Komitet Kontaktowy
Najwyższych Organów Kontroli Państw Unii Europejskiej

Kompendium kontroli

Cyberbezpieczeństwo w UE i państwach członkowskich UE

Kontrole dotyczące odporności krytycznych systemów informacyjnych i infrastruktury cyfrowej na cyberataki

Sprawozdania z kontroli
opublikowane w latach 2014–2020

PL

Grudzień 2020 r.

Komitet Kontaktowy najwyższych organów kontroli (NOK) Unii Europejskiej stanowi forum, na którym omawiane i rozpatrywane są kwestie związane z kontrolą publiczną w UE. Dzięki pogłębianiu dialogu i współpracy między członkami Komitet pomaga w zwiększeniu skuteczności zewnętrznej kontroli polityki i programów UE. Przyczynia się również do większej rozliczalności, usprawnienia zarządzania finansami UE i umocnienia dobrych rządów z korzyścią dla wszystkich obywateli Unii.

Kontakt: www.contactcommittee.eu

Spis treści

Wprowadzenie 6

Streszczenie 8

CZĘŚĆ I – Cyberbezpieczeństwo w kontekście europejskim 9

Czym jest cyberbezpieczeństwo? 10

Cyberbezpieczeństwo ma wpływ na życie codzienne wszystkich obywateli Unii 10

Istnieje wiele rodzajów zagrożeń dla cyberbezpieczeństwa 11

Cyberataki powodują znaczne skutki gospodarcze 15

Wraz z coraz częstszym występowaniem zagrożeń związanych z cyberbezpieczeństwem rośnie świadomość na ich temat 18

Cyberbezpieczeństwo jest istotne dla zapewnienia spójności społecznej i stabilności politycznej 20

Cyberbezpieczeństwo w UE – kompetencje, podmioty, strategie i prawodawstwo 28

Wydatki związane z cyberbezpieczeństwem w UE – rozproszone i niewystarczające 36

CZĘŚĆ II – Przegląd prac najwyższych organów kontroli 41

Wstęp 42

Metodyka kontroli i tematy objęte zakresem kontroli 42

Okres objęty kontrolą 44

Cele kontroli 44

Główne uwagi z kontroli 48

CZĘŚĆ III – Streszczenie sprawozdań najwyższych organów kontroli 55

Dania – *Rigsrevisionen* 56

Ochrona przed atakami typu ransomware 56

Estonia – *Riigikontroll* 60

Zapewnienie bezpieczeństwa i ochrony estońskich państwowych baz danych o krytycznym znaczeniu 60

Irlandia – *Office of the Comptroller and Auditor General* 64

Działania dotyczące cyberbezpieczeństwa kraju 64

Francja – *Cour des comptes* 68

Dostęp do szkolnictwa wyższego – wstępna ocena ustawy o doradztwie zawodowym i zdawalności wśród studentów 68

Łotwa – *Valsts Kontrole* 74

Czy administracja publiczna wykorzystała wszystkie możliwości, aby efektywnie zarządzać infrastrukturą ICT? 74

Litwa – *Valstybės Kontrolė* 78

Zarządzanie państwowymi zasobami informacyjnymi o znaczeniu krytycznym 78

Węgry – *Państwowa Izba Obrachunkowa* 83

Kontrola ochrony danych – kontrola krajowych ram ochrony danych i niektórych rejestrów danych priorytetowych w kontekście współpracy międzynarodowej 83

Niderlandy – *Powszechna Izba Obrachunkowa* 87

Cyberbezpieczeństwo infrastruktury gospodarki wodnej o znaczeniu krytycznym i kontroli granicznych w Niderlandach 87

Polska – *Najwyższa Izba Kontroli* 92

Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych 92

Portugalia – *Tribunal de Contas* 97

Kontrola dotycząca portugalskiego paszportu elektronicznego 97

Finlandia – *Valtiontalouden tarkastusvirasto* 104

Rozwiązania w zakresie cyberochrony 104

Szwecja – *Riksrevisionen* 109

Przestarzałe systemy informatyczne – przeszkoda na drodze do skutecznej transformacji cyfrowej 109

Unia Europejska – *Europejski Trybunał Obrachunkowy* 113

Dokument analityczny pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją” 113

Wykaz akronimów i skrótów 117

Glosariusz 119

Wprowadzenie

Szanowni Państwo!

Z transformacją cyfrową i coraz szerszym wykorzystywaniem technologii informacyjnych we wszystkich aspektach życia codziennego wiąże się wiele nowych możliwości. Jednocześnie wzrasta ryzyko, że osoby fizyczne, przedsiębiorstwa i organy publiczne padną ofiarą cyberprzestępczości lub cyberataku. Społeczne i gospodarcze oddziaływanie tego ryzyka również jest coraz większe.

W UE cyberbezpieczeństwo należy do kompetencji państw członkowskich. UE powierzono tworzenie wspólnych ram regulacyjnych jednolitego rynku UE i zapewnianie państwom członkowskim warunków do prowadzenia współpracy w atmosferze wzajemnego zaufania.

Cyberbezpieczeństwo i autonomia cyfrowa stały się kwestiami o strategicznym znaczeniu dla Unii i jej państw członkowskich. Uchybienia w zarządzaniu w zakresie cyberbezpieczeństwa są powszechne w sektorach publicznym i prywatnym w UE, choć zakres stwierdzanych uchybień jest zróżnicowany. Taka sytuacja zmniejsza zdolność Unii do ograniczania cyberataków i reagowania na nie w razie potrzeby. Rośnie skala dezinformacji, często pochodzącej spoza UE, co po raz kolejny uwidoczniło się podczas pandemii COVID-19. Dezinformacja stanowi zagrożenie dla spójności społecznej unijnych społeczeństw i zmniejsza zaufanie obywateli do europejskich systemów demokratycznych, dlatego zjawiska tego nie można w żadnym razie ignorować.

Jak wynika z ankiety przeprowadzonej wśród unijnych NOK w 2018 r., jak dotąd około połowa z tych organów nie przeprowadziła kontroli w zakresie cyberbezpieczeństwa. Od tego czasu NOK zintensyfikowały prace kontrolne w zakresie cyberbezpieczeństwa. Kontrolerzy położyli szczególny nacisk na kwestię ochrony danych, gotowość systemów na wypadek wystąpienia cyberataków oraz zabezpieczenie systemów zapewniających podstawowe usługi użyteczności publicznej. Zrozumiałe jest, że nie wszystkie z tych kontroli można podać do publicznej wiadomości, ponieważ niektóre z nich mogą obejmować informacje szczególnie chronione (dotyczące bezpieczeństwa narodowego).

W ostatnim roku kryzys związany z COVID-19 stał się sprawdzianem dla unijnych gospodarek i społeczeństw. Biorąc pod uwagę zależność UE od technologii informacyjnych, „cyberkryzys” może okazać się kolejną pandemią. Należy zachować gotowość i zwiększyć odporność krytycznych systemów informacyjnych i infrastruktury cyfrowej na cyberataki.

Mamy nadzieję, że przegląd przedstawiony w niniejszym kompendium dodatkowo zwiększy zainteresowanie kontrolerów publicznych w całej Unii tym doniosłym zagadnieniem.

