami szkół podstawowych oraz średnich, zadawaliśmy pytania o nawyki w korzystaniu ze smartfonów, a konkretniej z mediów społecznościowych. Pytaliśmy o budowanie relacji międzyludzkich poprzez najpopularniejsze komunikatory oraz codzienność funkcjonowania w Internecie. Założeniem projektu badawczego było odkrycie nowych, aktualnych dla młodych ludzi zasad komunikacyjnych funkcjonujących w sieci. Dążenie do tzw. kultury bezpieczeństwa, która to, według Twenge, wyróżnia najmłodsze pokolenie (4), było widoczne w wypowiedziach badanych przez nas uczniów. Większość z nich wykazywała się dużą świadomością potencjalnych zagrożeń i niebezpiecznych sytuacji w Internecie. Część zwracała również uwagę na bezpieczeństwo emocjonalne. W końcu środowisko, w którym młodzież funkcjonuje od początku swojego życia, powinno zaspokajać tę podstawową ludzką potrzebę. Nastolatki chcą w świecie online kreować rzeczywistość komfortową, otwartą i bezpieczną dla wszystkich.

Bezpieczna przestrzeń internetu

Hasło „bezpieczeństwo w Internecie" nie zawsze kojarzyło się uczestnikom naszego badania z tym, co intuicyjnie przypisujemy do kwestii zagrożeń w sieci – utratą danych logowania, złośliwymi oprogramowaniami czy zjawiskiem phishingu. Przyczyną tego jest zapewne fakt, że Internet dla młodych ludzi jawi się głównie jako przestrzeń rozrywki, dostępu do kultury oraz ośrodek życia społecznego. Bliższe młodzieży są zjawiska takie jak fake newsy, hejt, utrata dobrego wizerunku przez działania drugiej osoby czy, ogólnie rzecz biorąc, cyberprzemoc. Biorąc pod uwagę to, że przedstawiciele pokolenia Z cenią sobie indywidualizm oraz możliwość budowania i wyrażania własnej tożsamości, strach przed wyciekiem prywatnych zdjęć, a nie wyłudzeniem danych wydaje się dla współczesnej młodzieży po prostu bardziej naturalny.

Lęk przed utratą tego, co intymne, prywatne, przejawiał się w trakcie rozmów na temat autocenzury i kontrolowania tego, co i do kogo trafia za pośrednictwem komunikatorów i aplikacji. Młodzież kategoryzuje narzędzia (aplikacje) do komunikacji, dzieląc je na te bezpieczne i mniej bezpieczne. Jedna z uczestniczek badania powiedziała: „Właśnie jedną z najważniejszych i najlepszych dla mnie funkcji Snapchata (5) jest to, że jak się zrobi jakiegoś screenshota, nagra się ekran, cokolwiek się zrobi, to wszystko widać. Mam taką pełną kontrolę nad tym. Na Instagramie tego nie ma ani na Facebooku, ani na Messengerze". Inną kwestią natomiast jest dostrzeganie przez ludzi młodych tego, że nie każdej aplikacji w każdym okolicznościach możemy w pełni zaufać. Jeden z uczniów podzielił się z nami taką opinią: „Mam Telegram, ale on służy do komunikacji, kiedy Messenger nie jest wystarczająco bezpieczny. [...] Kiedy z tego mogą wyjść jakieś rzeczy niefajne, to wtedy lepiej jest korzystać z Telegrama, niż Messengera".

Badani wspominali o lęku przed utratą anonimowości czy ośmieszeniem się przed swoimi znajomymi, którzy ocenią pozostawiony przez nich w Internecie ślad (na przykład komentarz czy opublikowane zdjęcie). Młodzież ostrożnie podchodzi do dzielenia się swoim zdaniem na forum, a także uważnie selekcjonuje aplikacje i ich opcje, kiedy chce komunikować się ze swoimi dalszymi i bliższymi znajomymi. Współczesny nastolatek nie do każdego wyśle wiadomość głosową, na wideorozmowę połączy się jedynie z najlepszym przyjacielem, a opinię o obejrzanym tik toku (6) zamieści na zamkniętej grupie, a nie w komentarzu pod filmikiem.

Lęk przed utratą tego, co intymne, prywatne, przejawiał się w trakcie rozmów na temat autocenzury i kontrolowania tego, co i do kogo trafia za pośrednictwem komunikatorów i aplikacji.

Nastolatki a zagrożenia w internecie

Spędzając często ¼ doby w Internecie, młodzież jest narażona na różnego rodzaju naruszenia cyberbezpieczeństwa. Znane są im jednak mechanizmy, które mogą zapobiec atakom w sieci: ponad 40% uczniów twierdzi, że stosuje logowanie dwuetapowe, 38,1% deklaruje, że usuwa historię wyszukiwania, a 34,1% używa przeglądarek automatycznie chroniących prywatność. Jeśli chodzi o cyberprzemoc, to co piąty uczeń i uczennica deklarują, że doświadczyli przemocy w Internecie, ale co trzeci badany nie podejmuje żadnych działań, które mogłyby mu udzielić wsparcia w takiej sytuacji, włączając w to nawet rozmowę na ten temat z bliskimi (3).

Rodzice i opiekunowie mają średnio wyższy poziom poczucia zagrożenia dla prywatności niż ich dzieci. Dla prawie połowy rodziców przebadanych przez zespół NASK akceptowanie w mediach społecznościowych zaproszeń od osób nieznajomych to zachowanie ryzykowne. Tymczasem tego zdania jest jedynie 8,5% ich nastoletnich dzieci (3). To kolejny dowód na to, że osoby przyzwyczajone do funkcjonowania w przestrzeni internetowej nie dostrzegają tych samych zagrożeń, co starsze od nich pokolenie, których przedstawiciele założyli konta w mediach społecznościowych już w dorosłym życiu.

Rozwijanie kompetencji cyfrowych na miarę XXI wieku

Współczesny nastolatek przyjmuje inną postawę wobec korzystania z Internetu, bo nie pamięta czasów, zanim powszechnym stało się permanentne podłączenie do sieci. Skutkiem takiego stanu rzeczy jest zacieranie się granicy tego, co prywatne i tego, co publiczne oraz kształtowanie się zupełnie nowego podejścia wobec kwestii bezpieczeństwa. Współczesny nastolatek widzi inne zagrożenia, a pozbawiony wiedzy na temat przeciwdziałania tym zjawiskom, których są świadomi dorośli, może stać się ofiarą cyberprzestępstw.

Najważniejszą kwestią jest to, że uczniowie nie traktują świata online jako przestrzeni odrębnej od tej offline. Swobodne poruszanie się w obrębie narzędzi komunikacji zapośredniczonej odwraca uwagę najmłodszych od konieczności troski o podstawowe zasady bezpieczeństwa w sieci. Można zatem zastanawiać się, czy w polskiej szkole poświęca się odpowiednią uwagę tematowi komunikacji internetowej oraz, czy o bezpieczeństwie w sieci rozmawia się z dziećmi i młodzieżą w zrozumiałych dla nich kontekstach. Warto wziąć pod uwagę pokoleniowe różnice w postrzeganiu rzeczywistości i pod tym kątem dostosowywać program nauczania.

To, że młodzi ludzie korzystają z pewnych udogodnień XXI wieku instynktownie, nie oznacza, że robią to świadomie. Zadania nauczycieli i rodziców w tej kwestii powinny zatem wykraczać poza edukowanie na temat bezpiecznego korzystania z Internetu. Rozwijanie kompetencji cyfrowych i medialnych współczesnych dzieci i nastolatków wymaga od

dorosłych próby zrozumienia ich podejścia do funkcjonowania w świecie online poprzez wejście do ich świata oraz zaakceptowania zmian, które niosą ze sobą nowe mechanizmy komunikowania w Internecie.

Przypisy:

(1) Digital 2022, https://datareportal.com/reports/digital-2022-global-overview-report [7.12.2022].

(2) Rowicka M., Bujalski M., Raport z badania: „Brzdąc w sieci – zjawisko korzystania z urządzeń mobilnych przez dzieci w wieku 0-6 lat", https://twojasprawa.org.pl/file/e5f1f74a-0b05-11ec-abb0-0022480e68c2 [7.12.2022].

(3) *NASTOLATKI 3.0, Raport z ogólnopolskiego badania uczniów*, https://thinkstat.pl/publikacje/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-2021-r [7.12.2022].

(4)Twenge J.M., iGene. *Dlaczego dzieciaki dorastające w sieci są mniej zbuntowane, bardziej tolerancyjne, mniej szczęśliwe i zupełnie nie przygotowane do dorosłości i co to znaczy dla wszystkich*, Sopot 2019.

(5) Snapchat – aplikacja mobilna do wysyłania filmów i zdjęć.

(6) Tik tok – potocznie: krótki materiał wideo opublikowany w aplikacji mobilnej TikTok.

.

Zuzanna Czachorek
studentka nowych mediów w komunikacji i absolwentka dziennikarstwa i komunikacji społecznej na WNPiD UAM. Interesuje się nowymi mediami oraz marketingiem internetowym.
kontakt: zuzanna.czachorek@gmail.com

System ochrony informacji niejawnych w Polsce. Wybrane zagadnienia

W ramach współczesnej rzeczywistości społeczno - politycznej tematyka związana z tworzeniem, udostępnianiem i przepływem informacji odgrywa niezwykle istotną rolę m.in. w kontekście bezpieczeństwa państwa. Bezpieczeństwo informacyjne stanowi jeden z obszarów bezpieczeństwa w ujęciu przedmiotowym. Analizując pozycję państwa, możliwości i ograniczenia jego działania nie sposób pominąć kwestię bezpieczeństwa informacji, w tym informacji niejawnych.

Celem niniejszego artykułu jest syntetyczne przybliżenie systemu ochrony informacji niejawnych w Polsce. Z uwagi na złożoność i wieloaspektowość podjętego zagadnienia, jak również ograniczone ramy szkicu, w szczególności uwzględniono wymiar normatywny wspomnianego systemu. W trakcie badań podstawowe znaczenie miało podejście instytucjonalno-prawne. Uwzględniając bazę źródłową należy wskazać, iż dla treści artykułu szczególne znaczenie miała ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Zgodnie z Konstytucją RP z 1997 r., „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji" (art. 54 ust. 1). Ustawa zasadnicza w części wolności i prawa polityczne przewiduje również prawo do informacji publicznej. „Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu" (art. 61 ust. 1-2).

