BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2020
ISSN 1899-6264 Nr 3 (XL)

DOI: 10.48269/2451-0718-btip-2020-3-002
Data wpłynięcia: 25.11.2019
Data akceptacji: 6.09.2020

Maciej Siwicki

dr hab., LL.M., prof. UMK, Uniwersytet Mikołaja Kopernika w Toruniu
ORCID: 0000-0002-3120-021

Odpowiedzialność prawna z tytułu nieodpowiedniego zabezpieczenia sprzętu IT przed promieniowaniem swobodnie eksponującym

Wprowadzenie

Podstawową metodą ochrony przed cyberprzestępczością stosowaną przez podmioty odpowiedzialne za ochronę informacji przetwarzanej elektronicznie jest wdrażanie i rozwijanie programów komputerowych, których zadaniem jest wykrywanie, zwalczanie i usuwanie szkodliwego oprogramowania. Pakiety antywirusowe, zapory sieciowe, moduły kontrolujące pocztę elektroniczną i pliki pobierane z sieci, czy też innego rodzaju programy zabezpieczające zapewniają jednak tylko częściową ochronę. Są one nieskuteczne w przypadku ataków skierowanych na elementy sprzętowe sieci i systemów informatycznych.

Przeprowadzenie ataku sprzętowego, w szczególności w fazie podłączenia odpowiedniego urządzenia (np. do monitorowania klawiatury) lub manipulacji sprzętowej wymaga fizycznej obecności sprawcy albo osoby, którą się on posługuje. Wiąże się to oczywiście z ryzykiem pozostawienia śladów przestępstwa. Aby zminimalizować to ryzyko, sprawcy korzystają z metody, która bazuje na fakcie, że każde urządzenie elektroniczne emituje fale elektromagnetyczne, tzw. obrazy szumowe (takie sygnały określane są również jako „promieniowanie swobodnie eksponujące")[1]. Znajdując się w pobliżu sprzętu, sprawca dzięki specjalnym

[1] P. Huppertz, *Gesetzliche Pflichten und Haftungsrisiken im Zusammenhang mit mangelnder Absicherung von IT-Hardware*, „Computer und Recht" 2019, Heft 10, s. 625.

urządzeniom podsłuchowym przechwytuje niezabezpieczone sygnały elektromagnetyczne[2]. Sygnały, które mogą być podsłuchiwane i analizowane przez cyberprzestępców, obejmują m.in. sygnały wydostające się z płyty głównej poprzez zasilanie komputera. Dzięki podsłuchowi sprawca, obserwując ślad, stara się zrozumieć sposób działania urządzenia, m.in. poprzez analizę schematu szyfrowania. Ma to mu umożliwić wydedukowanie klucza[3] i na przykład odczytanie zaszyfrowanej wiadomości przesyłanej między dwiema komunikującymi się stronami za pośrednictwem sieci publicznych[4].

Fakt, iż sieci energetyczne mogą być wykorzystywane do podsłuchiwania niewłaściwie zabezpieczonego sprzętu IT, znany jest w zasadzie od 1985 r.[5]. Metoda ta określana była jako „TEMPEST" w odniesieniu do tajnego projektu rządu USA, którego celem było zbadanie podatności niektórych urządzeń komputerowych i telekomunikacyjnych na emitowanie promieniowania elektromagnetycznego (EMR) w sposób, który dawałby możliwość odczytania danych[6]. W późniejszym okresie zauważono, że z pewnej odległości możliwe jest odczytanie promieniowania z okablowania sprzętów komputerowych, zaś podsłuch dźwięków klawiatury daje możliwość zrekonstruowania wprowadzanego tekstu[7].

Korzystanie przez cyberprzestępców z tej metody stawia przed organami ścigania i karania nowe wyzwania (wykrycie sprawcy, zebranie dowodów przestępstwa itp.). Staje się także znaczącym problemem dla podmiotów odpowiedzialnych za bezpieczeństwo systemów i sieci informatycznych. Problem ten potęguje przy tym fakt, że obecnie większość komunikacji między urządzeniami (m.in. płatności online, wypłaty i wpłaty bankomatowe, hasła komputerowe, handel elektroniczny) jest prowadzona z wykorzystaniem cyfrowych urządzeń elektronicznych emitujących fale elektromagnetyczne. Szacuje się, że w 2017 r. za pomocą Internetu połączonych było 8,4 mld urządzeń (wzrost o 31% w stosunku do roku poprzedniego)[8], zaś pod koniec 2019 r. – 7,6 mld. Jednocześnie przewiduje się, że liczba ta wzrośnie

---

2 Przyjmuje się, że zasadniczo, aby „podsłuchać" promieniowanie, konieczne jest posiadanie odpowiedniego sprzętu, ponieważ wartości graniczne zakresu takich sygnałów są za małe. Takie sygnały mogą być przy tym wzmacniane poprzez np. odpowiednio zmodyfikowany kabel do monitora. Zob. Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kataloge, M 4.89 Abstrahlsicherheit*, http://www.suicidal.de/doc/sicherheit/m/m489.htm [dostęp: 23.10.2019].