Klaus-Heiner Lehne

Prezes Europejskiego Trybunału Obrachunkowego
Przewodniczący Komitetu Kontaktowego
i koordynator projektu

Streszczenie

I Cyberbezpieczeństwo i autonomia cyfrowa stały się **kwestiami o strategicznym znaczeniu dla UE i państw członkowskich UE**. Wraz ze wzrostem poziomu zagrożenia należy wzmóc wysiłki na rzecz ochrony unijnych krytycznych systemów informacyjnych i infrastruktury cyfrowej przed cyberatakami. Cyberbezpieczeństwo dotyczy nie tylko infrastruktury użyteczności publicznej, obronności i systemów opieki zdrowotnej, ale również ochrony naszych danych osobowych, modeli biznesowych i własności intelektualnej. Co za tym idzie, cyberbezpieczeństwo oznacza ochronę unijnych społeczeństw demokratycznych, naszej niezależności jako Europejczyków oraz naszego wspólnego sposobu życia.

II W pierwszej części niniejszego trzeciego kompendium Komitetu Kontaktowego określono, **czym jest cyberbezpieczeństwo**. Opisano w niej, jak istotnym wyzwaniem dla organów publicznych, przedsiębiorstw i osób prywatnych jest cyberbezpieczeństwo, oraz zwrócono uwagę na dezinformację – nowe zjawisko, które stanowi coraz większe zagrożenie dla spójności społecznej unijnych społeczeństw i systemów demokratycznych. Wyjaśniono również kompetencje UE w zakresie cyberbezpieczeństwa i przedstawiono unijne podmioty zajmujące się tą dziedziną, streszczono strategię i prawodawstwo Unii, a także omówiono finansowanie unijne dostępne w tym obszarze.

III W drugiej części kompendium streszczono **wyniki wybranych kontroli przeprowadzonych przez NOK 12 państw członkowskich uczestniczących w przygotowaniu publikacji oraz Europejski Trybunał Obrachunkowy** opublikowane w latach 2014–2020. Kontrole te dotyczyły istotnych aspektów cyberbezpieczeństwa, takich jak ochrona danych prywatnych, integralność krajowych ośrodków przetwarzania danych, bezpieczeństwo instalacji użyteczności publicznej oraz wdrażanie szeroko rozumianych krajowych strategii w zakresie cyberbezpieczeństwa.

IV Trzecia część kompendium zawiera szczegółowe **zestawienia informacji dotyczące wybranych kontroli** wraz z wykazem innych kontroli związanych z tematem cyberbezpieczeństwa opublikowanych przez NOK.

CZĘŚĆ I – Cyberbezpieczeństwo w kontekście europejskim

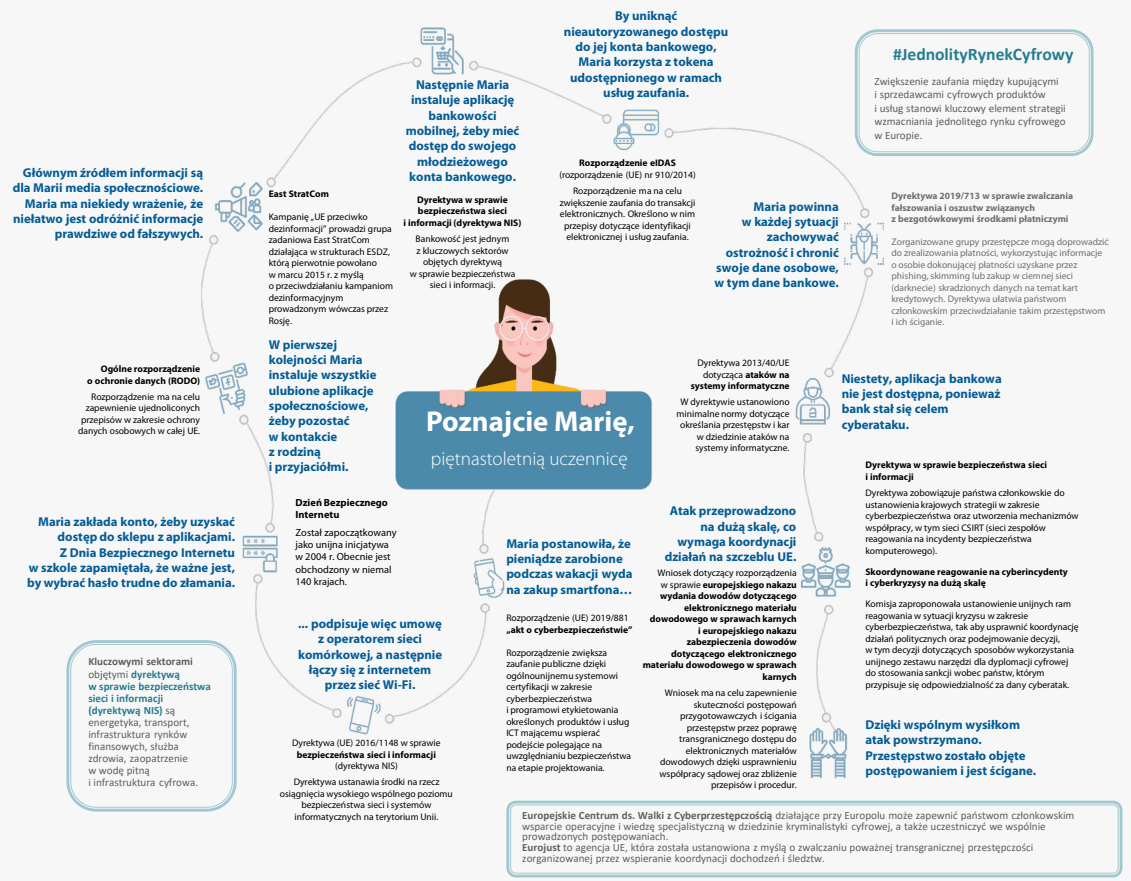
Czym jest cyberbezpieczeństwo?

1 Nie ma standardowej, powszechnie stosowanej **definicji cyberbezpieczeństwa**. W niniejszym dokumencie „cyberbezpieczeństwo" oznacza **działania niezbędne do ochrony sieci i systemów informacyjnych, ich użytkowników oraz innych osób narażonych na cyberataki**. Obejmuje to zapobieganie cyberincydentom, ich wykrywanie, reagowanie na nie oraz przywracanie działalności po takich incydentach. Incydenty te mogą zostać wywołane umyślnie lub nieumyślnie. Obejmują one różnorodne wydarzenia, począwszy od niezamierzonego ujawnienia informacji po ataki na przedsiębiorstwa i infrastrukturę krytyczną, kradzież danych osobowych, a nawet przypadki zakłócenia przebiegu procesów demokratycznych, w tym wyborów, oraz ogólne kampanie dezinformacyjne mające wpłynąć na debatę publiczną.

Cyberbezpieczeństwo ma wpływ na życie codzienne wszystkich obywateli Unii

2 Cyberbezpieczeństwo wpływa na życie codzienne wszystkich obywateli Unii, ilekroć korzystają oni z osobistych urządzeń cyfrowych takich jak smartfony, z sieci Wi-Fi, mediów społecznościowych lub bankowości elektronicznej. W 2020 r. najpilniejsze pytanie nie dotyczy już tego, czy cyberataki będą miały miejsce, ale w jaki sposób i kiedy zostaną przeprowadzone. Odnosi się to do wszystkich: **osób fizycznych, przedsiębiorstw i organów publicznych**. Na *ilustracji 1* przedstawiono, w jaki sposób UE wspiera cyberbezpieczeństwo, i opisano utworzone przez Unię ramy służące ochronie codziennych elektronicznych czynności obywateli przed cyberatakami. Ochrona krytycznych systemów informacyjnych i infrastruktury cyfrowej przed cyberatakami stała się wyzwaniem strategicznym.