Nie wszystkie jednak kategorie informacji mogą być powszechnie dostępne w ramach prawa do informacji publicznej – niektóre spośród nich podlegają specjalnej ochronie i są udostępniane wyłącznie uprawnionym osobom. Wynika to m.in. z konieczności ochrony porządku publicznego i bezpieczeństwa państwa. W tym miejscu należy dodać, iż obowiązujące prawo przewiduje ściśle określone przesłanki, kiedy może dojść do wskazanej sytuacji. Jak stanowi Konstytucja RP, ograniczenie prawa do informacji publicznej „może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa" (art. 61 ust. 3).

Tak więc na gruncie wyżej przytoczonych przepisów ustrojodawca ustanowił prawo do informacji publicznej. Podstawowym aktem prawnym w tym zakresie jest ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. 2022, poz. 902). Zgodnie z art. 1 wskazanego aktu normatywnego, „każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie" (art. 1 ust. 1). Co istotne, dostęp do pewnych kategorii informacji jest ograniczony. „Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych" (art. 5 ust. 1). W dalszej części artykułu skupiono się na jednej z przytoczonych kategorii, tj. na ochronie informacji niejawnych.

Zgodnie z definicją legalną zawartą w stosownej ustawie, informacje niejawne charakteryzują się tym, iż ich „nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposo-

bu ich wyrażania" (art. 1 ust. 1). Z uwagi na znaczenie informacji niejawnych dla bezpieczeństwa państwa, mogą być one udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych (art. 4 ust. 1). Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych przewiduje następująca klasyfikację przedmiotowych informacji (art. 5):

- „ściśle tajne" – jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla RP m.in. przez to, że: zagrozi niepodległości, suwerenności lub integralności terytorialnej RP; zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu RP; zagrozi sojuszom lub pozycji międzynarodowej RP;
- „tajne" – jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla RP m.in. przez to, że: uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP; pogorszy stosunki RP z innymi państwami lub organizacjami międzynarodowymi; zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych RP;
- „poufne" – jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla RP m.in. przez to, że: utrudni prowadzenie bieżącej polityki zagranicznej RP; utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych RP; zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
- „zastrzeżone" – jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP.

Informacje niejawne, którym nadano określoną klauzulę tajności mogą być udostępnione wyłącznie osobie uprawnionej, muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, jak również muszą być chronione, odpowiednio do nadanej klauzuli tajności (art. 8).

Nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych należy do właściwości Agencji Bezpieczeństwa Wewnętrznego (ABW) i Służby Kontrwywiadu Wojskowego (SKW). W ramach tak określonego zakresu kompetencji wskazane służby (art. 10 ust. 1):

- prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
- realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
- prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;
- zapewniają ochronę informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;
- prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych (art. 14 ust. 1-2). Ustawa zawiera wymagania, które musi spełniać osoba zatrudniona na rozważanym stanowisku (pełnomocnik ochrony musi m.in. posiadać obywatelstwo polskie i wykształcenie wyższe).

Zgodnie z ustawą, dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej (a więc o klauzuli „tajne" lub „ściśle tajne") może nastąpić po uzyskaniu poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych (art. 21 ust. 1). Z kolei dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organi-

zacyjnej (jeżeli dana osoba nie posiada poświadczenia bezpieczeństwa) oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych (art. 21 ust. 4). Tym samym w przypadku informacji niejawnych o najniższej klauzuli tajności („zastrzeżone") nie jest wymagane posiadanie poświadczenia bezpieczeństwa (wystarcza pisemne upoważnienie kierownika jednostki organizacyjnej).

Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z: przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie; zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby; sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia (art. 19 ust. 1). Szkolenie (w zależności od podmiotów, do których jest skierowane) przeprowadzają odpowiednio: ABW, SKW lub pełnomocnik ochrony.

Jak wspomniano wcześniej, dostęp do informacji niejawnych o klauzuli „poufne" lub wyższej wymaga posiadania poświadczenia bezpieczeństwa. W celu jego uzyskania dana osoba przechodzi zwykłe lub poszerzone postępowanie sprawdzające.

Zwykłe postępowanie sprawdzające przeprowadza się, co do zasady, przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne". Z kolei poszerzone postępowanie sprawdzające przeprowadza się m.in. przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" (art. 22 ust. 1). Celem postępowania jest sprawdzenie, czy dana osoba daje rękojmię zachowania tajemnicy, a zatem ustalana jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem. Procedura rozpoczyna się od wypełnienia przez kandydata ankiety bezpieczeństwa osobowego, której wzór stanowi załącznik do ustawy z 2010 r. o ochronie informacji niejawnych. Postępowanie sprawdzające może zakończyć się jednym z trzech rozstrzygnięć, tj.: wydaniem poświadczenia bezpieczeństwa, odmową wydania poświadczenia bezpieczeństwa, umorzeniem (art. 28). W sytuacji, gdy postępowanie sprawdzające zakończy się wydaniem poświadczenia bezpieczeństwa, dana osoba uzyskuje dostęp do określonej kategorii informacji niejawnych (oczywiście jeśli spełnia również pozostałe, wcześniej zasygnalizowane warunki).

Podsumowując, określone kategorie informacji z uwagi na ich znaczenie dla bezpieczeństwa państwa nie mogą być ujawniane w ramach konstytucyjnie ustanowionego prawa do informacji publicznej. Wskazane prawo jest ograniczone m.in. poprzez system ochrony informacji niejawnych, w ramach którego obowiązują przepisy prawa (przede wszystkim stosowna ustawa i akty wykonawcze do ustawy), funkcjonują odpowiednie instytucje (ABW, SKW, pełnomocnicy do spraw ochrony informacji niejawnych i piony ochrony), jak również są stosowane środki bezpieczeństwa fizycznego. Wszystkie działania powinny być podejmowane przy zachowaniu najwyższej staranności, aby nie dochodziło do ujawniania tytułowej kategorii informacji osobom nieuprawnionym. Prawidłowo działający system ochrony informacji niejawnych ma bardzo duże znaczenie w kontekście bezpieczeństwa państwa.

Bibliografia:

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. 1997, Nr 78, poz. 483, z późn. zm.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, t.j. Dz. U. 2022, poz. 902.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. 2019, poz. 742, z późn. zm.

Jak wspomniano wcześniej, dostęp do informacji niejawnych o klauzuli „poufne" lub wyższej wymaga posiadania poświadczenia bezpieczeństwa. W celu jego uzyskania dana osoba przechodzi zwykłe lub poszerzone postępowanie sprawdzające.

Marcin Rachwał
profesor uczelni w Zakładzie Teorii Polityki Wydziału Nauk Politycznych i Dziennikarstwa UAM w Poznaniu. Członek Grupy Badawczej „Inicjatywa Helwecka", Ośrodka Badań i Edukacji Europejskiej, członek redakcji „Przeglądu Politologicznego", prezes Polskiego Towarzystwa Nauk Politycznych o/Poznań, członek Komisji Rewizyjnej przy Zarządzie Głównym PTNP. Recenzent w następujących czasopismach naukowych: „Przegląd Europejski", „Środkowoeuropejskie Studia Polityczne", „Political Preferences", „Public Policy and Economic Development".

PERSPEKTYWA WSPÓLNEGO CELU I BUDOWANIA ZESPOŁU W OPARCIU O AUTORSKI PLAN ROZWOJU. DETERMINACJA, PRACA NAS SOBĄ, SYSTEMATYCZNOŚĆ POŁĄCZONA Z KREATYWNOŚCIĄ

Rozmowa Mikołaja Tomaszyka z Konradem Glejem

Do rozmowy na temat cyberbezpieczeństwa, bezpieczeństwa w mieście zaprosiłem Konrada Glejta, absolwenta studiów licencjackich na kierunku bezpieczeństwo narodowe prowadzonych na WNPiD UAM. Konrad Glejt w trakcie studiów, w szkole policealnej uzyskał zawód technika informatyki. Studia magisterskie z zarządzania odbył na Uniwersytecie Ekonomicznym w Poznaniu. Jest absolwentem cyberbezpieczeństwa w Polsko-Japońskiej Akademii Technik Komputerowych oraz zarządzania projektem informatycznym na Akademii Leona Koźmińskiego w Warszawie. Jest stałym współpracownikiem Zakładu Studiów nad Bezpieczeństwem WNPID UAM. Jego pierwszym miejscem pracy był dział IT w Polpharma S. A, aktualnie pracuje w Grupie ORLEN. Konrad swoje pasje rozwija jako ko szkoleniowiec i założyciel Cybear. Jest też youtuberem. Prywatnie zajmuje się nagłaśnianiem imprez okolicznościowych, jest świetnym konferansjerem. Rozmowa została przeprowadzona w okresie przedświątecznym.

[MT:] Cześć Konradzie, trochę czasu minęło odkąd zakończyłeś przygodę z WNPiD. W ich trakcie odbyłeś dodatkowe praktyki zawodowe w Stowarzyszeniu Metropolia Poznań, wiem, że mile wspominasz Poznań i często jesteś naszym gościem. Konradzie, jesteś absolwentem WNPID UAM, studiów licencjackich na kierunku bezpieczeństwo narodowe, proszę powiedz jakie umiejętności i jaka wiedza są tobie przydatne przy wykonywaniu aktualnych zadań zawodowych?

[KG:] Studia to nie tylko proces edukacji, ale przede wszystkim rozwoju osobowego i poznawania swoich predyspozycji do funkcjonowania w dorosłym świecie. To również czas, w którym można zaobserwować różne dziedziny nauki z perspektywy teoretycznej i praktycznej, ale szczególnie istotny jest wymiar naukowy, który pobudzając procesy myślowe prowadzi do analitycznego spojrzenia na rzeczywistość. I właśnie takie umiejętności rozpatruję jako najcenniejsze i najbardziej przydatne na drodze zawodowej.

[MT:] A jak dzisiaj, po kilku latach wspominasz studia na WNPiD UAM? Jakieś wspomnienia szczególnie zapadły Tobie w pamięci?