3 Algorytm szyfrowania wykorzystuje klucz, tzw. klucz tajny, który w połączeniu z matematycznie zdefiniowanym algorytmem przekształca zwykły tekst w tekst zaszyfrowany.

4 Szerzej zob. A. Do, S. Thet Ko, A. Thu Htet, *Electromagnetic side-channel analysis on Intel Atom Processor,* https://web.wpi.edu/Images/CMS/ECE/MQP_Report_EM_Analysis__6.pdf [dostęp: 23.10.2019].

5 R. Lehtinen, D. Russell, G.T. Gangemi, *Computer Security Basics*, O'Reilly & Associates, Sebastopol, CA 1991, s. 253, [za:] P. Huppertz, *op. cit.*, s. 627.

6 Szerzej zob. M. Rouse, *Tempest*, https://searchsecurity.techtarget.com/definition/Tempest [dostęp: 23.10.2019].

7 *Schweizer Studenten hören Tastaturen ab*, https://www.pcwelt.de/news/Lauschangriff-Schweizer-Studenten-hoeren-Tastaturen-ab-323322.html [dostęp: 23.10.2019].

8 R. Köhn, *Online-Kriminalität: Konzerne verbünden sich gegen Hacker*, https://www.faz.net/aktuell/wirtschaft/diginomics/grosse-internationale-allianz-gegen-cyber-attacken-15451953-p2.html?printPagedArticle=true#pageIndex_1 [dostęp: 21.02.2019].

do 24,1 mld w 2030 r.[9] Przewiduje się także, że wartość tzw. rynku Internetu przedmiotów/rzeczy (ang. *Internet of Things*, IoT) na świecie wyniesie 7,1 bln USD do 2020 r.[10], zaś do 2025 r. – 11,1 bln USD[11].

Biorąc pod uwagę powyższe dane, należy założyć, że konieczność szczególnego zabezpieczenia infrastruktury sprzętowej systemów sterowania i transmisji danych oraz sieci energetycznych przed podsłuchem staje naglącą koniecznością. Tempo rozwoju nowoczesnej elektroniki skłania przy tym do wniosku, że także dostęp do odpowiednich narzędzi sprzętowych i programowych umożliwiający podsłuch będzie coraz łatwiejszy. Na tym tle pojawia się konieczność zwiększenia wymogów, w szczególności w stosunku do podmiotów odpowiedzialnych za przetwarzanie i gromadzenie danych, aby zaczęły stosować odpowiednie urządzenia niskoemisyjne lub umożliwiające ochronę przed promieniowaniem oraz stosowały tzw. gniazda filtrów chroniące przed podsłuchem przez kable sieciowe czy zasilające[12].

Odpowiedzialność prawna za naruszenie obowiązków związanych z zabezpieczeniem systemów sterowania i transmisji danych

Usługi świadczone drogą elektroniczną przez dostawców usług internetowych (ang. *Internet service provider*) obejmują m.in.: umożliwienie dostępu do Internetu, rejestrację nazw domen, hosting, transmisję i gromadzenie danych, dostarczanie i przechowanie gotowych do przywołania obcych ofert i usług, dostarczanie usług chmury obliczeniowej, poczty elektronicznej itd. Cześć tych usług ze względu na istotne znaczenie dla utrzymania krytycznej działalności społecznej jest szczególnie chroniona. Dotyczy to przede wszystkim usług istotnych dla całego społeczeństwa, np. platform handlu elektronicznego, internetowych portali płatniczych, portali społecznościowych, wyszukiwarek, usług chmur obliczeniowych, sklepów z aplikacjami, jak również całego sektora łączności elektronicznej[13].

---

9 Szerzej zob. *How Many IoT Devices Are There in 2020? [All You Need To Know]*, https://techjury.net/blog/how-many-iot-devices-are-there/#gref [dostęp: 3.10.2020].