Ilustracja 1 – W jaki sposób UE wspiera cyberbezpieczeństwo w codziennym życiu obywateli Unii



Źródło: Europejski Trybunał Obrachunkowy. Ikony wykonane przez Pixel perfect pochodzące z https://flaticon.com.

Istnieje wiele rodzajów zagrożeń dla cyberbezpieczeństwa

3 Można wyodrębnić różne kategorie zagrożeń dla cyberbezpieczeństwa, na jakie narażone są europejskie społeczeństwa, w zależności od tego, **w jaki sposób wpływają one na dane – czy chodzi o ujawnienie, modyfikację, zniszczenie danych lub uniemożliwienie do nich dostępu –** oraz tego, jakie podstawowe zasady bezpieczeństwa informacji zostały naruszone (zob. ***rys. 1***).

Rys. 1 – Rodzaje zagrożeń i zasady dotyczące bezpieczeństwa informacji, które mogą zostać naruszone w wyniku tych zagrożeń

Kłódka oznacza brak oddziaływania na bezpieczeństwo; wykrzyknik oznacza zagrożenie dla bezpieczeństwa.

Źródło: Europejski Trybunał Obrachunkowy na podstawie badania Parlamentu Europejskiego[1].

4 Wraz z podłączeniem każdego urządzenia do sieci lub połączeniem go z innymi urządzeniami zwiększa się tak zwana powierzchnia ataku. Gwałtownemu rozwojowi internetu rzeczy, przetwarzania w chmurze, dużych zbiorów danych i cyfryzacji przemysłu towarzyszy coraz większe narażenie na ataki, umożliwiające sprawcom dosięgnięcie coraz większej liczby ofiar. Zróżnicowanie i coraz bardziej zaawansowany charakter cyberataków sprawiają, że nadążenie za rozwojem sytuacji staje się trudne[2]. W ***ramce 1*** opisano przykłady **możliwych cyberataków**.

[1] Parlament Europejski, „Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses”, badanie zlecone przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych PE, wrzesień 2015 r.

[2] ENISA, „ENISA Threat Landscape Report 2017”, 18 stycznia 2018 r.

Ramka 1

Rodzaje cyberataków

Złośliwe oprogramowanie ma na celu wyrządzenie szkody w urządzeniach lub sieciach. Może obejmować wirusy komputerowe, trojany, oprogramowanie typu ransomware, robaki komputerowe, oprogramowanie reklamowe i szpiegujące (np. NotPetya).

Działanie **oprogramowania typu ransomware** polega na szyfrowaniu danych, tak aby uniemożliwić użytkownikom dostęp do plików do momentu, aż zostanie opłacony okup (ang. *ransom*), zazwyczaj w kryptowalucie, albo użytkownicy wykonają określone działanie. Zgodnie z danymi Europolu ataki typu ransomware są ogólnie najpowszechniejszym typem ataków, a liczba rodzajów takiego oprogramowania gwałtownie wzrosła w ostatnich latach (np. Wannacry[3]).

Coraz powszechniejsze stają się ponadto **rozproszone ataki typu „odmowa usługi" (ataki typu DDoS)**, które uniemożliwiają dostęp do usług i zasobów, zalewając systemy ogromną ilością zapytań, których nie sposób obsłużyć. W 2017 r. niemal jedna trzecia podmiotów musiała stawić czoła atakom tego rodzaju[4].

Ataki sieciowe są atrakcyjną metodą, dzięki której agresorzy mogą zwodzić ofiary, wykorzystując systemy i usługi internetowe jako wektor zagrożenia. Ten rodzaj zagrożeń obejmuje szeroką powierzchnię ataku, na przykład wykorzystanie złośliwych adresów URL lub złośliwych skryptów w celu skierowania użytkownika lub ofiary na wskazaną stronę internetową lub skłonienia go do pobrania złośliwych treści (ataki metodą wodopoju – ang. watering hole attacks, ataki typu drive-by) oraz **wstrzyknięcie** złośliwego kodu w wiarygodną stronę internetową, na którą jednak się włamano w celu wykradzenia danych (np. przechwycenie formularza), aby uzyskać korzyści finansowe lub nielegalnie pozyskać informacje[5].

Użytkownicy mogą paść ofiarą manipulacji i nieświadomie wykonać określoną czynność lub ujawnić poufne informacje. Takie oszustwa mogą być wykorzystywane do celów kradzieży danych lub cyberszpiegostwa i są znane pod nazwą **manipulacji z zakresu inżynierii społecznej**. Istnieją różne sposoby przeprowadzania tego rodzaju ataków. Jedną z powszechnie stosowanych metod jest **phishing**, polegający na przesyłaniu pocztą elektroniczną wiadomości sprawiających wrażenie, że pochodzą z wiarygodnych źródeł, tak aby skłonić użytkowników do ujawnienia informacji lub kliknięcia na łącza instalujące w urządzeniu złośliwe oprogramowanie. Ponad połowa państw członkowskich zgłosiła prowadzenie dochodzeń dotyczących takich ataków sieciowych[6].

Do najbardziej szkodliwych rodzajów zagrożeń należą **zaawansowane, trwałe zagrożenia** (ang. *advanced persistent threat* – APT). Źródłem tych zagrożeń są podmioty dopuszczające się ataków z wykorzystaniem zaawansowanych metod, prowadzące długoterminowe monitorowanie i kradzież danych, a czasem dążące do wywołania zniszczeń. Atak jest tak pomyślany, by pozostać niewidocznym przez możliwie jak najdłuższy okres. Ataki typu APT są często powiązane z określonymi państwami i ukierunkowane na szczególnie newralgiczne sektory, takie jak technologia, obronność i infrastruktura krytyczna. Szacuje się, że ten rodzaj **cyberszpiegostwa** odpowiada za co najmniej jedną czwartą wszystkich cyberincydentów[7].

[3] Oprogramowanie typu ransomware Wannacry wykorzystywało luki w protokole Microsoft Windows pozwalające na zdalne przejęcie kontroli nad dowolnym komputerem. Po tym, jak luka została odkryta, Microsoft udostępnił odpowiednią łatkę. Niemniej oprogramowanie setek tysięcy komputerów nie zostało zaktualizowane i wiele z nich padło w konsekwencji ofiarą ataku. *Źródło*: A. Greenberg, „Hold North Korea Accountable For Wannacry—and the NSA, too", Wired, 19 grudnia 2017 r.

[4] Europol, „Internet Organised Crime Threat Assessment 2018".

[5] ENISA, „ENISA Threat Landscape 2020 – Web-based attacks", 20 października 2020 r.

[6] Europol, zob. powyżej, 2018.

[7] European Centre for Political Economy, „Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?", dokument okolicznościowy nr 2/18, luty 2018 r.