[KG:] Duża liczba zajęć na uczelni determinowała dużą ilość spędzonego tam czasu. To z pewnością był dobry okres, który zaowocował wieloma przyjaźniami trwającymi po dziś. Korytarze budynku na pewno pamiętają ten przedegzaminacyjny stres, wymieniane notatki, opracowywane wystąpienia. Siłą rzeczy znacząca część życia studenckiego miała miejsce „po godzinach" zajęć i to tam powstało najwięcej wspomnień. Część studentów starała się dać od siebie coś więcej, dlatego warto wspomnieć o atmosferze przed konferencjami naukowymi organizowanymi na wydziale, w które my jako studenci byliśmy zaangażowani. Po pierwsze były to cenne doświadczenia z perspektywy zarządzania, a po drugie można było usłyszeć o najnowszych obserwacjach wynikających z badań przeprowadzonych przez doświadczonych pracowników dydaktycznych różnych uczelni w Polsce. Takie konferencje i seminaria naukowe generowały w nas troskę, aby nie zawiodły kwestie techniczne; aby prelegenci otrzymali swoje pakiety powitalne; aby po wydarzeniu powstała notatka, a na końcu zbiorowa publikacja naukowa.
Teraz śmiało mogę powiedzieć, że te doświadczenia bardzo mocno i pozytywnie przekładają się na moje funkcjonowanie w ramach korporacji. Dzięki organizacji wydarzeń uczelnianych patrzy się szerzej na perspektywę wspólnego celu, a nie jedynie przez pryzmat indywidualnego sukcesu.

[MT:] Od nowego roku akademickiego przygotowaliśmy dwie nowe specjalności: bezpieczeństwo miejskie oraz cyberbezpieczeństwo, zaś na studiach licencjackich analityk bezpieczeństwa, jakie Twoim zdaniem kompetencje zawodowe, społeczne, personalne powinny cechować kandydatów na studentów tych specjalności?

Dodatkowo rynek premiuje osoby sprawnie funkcjonujące w środowisku cyfrowym i wykorzystujących jego narzędzia.

[KG:] Przede wszystkim gratuluję inicjatywy oraz próby odpowiedzi uczelni na zapotrzebowanie rynku. Cieszę się, że na etapie budowania programu tych studiów mieliśmy okazję wymienić opinie na temat oferowanych przedmiotów.

Sytuacja gospodarcza i polityczna zmuszają do większej elastyczności i sprofilowania się na aktualne oczekiwania słuchaczy studiów. Jednak z drugiej strony należy pamiętać, że uniwersytet nie jest szkołą zawodową i jego zadaniem nie jest bezpośrednie przygotowanie do konkretnej profesji. Uczelni powinna uczyć jak zrobić wędkę, a nie są dawać lub nawet od razu wręczać złowioną rybę. Dlatego to co wydaje się kluczowe dla odnalezienia się na rynku pracy to umiejętność wyszukiwania prawdziwych informacji, zdolność do samodyscypliny i uczenia się, ciekawość świata oraz posiadanie twardych umiejętności popartych odpowiednią wrażliwością i kulturą wobec drugiego człowieka. Niektórzy nazywają to „soft skills", ale bycia „dla kogoś" nie można nazwać umiejętnością i nauczyć się na jakimś kursie. Wydaje się, że zwinne łączenie umiejętności zawodowych poparte rozbudowanymi cechami współpracy będą kluczem do osiągania stawianych przez pracodawców celów.

[MT:] No tak, twarde umiejętności, weryfikowanie źródeł wiedzy, samodyscyplina czy to są te cechy pożądanych pracowników w sektorze IT i nie tylko? Przecież obserwujesz rynek pracy już z innej, niestudenckiej perspektywy, czy możesz powiedzieć jacy specjaliści będą pożądani za 4, 5 lat?

[KG:] Młodzi adepci rynku pracy mają paradoksalnie ułatwione zadanie. Informacje oraz wiedza są na wyciągnięcie ręki, bo włączając YouTube można zostać ekspertem w dowolnej dziedzinie; bezpłatnie (sic!). Dodatkowo rynek premiuje osoby sprawnie funkcjonujące w środowisku cyfrowym i wykorzystujących jego narzędzia. Kiedyś wpisywano w CV pozycję „znajomość pakietu Office"; dzisiaj bierze się to za pewnik i wręcz wrodzoną umiejętność. Jak będzie za kilka lat? Trudno jest przewidzieć, bo rynek szybko się zmienia, natomiast mogą zyskiwać kompetencje analityczne i krytycznego myślenia. Celowo nie wskazuję tu na programowanie, media społecznościowe, czy inżynierię, bo to coś co jest w zasięgu, jeśli posada się wystarczającą determinację. Natomiast wartość stanowi to, że na bazie doświadczenia, zebranych danych oraz ich interpretacji będziemy potrafili wysnuć adekwatne wnioski i podjąć decyzję, a na końcu wzięcie za nią odpowiedzialności. Ważna wydaje się samodzielność w działaniu. Być może za jakiś czas wielu pracowników będzie zmuszonych do zmiany formy świadczenia swoich usług. Mam tu na myśli uruchamianie swojej działalności gospodarczej jako formy bycia np. konsultantem dla wielu przedsiębiorstw. Organizacje za jakiś czas mogą szukać optymalizacji kosztów, a co za tym idzie nie tyle redukcji etatów co lepszego wykorzystania potencjału swoich pracowników. Pracujesz dla nas efektywnie 25 godzin, więc za tyle chcemy tobie płacić. Dodatkowo pracodawca może oczekiwać, że pracownik będzie innowacyjny, czyli będzie starał się rozwijać organizację, dla której świadczy usługi. Cenione mogą być zmiany upraszczające procesy, optymalizacja działania, a także cyfryzacja czynności. Coraz większy obszar rynku adresuje AI (artificial intelligence, sztuczna inteligencja), której modele wciąż się trenują, poprawiają, ale dalej nie są doskonałe. Czy należy się bać tego, że programista zostanie zastąpiony przez komendę „napisz dla mnie program na kalkulator w języku JAVA"? I tak i nie, bo ktoś musi sprawdzić czy AI nie kłamie, bo ma do tego tendencje, gdy jest w procesie uczenia się zatruwana niewłaściwymi danymi (data poisoning).

[MT:] Zaserwowałeś nam garść kompetencji, które w społeczeństwie postmodernistycznym są zagrożone. Z drugiej strony, mogą być źródłem nowej zmiany – nie zawsze zagrażającej temu co znamy. Dodałbym zatem, że ważna jest gotowość do zmiany i brak lęku przed nowościami, otwartość na nie. Dzisiaj jesteś nie tylko pracownikiem Grupy ORLEN, ale również zostałeś YouTuberem, o czym i gdzie komunikujesz w sieci? Dlaczego wybrałeś dla siebie taką rolę?

[KG:] YouTube to tylko medium do przekazywania informacji, tak samo jak książki, gazety, ulotki, artykuły. Treści mogą być dla kogoś wartościowe lub nie. Staram się publikować filmy, które mogą coś wnieść do życia odbiorców. Moim celem jest to, aby uświadamiać o zagrożeniach w sieci i o tym jak skutecznie bronić się przed atakami. Na takiej aktywności nie zarabia się pieniędzy i jest ona wykonywana pro publico bono. Wychodzę z założenia, że wiedza o bezpieczeństwie powinna być bezpłatna. Filmy ukazują się na kanale partnera, czyli @VIDA-PL. Cykl nazwaliśmy CyberWtorki i mamy za sobą ponad 20 odcinków tej serii. Staramy się zachować przystępny język z uwagi na to, że słuchacze mogą być na różnym stopniu zaawansowania technologicznego. Współcześnie wielu z nas staje się twórcą cyfrowych treści, jest to łatwe, a bariera wejścia jest bardzo niska. Natomiast w procesie tworzenia materiałów zależało nam na zachowaniu wysokiej jakości merytoryki oraz nagrania warstwy audio i wideo. Pozostaje mi zaprosić do śledzenia aktywności mojej osobistej marki cybear oraz partnera - VIDA.

[MT:] A które z Twoich filmów spotykają się z największym zainteresowaniem internautów? Czy dzięki Twemu kanałowi nawiązałeś nowe relacje, nowe zlecenia?

[KG} Statystki wskazują, że słuchacze poszukują treści, które są im najbliższe, czyli realnym problemom i wyzwaniom bezpieczeństwa. Dla przykładu – jak zabezpieczyć smartfon, komputer, sieć Wi-Fi, a także o tym jak chroniona jest bankowość elektroniczna. Część z filmów jest skierowana do przedsiębiorstw, bo to one są najczęściej atakowane przez cyberprzestępców. Dlatego zabezpieczenia w firmach powinny być na najwyższym poziomie. Firmy są w stanie dostarczyć atakującym więcej pieniędzy niż osoba prywatna. W ostatnich latach dostrzegamy rosnące koszty obsługi incydentów spowodowanych złośliwym oprogramowaniem ransomware, które ma na celu zaszyfrowanie danych i zażądanie okupu za ich odszyfrowanie. W Polsce mamy wciąż sporo do zrobienia w obszarze edukacji o cyberspołeczeństwie. Raport CERT Polska dt. zagrożeń w 2021 roku wskazuje, że

W Polsce mamy wciąż sporo do zrobienia w obszarze edukacji o cyberspołeczeństwie. Raport CERT Polska dt. zagrożeń w 2021 roku wskazuje, że 77% udanych cyberataków pochodziło z zastosowania socjotechniki, czyli wykorzystania słabości człowieka do ulegania różnego rodzaju przynętom.

77% udanych cyberataków pochodziło z zastosowania socjotechniki, czyli wykorzystania słabości człowieka do ulegania różnego rodzaju przynętom. Ucząc użytkowników sieci o możliwych rodzajach ataków zmniejszamy prawdopodobieństwo przedostania się cyberprzestępców od naszej prywatności albo organizacji.

[MT:] Na koniec zapytam o kwestie bardziej osobiste, powiedz mi proszę jakich umiejętności, kompetencji, zdolności oczekiwałbyś jako przyszły pracodawca?