10 H. Chin-Lung, J. Chuan-Chuan Lin, *An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*, "Computers in Human Behavior" 2016, Vol. 62, s. 516–527, https://www.sciencedirect.com/science/article/pii/S0747563216302990?via%3Dihub [dostęp: 21.02.2019].

11 Zob. *The Internet of Things: Mapping the value beyond the hype*, https://www.mckinsey.com/The-Internet-of-things-Mapping-the-value-beyond-the-hype.pdf [dostęp: 3.10.2020].

12 Na potrzebę takiej ochrony zwraca się uwagę m.in. w Niemczech. Zob. *IT-Grundschutz-Kompendium - Edition 2019*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html [dostęp: 23.10.2019].

13 Por. Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, COM/2013/048 final –2013/0027 (COD), https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:52013PC0048 [dostęp 29.10.2019]. Zob. też M. Siwicki, *Klika uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9, s. 13–21.

Na gruncie polskiego ustawodawstwa ochronie infrastruktury krytycznej, w tym m.in. sieci telekomunikacyjnej, poświęcona jest Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[14], zaś w celu poprawy bezpieczeństwa systemów informatycznych w szczególności w obszarach wrażliwych przyjęta została Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[15].

Ochrona infrastruktury krytycznej

Na gruncie ustawy o zarządzaniu kryzysowym pod pojęciem infrastruktury krytycznej rozumie się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Jak wskazuje się na stronie internetowej Rządowego Centrum Bezpieczeństwa, o tym, czy dany obiekt zalicza się do infrastruktury krytycznej decydują szczegółowe kryteria zapisane w niejawnym załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej.

Wśród systemów, które zostały objęte ochroną, znalazł się m.in. system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych, system ochrony zdrowia czy system zapewniający ciągłość działania administracji publicznej. W tej kategorii nie znalazły się jednak systemy odpowiedzialne za segregację odpadów, związane z przemysłem zbrojeniowym, z funkcjonowaniem giełdy papierów wartościowych ani systemy odpowiedzialne za funkcjonowanie komunikacji społecznej, w szczególności mediów masowych, czy też za sektor kultury. Mając na względzie wagę tych obszarów dla funkcjonowania społeczeństwa, powyższą lukę w ochronie należy uznać za poważną i wymagającą podjęcia odpowiednich zmian ustawodawczych.

Ustawodawca do systemów infrastruktury krytycznej nie zaliczył także ogólnie technologii komunikacyjnych i informacyjnych (takich jak radio i telewizja, sprzęt i sieci komputerowe, w tym Internet), ale jedynie „sieci teleinformatyczne”[16], których podstawową funkcją jest połączenie wszystkich urządzeń w jeden sprawnie działający system. Powyższą lukę częściowo koryguje fakt, że obecnie w skład niemalże każdej infrastruktury krytycznej wchodzi infrastruktura techniczna i informatyczna, w tym sieci i systemy telekomunikacyjne oraz wszelkie usługi związane ogólnie z ruchem sieciowym.

Ze względu na architekturę sieci teleinformatycznej do jej podstawowych elementów należy zaliczyć:

- media transmisyjne, których podstawową funkcją jest przesyłanie i wymiana sygnałów – m.in. technologie wykorzystujące media przewodowe (np. światłowód, przewód elektryczny, kabel koncentryczny) i bezprzewodowe (np. karty sieciowe, punkty dostępowe, anteny z okablowaniem) oraz węzły sieciowe (np.

[14] Dz.U. z 2018 r., poz. 1401, 1560, tekst jedn. z dnia 5 lipca 2019 r., Dz.U. z 2019 r., poz. 1398 (dalej: uozk).

[15] Dz.U. z 2018 r. poz. 1560, tekst jedn. z dnia 22 lipca 2020 r., Dz.U. z 2020 r., poz. 1369 (dalej: uoksc).

[16] Szerzej zob. M. Siwicki, *op. cit*.

interfejsy sieciowe, repeatery i huby, mosty, przełączniki, routery, modemy i tzw. zapory ogniowe);
- protokoły komunikacyjne, które służą do organizowania ruchu w sieci poprzez określenie reguły, składni, semantyki i synchronizację takiej komunikacji oraz możliwe sposoby naprawy w przypadku wystąpienia błędu;
- różnego rodzaju mechanizmy kontroli i nadzoru nad ruchem sieciowym, takie jak IPS (ang. Intrusion Prevention System), do których zadań należy wykrywanie ataków i ich skuteczne blokowanie, monitorowanie stanu bezpieczeństwa sieci, korelacja zdarzeń i generowanie raportów, oraz różnego rodzaju oprogramowanie umożliwiające np. kształtowanie ruchu sieciowego.