Cyberataki powodują znaczne skutki gospodarcze

5 Zagrożenie **cyberatakami i cyberprzestępczością** stało się w ostatnich latach poważnym problemem. Już w 2016 r. 80% europejskich przedsiębiorstw doświadczyło co najmniej jednego cyberincydentu[8]. Zgodnie z wynikami ankiety przeprowadzonej w 2018 r. 40% respondentów z organizacji wykorzystujących rozwiązania z zakresu robotyki lub automatyzacji wskazało, że najpoważniejszą konsekwencją cyberataku na ich systemy byłoby zakłócenie działalności. Niemniej pomimo świadomości istnienia szkodliwego ryzyka w cyberprzestrzeni przedsiębiorstwa często nie dysponują żadnym systemem, który mógłby zaradzić temu ryzyku[9].

6 Od tego czasu liczba i dotkliwość cyberataków stale rośnie, podobnie jak związane z nimi koszty finansowe. W 2021 r. cyberprzestępczość – na tyle, na ile można oszacować jej **wpływ finansowy** – będzie już kosztować gospodarkę światową **6 bln dolarów rocznie**, co stanowi wzrost z szacowanych 3 bln dolarów w 2015 r.[10] (szacunkowy światowy PKB w 2020 r. wynosi 138 bln dolarów). Koszty cyberprzestępczości obejmują uszkodzenie i zniszczenie danych, kradzież pieniędzy, utratę produktywności, kradzież własności intelektualnej, kradzież danych osobowych i finansowych, zakłócenie normalnego przebiegu działalności po ataku, utratę reputacji. Europejska Rada ds. Ryzyka Systemowego (ERRS) szacuje, że średni koszt cyberincydentów wzrósł w latach 2015–2020 o 72%[11].

7 Jak wynika z badania przeprowadzonego w 2020 r., cyberprzestępczość **oddziałuje niekorzystnie na poszczególne sektory gospodarki na różne sposoby**[12]: była to najbardziej destruktywna forma oszustwa w sektorze rządowym i administracji publicznej, sektorze technologii, mediów i telekomunikacji oraz w sektorze zdrowia

---

8 Europol, „Internet Organised Crime Threat Assessment 2017".

9 PWC, „Global State of Information Security (GSISS) Survey – Strengthening digital society against cyber shocks", 2017.

10 Cybersecurity Ventures, „2019 Official Annual Cybercrime Report", sprawozdanie sfinansowane przez Herjavec Group, 2019 r.

11 ERRS, Europejska Rada ds. Ryzyka Systemowego, „Systemic cyber risk", luty 2020 r.

12 PWC, „Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey", 2020 r.

(zob. ***ramka 2***); była to również druga najbardziej destruktywna forma oszustwa w sektorze finansowym oraz w sektorze przemysłowym i wytwórczym.

Ramka 2

Fińscy pacjenci uczestniczący w psychoterapii szantażowani z wykorzystaniem prywatnych danych medycznych skradzionych w latach 2018–2019

W 2020 r. pacjenci dużej fińskiej kliniki psychoterapeutycznej z oddziałami na terenie całego kraju otrzymali prywatne wiadomości od szantażysty, po tym jak w listopadzie 2018 r. doszło do kradzieży ich danych osobowych, a następnie do kolejnego potencjalnego naruszenia w marcu 2019 r. Dane te prawdopodobnie zawierały informacje umożliwiające zidentyfikowanie pacjentów i zapis treści sesji terapeutycznych.

Zarówno klinika, jak i pacjenci otrzymali żądanie zapłacenia okupu w bitcoinach pod groźbą podania danych do wiadomości publicznej. W wyniku tego incydentu rząd Finlandii zwołał posiedzenie nadzwyczajne[13].

8 W 2019 r. Europol[14] ponownie zwrócił uwagę na fakt, że **szereg istotnych zagrożeń związanych z cyberprzestępczością ma charakter trwały i poważny**:

- największe zagrożenie nadal stanowią ataki typu ransomware – są coraz precyzyjniej wymierzone, coraz bardziej opłacalne i powodują większe szkody gospodarcze. Jeśli oprogramowanie typu ransomware będzie zapewniać cyberprzestępcom stosunkowo łatwy zysk oraz powodować znaczne szkody i straty finansowe, prawdopodobnie nadal będzie stanowiło największe zagrożenie związane z cyberprzestępczością;
- najważniejszymi wektorami infekowania złośliwym oprogramowaniem są phishing i podatne na ataki protokoły RDP;

[13] BBC News, „Therapy patients blackmailed for cash after clinic data breach”, 26 października 2020 r.

[14] Europol, „INTERNET organised crime threat assessment (IOCTA)”, 2019 r.

- głównym celem i towarem cyberprzestępczości oraz czynnikiem sprzyjającym jej rozwojowi w dalszym ciągu są dane.

9 W **sprawozdaniu z 2020 r. pt. „Main incidents in the EU and worldwide”**[15] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przedstawiła wiele przykładów cyberincydentów (zob. ***ramka 3***).

Ramka 3

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA): Cyberincydenty w latach 2019–2020

Platforma poczty elektronicznej verifications.io padła ofiarą poważnego naruszenia ochrony danych z powodu niezabezpieczonej bazy danych MongoDB. Ujawniono dane z ponad 800 mln wiadomości elektronicznych, zawierających informacje szczególnie chronione, w tym informacje pozwalające ustalić tożsamość.

Na popularnym forum hakerskim hostowanym za pośrednictwem usługi w chmurze MEGA1 opublikowano ponad 770 mln adresów poczty elektronicznej i 21 mln indywidualnych haseł. Był to największy w historii zbiór wykradzionych danych osobowych, nazwany „Collection #1”.

Citrix, dostawca usług w chmurze i usług wirtualizacji, padł ofiarą ukierunkowanego cyberataku. Aby uzyskać dostęp do systemów Citrix, sprawcy wykorzystali kilka krytycznych słabych punków w oprogramowaniu, takich jak CVE-2019-19781, i zastosowali technikę zwaną atakiem rozproszonym na hasła (ang. *password spraying*).

Dostawca usług hostowania w chmurze, przedsiębiorstwo iNSYNQ19, padł ofiarą ataku z wykorzystaniem oprogramowania typu ransomware, w wyniku którego klienci nie mieli dostępu do swoich danych przez ponad tydzień, co zmusiło ich do korzystania z lokalnych kopii zapasowych.

10 Według Europolu liczba cyberataków mających na celu spowodowanie **trwałych szkód** podwoiła się w pierwszych sześciu miesiącach 2019 r., głównie w przemyśle wytwórczym. W przeciwieństwie do zwykłych ataków z wykorzystaniem

[15] ENISA, „Main incidents in the EU and worldwide – January 2019 to April 2020”, październik 2020 r.

oprogramowania typu ransomware są to akty sabotażu, które trwale wymazują lub w inny sposób nieodwracalnie uszkadzają dane przedsiębiorstwa (zob. ***ramka 4***).

Ramka 4

Oprogramowanie typu ransomware mające na celu zniszczenie danych – ataki Germanwiper w 2019 r.

W 2019 r. zidentyfikowano serię ataków z wykorzystaniem oprogramowania typu ransomware skierowanych przeciwko firmom działającym w Niemczech. To oprogramowanie typu ransomware, które nazwano Germanwiper, może zastępować dane w zainfekowanych plikach zerami i jedynkami, uniemożliwiając tym samym ich odzyskanie. Oprogramowanie to rozprzestrzenia się za pośrednictwem phishingowych wiadomości elektronicznych – skierowanych w szczególności do pracowników działów kadr najlepszych firm, ponieważ zagnieżdżono je w fałszywych podaniach o pracę[16].