[KG:] Inicjatywa – czyli przyjście z pomysłem i planem na jego realizację. Cyberbezpieczeństwo jako sfera zawodowa nie jest oczywista. Nie ma czegoś takiego, że ktoś powie „jestem ekspertem i już". Na przestrzeni lat branża niesamowicie się rozrosła i ewoluowała na różne specjalności dziedzinowe. Ktoś zajmuje się bezpieczeństwem aplikacji, ktoś testami penetracyjnymi, ktoś badaniem podatności, ktoś zarządzaniem tożsamością, a ktoś bezpieczeństwem sieci. Z perspektywy pracodawcy im bardziej różnorodny zespół tym większe są zdolności do zbudowania wielowarstwowego bezpieczeństwa firmy (defense in depth). Jedną z kluczowych cech będzie specjalizacja i umiejętności określenia się co jest moim atutem. Co nie znaczy, że taki ekspert ma być zwolniony z zainteresowania pozostałymi gałęziami branży, wręcz przeciwnie. Pracownik, który będzie się rozwijał poza godzinami swoich obowiązków zawodowych, a następnie na bazie obserwacji zaproponuje zmiany mające na celu poprawę bezpieczeństwa organizacji będzie ceniony przez przełożonych.

[MT:] A jakich cech u przyszłych pracowników unikałbyś?

[KG:] Trudno jednoznacznie wskazać co jest „złe" a co „dobre". Wszystko zależy od obowiązków i okoliczności. Natomiast trzeba pamiętać, że bezpieczeństwo to gra zespołowa. W obliczu sytuacji kryzysowej, którą jest np. trwający cyberatak mający na celu przerwanie ciągłości działania nie można pozwolić sobie na egoizm, albo forsowanie indywidualnych pomysłów nie licząc się z resztą

zespołu. Nie ma tu również miejsca na jakieś osobiste konflikty. To samo tyczy się zleconych zadań, jeśli w obliczu cyberataku powierza się komuś określone zadanie to druga strona liczy na to, że ten obszar zostanie rzetelnie zrealizowany, a następnie zakomunikowany status jego realizacji. Tu również należy wskazać zdolność do odporności na stres i presję czasu oraz np. oczekiwania zarządu spółki. Często jest tak, że w cyberbezpieczeństwie potrzeba umiejętności bycia liderem. To nie znaczy bycia najlepszym ekspertem, tylko wskazania kierunku prac i umiejętności dobrania takich kompetencji, które sprawdzą się w danej sytuacji.

[MT:] Konradzie, uprzejmie dziękuję za inspirującą rozmowę. Życzę sukcesów zawodowych, wielu subskrypcji i satysfakcji z tego co robisz. Do zobaczenia w Poznaniu!

Konrad Glejt
Absolwent najlepszych uczelni w Poznaniu i Warszawie. Pasjonat zagadnień cyberbezpieczeństwa. Zawodowo specjalizuje się w zagadnieniach cloud security, systemach operacyjnych Windows oraz w działaniach edukacyjnych w zakresie zagrożeń w sieci i sposobów ochrony przed nimi. Doświadczenie zawodowe zdobywał w największej polskiej firmie farmaceutycznej oraz spółce Skarbu Państwa z sektora energetycznego. Zabezpieczał infrastrukturę krytyczną państwa realizując wytyczne i rekomendacje instytucji nadzorujących. Tworzy swoją markę pod nazwą cybear. Jedno z ulubionych powiedzeń branżowych to – „Nie jest kwestią czy zostaniesz zhakowany, ale kiedy to się stanie". Prywatnie miłośnik podróży oraz aktywnej formy spędzania czasu i dobrego sprzętu audio.

prof. UAM dr hab. Mikołaj Tomaszyk
Redaktor naczelny
„Nowiny Nauki o Bezpieczeństwie"

Wykorzystanie technologii informatycznych w praktyce administracyjnej na przykładzie ZTM (1)

Technologia informatyczna (IT) kategoria, zawierająca wiele obszarów, w tym informatykę, telekomunikację oraz narzędzia i techniki umożliwiające przetwarzanie informacji. IT pozwala m.in. na gromadzenie i dystrybuowanie informacji. Artykuł krótko charakteryzuje wybrane rozwiązania informatyczne zastosowane w jednostce budżetowej ZTM Poznań.

Informatyzacja administracji

Trudno sobie wyobrazić dziedzinę ludzkiej aktywności, bez zastosowania technologii informatycznych. Jesteśmy społeczeństwem informacyjnym. Popyt na rozwiązania informatyczne jest coraz większy. W administracji IT to narzędzie do zarządzania i interakcji z klientem. Informatyzacja wypiera tradycyjne rozwiązania. Stosowane w Zarządzie Transportu Miejskiego w Poznaniu, technologie pozwalają na zautomatyzowanie procesów, usprawnienie pracy pracownikom a dla korzystających z usług urzędu interesantów, uproszczenie i skrócenie dystansu w kontaktach. Zwiększamy dostępność urzędu, bez względu na miejsce i czas korzystania z naszych usług, minimalizujemy koszty i czas świadczenia usługi (2).

ZTM Poznań [dalej: jednostka] wykonując szereg zadań statutowych, pozyskuje różnorodne dane, które muszą być szczególnie chronione. Dlatego do zagadnień związanych z cyberbezpieczeństwem przykładamy ogromną wagę. Rozbudowujemy infrastrukturę, kompatybilność sieci i dbamy o standardy bezpieczeństwa sieciowego. Wyposażenie urzędu w nowe technologie informatyczne obwarowane jest spełnieniem szeregu przesłanek organizacyjnych, budżetowych i zamówień publicznych. Działania te mają przyczynić się do stworzenia warunków, w których komunikacja z urzędem będzie przyjazna a załatwienie sprawy nie będzie oznaczało przymus osobistego stawiennictwa w jednostce. Wzrastające kompetencje cyfrowe mieszkanek i mieszkańców Poznania, rozwijający się system tożsamości cyfrowej, funkcjonujące metody identyfikacji takie jak profil zaufany, systemy bankowe, e-dowód, aplikacja mobilna m0bywatel, zwiększają możliwości załatwienia spraw urzędowych on-line. Identyfikujemy przy tym szereg problemów, które staramy się rozwiązać. Brak pełnej interoperacyjności, powielanie gromadzonych danych, niejednolita identyfikacja zasobów, brak modelu współpracy pomiędzy instytucjami administracji centralnej z JST oraz niskie kompetencje cyfrowe części obywateli, są wymieniane przez wielu pracowników administracji publicznej.

ZTM wybrane rozwiązania

ZTM przetwarza potężną ilość informacji. Wykorzystuje do tego systemy informatyczne. Jednostka zapewnia kontakt poprzez e-usługę, telefon i osobistą wizytę w urzędzie. Korzysta z nowoczesnych kanałów komunikacyjnych np. Biuletyn Informacji Publicznej (BIP). Umożliwia udział w konsultacjach publicznych, zapewnia dostęp do informacji publicznych. Prezentuje jednolite podejście do załatwiania spraw bez względu na drogę wpływu. Wdraża rozwiązania organizacyjne i technologiczne, by zapewnić jakość i szybkość świadczonych usług, przy jednoczesnej dbałości o bezpieczeństwo w cyberprzestrzeni.

Platforma internetowa ZTM zawiera informacje dla użytkowników, formularze umożliwiające składanie on-line wniosków, skarg, reklamacji, przyjmowanie płatności elektronicznych. Urząd zastosował rozwiązania organizacyjne zapewniające elektroniczny obieg dokumentów, system wewnętrznego przepływu informacji, wykorzystania baz danych, digitalizację zasobów informatycznych i dokumentów.

Kryterium podmiotowe to korzyści z e-administracji dla obywateli w kontekście relacji z urzędem (3). Większa dostępność informacji dla obywateli, które mogą wykorzystać w celach im niezbędnych. Dane kompletne, aktualne, upubliczniane w sposób umożliwiający ich odczytanie bez ograniczeń (4). E-administracja świadczy usługi na czterech poziomach:

I. informacji on-line – wyszukanie informacji o urzędzie oraz usługach na stronie internetowej,
II. interakcji jednokierunkowej –wyszukanie informacji, pobrania formularzy ze strony internetowej,
III. interakcji dwukierunkowej – wyszukanie informacji, pobranie i odesłania wypełnionych formularzy przez Internet
IV. transakcji – pełna obsługa procesu tj. dokonania wszystkich czynności niezbędnych do załatwienia sprawy urzędowej drogą elektroniczną (5).

Komunikacja jednostronna

W myśl Ustawy o dostępie do informacji publicznej, istnieje obowiązek prowadzenia urzędowego publikatora teleinformatycznego BIP. Strona ułatwia dostęp do informacji o rozstrzygnięciach jednostki, sposobach załatwiania spraw, naborach na wolne stanowiska pracy.

Komunikacja dwustronna

Narzędzie dla interesanta pozwalające na otrzymanie informacji z jednostki i wysłanie wiadomość do urzędu, w oparciu o funkcjonalności takie jak podpis kwalifikowany, profil zaufany (6) oraz ePUAP (Elektronicznej Platformy Usług Administracji Publicznej). Obywatele mają możliwość elektronicznego załatwienia spraw bez konieczności przybycia do siedziby. Zwiększamy dostępność, minimalizujemy potrzebę osobistego kontaktu z urzędem. Ograniczenie to brak konta na platformie ePUAP. W zależności od rodzaju sprawy urząd wprowadził określone wymagania identyfikacji, których spełnienie otwiera możliwość procedowania.