Wymienione powyżej elementy infrastruktury chronione są niezależnie od tego, czy ochronę tę realizuje operator, czy też jego podwykonawca. Jest to związane z koniecznością zapewnienia funkcjonalności całego systemu, w którego skład wchodzą powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, a także usługi (art. 3 pkt 2 uozk). Jednakże ochroną powinny być objęte nie tylko ściśle powiązane elementy danego systemu, obejmujące m.in. elementy sprzętowe składające się na infrastrukturę techniczną, ale również te, które tworzą powiązaną ze sobą funkcjonalnie całość. Sieć telekomunikacyjna nie może przykładowo działać bez zaopatrzenia w energię, bez łączności czy też niezależnie od łańcucha dostaw.

Z art. 5b ust. 1 pkt 1–4 uozk wynika, że ochrona infrastruktury krytycznej polega na:
1) zapobieganiu zakłóceniom funkcjonowania infrastruktury krytycznej;
2) przygotowaniu na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną;
3) reagowaniu w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej;
4) odtwarzaniu infrastruktury krytycznej.

Pod względem faktycznym ochrona infrastruktury krytycznej obejmować będzie szereg różnego rodzaju działań, m.in.: ochronę fizyczną, techniczną, osobową oraz tzw. ochronę teleinformatyczną związaną z zabezpieczeniem systemów sterowania i transmisji danych[17].

Zgodnie z art. 6 ust. 5 uozk właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają „obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia". W ustawie tej nie wskazano jednak, że wprowadzane systemy bezpieczeństwa muszą uwzględniać „najnowszy stan wiedzy", czy też być zgodne z określonymi

[17] Szerzej zob. W. Jobda, *Ochrona infrastruktury krytycznej przed cyberterroryzmem*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski *et al.*, Wyższa Szkoła Policji, Warszawa–Szczytno 2013, s. 449 i n. Zob. też *Narodowy Program Ochrony Infrastruktury Krytycznej*, 2018, s. 31–32, https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf [dostęp: 30.10.2019].

normami czy standardami[18]. Wydaje się oczywiste, że od wyżej wymienionych podmiotów wymagać należałoby w szczególności dbałości o dostępność, integralność, poufność i autentyczność dostarczanych rozwiązań stanowiących element wykorzystywanych w danym sektorze systemów teleinformatycznych. Wprowadzane rozwiązania techniczne powinny także odpowiadać najnowszemu stanowi wiedzy, aby uniknąć awarii lub uszkodzenia elementów kluczowych.

Ustawodawca w art. 6 uozk nie określił także zakresu takiego obowiązku. Na tym tle powinno pojawić się pytanie, czy obowiązki związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa powinny być proporcjonalne do ryzyka wystąpienia awarii lub uszkodzenia infrastruktury, czy też od takich podmiotów należy wymagać zapewnienia 100% bezpieczeństwa niezależnie od kosztów z tym związanych? Mając na względzie dynamikę rozwoju nowoczesnych technologii oraz dane statystyczne podawane przez organizacje zajmujące się cyberprzestępczością, można odnieść wrażenie, że poziom bezpieczeństwa w sektorze IT na przestrzeni kilku lat nie uległ poprawie, a wręcz pogorszeniu. Ze względu na istotność infrastruktury technicznej dla całego społeczeństwa wydaje się oczywiste, że od podmiotów odpowiedzialnych za infrastrukturę krytyczną wymagać należy nie tylko wprowadzania systemów bezpieczeństwa uwzględniających „najnowszy stan wiedzy", ale także „odpowiednich" środków, planów ochrony i systemów rezerwowych proporcjonalnych do ryzyka negatywnych konsekwencji wystąpienia awarii systemu. *De lege ferenda* w art. 6 uozk należałoby wprowadzić wymóg wdrożenia „[…] odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy […]", na wzór rozwiązania przyjętego w art. 8 uoksc.

Oprócz powyższego jest oczywiste, że sieci i systemy teleinformatyczne powinny być zaprojektowane tak, aby tylko osoby upoważnione mogły uzyskać do nich dostęp. Systemy te powinny być przy tym chronione w sposób uwzględniający wymogi wynikające zarówno z przepisów krajowych, jak i – ze względu na ogólnoświatowy charakter sieci – z międzynarodowych standardów takich jak DIN, ISO lub ISO/IEC czy też innych rozwiązań, które okazały się skuteczne w praktyce. W tym kontekście zasadne jest wymaganie określenia przez Radę Ministrów w drodze uchwały dotyczącej Narodowego Programu Ochrony Infrastruktury Krytycznej odpowiednich standardów i norm dotyczących zabezpieczenia infrastruktury krytycznej. Taka uchwała powinna być także odpowiednio często aktualizowana.