Wraz z coraz częstszym występowaniem zagrożeń związanych z cyberbezpieczeństwem rośnie świadomość na ich temat

11 Do niedawna wiedza na temat zagrożeń związanych z cyberbezpieczeństwem i świadomość ich występowania były jeszcze stosunkowo niewielkie. W 2017 r. 69% unijnych przedsiębiorstw nie posiadało żadnej wiedzy na temat własnego **narażenia na cyberzagrożenia**[17] lub posiadało taką wiedzę jedynie w podstawowym zakresie, a 60% nigdy nie szacowało **potencjalnych strat finansowych**[18]. Ponadto, jak wynika z globalnego badania ankietowego przeprowadzonego w 2018 r., jedna trzecia

[16] Cybersecurity Insiders, „GermanWiper Ransomware attack warning for Germany”, nieopatrzone datą.

[17] Opracowane przez Komisję Europejską zestawienie danych na temat cyberbezpieczeństwa, wrzesień 2017 r.

[18] Straty te mogą obejmować: utracone przychody; koszty naprawy uszkodzonych systemów; potencjalne zobowiązania związane ze skradzionymi zasobami lub informacjami; zachęty na rzecz zatrzymania klientów; wyższe składki ubezpieczeniowe; zwiększone koszty ochrony (nowe systemy i nowi pracownicy, szkolenia); uregulowanie ewentualnych kosztów przestrzegania przepisów lub wynikających ze sporów.

podmiotów zapłaciłaby raczej hakerom okup niż inwestowała w bezpieczeństwo informacji[19].

12 W **badaniu Eurobarometru z 2020 r. dotyczącym postaw Europejczyków wobec cyberbezpieczeństwa**[20] stwierdzono rosnącą świadomość – i rosnące obawy – obywateli Unii:

- Respondenci korzystający z internetu najczęściej obawiają się, że ktoś nieuczciwie wykorzystuje ich dane osobowe (46%), martwią się o bezpieczeństwo wykonywanych płatności online (41%), obawiają się, że nie będą mieli możliwości sprawdzenia towarów lub zwrócenia się do kogoś o poradę osobiście, bądź że mogą nie otrzymać towarów lub usług, które kupują w internecie (w obu przypadkach 22%).
- Ponad trzy czwarte (76%) respondentów uważa, że ryzyko stania się ofiarą cyberprzestępstwa jest coraz większe. Natomiast znacznie mniej (52%) respondentów uważa, że może się przed tym wystarczająco zabezpieczyć – co oznacza spadek o dziewięć punktów procentowych w stosunku do 2018 r.
- Nieco ponad połowa respondentów (52%) uważa, że jest dobrze poinformowana o cyberprzestępczości, ale jedynie 11% twierdzi, że jest bardzo dobrze poinformowanych.

[19] NTT Security, „Risk: Value 2018 Report".

[20] Komisja Europejska, „Special Eurobarometer 499 – Europeans' attitudes towards cyber security", styczeń 2020 r.

Cyberbezpieczeństwo jest istotne dla zapewnienia spójności społecznej i stabilności politycznej

Nowe zagrożenie – cyberbezpieczeństwo i dezinformacja

13 Umyślna, systematyczna **dezinformacja na dużą skalę stanowi dla europejskich demokracji poważne wyzwanie strategiczne**[21]. Dezinformacja i nieprawdziwe informacje (fake news) mogą prowadzić do podziałów w społeczeństwie, siać nieufność, a nawet podważać spójność społeczną i zaufanie do procesów demokratycznych (zob. ***ramka 5***).

Ramka 5

Dezinformacja

Komisja Europejska definiuje dezinformację jako tworzenie, przedstawianie i rozpowszechnianie możliwych do zweryfikowania nieprawdziwych lub wprowadzających w błąd informacji w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, w przypadkach gdy może to wyrządzić szkodę publiczną[22]. Szkoda publiczna może obejmować osłabienie procesów demokratycznych lub zagrożenia dla dóbr publicznych związanych np. ze zdrowiem, środowiskiem i bezpieczeństwem.

W przeciwieństwie do treści niezgodnych z prawem (które obejmują nawoływanie do nienawiści, treści o charakterze terrorystycznym lub materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych) dezinformacja obejmuje treści, których publikowanie jest legalne. Zjawisko to wiąże się więc z głównymi podstawowymi wartościami UE, takimi jak wolność wypowiedzi i wolność mediów. Zgodnie z definicją Komisji dezinformacja nie obejmuje wprowadzającej w błąd reklamy, błędów sprawozdawczych, satyry i parodii ani wyraźnie oznaczonych stronniczych wiadomości i komentarzy.

---

[21] Według badania pt. „The Global Disinformation Order" opublikowanego przez Uniwersytet Oksfordzki we wrześniu 2019 r. liczba krajów prowadzących polityczne kampanie dezinformacyjne wzrosła w ciągu ostatnich dwóch lat ponad dwukrotnie – do 70.

[22] Komisja Europejska, *komunikat w sprawie zwalczania dezinformacji w internecie*, (COM(2018) 236).

14 Nowe technologie i oprogramowanie umożliwiają łatwe i stosunkowo tanie rozpowszechnianie dezinformacji za pośrednictwem **mediów społecznościowych i innych mediów internetowych**. Dezinformacja zazwyczaj skupia się na drażliwych tematach, które mogą polaryzować opinię publiczną i wzbudzać silne emocje, a zatem jest bardziej prawdopodobne, że taka dezinformacja będzie się rozprzestrzeniać. Tematy te obejmują zagadnienia dotyczące zdrowia (np. kampanie antyszczepionkowe), migracji, zmiany klimatu lub sprawiedliwości społecznej.

Kampanie dezinformacyjne prowadzone przez państwa trzecie w celu wywarcia wpływu na procesy demokratyczne

15 Dezinformacja ma na celu spolaryzowanie głosów w ramach debaty demokratycznej, wywołanie lub zwiększenie napięć w społeczeństwie i osłabienie systemów wyborczych. Ma szerszy wpływ na europejskie społeczeństwa i bezpieczeństwo. Ostatecznie szkodzi ona wolności poglądów i wypowiedzi. Dezinformacja jest często **finansowana przez podmioty w państwach trzecich**, których celem jest destabilizacja europejskich społeczeństw i systemów demokratycznych. W tym kontekście zakrojone na szeroką skalę kampanie dezinformacyjne mogą również wiązać się z włamywaniem się do sieci. Przykładem takiego działania jest rosyjska kampania, której celem było wpłynięcie na wyniki brytyjskiego referendum w sprawie wystąpienia z Unii Europejskiej (zob. ***ramka 6***).

Ramka 6

Rosyjskie kampanie dezinformacyjne wymierzone w demokratyczne procesy decyzyjne[23]

W połowie 2016 r. podmioty z Rosji rozpoczęły kampanię mającą na celu wywarcie wpływu na wynik głosowania w brytyjskim referendum w sprawie wystąpienia z UE, które odbyło się w czerwcu 2016 r. W jednej z analiz tweetów wykazano, że w ciągu 48 godzin poprzedzających głosowanie ponad 150 000 rosyjskich kont udostępniło informacje na temat brexitu (*#Brexit*) i zamieściło ponad 45 000 wpisów o głosowaniu. W dniu referendum rosyjskie konta opublikowały 1 102 tweetów z hasztagiem *#ReasonsToLeaveEU* („powody, dla których należy wyjść z UE").