System PEKA, umożliwia pasażerom załatwienie spraw związanych z wyrobieniem i użytkowaniem karty PEKA drogą elektroniczną. Uwzględniając możliwości jednostki podążamy za oczekiwaniami klientów i wdrażamy nowe lub aktualizujemy istniejące rozwiązania. Aktualnie opracowywane jest rozwiązanie polegające na unowocześnieniu systemu PEKA. Od 3 listopada br., bilet okresowy kupowany on-line nie musi być transferowany w pojeździe, a ulgę studencką zapiszemy automatycznie (7). Wezwanie do zapłaty za brak ważnego biletu również uiścimy drogą elektroniczną, w taki sam sposób wniesiemy reklamację, czy uzyskamy informację na temat ciążącego zadłużenia. Aby utrzymać ciągłość działania jednostki, wytypowano sytuacje, w których pracownik może korzystać z zasobów zdalnie, co było pomocne w czasie pandemii, kiedy urząd zrezygnował z osobistych wizyt klientów, a sprawy nadal procedowano. Technologie informatyczne zastosowane w jednostce:

1. portal ZTM on-line o charakterze otwartym, w ramach którego udostępniane są informacje oraz usługi w zakresie zadań statutowych, prezentacja rozkładów jazdy, aktualności i komunikatów o funkcjonowaniu ptz, rozwiązania związane z obsługa klientów, kontrolą biletów, ochroną danych osobowych,
2. zaawansowany technologicznie system PEKA umożliwia obsługę systemu sprzedażowego, zasilenie biletu przez Internet, korzystanie z tPortmonetki, z Park&Ride, szereg operacji na koncie użytkownika, integracja różnych form przemieszczania się,
3. wdrożenie płatności zbliżeniowych w pojazdach, można kupić bilety jednorazowe przy użyciu zbliżeniowej karty płatniczej, smartfonu obsługującego technologię HCE lub NFC w Poznaniu i aglomeracji,
4. Wirtualny Monitor informacje o odjazdach autobusów i tramwajów z wybranego przystanku w czasie rzeczywistym,
5. klienci mogą kontaktować się z urzędem drogą elektroniczną, umówić się na spotkanie z dyrektorem ZTM on-line,
6. wdrożenie systemu wideokonferencji umożliwienia bezpieczne spotkania on-line w czasie pandemii,
7. wzory dokumentów dla interesantów, do pobrania wypełnienia i wysłania zwrotnie,
8. indywidualne numery rachunków

bankowych przypisane do opłat dodatkowych,
9. udostępniamy treści dla Dewelopera umożliwiające podmiotom zainteresowanym tworzenie oprogramowania na potrzeby ptz,
10. klienci mogą ocenić pracę ZTM poprzez wypełnienie elektronicznej ankiety oceny jakości świadczonych usług (8).

Funkcjonują aplikacje: Smart City Poznań, tu sprawdzimy aktualne informacje o pracach drogowych i awariach; jakdojade.pl, rozkłady jazdy, zidentyfikujemy najkorzystniejsze połączenie; Kiedy Pojadę – PEKA, KiedyBus, take&drive pomocne w planowaniu podróży. Przy zakupie biletów jednorazowych pasażerowie mogą skorzystać z aplikacji mobilnych (9).

Zakończenie

Rozwój technologii informatycznych w urzędzie skorelowany jest z możliwościami budżetowymi. Aktualnie sytuacja jest trudna, dlatego implementacja rozwiązań informatycznych nieco spowolniła. Oprócz korzyści z informatyzacji urzędy ponoszą koszty tego procesu zakup sprzętu, oprogramowania, serwis, digitalizacja danych, szkolenia pracowników i zmiany w sposobie obiegu dokumentów, modernizacja systemu, aktualizacja strony itp. Mimo to, nie ma wątpliwości, że technologie informatyczne w administracji poprawiają jakość życia obywateli, dostępność i szybkość procedowania spraw.

Przypisy:

(1) Zarząd Transportu Miejskiego w imieniu Miasta Poznania realizuje zadania organizatora ptz w rozumieniu ustawy o publicznym transporcie zbiorowym, https://www.ztm.poznan.pl/pl/o-ztm/, dostęp 10.12.2022.
(2) K. Celarek, *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego*, Warszawa 2013, s. 42 i n.
(3) W. Puzyna, *Wpływ technik informatycznych na funkcjonowanie administracj*i, w: A. Dębicka, M. Dmochowski, B. Kudrycka (red.), *Profesjonalizm w administracji publicznej*, Białystok 2004, s. 37.
(4) M. Sakowska-Baryła, *Standard prawny dla otwartych danych*, ITwA 2019, Nr 2, s. 40 i n.
(5) Środki komunikacji elektronicznej https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=%C5%9Arodki_komunikacji_elektronicznej, dostęp 10.12.2022.
(6) T. Rakoczy, „Profil zaufany ePUAP, Opracowania, Studia, Materiały Centrum Projektów Informatycznych" MSWiA, Zeszyt 1A/2011, https://docplayer.pl/2722147-Projekty-realizowane-przez-c-pi-mswia.html, dostęp 11.12.2022.
(7) Nowa era systemu PEKA – pierwsze korzyści już od października, https://www.ztm.poznan.pl/pl/aktualnosci/nowa-era-systemu-peka-pierwsze-korzysci-juz-od-pazdziernika, dostęp 11.12.2022.
(8) Oceń nas, https://www.ztm.poznan.pl/pl/kontakt/, dostęp 11.12.2022.
(9) Więcej informacji na https://www.ztm.poznan.pl/pl/cennik/sprzedaz-biletow/, dostęp 11.12.2022.

Bibliografia:

Celarek K., *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego*, Warszawa 2013, s. 42 i n.
https://mfiles.pl/pl/index.php/Technologia_informatyczna , dostęp 10.12.2022.

Janowski J., *Administracja elektroniczna. Kształtowanie się informatycznego prawa administracyjnego i elektronicznego postępowania administracyjnego w Polsce*, Warszawa 2009, s. 55-58.

Nowa era systemu PEKA – pierwsze korzyści już od października, https://www.

ztm.poznan.pl/pl/aktualnosci/nowa-era-systemu-peka-pierwsze-korzysci-juz-od-pazdziernika, dostęp 11.12.2022.

Oceń nas, https://www.ztm.poznan.pl/pl/kontakt/, dostęp 11.12.2022.

Puzyna W., *Wpływ technik informatycznych na funkcjonowanie administracji,* w: Dębicka A., Dmochowski M., Kudrycka B. (red.), *Profesjonalizm w administracji publicznej,* Białystok 2004, s. 37.

Rakoczy T., „Profil zaufany ePUAP, Opracowania, Studia, Materiały Centrum Projektów Informatycznych" MSWiA, Zeszyt 1A/2011, https://docplayer.pl/2722147-Projekty-realizowane-przez-c-pi-mswia.html, dostęp 11.12.2022.

Sakowska-Baryła M., *Standard prawny dla otwartych danych*, ITwA 2019, Nr 2, s. 40 i n.

Środki komunikacji elektronicznejhttps://epodrecznik.mc.gov.pl/mediawiki/index.php?title=%C5%9Arodki_komunikacji_elektronicznej, dostęp 10.12.2022.

Więcej informacji na https://www.ztm.poznan.pl/pl/cennik/sprzedaz-biletow/, dostęp 11.12.2022.

Zarząd Transportu Miejskiego w imieniu Miasta Poznania realizuje zadania organizatora ptz w rozumieniu ustawy o publicznym transporcie zbiorowym, https://www.ztm.poznan.pl/pl/o-ztm/, dostęp 10.12.2022.

mgr Małgorzata Pilichowska-Woźniak
Z jednostką budżetową realizującą zadania organizatora publicznego transportu zbiorowego związana od 2009 roku. Aktualnie na stanowisku Zastępcy Dyrektora. Od kilku lat współpracuje z Zakładem Studiów nad Bezpieczeństwem WNPiD UAM. Zainteresowania to publiczny transport zbiorowy, bezpieczeństwo i porządek publiczny, bezpieczeństwo i higiena pracy. Niniejszy tekst jest efektem Porozumienia pomiędzy ZTM Poznań a Wydziałem Nauk Politycznych i Dziennikarstwa UAM w Poznaniu zawartym pomiędzy jednostkami 26 listopada 2019 roku.
kontakt: M.Pilichowska-Wozniak@mail.ztm.poznan.pl

Rynek pracy dla specjalistów z dziedziny cyberbezpieczeństwa

Praca w dziedzinie cyberbezpieczeństwa to nowy trend, który stał się bardzo popularny i coraz częściej można odnaleźć ogłoszenia związane z ofertami pracy dla osób, które będą w stanie poradzić sobie z zapewnieniem bezpieczeństwa w sieci. Cyberbezpieczeństwo to bardzo szeroka dziedzina, zajmuje się m.in. ochroną danych oraz systemów wewnętrznych przed cyberatakami, które naruszają integralność, autentyczność i poufność przechowywanych danych

Ochrona zasobów informatycznych urzędów

Szybki rozwój informatyzacji, obejmujący także jednostki samorządu terytorialnego, w których w coraz większym stopniu wykorzystywane są systemy teleinformatyczne, niesie ze sobą zagrożenia związane z bezpieczeństwem informacji. Zagrożenia te można opisać za pomocą trzech podstawowych zagadnień składających się na bezpieczeństwo informacji, tj. utrata poufności, ograniczenie dostępności oraz naruszenie integralności informacji. Każde z nich może mieć charakter zdarzenia przypadkowego takiego jak awaria, błąd oprogramowania lub pomyłka ludzka. W ostatnich latach zauważono zmianę dotyczącą zagrożeń związanych z bezpieczeństwem informacji. Kiedyś dotyczyły głównie awarii sprzętu, zakłóceniach łączności, wirusów bądź błędów w oprogramowaniu. Obecnie stosowane są celowe ataki na systemy informatyczne. Łączą one w sobie wiele elementów technicznych oraz socjotechnik, często są prowadzone w sposób długotrwały. W przeszłości głównym celem takich ataków były osoby indywidualne, jednak dzisiaj są to przedsiębiorstwa i instytucje, które posiadają więcej środków finansowych oraz wrażliwych danych. Dlatego należy zwrócić szczególną uwagę na sposób zarządzania uprawnieniami w dostępie do plików oraz plików konfiguracyjnych urządzenia.

Perspektywy zawodowe

Od niedawna rynek pracy dla osób związanych z cyberbezpieczeństwem jest bogaty w oferty. Natomiast ze względu na charakterystykę branży, nie ma ona jeszcze ustandaryzowanych ról czy stanowisk, więc rozróżnia się je pomiędzy rolami ofensywnymi i defensywnymi. Na początku kariery można spróbować ubiegać się o stanowisko Cybersecurity Analyst, Security Engineer, bądź też Security Consultant. Każde ze stanowisk nieco różni się od siebie obszarem działania, natomiast praca w większości z nich będzie polegała na ochronie sprzętu firmowego, reagowaniu na incydenty związane z naruszaniem bezpieczeństwa, planowaniem strategii bezpieczeństwa firmy czy też celowym atakowaniem sieci komputerowej firmy, w celu odnalezienia jej słabych punktów.