Ochrona usług kluczowych

Na gruncie polskiego ustawodawstwa, zgodnie z wymogami przyjętej w dniu 6 lipca 2016 r. Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii[19], podjęto decyzję o szczegółowym określeniu obowiązków usługodawców internetowych, dzieląc ich na operatorów usług kluczowych oraz na

[18] Z art. 5b uozk wynika jednak, że Rada Ministrów ma przyjąć, w drodze uchwały, Narodowy Program Ochrony Infrastruktury Krytycznej, który określa m.in. „narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej".

[19] Dz.Urz. UE, L 194, s. 1.

podmioty świadczące usługi cyfrowe. Obowiązki tej drugiej grupy zostały wyraźnie ograniczone ze względu na niższy poziom ryzyka i mniejsze znaczenie ich usług.

W załączniku nr 1 do uoksc do zidentyfikowanych operatorów usług kluczowych zaliczono podmioty, które świadczą usługi systemu nazw domenowych (ang. Domain Name System, DNS), prowadzą punkt wymiany ruchu internetowego (ang. Internet Exchange Point, IXP) oraz zarządzają rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (ang. Top Level Domains, TLD).

Na powyższe podmioty nałożone są liczne obowiązki, obejmujące m.in. konieczność wdrożenia odpowiednich zabezpieczeń, zarządzania incydentami czy stosowania takich środków, które zapobiegają i ograniczają wpływ incydentów na bezpieczeństwo systemów. Przykładowo, stosownie do art. 8 pkt 2 uoksc operator usługi kluczowej został zobowiązany do wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych. Przepis ten nie wskazuje, o jakie konkretne środki ochrony chodzi, ale jest jasne, że każdy podmiot przetwarzający dane w systemie IT powinien zapewnić co najmniej minimalne normy bezpieczeństwa, które są wystarczające do zapewnienia poufności, integralności i dostępności systemów i usług związanych z przetwarzaniem i gromadzeniem danych.

Ochrona danych osobowych

Obecnie w systemach informatycznych przetwarzane są m.in. dane pracowników, przedsiębiorców, klientów, dostawców, operatorów usług itd. Zwiększenie ochrony danych osobowych powoduje zatem konieczność zwiększenia standardów bezpieczeństwa ich przetwarzania, także w systemach teleinformatycznych.

Od maja 2018 r. obowiązuje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[20]. Zgodnie z art. 4 ust. 1 „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").

Podstawowe regulacje dotyczące sposobu przetwarzania danych osobowych znajdują się w art. 32 RODO. Zgodnie z tym przepisem dane takie powinny być przetwarzane z uwzględnieniem „stanu wiedzy technicznej", zaś administrator i podmiot przetwarzający wdraża „odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku".

Podobnie jak w opisanych wyżej regulacjach normatywnych nie zostało wskazane, o jakie konkretne środki chodzi, ale również w tym przypadku wnioski wydają się jasne. W szczególności ze względu na obowiązek dbałości o poufność przetwarzania takich danych jest oczywiste, że systemy te powinny w odpowiedni sposób chronić przez szpiegowaniem. Wynika to także z art. 5 ust. 1 lit. f, który wymaga ochrony przed „niedozwolonym lub niezgodnym z prawem przetwarzaniem" za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"). Także w motywie nr 39 podkreśla się, że dane osobowe

[20] Dz.Urz. UE, L 119, s. 1 (dalej: RODO).

powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed „nieuprawnionym dostępem". Jednocześnie zakres obowiązków nakładany na poszczególne podmioty uzależniony jest od ryzyka związanego z przetwarzaniem odpowiednich danych (np. danych wrażliwych). Z treści rozporządzenia można także wyciągnąć wniosek, że czym większe jest ryzyko dla bezpieczeństwa danych, tym większe wymogi stawiane są przed podmiotami je przetwarzającymi. Po stronie podmiotów przetwarzających dane pojawia się obowiązek oceny ryzyka dla interesów i praw osoby, której dane dotyczą, poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych.