16 Zwalczanie dezinformacji stanowi poważne wyzwanie, ponieważ wymaga znalezienia odpowiedniej równowagi między bezpieczeństwem a unijnymi podstawowymi prawami i wolnościami, tak aby zachęcić do innowacji i wspierać otwarty rynek. UE podjęła ostatnio szereg działań mających na celu **zwalczenie tego problemu**.

- W 2015 r. utworzono w obrębie ESDZ **grupę zadaniową East StratCom** mającą rozwiązać problem rosyjskich kampanii dezinformacyjnych[24]. Specjaliści z zadowoleniem przyjęli prace grupy na rzecz promowania polityki UE, wspierania niezależnych mediów w państwach objętych europejską polityką sąsiedztwa oraz antycypowania, śledzenia i zwalczania dezinformacji[25].

[23] Park advisors, „Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age", Christina Nemr i William Gangware, 2019.

[24] Konkluzje Rady Europejskiej EUCO 11/15, 20 marca 2015 r. Od tamtego czasu utworzono dwie dodatkowe grupy zadaniowe, do spraw Bałkanów Zachodnich i państw południowego sąsiedztwa.

[25] W sprawozdaniu Atlantic Council wezwano UE, by nałożyła na wszystkie państwa członkowskie wymóg oddelegowania ekspertów krajowych do grupy zadaniowej. Zob. D. Fried oraz A. Polyakova, „Democratic Offense Against Disinformation", 5 marca 2018 r.

- W 2018 r. ENISA opublikowała **komunikat w sprawie zwalczania dezinformacji w internecie**[26]. Działania przewidziane w komunikacie obejmują pomoc w zwiększeniu wiarygodności treści oraz wspieranie wysiłków na rzecz zwiększenia umiejętności korzystania z mediów i serwisów informacyjnych.

- Wspólne Centrum Badawcze Komisji opracowało **dobrowolny kodeks postępowania w ramach samoregulacji** bazujący na istniejących instrumentach politycznych. Został on przyjęty przez platformy internetowe i branżę reklamową[27].

- Uruchomiono niezależną europejską **sieć osób weryfikujących informacje**.

Dezinformacja w czasach COVID-19 i reakcja UE

17 Dezinformacja stanowi problem również w kontekście **kryzysu zdrowotnego związanego z pandemią COVID-19**[28] (zob. przykłady takiej dezinformacji w ***ramce 7***).

[26] ENISA, „Strengthening Network & Information Security & Protecting Against Online Disinformation (»Fake News«)", kwiecień 2018 r.

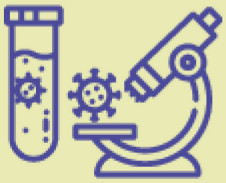
[27] JRC, „The digital transformation of news media and the rise of disinformation and fake news", sprawozdania techniczne JRC, dokument roboczy JRC poświęcony gospodarce cyfrowej 2018-02, kwiecień 2018 r.

[28] Reuters Institute i Uniwersytet Oksfordzki, „Types, Sources, and Claims of Covid-19 Misinformation", kwiecień 2020 r.

Ramka 7

Przykłady dezinformacji dotyczącej COVID-19 zgłoszone przez Komisję[29]

Fałszywe twierdzenia takie jak „wypicie wybielacza lub czystego alkoholu może wyleczyć infekcję koronawirusem". Tymczasem wypicie wybielacza lub czystego alkoholu może być bardzo szkodliwe. **Belgijski ośrodek zwalczania zatruć odnotował wzrost liczby przypadków związanych z wybielaczami o 15%.**



Teorie spiskowe takie jak twierdzenie, że koronawirus to „zakażenie wywoływane przez światowe elity w celu zmniejszenia wzrostu populacji". Z dowodów naukowych jasno wynika tymczasem, że wirus należy do rodziny wirusów pochodzących od zwierząt, która obejmuje inne wirusy, takie jak SARS i MERS.

Nienaukowe twierdzenia jakoby „instalacje sieci 5G przyczyniały się do rozprowadzania wirusa". Teorie te nie miały żadnego konkretnego uzasadnienia i doprowadziły do ataków na maszty sieciowe.

18 W marcu 2020 r. Komisja, ENISA, CERT-UE i Europol wydały **wspólne oświadczenie w sprawie zagrożeń związanych z COVID-19**[30], w którym stwierdzono, że podmioty działające w złej wierze aktywnie wykorzystują trudne okoliczności wynikające z kryzysu zdrowia publicznego, aby dotrzeć do pracowników zdalnych, przedsiębiorstw i osób prywatnych. Ponadto ENISA przygotowała specjalne kampanie informacyjne dla sektorów dotkniętych dezinformacją podczas pandemii COVID-19[31].

[29] Komisja Europejska, „Tackling coronavirus disinformation", nieopatrzone datą.

[30] Wspólne oświadczenie Komisji Europejskiej, ENISA, CERT-UE i Europolu w sprawie epidemii koronawirusa, 20 marca 2020 r.

[31] ENISA, arkusze informacyjne dotyczące COVID-19, 2020 r.

Weryfikowanie informacji ma zasadnicze znaczenie dla zwalczania dezinformacji

19 UE zintensyfikowała również wysiłki na rzecz wspierania osób weryfikujących informacje i naukowców zajmujących się badaniami nad dezinformacją w Europie. W szczególności utworzyła **Europejskie Obserwatorium Mediów Cyfrowych** w celu zbadania i lepszego zrozumienia zjawisk związanych z dezinformacją: zaangażowanych podmiotów, wektorów, narzędzi, metod, dynamiki rozpowszechniania, głównych celów i oddziaływania na społeczeństwo. Wśród innych sfinansowanych ze środków UE projektów dotyczących dezinformacji można wymienić PROVENANCE, SocialTruth, EUNOMIA i WeVerify.

20 W 2018 r. UE przyjęła **kodeks postępowania w zakresie zwalczania dezinformacji**[32], w którym zaproponowała pierwszy na świecie samoregulacyjny zestaw standardów w zakresie zwalczania dezinformacji. Platformy, główne sieci społecznościowe, reklamodawcy i branża reklamowa podpisały ten dobrowolny kodeks w październiku 2018 r. Jego sygnatariuszami są Facebook, Twitter, Mozilla, Google oraz stowarzyszenia i członkowie branży reklamowej. Microsoft podpisał kodeks postępowania w maju 2019 r. W czerwcu 2020 r. do grona sygnatariuszy kodeksu dołączył TikTok.

Zabezpieczenie wyborów do Parlamentu Europejskiego w 2019 r.

21 Legitymacja europejskich systemów demokratycznych opiera się na wyrażaniu przez świadomy elektorat demokratycznej woli w ramach **wolnych i uczciwych wyborów**. Wszelkie próby wrogiego i celowego podważania opinii publicznej i manipulowania nią stanowią zatem poważne zagrożenie dla europejskich społeczeństw. Ingerencja w wybory i infrastrukturę wyborczą może mieć na celu wpłynięcie na preferencje wyborców, frekwencję lub sam proces wyborczy, w tym faktyczne głosowanie, jak również w zestawianie i przekazywanie wyników głosowania. Wybory odbywające się w Europie w 2019 r., już po referendum w Zjednoczonym Królestwie, stały się pierwszą okazją do przeprowadzenia przez państwa członkowskie skoordynowanych działań mających na celu **ochronę integralności wyborów demokratycznych**. Dotyczyło to zarówno wyborów do Parlamentu Europejskiego, jak również wyborów do parlamentów narodowych.