Dzięki takiemu wykształceniu równie łatwo będzie nam szukać pracy w charakterze dyspozytora monitoringu miejskiego, czy też IODO (Inspektor ochrony danych osobowych). Dyspozytor obserwuje i rejestruje zdarzenia za pomocą urządzeń monitorujących. Celem jego pracy jest zapobieganie wykroczeniom, przestępstwom a także współpraca z pracownikami ochrony lub służbami takimi jak policja czy straż miejska do ujęcia sprawców oraz pozyskania materiału dowodowego w sprawie. System monitoringu miejskiego, dostęp do informacji pozyskanym dzięki niemu jest ważnym elementem bezpieczeństwa miejskiego. Praca dyspozytora pozwala także na szybsze podejmowanie decyzji w sprawie wysyłania powiadomień do straży pożarnej lub pogotowia ratunkowego w razie pożaru, nagłej utraty przytomności, kolizji i wypadków drogowych. Pracownik na tym stanowisku korzysta z kamer i elektronicznych systemów łączności. Obserwuje w czasie rzeczywistym na wyznaczonym obszarze: ludzi, pojazdy i zdarzenia. Momentem jego reakcji jest spostrzeżenie zdarzenia zakwalifikowanego takiego jak przedsta-

wiono powyżej. Rejestruje, rozpoznaje i analizuje, a następnie decyduje o podjęciu działań zgodnie z procedurami.

Inspektor ochrony danych osobowych to stanowisko, które musi zostać utworzone w każdym organie państwowym oraz w miejscach pracy, gdzie przetwarza się dane osobowe. Do obowiązków inspektorów należą m.in: informowanie o zakresie ochrony danych, monitorowanie przestrzegania prawa, sporządzanie oceny ryzyka naruszenia zapisów ustawy, doradzanie oraz rozwiązywanie kwestii prawnych. Miejscami pracy są urzędy, placówki ochrony zdrowia, prywatne firmy oraz instytucje państwowe.

Wymagania

Osobie poszukującej pracy w dziedzinie związanej z cyberbezpieczeństwem najczęściej będą stawiane dość duże wymagania, ponieważ będą jej powierzane odpowiedzialne zadania. Zazwyczaj poszukiwany kandydat powinien posiadać wiedzę z zakresu:

- Programowania: poznanie przynajmniej jednego języka programowania.
- Inżynierii odwrotnej (eng. Reverse engineering): jest to proces mający na celu zbadanie, w jaki sposób powstał program i na jakiej zasadzie funkcjonuje.
- Kryptografii: polega na konstruowaniu i analizowaniu protokołów, które uniemożliwiają osobom trzecim lub opinii publicznej czytanie prywatnych wiadomości.
- Uczenia maszynowego: jest to obszar sztucznej inteligencji, który obejmuje swoim zakresem automatycznie udoskonalające się algorytmy komputerowe.
- Technologii chmurowych: najczęściej jest to magazyn plików. Przez wgląd na popularność tego rozwiązania, przechowywane tam dane są bardzo atrakcyjnym celem do ataków.
- Znajomość języka angielskiego: większość dokumentacji napisana jest w języku angielskim, aby sobie z nimi poradzić i otrzymać interesujące nas informacje znajomość tego języka będzie niezbędna.
- Podstawowej wiedzy z zakresu służb, inspekcji i straży, ustroju samorządu terytorialnego i systemu zarządzania kryzysowego.

Zadania

Aby dokładniej nakreślić zakres obowiązków specjalisty ds. cyberbezpieczeństwa, poniżej wymieniono czynności wykonywane na równorzędnych stanowiskach w poszczególnych kategoriach.

- Sieci komputerowe: ochrona danych przed wyciekiem, ze szczególnym uwzględnieniem danych wrażliwych, sprawne reagowanie na nietypowe działania w sieci, np. filtrowanie adresów, dbałość o odpowiednią konfigurację sieci, oddzielanie fizyczne i logiczne podsieci.
- Urządzenia: zapewnienie nieprzerwanego działania urządzeń sieciowych w zakresie odporności na ataki z zewnątrz.
- Systemy: stworzenie scenariuszy na wypadek awarii, planowanie ciągłości działania, wyszukiwanie luk w zabezpieczeniach sieci, systemów, baz danych oraz urządzeń, a także regularna aktualizacja oprogramowania.
- Ochrona użytkowników: dobór uprawnień użytkowników wraz z dostępem do raportów z działania programów ich aktywności w sieci, edukowanie użytkowników o dobrych praktykach (niezapisywanie haseł na kartkach i zostawianie ich w widocznych miejscach, nierozpowszechnianie haseł osobom postronnym, niepodłączanie do urządzeń nośników pamięci nieznanego pochodzenia itd.) oraz dbałość o to aby hasła użytkowników były na bieżąco zmieniane w sposób taki, aby nie można było ich łatwo złamać znanymi metodami.

inż. Radosław Tyl
magistrant kierunku Bezpieczeństwo Narodowe
kontakt: radtyl@st.amu.edu.pl

Alert RCB w sieci. Czy jesteśmy w stanie efektywnie ostrzegać przed zagrożeniami w cyberprzestrzeni?

Człowiek jest gatunkiem posiadającym niebywałe zdolności adaptacji do zmieniających się na świecie warunków. Ok. 12 tys. lat temu przeszliśmy z wędrownego na osiadły tryb życia, w konsekwencji czego zbudowaliśmy miasta w których żyjemy i wykształciliśmy społeczne idee według których żyjemy. Na obecnym etapie rozwoju technologicznego oraz społecznego coraz większą część swoich interakcji społecznych przenosimy do przestrzeni internetowej będącej naszym oknem na świat i drugiego człowieka.

Współczesną Agorą stał się Facebook oraz Tweeter, teatrami YouTube a koncertami Spotify. Zmiany te w sposób diametralny zmieniają nasze środowisko bezpieczeństwa jak i również ujawniają nowe, nieznane wcześniej zagrożenia, zagrożenia w cyberprzestrzeni. Według III zasady dynamiki Newtona (i na szczęście) każda akcja wywołuje reakcję o równej wartości, dlatego w wyniku analizy specyfiki zagrożeń powstały sposoby, aby efektywnie ich unikać, zwalczać je oraz niwelować ich skutki. Najpierw należy jednak zastanowić się, czym właściwie te zagrożenia są?

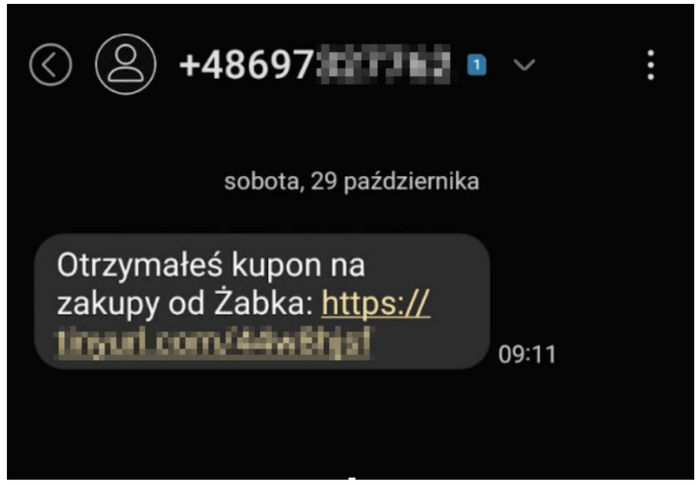
Zagrożenia w cyberprzestrzeni. Charakterystyka zjawiska, cechy oraz dynamika zmian

Wg. „Raportu grupy analitycznej IDC" w III kwartale 2021 sprzedanych zostało 86,7 milionów komputerów osobistych (wg. autorów do grupy tej zaliczamy laptopy, notebooki oraz stacje robocze). To właśnie komputery osobiste, dzięki swojej wszechstronności są najbardziej narażone na zagrożenia w cyberprzestrzeni. Sytuacji nie poprawia stały dostęp do Internetu (często opartego na technologii światłowodowej) który pozwala na szybki przesył dużych pakietów danych. Liczba komputerów oraz ich specyfika działania (ściśle oparta na architekturze klient-serwer) sprawiają, iż zagrożenia ich dotyczące mają charakter masowy, utrudnia to również właściwą reakcję na takie zdarzenie utrudniając izolację zaatakowanej jednostki od reszty systemu. Charakteryzując powyższe zjawisko, zdefiniować możemy trzy, stałe elementy wg. których ono funkcjonuje. Są nimi :

1. Sprawca postrzegany jako osoba/instytucja, której szkodliwa działalność w cyberprzestrzeni jest zorganizowana, określana przez cel jaki sprawca chce uzyskać w wyniku swojego działania. Spektrum jest szerokie, od pojedynczych jednostek do zorganizowanych grup przestępczych/wywiadowczych działających w domenie cyberprzestrzeni;
2. Ofiara – postrzegana jako osoba/ instytucja ,która może ucierpieć w wyniku ataku cybernetycznego możemy na wiele sposobów, narażone są informacje, pieniądze, dane osobiste czy własność intelektualna
3. Modus Operandi, uzależniony od możliwości sprawcy, celu ataku na ofiarę oraz punktów dostępu, które są możliwymi wektorami ataku.

Aby taki atak mógł zostać przeprowadzony musi zaistnieć związek między sprawcą a ofiarą. Nasz udostępniony w formularzu kontaktowym adres e-mail bądź numer telefonu, zalogowanie się na konto bankowe przez podstawiony, fałszywy ekran logowania czy związek z innym urządzeniem które padło ofiarą ataku są przykładowymi „punktami dostępu". Analizując to zjawisko, ten proces należy wspomnieć o fakcie, iż domena cyberprzestrzeni pozwala uzyskać nieznaną wcześniej dynamikę zmian cech charakterystycznych. Zmienia się również format ataków poprzez coraz większy procentowy udział urządzeń mobilnych w architekturze. Urządzenia te przez swój specyficzny format są narażone na inne zagrożenia niż komputery osobiste, dlatego wymagają odmiennych zabezpieczeń.

Mogą być jednak dla nas cennym narzędziem, ponieważ przez swoją mobilność (sic!) pozwalają nam natychmia-



Zdjęcie: Przykład phishingu, wersja z strony internetowej CBZC

stowo odbierać komunikaty nt. Obecnych zagrożeń tworząc swoisty system wczesnego ostrzegania.

Systemy ostrzegania przed zagrożeniami w cyberprzestrzeni.