Mając na względzie treść art. 32 ust. 1 RODO jest oczywiste, że obowiązek podjęcia odpowiednich środków technicznych przeciwko szpiegowaniu wymaga wprowadzenia odpowiednich zabezpieczeń nie tylko o charakterze programowym, ale także technicznym, obejmujący m.in. ochronę przez nadmiernym promieniowaniem. Obowiązek ten dotyczy w szczególności podmiotów działających w branżach, gdzie przetwarzane są dane wrażliwe, m.in. w branży bankowej, ubezpieczeniowej, medycznej i prawniczej.

Odpowiedzialność prawna za naruszenie obowiązków związanych z zabezpieczeniem systemów IT

Organ właściwy do spraw cyberbezpieczeństwa może nałożyć kary pieniężne na operatorów usług kluczowych i dostawców usług cyfrowych, m.in. za nieprzeprowadzanie systematycznego szacowania ryzyka, brak zarządzania ryzykiem wystąpienia incydentu czy też niewdrożenie odpowiednich środków technicznych i organizacyjnych. Kara ta może osiągnąć wymiar do 200 tys. zł, zaś jeżeli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy, kara ta może wzrosnąć do 1 mln zł (art. 73 uoksc).

W przypadku naruszenia obowiązków związanych z zapewnieniem bezpieczeństwa przetwarzania danych osobowych na podstawie art. 83 ust. 4 w zawiązku z art. 32 RODO grozi grzywna w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Przy czym zastosowanie może mieć kwota wyższa w zależności od tego, czy podmiot należy do grupy określonej w art. 83 ust. 4 lit. a do lit. c. Ponadto organ nadzorczy w odniesieniu do przedsiębiorstw według art. 58 ust. 2 może stosować wymienione w tym przepisie uprawnienia naprawcze, obejmujące m.in. wydawanie ostrzeżeń, udzielanie upomnień, nakazanie dostosowania operacji przetwarzania, czy też nałożyć na mocy art. 83, oprócz lub zamiast środków o których mowa w art. 58, administracyjną karę pieniężną. Oprócz powyższego, w przypadku kolejnych naruszeń, zgodnie z art. 83 ust. 5 może być nałożona administracyjna kara pieniężna w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu.

Od momentu wejścia w życie RODO europejskie organy ochrony danych osobowych nałożyły liczne kary. I tak na przykład austriacki organ ochrony danych osobowych nałożył karę w wysokości ok. 4800 euro na prywatnego przedsiębiorcę za nieprawidłowe umieszczenie monitoringu wizyjnego. W Portugalii nałożono karę w wysokości ok. 400 000 euro na szpital Barreiro Montijo za m.in. nieuprawniony dostęp do danych klinicznych udzielony osobom trzecim poprzez utrzymywanie w systemie kilkukrotnie większej liczby kont niż faktyczna liczba pracowników. W Niemczech miejscowy organ nadzorczy nałożył 20 tys. euro kary na niemiecki portal randkowy Knuddels.de. Portal padł ofiarą ataku hakerskiego, w wyniku którego skradziono dane prawie 2 milionów kont zarejestrowanych użytkowników[21]. Francuski organ ochrony danych CNIL (Commission Nationale de l'Informatique et des Libertés) 21 stycznia 2019 r. nałożył karę finansową w wysokości 50 milionów euro na Google LLC za brak przejrzystości, nieodpowiednie informacje i brak ważnej zgody na personalizację reklam[22]. Brytyjski organ ochrony danych ICO (Information Commissioner's Office) nałożył 8 lipca 2019 r. na linie lotnicze British Airways grzywnę około 205 mln euro z powodu niewłaściwego zabezpieczenia systemów IT, co umożliwiło nieautoryzowany dostęp do danych klientów[23]. Również w Polsce doszło do nałożenia kar związanych z naruszeniem przepisów o ochronie danych osobowych. Karę miliona złotych ma zapłacić firma z Warszawy, która o fakcie przetwarzania danych informowała tylko tych przedsiębiorców, którzy w publicznych rejestrach ujawnili adres mailowy. Do tych, którzy tego adresu nie podawali, nie wysyłała żadnej informacji o przetwarzaniu ich danych ze względu na to, że wysłanie listu do takich podmiotów wymagałoby „niewspółmiernie dużo wysiłku"[24]. Prezes Urzędu Ochrony Danych Osobowych nałożył także ponad 2,8 mln złotych kary na spółkę Morele.net za niewystarczające zabezpieczenie danych osobowych[25].