[32] Unijny kodeks postępowania w zakresie zwalczania dezinformacji, wrzesień 2018 r.

22 Jak już wspomniano powyżej, w kwietniu 2018 r. Komisja opublikowała **komunikat pt. „Zwalczanie dezinformacji w internecie: podejście europejskie”**[33]. Następnie we wrześniu 2018 r. opublikowała **pakiet w sprawie wyborów**[34] mający na celu ochronę wyborów w UE i państwach członkowskich przed dezinformacją i cyberatakami. W pakiecie tym największy nacisk położono na ochronę danych, przejrzystość reklamy politycznej i finansowania działalności politycznej, cyberbezpieczeństwo i wybory, a także na sankcje za naruszanie przepisów o ochronie danych przez partie polityczne. Ponadto przeprowadzono **wspólne działanie** mające na celu sprawdzenie skuteczności praktyk w zakresie reagowania i planów kryzysowych państw członkowskich i UE, jeśli chodzi o ochronę wyborów do Parlamentu Europejskiego (zob. ***ramka 8***).

[33] Komunikat Komisji Europejskiej pt. „Zwalczanie dezinformacji w internecie: podejście europejskie” (COM(2018) 236 final).

[34] Komisja Europejska, orędzie o stanie Unii w 2018 r., wrzesień 2018 r.

Ramka 8

ELEx19 – ochrona wyborów do Parlamentu Europejskiego w 2019 r.[35]

Inicjatywa ELEx19 dotycząca zapewnienia odporności w obliczu zbliżających się wyborów do Parlamentu Europejskiego miała na celu określenie sposobów zapobiegania cyberincydentom, które mogłyby niekorzystnie wpłynąć na wybory w 2019 r., wykrywania takich cyberincydentów i łagodzenia odnośnych skutków.

Dzięki inicjatywie – opartej na różnych scenariuszach występowania zagrożeń i incydentów związanych z cyberbezpieczeństwem – uczestnicy mieli możliwość:

— uzyskać ogólny obraz poziomu odporności (w zakresie przyjętej polityki, dostępnych możliwości i umiejętności) systemów wyborczych w całej UE;

— zacieśnić współpracę między właściwymi organami na szczeblu krajowym (w tym organami wyborczymi oraz innymi właściwymi organami i agencjami);

— poddać testom istniejące plany zarządzania kryzysowego, jak również odpowiednie procedury zapobiegania cyberatakom i zagrożeniom hybrydowym, w tym kampaniom dezinformacyjnym, a także procedury wykrywania ich, radzenia sobie z nimi oraz reagowania na nie;

— uprawnić współpracę transgraniczną i wzmocnić powiązania z odpowiednimi grupami współpracy na szczeblu UE (np. siecią współpracy wyborczej, grupą współpracy ds. bezpieczeństwa sieci i informacji, siecią CSIRT);

— rozpoznać wszelkie inne potencjalne luki, jak również odpowiednie działania w zakresie ograniczania ryzyka, które należy podjąć przed wyborami do Parlamentu Europejskiego.

W inicjatywie tej wzięło udział ponad 80 przedstawicieli państw członkowskich UE oraz obserwatorzy z Parlamentu Europejskiego, Komisji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa.

[35] ENISA, „EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections”, 5 kwietnia 2019 r.

23 Ponadto w grudniu 2018 r. Rada Europejska przyjęła **plan działania na rzecz zwalczania dezinformacji**[36] w celu zapewnienia skoordynowanej reakcji i uzupełnienia działań krajowych. Ten plan działania obejmuje konkretne działania oparte na czterech filarach: zwiększenie zdolności instytucji Unii do wykrywania, analizowania i ujawniania dezinformacji; wzmocnienie skoordynowanej i wspólnej reakcji na dezinformację; mobilizowanie sektora prywatnego do zwalczania dezinformacji; podnoszenie świadomości i zwiększanie odporności społecznej.

Cyberbezpieczeństwo w UE – kompetencje, podmioty, strategie i prawodawstwo

Odpowiedzialność za cyberbezpieczeństwo spoczywa przede wszystkim na państwach członkowskich

24 W UE za cyberbezpieczeństwo **odpowiadają przede wszystkim państwa członkowskie**. Dotyczy to w szczególności ochrony informacji szczególnie chronionych związanych z bezpieczeństwem narodowym. Wszystkie państwa członkowskie posiadają **krajową strategię w zakresie cyberbezpieczeństwa**. Ma ona pomóc im w walce z zagrożeniami mogącymi utrudnić czerpanie korzyści gospodarczych i społecznych z cyberprzestrzeni. Różne są jednak zdolności państw członkowskich w zakresie cyberbezpieczeństwa oraz ich zaangażowanie w tej dziedzinie.

25 UE ma rolę do odegrania w budowaniu **wspólnych ram regulacyjnych** w obrębie jednolitego rynku UE i zapewnianiu państwom członkowskim warunków dla prowadzenia skutecznej współpracy w różnych obszarach polityki istotnych w kontekście cyberbezpieczeństwa, takich jak wymiar sprawiedliwości i sprawy wewnętrzne, jednolity rynek, transport, zdrowie publiczne, polityka konsumencka i badania. W polityce zewnętrznej kwestie dotyczące cyberbezpieczeństwa pojawiają

[36] Komisja Europejska, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, plan działania na rzecz zwalczania dezinformacji (JOIN(2018) 36 final). Plan jest ukierunkowany na: zwiększenie zdolności instytucji Unii do wykrywania, analizowania i ujawniania dezinformacji; wzmocnienie skoordynowanej i wspólnej reakcji na dezinformację; mobilizowanie sektora prywatnego; podnoszenie świadomości i zwiększanie odporności społecznej.

się w dyplomacji i w coraz większym stopniu stanowią element kształtującej się unijnej polityki obronnej i polityki bezpieczeństwa.

26 Główne **podmioty na szczeblu UE** zajmujące się cyberbezpieczeństwem opisano w *ramce 9* poniżej.

Ramka 9

Najważniejsze podmioty na szczeblu UE odpowiedzialne za cyberbezpieczeństwo

Komisja Europejska dąży do zwiększenia zdolności w zakresie cyberbezpieczeństwa oraz zacieśnienia współpracy i wzmocnienia roli UE w tej dziedzinie, a także do włączenia cyberbezpieczeństwa do innych strategii politycznych UE.

Komisję wspiera szereg agencji UE, w szczególności **ENISA**, **EC3** i **CERT-UE**. **Agencja Unii Europejskiej ds. Cyberbezpieczeństwa** (znana jako **ENISA** ze względu na swoją pierwotną nazwę – Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji) jest przede wszystkim organem doradczym i wspiera rozwój polityki, budowanie zdolności i zwiększanie świadomości. Działające przy Europolu **Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3)** utworzono w celu usprawnienia reakcji unijnych organów ścigania na przypadki cyberprzestępczości. W obrębie Komisji działa ponadto **zespół reagowania na incydenty komputerowe (CERT-UE)**, który wspiera wszystkie unijne instytucje, organy i agencje.