Charakterystyka oraz adaptacja do występujących zagrożeń

Aby skutecznie radzić sobie z jakimkolwiek zagrożeniem musimy być jego świadomi, przeciwdziałanie bądź niwelowanie skutków jest nieefektywne jeśli nie możemy zlokalizować przyczyny wystąpienia danej sytuacji. Z tego powodu projektując oraz analizując nasze środowisko bezpieczeństwa musimy wdrożyć wydajny oraz szybki system informowania o nadchodzących (bądź już występujących) zagrożeniach. W przypadku dziedziny o tak wysokim dynamizmie zmian czynnik ten urasta do rangi kluczowego, predefiniując również naszą możliwość do zarządzania ryzykiem wystąpienia danego zagrożenia. Skoro kluczowy w przeciwdziałaniu zagrożeniom w cyberprzestrzeni jest czas reakcji, to jak efektywnie dostarczyć użytkownikom dane dotyczące aktualnych zagrożeń w sposób aby informacja była na tyle treściwa żeby wystarczająco treściwie opisać zagrożenie, a zarazem na tyle krótka żeby w obecnych czasach charakteryzujących się zbyt dużą ilością otrzymywanych informacji z każdej strony nie została uznana za spam? Na chwilę obecną w Polsce wyróżnić możemy co najmniej dwie koncepcje reagowanie na zagrożenia w cyberprzestrzeni:

1. Państwową, która realizowana jest przez Centralne Biuro Zwalczania Cyberprzestępczości (CBZC)
2. Prywatną, realizowaną przez podmioty biznesowo związane z domeną cyber, w kontekście szkoleń z zakresu bezpieczeństwa, testów penetracyjnych, kursów itd. Na podanie jako przykład podajmy firmę Niebezpiecznik.

Działalność CBZC opiera się publikowaniu aktualnych zagrożeń na swojej stronie WWW, oraz informowaniu potencjalnie poszkodowanych osób za pomocą wiadomości SMS/ e-mail nt. Wykrytych przestępstw. Na szczególną uwagę zasługuje fakt, jak w wymienionych w komunikacie CBZC wiadomościach SMS (metoda ta nazywana jest phishingiem i polega na wyłudzeniu danych poprzez podszywanie się pod firmy/instytucje i często wykorzystuje odnośniki do fałszywych stron WWW, ekranów logowania do bankowości elektronicznej, czego przykładem może być ostatni atak skierowany do klientów banku ING przeprowadzony 17.11.2022 itd.) zmienia się adres odnośnika. Najczęściej jest do zmiana adresu samej domeny, rzadziej zmiana dalszej części treści odnośnika. Ma to na celu uniknięcie algorytmów automatycznie określających dany odnośnik jako próbę phishingu oraz blokujących go. W praktyce oznacza to, że jeśli dany atak zostanie zablokowany na podstawie określenia odnośnika jako ”niebezpieczny”, blokada będzie skuteczna do momentu zmiany (najczęściej wg. podanych danych występują one średnio co 2 dni). Niewątpliwym atutem CBZC jest jego policyjny charakter, który pozwala kompleksowo ścigać przestępstwa w cyberprzestrzeni poprzez współpracę z pozostałymi jednostkami organizacyjnymi Policji.

Działalność prywatna (komercyjna) opisana na przykładzie firmy Niebezpiecznik opiera się na stworzeniu aplikacji na urządzenia mobilne (jest to również przykład wykorzystania potencjału do informowania nt. Zagrożeń, jakie te urządzenia posiadają), prowadzeniu strony WWW z opisami wydarzeń zgłaszanych przez samych użytkowników oraz prowadzeniu szkoleń. Stworzony przez siebie system ostrzeganie w formacie aplikacji pozwala szybko informować o wykrytych zagrożeniach oraz kompleksowo je opisywać. Aplikacja działa na zasadzie wykorzystywania powiadomień na telefonie wystosowując krótkie komunikaty tekstowe. Minusem takiego rozwiązania jest fakt, iż Niebezpiecznik to podmiot prywatny, który ma zupełnie inny autorytet niż CBZC który jest bądź co bądź jednostką organizacyjną Policji. W naszej perspektywy najważniejsza jest jednak skuteczność w działaniu. Jak wygląda ona w praktyce? Sprawdźmy!

Na warsztat postanowiłem wziąć ostatnio ujawnione zagrożenie w cyberprzestrzeni, dotyczyło ono odbioru rzekomych kuponów do sklepów Żabka o wartości nawet 1000 złotych. Wydarzenie jest o tyle ciekawe, iż zostało opisane zarówno przez CBZC jak i Niebezpiecznika. W obu komunikatach pojawia

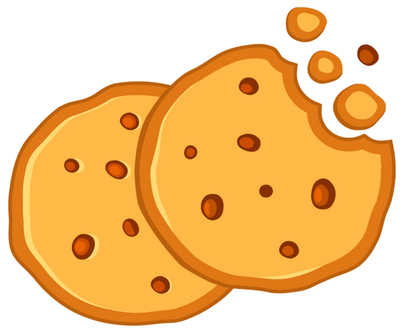
się to samo zdjęcie będące przykładem takiej próby, zasadniczą różnicą jest anonimizacja przykładu na stronie CBZC poprzez zamazanie fragmentu numeru telefonu oraz odnośnika.

Skoro kluczowy w walce z zagrożeniami w cyberprzestrzeni jest czas reakcji na zagrożenie, to jak wygląda on w tym wypadku? Z podanej wyżej wiadomości możemy precyzyjnie określić czas oraz datę jej odebrania przez zaatakowane urządzenie, jest to 29.10 o godz. 09:11. Artykuł dotyczący tego zdarzenia pojawił się na niebezpieczniku już tego samego dnia o godz. 13:04 (dane z samego artykułu), na stronie CBZC artykuł pojawił się dopiero 31.10. Oznacza to, iż musieliśmy czekać ok. 48 godzin na "państwowy" komunikat, który jednak nie został dostarczony bezpośrednio na nasze telefony, a opublikowany na stronie WWW co dodatkowo mogło opóźnić odebranie komunikatu. Czy to oznacza że państwowe podejście do tematyki cyberzagrożeń jest nieefektywne? W mojej ocenie nie, jest ona odmienne od podejścia komercyjnego ponieważ ma inne założenie. Priorytetem w podejściu komercyjnym jest ochrona swoich konsumentów, ponieważ oznacza to zysk. W podejściu państwowym priorytetem jest uderzenie w sprawców co w założeniu wyeliminuje takie zagrożenia w przyszłości, i wymaga czasu potrzebnego na zebranie i analizę danych.

Kluczowym z perspektywy bezpieczeństwa elementem jest możliwość współpracy komponentów publicznych i prywatnych, która pozwoli stworzyć kompleksowe systemy chroniące nas przed ciągle pojawiającymi się zagrożeniami w cyberprzestrzeni.

Krzysztof Łukaszewski
Student 4 roku Bezpieczeństwa Narodowego
na WNPID UAM w Poznaniu
kontakt: krzluk1@st.amu.edu.pl

Wyrażanie zgody online - zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych: pomocna tarcza czy permanentna uciążliwość?



Przeciętny użytkownik Internetu odwiedza ponad sto stron internetowych dziennie. Jeśli mieszka w Unii Europejskiej, to zostanie poproszony o wyrażenie zgody na przetwarzanie danych osobowych i stosowanie plików cookies. Jest tak, ponieważ w 2016 roku unijny ustawodawca wydał RODO, które weszło w życie dwa lata później. RODO oznacza Rozporządzenie o Ochronie Danych Osobowych i chroni prawo do prywatności przy przetwarzaniu danych.

Wraz z wejściem w życie RODO na stronach internetowych pojawiły się okienka z powiadomieniem o przetwarzaniu danych osobowych użytkownika i prośbą o wyrażenie zgody na ich przetwarzanie. Jednak pod koniec 2019 roku, w Internecie pojawiły się nowe okna, tym razem z prośbą o zgodę na wykorzystanie plików cookies, ale w bardziej angażujący sposób. Od tego czasu europejscy internauci są otoczeni wspomnianymi prośbami o zgodę, a słowo „cookies" widzą w Internecie niezliczoną ilość razy.

Czym są internetowe ciasteczka?

Termin cookies oznacza małe pliki tekstowe, które są zapisywane przez stronę internetową w pamięci urządzenia użytkownika podczas jej wyświetlania. Pliki cookies służą przede wszystkim do zbierania i zapisywania informacji o odwiedzających stronę poprzez śledzenie ich sesji w celu dostarczania spersonalizowanych treści i poprawy komfortu przeglądania stron internetowych. Cookies mogą być zatem wykorzystywane z korzyścią dla użytkowników i mogą być pomocne w tworzeniu różnych zestawień statystycznych dotyczących np. ruchu na stronach internetowych. Niektóre rodzaje tych plików mogą być wykorzystywane przez cyberprzestępców do nielegalnego gromadzenia i wykorzystywania danych. Dlaczego zatem właściciele stron internetowych tak skrupulatnie pytają internautów o zgodę na ich stosowanie? Przecież skoro przestępcy nawet nie przejmują się zgodą, a praworządni administratorzy wykorzystują pliki cookies z dobrymi intencjami i ostatecznie ułatwiają korzystanie z witryny, to czy zamiast zgody nie wystarczyłaby zwykła informacja?

Wyrażanie zgody - co na to prawo?

Odpowiedź na to pytanie oraz na pytanie, dlaczego sposób wyrażania zgody na pliki cookies ewoluował pod koniec 2019 roku, zawiera wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-673/17. Wyrok ten określa, jaki jest jedyny skuteczny sposób wyrażenia zgody na korzystanie z plików cookies, który pozostaje w zgodzie z RODO. Zgodnie z art. 4 RODO zgoda na przetwarzanie danych osobowych oznacza działanie użytkownika, którego skutkiem jest złożenie oświadczenia woli zezwalającego na przetwarzanie jego danych osobowych, przy czym oświadczenie to musi być dobrowolne, konkretne, świadome i jednoznaczne. TSUE ustalił, że zwrot "wyrazić zgodę" opisuje konkretne działanie jako faktyczne udzielenie zgody przez użytkownika w wyniku fizycznego zaznaczenia pola wyboru potwierdzającego zgodę. Oznacza to, że prośby o zgodę na pliki cookies skonstruowane w taki sposób, że pole potwierdzenia zgody jest domyślnie zaznaczone, a użytkownik ma jedynie możliwość odznaczenia pola w celu odmowy zgody, uniemożliwiają wyrażenie zgody w sensie prawnym. Zgoda udzielona w ten sposób jest nieważna w świetle RODO. Wyrażenie zgody na przetwarzanie danych osobowych i stosowanie plików cookies powinno zatem zawsze odbywać się poprzez podjęcie czynności polegającej na zaznaczeniu pola „Zgadzam się" lub dostosowaniu ustawień plików cookies. Bierna i milcząca zgoda jest nieważna.