Podmioty świadczące różnego rodzaju usługi związane z dostarczanie infrastruktury sieci telekomunikacyjnego mogą ponosić także odpowiedzialność kontraktową na zasadach ogólnych. Nie budzi przecież wątpliwości, że w przypadku różnego rodzaju usług świadczonych drogą elektroniczną istotnym elementem jest nie tylko dostarczenie jakiejś konkretnej usług, np. poczty elektronicznej, przestrzenni dyskowej itd., ale także zapewnienie bezpieczeństwa danych. Niewątpliwie w interesie

---

21 *Pierwsza kara za naruszenie przepisów RODO!*, https://gdpr.pl/aktualnosci/pierwsza-kara-za-naruszenie-przepisow-rodo [dostęp: 28.10.2019].

22 *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [dostęp: 28.10.2019].

23 Incydent ten częściowo polegał na przekierowaniu ruchu użytkowników ze strony internetowej British Airways na fałszywą witrynę. Za jej pośrednictwem osoby atakujące pozyskały dane osobowe około 500 000 klientów. Szerzej zob. *Intention to fine British Airways £183.39m under GDPR for data breach*, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ [dostęp: 28.10.2019].

24 *Milion złotych kary za przetwarzanie danych osobowych? Pierwsza kara za naruszenie RODO*, https://gloswielkopolski.pl/milion-zlotych-kary-za-przetwarzanie-danych-osobowych-pierwsza-kara-za-naruszenie-rodo/ar/c3-13996729 [dostęp 28.10.2019].

25 *Duża kara za naruszenie RODO. „Wyciekły dane ponad dwóch milionów osób"*, https://tvn24bis.pl/z-kraju,74/morele-net-ukarane-przez-uodo-najwyzsza-kara-za-naruszenie-rodo,970759.html [dostęp: 28.10.2019].

użytkownika jest zabezpieczenie się przed ryzykiem ujawienia informacji. Sankcją za naruszenie wskazanego obowiązku może być kara zastrzeżona w umowie.

Podmioty dostarczające usługi będą odpowiedzialne za niezachowanie należytej staranności, a więc staranności ogólnie wymaganej w stosunkach danego rodzaju. Należytą staranność związaną z odpowiednim zabezpieczeniem systemów IT w zakresie prowadzonej działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności (art. 355 kc[26]). Zakres tego obowiązku uzależniony będzie przy tym od charakteru przetwarzanych elektronicznie informacji. Nie budzi jednak wątpliwości, że wymagania związane z zapewnieniem bezpieczeństwa są coraz wyższe, zaś podejmowane środki muszą być stosowne do pojawiających się zagrożeń. Warto przy tym podkreślić, że po stronie tych podmiotów pojawia się konieczność wykazania, że staranność była należyta, tzn. dostosowana i odpowiednia do działalności w branży IT i zagrożeń, z jakimi ta branża jest związana, w szczególności w aspekcie zachowania poufności oraz odpowiedniego zabezpieczania i zachowania informacji przetwarzanych elektronicznie.

Podsumowanie

Z systematycznie zwiększającą się liczbą włamań do systemów komputerowych, kradzieży tożsamości, naruszenia poufności informacji, już od lat związane jest pytanie o skuteczne środki przeciwdziałania (zapobiegania i ścigania). Mając na względzie tendencje do znaczącego rozszerzania obowiązków związanych z ochroną danych osobowych oraz systematycznie zwiększające się ryzyko ataku zarówno na infrastrukturę programową, jak i sprzętową, po stronie podmiotów przetwarzających dane osobowe pojawia się szczególna konieczność oceny ryzyka związanego z wykorzystaniem określonego sprzętu – w celu m.in. weryfikacji, czy przetwarzane za jego pomocą dane osobowe są odpowiednio zabezpieczone. W szczególności od podmiotów przetwarzających dane wrażliwe wymagać należy zabezpieczenia sprzętu przed promieniowaniem. Konieczność wzmożonej ochrony pojawia się także w przypadku instytucji odpowiedzialnych za obronę narodową i bezpieczeństwo infrastruktury krytycznej, która jest przedmiotem coraz groźniejszych aktów, także ze strony obcych agencji wywiadowczych.

Bibliografia

Chin-Lung H., Chuan-Chuan Lin J., *An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*, "Computers in Human Behavior" 2016, Vol. 62, https://www.sciencedirect.com/science/article/pii/S0747563216302990?via%3Dihub [dostęp: 21.02.2019].

Do A., Thet Ko S., Thu Htet A., *Electromagnetic side-channel analysis on Intel Atom Processor*, https://web.wpi.edu/Images/CMS/ECE/MQP_Report_EM_Analysis__6.pdf [dostęp: 23.10.2019].

[26] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tekst jedn. z dnia 16 maja 2019 r., Dz.U. z 2019 r., poz. 1145.

How Many IoT Devices Are There in 2020? [All You Need To Know], https://techjury.net/blog/how-many-iot-devices-are-there/#gref [dostęp: 3.10.2020].

Huppertz P., *Gesetzliche Pflichten und Haftungsrisiken im Zusammenhang mit mangelnder Absicherung von IT-Hardware*, „Computer und Recht" 2019, Heft 10.

Jobda W., *Ochrona infrastruktury krytycznej przed cyberterroryzmem*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski *et al.*, Wyższa Szkoła Policji, Warszawa–Szczytno 2013.

Köhn R., *Online-Kriminalität: Konzerne verbünden sich gegen Hacker,* https://www.faz.net/aktuell/wirtschaft/diginomics/grosse-internationale-allianz-gegen-cyber-attacken-15451953-p2.html?printPagedArticle=true#pageIndex_1 [dostęp: 21.02.2019].

Narodowy Program Ochrony Infrastruktury Krytycznej, 2018, https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf [dostęp: 30.10.2019].

Rouse M., *Tempest*, https://searchsecurity.techtarget.com/definition/Tempest [dostęp: 23.10.2019].

Siwicki M., *Klika uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9.

The Internet of Things: Mapping the value beyond the hype, https://www.mckinsey.com/The-Internet-of-things-Mapping-the-value-beyond-the-hype.pdf [dostęp: 3.10.2020].

Odpowiedzialność prawna z tytułu nieodpowiedniego zabezpieczenia sprzętu IT przed promieniowaniem swobodnie eksponującym
Streszczenie

Opracowanie przedstawia wybrane problemy prawne związane z przeciwdziałaniem atakom cyberprzestępców na systemy IT bazującym na przechwytywaniu emitowanych przez urządzenia fal elektromagnetycznych (tzw. obrazów szumowych). Skupia się ono przede wszystkim na kwestii odpowiedzialności dostawców i operatorów usług świadczonych drogą elektroniczną za właściwe zabezpieczenie systemów i sieci komputerowych, w tym także na kwestii ochrony przez nich danych osobowych.

Słowa kluczowe: infrastruktura krytyczna, cyberprzestępczość, dostawcy i operatorzy usług świadczonych drogą elektroniczną, Internet, promieniowanie swobodnie eksponujące, dane osobowe

Legal liability for the lack of adequate security of IT equipment
Abstract

The study presents selected legal problems related to counteracting cybercriminals' attacks on IT systems based on the interception of electromagnetic waves emitted by devices, i.e. "noise images." It focuses on the issue of the liability of providers and operators of services provided by electronic means for the proper protection of computer systems and networks, including the issue of their protection of personal data.

Key words: critical infrastructure, cybercrime, providers and operators of electronic services, Internet, free exposure radiation, personal data

Maciej Siwicki

Die gesetzliche Haftung wegen der unzureichenden Absicherung der IT – Ausrüstung vor der austretenden Strahlung
Zusammenfassung

Die Arbeit stellt ausgewählte rechtliche Probleme dar, die mit der Bekämpfung der Angriffe der Cyberkriminellen gegen die, sich auf die Überwachung der durch die Geräte emmitierten elektromagnetischen Welen stützenden IT Systeme (die sog. „verrauschte Bilder“) verbunden sind. Die Bekämpfung konzentriert sich vor allem auf das Problem der Verantwortung von Lieferanten und Betreibern der auf elektronischem Wege geleiststen Dienstleistungen für die richtige Absicherung der Systeme und Computernetze, darin auch das Problem der von ihnen geschützten Personaldaten.
Schlüsselwörter: kritische Infrastruktur, Cyberkriminalität, Lieferanten und Betreiber der auf elektronischem Wege geleisteten Dienstleistungen, Internet, frei austretende Strahlung, Personaldaten

Юридическая ответственность за отсутствие надлежащего обеспечения безопасности ИТ-оборудования от воздействия электромагнитного излучения
Резюме

В статье представлены некоторые юридические проблемы, связанные с мерами противодействия киберпреступности – защитой ИТ-систем от перехвата, излучаемых устройствами электромагнитных волн. В исследовании внимание сосредоточено, прежде всего, на вопросах ответственности провайдеров и операторов, предоставляемых электронным путем, услуг за надлежащее обеспечение безопасности систем и компьютерных сетей, в том числе связанных с защитой персональных данных.
Ключевые слова: критическая информационная инфраструктура, киберпреступность, провайдеры услуг предоставляемых в электронном виде, интернет, электромагнитное излучение, персональные данные