Orzeczenie to jest kamieniem milowym dla pop-upów pytających użytkowników sieci o zgodę na pliki cookies. Od publikacji wyroku w dniu 1 października 2019 r. pola zgody na pliki cookies zyskały swój obecny kształt. W Unii Euro-

pejskiej internauci nie powinni natknąć się już na okna z domyślnie zaznaczoną opcją zgody. Witryny korzystające z takich pop-upów musiały je zmodyfikować. Obecnie odwiedzający strony sami wybierają opcję i mają wybór, na które ciasteczka pozwalają.

Okienka pod lupą...

Może być też tak, że użytkownik nie zapoznał się z treścią pola zgody lub całkowicie ją zignorował. W związku z tym, co użytkownicy myślą o wyskakujących okienkach z prośbą o zgodę na przetwarzanie danych i plikach cookies oraz jak się wobec nich zachowują?

Grupa badaczy przeprowadziła badanie dotyczące powiadomień o plikach cookie stosowanych na stronach internetowych. Głównym celem badania było określenie zależności między cechami okna dialogowego plików cookie a działaniami podejmowanymi przez użytkowników wobec nich.

Okazało się, że większość badanych powiadomień nie uniemożliwiała korzystania ze strony przed wyrażeniem zgody. Dominującą pozycją okien była dolna część strony. Niestety, przytłaczająca liczba z nich nie pozostawiała użytkownikom żadnego wyboru w zakresie rodzajów plików cookie czy opcji personalizacji. Jedyną akcją, jaką można było podjąć na tych okienkach, było wyrażenie zgody, gdyż nie było nawet przycisku odrzucenia. Podżeganie do wyrażenia zgody, czyli wyróżnienie przycisku kolorem, było widoczne w ponad połowie przypadków.

... i internauci również

W badaniu wzięło udział prawie 83 tysiące osób. Informacje o ich aktywności uzyskano z jednej i tej samej strony internetowej, dzięki czemu możliwe było sterowanie pozycjonowaniem powiadomień o plikach cookies oraz zmiana ich rodzaju.

Jak zatem pozycja i struktura pop-upów z prośbą o zgodę na pliki cookies wpływa na odwiedzających stronę? Wyniki pokazały, że większość pop-upów była ignorowana przez odwiedzających. Znacząca część użytkowników nie wchodziła w żadną interakcję z wyskakującymi ciasteczkami. Ci, którzy zainteresowali się okienkami, odmówili zgody na wykorzystanie ciasteczek w mniej więcej 1/5 przypadków. Większość odwiedzających reagujących na powiadomienia korzystała z urządzeń mobilnych. Wynika to prawdopodobnie z faktu, że powiadomienia na smartfonach zajmują większą część ekranu niż na komputerach.Autorzy badania zamieścili ankietę, w której chcieli poznać przyczyny reakcji użytkowników na powiadomienia o stosowaniu plików cookies. W ankiecie wzięło udział 110 osób. 55% uczestników zadeklarowało, że weszło w interakcję z okienkiem. 45% osób zignorowało pop-up. 72% respondentów, którzy podjęli działanie na powiadomienie, uzasadniło to stwierdzeniem, że pop-up ich zirytował. Pozostałe powody wymieniane w tej grupie to: obawa przed niedziałającą stroną, klikanie z przyzwyczajenia, chęć ochrony prywatności, chęć zapewnienia bezpieczeństwa, ograniczenie liczby reklam. Wśród nich 41% zrobiło to, ponieważ nie zauważyło pop-upu. Pozostałe powody wymieniane w tej grupie to: kliknięcie nie przyniosłoby żadnego efektu, brak zainteresowania tym, jakie dane zbierają ciasteczka na tej stronie, zbyt mała personalizacja, nieznajomość technologii cookies.

Internet ignorancją stoi

Większość internautów nie reaguje na żadne pop-upy informujące o zbieraniu danych osobowych. Badacze udowodnili jednak, że w Internecie istnieje spora grupa osób, które nie pozostają obojętne na te okienka. Pomijając tych, którzy klikają ze złości, inni robią to, bo chcą chronić swoją prywatność w sieci. Wyniki badań rzucają światło na same powiadomienia oraz na właścicieli stron internetowych. Niestety, okna pytające o zgodę, swoją konstrukcją manipulują zachowaniem użytkowników, dostarczając im zbyt mało lub nieistotne informacje i stosując techniki, które w jakiś sposób zmuszają do kliknięcia przycisku „Zgadzam się". W ten sposób właściciele stron internetowych uzyskują niewłaściwie udzielone zgody, które są bez znaczenia w świetle RODO, i w nieuczciwy sposób wykorzystują użytkowników. Orzeczenie TSUE nie jest w stanie powstrzymać tych praktyk.

Sposób, w jaki właściciele stron internetowych tworzą zapytania o zgodę na przetwarzanie danych i stosowanie plików cookies, można odczytać jako jasną deklarację ich zamiarów wobec da-

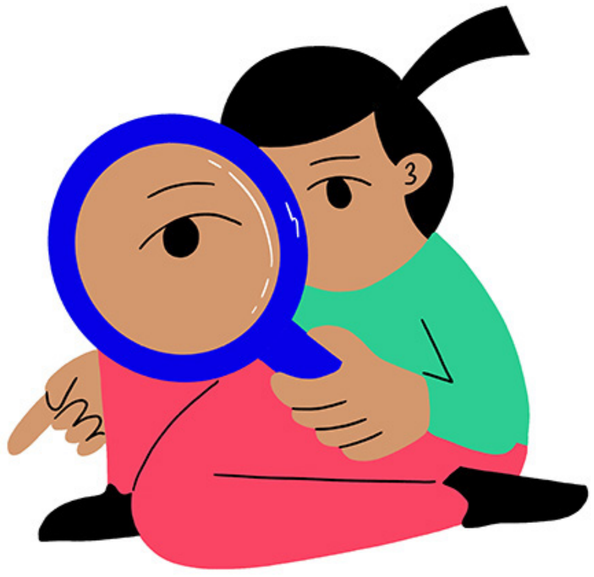
nych osobowych użytkowników. Zależy im na pozyskaniu danych, nad którymi, po ich zdobyciu, nikt inny nie ma już kontroli. Wydaje się, że ze względu na wysokie ryzyko utraty danych osobowych i ogromne rozpowszechnienie technologii cookies, tak duża liczba wymaganych prawem zgód jest niezbędna do zapewnienia bezpieczeństwa w sieci.

Większość użytkowników nie dba o podjęcie jakichkolwiek działań wobec próśb o zgodę. Niektóre osoby są nawet nimi zirytowane. Fakt ten prowadzi do smutnego wniosku, że większość społeczeństwa europejskiego jest zmęczona licznymi powiadomieniami i stała się nieczuła na problem ochrony danych osobowych. Na tej podstawie można założyć, że większość użytkowników nie docenia istotnej roli RODO i nie dostrzega zagrożeń, na jakie narażona byłaby ich prywatność, gdyby ta regulacja nie istniała.

Pomocna tarcza czy permanentna uciążliwość?

A zatem, czy udzielanie zgody online na gromadzenie i przetwarzanie danych osobowych zgodnie z RODO jest pomocną tarczą chroniącą prywatność, czy też stałym utrapieniem ograniczającym przyjemność korzystania z Internetu? Bezpiecznie będzie powiedzieć, że udzielanie zgody w erze RODO jest uciążliwe. Jest złem, ale jest złem koniecznym, aby obywatele Unii Europejskiej mogli czuć się bezpiecznie w Internecie, wiedząc, że unijny ustawodawca uzbroił ich w pomocną tarczę.

lic. Jonasz Żak
student I roku II stopnia na kierunku Bezpieczeństwo Narodowe
kontakt: jonzak@st.amu.edu.pl



ZAPROSZENIE DO PUBLIKACJI
Biuletyn „Nowiny Nauki o Bezpieczeństwie" nr 2(2)2023
EKOMIASTA

Zapraszamy do publikacji na łamach e-biuletynu WNPiD UAM pt. „Nowiny Nauki o Bezpieczeństwie". Wyniki Państwa badań, tezy eksperckie, przemyślenia poparte doświadczeniami w pracy w środowisku, w którym funkcjonujecie poza pracą dydaktyczną, mają niebagatelne znaczenie i często prekursorski charakter.

Biuletyn, jest na ten czas, wydawany tylko w Internecie i kolportowany wśród naszych studentów, absolwentów, pracowników administracji rządowej i samorządowej. Jego zasięg się zwiększa.

Aktualny numer będzie poświęcony zagadnieniu: ***bezpieczeństwu ekologicznemu miast***. Zapraszamy do składania opracowań w formie publicystycznej, popularnonaukowej, nawiązujących do poniższych zagadnień:

- Aktualne regulacje dotyczące ekologii
- Zielona Agenda UE i jej konsekwencje dla krajowej polityki ekologicznej
- Przykłady lokalnych działań proekologicznych
- Formy ochrony zasobów przyrody w polskich miastach
- Lokalne bezpieczeństwo ekologiczne
- Międzynarodowe bezpieczeństwo ekologiczne
- Zagrożenia ekologiczne
- Ekologia w mobilności miejskiej
- Problem smogu i zwalczania jego przyczyn w miastach i na wsi
- Ubóstwo energetyczne i jego konsekwencje
- Systemy teleinformatyczne w bezpieczeństwie ekologicznym: monitoring środowiska(w praktyce służb, inspekcji i straży)

Wymogi formalne tekstów:

1. Tekst: Word; Times New Roman, 12 pkt, 1,5 odstępu między wierszami, obustronnie wyjustowany.
2. Przypisy końcowe
3. Objętość: znaki ze spacjami od 8000 do 10000.
4. Tekst podzielony śródtytułami
5. Nota biograficzna, adres kontaktowy, tytuł naukowy, miejsce pracy, doświadczenie zawodowe (krótko) i obszary zainteresowań

Prosimy o zgłoszenie tytułów tekstów w terminie do 15.III br. na adres ***mikolaj.tomaszyk@amu.edu.pl***.
Teksty do publikacji należy nadesłać w terminie do 15.IV br. na ten sam adres.