Europejska Służba Działań Zewnętrznych (ESDZ) odgrywa rolę przewodnią w dziedzinie cyberobrony, cyberdyplomacji i komunikacji strategicznej, a w jej strukturach działają ośrodki wywiadowcze i analityczne. Celem **Europejskiej Agencji Obrony** jest budowanie zdolności w zakresie cyberobrony.

Na szczeblu UE państwa członkowskie podejmują działania za pośrednictwem **Rady**, w ramach której działają liczne organy zajmujące się koordynacją działań i dzieleniem się informacjami (w tym Horyzontalna Grupa Robocza ds. Cyberprzestrzeni). **Parlament Europejski** pełni funkcję współprawodawcy.

Organizacje sektora prywatnego, w tym podmioty branżowe, organy zarządzające internetem i środowiska akademickie są partnerami, którzy przyczyniają do opracowywania i wdrażania polityki, np. za pośrednictwem umownego partnerstwa publiczno-prywatnego.

Strategia UE w dziedzinie cyberprzestrzeni – kwestia cyberbezpieczeństwa budziła poważne obawy od 2013 r.

27 Cyberbezpieczeństwo jest jednym z głównych problemów politycznych co najmniej od 2013 r., kiedy to Komisja przyjęła **strategię bezpieczeństwa cybernetycznego**[37]. Strategia ta obejmuje pięć podstawowych celów:

- zwiększenie cyberodporności;
- ograniczenie cyberprzestępczości;
- opracowanie polityki i rozbudowa zdolności w dziedzinie cyberobrony;
- rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
- ustanowienie międzynarodowej polityki w zakresie cyberprzestrzeni zgodnej z podstawowymi wartościami UE.

W kolejnych latach kwestię cyberbezpieczeństwa uwzględniono również w innych unijnych strategiach (zob. ***ramka 10***).

[37] Komisja Europejska, „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń” (JOIN(2013) 1 final z 7.2.2013).

Ramka 10

Inne strategie UE dotyczące kwestii cyberbezpieczeństwa

- **Europejska agenda bezpieczeństwa** z 2015 r.[38], której celem było usprawnienie ścigania przestępstw i reakcji wymiaru sprawiedliwości na przypadki cyberprzestępczości, zwłaszcza przez aktualizację obowiązujących strategii politycznych i przepisów.
- **Strategia jednolitego rynku cyfrowego** (2015 r.)[39], która miała na celu ulepszenie dostępu do towarów i usług cyfrowych: kluczowym elementem tej strategii wzmocnienie bezpieczeństwa w internecie, zaufania i włączenia społecznego.
- **Globalna strategia UE** (2016 r.)[40], w której określono szereg inicjatyw na rzecz umocnienia pozycji UE na świecie. Jednym z zasadniczych elementów strategii było cyberbezpieczeństwo oraz zwalczanie dezinformacji za pomocą komunikacji strategicznej.

28 Ponadto w 2017 r. Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa wydali **wspólny komunikat w sprawie cyberbezpieczeństwa w UE**[41], w którym wezwano do stworzenia solidniejszych i skuteczniejszych struktur służących wspieraniu cyberbezpieczeństwa i reagowaniu na cyberataki w państwach członkowskich, ale również w instytucjach, agencjach i organach UE.

---

[38] Komisja Europejska, „Europejska Agenda Bezpieczeństwa" (COM(2015) 185 final z 28.4.2015).

[39] Komisja Europejska, „Strategia jednolitego rynku cyfrowego dla Europy" (COM(2015) 192 final z 6.5.2015).

[40] ESDZ, „Wspólna wizja, wspólne działanie: Silniejsza Europa. Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej, czerwiec 2016 r.

[41] Komisja Europejska, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, plan działania na rzecz zwalczania dezinformacji (JOIN(2018) 36 final). budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" (JOIN(2017) 450 final z 13.9.2017).

29 W lipcu 2020 r. Komisja Europejska zaktualizowała swoją agendę z 2015 r. i przyjęła **strategię UE w zakresie unii bezpieczeństwa**[42] na lata 2020–2025, w której wskazała cyberbezpieczeństwo jako kwestię o znaczeniu strategicznym. W strategii tej Komisja zwraca w szczególności uwagę na tzw. zagrożenia hybrydowe, obejmujące zarówno cyberataki, jak i kampanie dezinformacyjne, w ramach których podmioty państwowe i niepaństwowe z państw trzecich podejmują wspólne działania w celu manipulowania środowiskiem informacyjnym i atakowania infrastruktury podstawowej.

Unijne przepisy dotyczące cyberbezpieczeństwa – dyrektywa w sprawie bezpieczeństwa sieci i informacji, RODO, akt o cyberbezpieczeństwie oraz nowy mechanizm sankcji

30 Głównym filarem strategii w zakresie cyberbezpieczeństwa z 2013 r. i zasadniczym aktem prawnym w tej dziedzinie jest **dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS)**[43] z 2016 r., będąca pierwszym ogólnounijnym aktem prawnym w dziedzinie cyberbezpieczeństwa. Dyrektywa ma pozwolić państwom członkowskim na osiągnięcie minimalnego jednorodnego poziomu zdolności. W tym celu nakłada na te państwa obowiązek przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i informacji oraz utworzenia pojedynczych punktów kontaktowych i zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych CSIRT)[44]. W dyrektywie ustanowiono ponadto wymogi dotyczące bezpieczeństwa i zgłaszania incydentów obowiązujące operatorów usług kluczowych w sektorach o krytycznym znaczeniu oraz dostawców usług cyfrowych.

---

[42] Komisja Europejska, komunikat w sprawie strategii UE w zakresie unii bezpieczeństwa (COM(2020) 605 final z 24.7.2020).

[43] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[44] Są one włączone do struktur współpracy ustanowionych na mocy dyrektywy, sieci CSIRT (w której uczestniczą CSIRT wyznaczone przez państwa członkowskie UE i CERT-UE, przy czym usługi sekretariatu świadczy ENISA) oraz grupy współpracy (która wspiera i ułatwia współpracę strategiczną i wymianę informacji między państwami członkowskimi, przy czym w tym wypadku usługi sekretariatu świadczy Komisja).

31 Państwa członkowskie miały dokonać transpozycji **dyrektywy w sprawie bezpieczeństwa sieci i informacji do swojego prawa krajowego** do maja 2018 r. Do listopada 2018 r. musiały również zidentyfikować tzw. operatorów usług kluczowych. Komisja Europejska ma obowiązek dokonywania okresowego przeglądu funkcjonowania dyrektywy. W okresie od lipca do października 2020 r. – w ramach realizacji głównego celu polityki, jakim jest „Europa na miarę ery cyfrowej", a także zgodnie z celami unii bezpieczeństwa – Komisja przeprowadziła konsultacje, których wyniki zostaną wykorzystane do przeprowadzenia pierwszej ewaluacji i oceny *ex post* skutków dyrektywy w sprawie bezpieczeństwa sieci i informacji.

32 Jednocześnie w 2016 r. weszło w życie **ogólne rozporządzenie o ochronie danych**[45] (RODO), a jego przepisy mają zastosowanie od maja 2018 r. Celem rozporządzenia jest zapewnienie ochrony danych osobowych obywateli UE dzięki ustanowieniu zasad regulujących przetwarzanie i rozpowszechnianie tych danych. Przepisy rozporządzenia przyznają osobom, których dane dotyczą, pewne prawa, a na administratorów danych (dostawców usług cyfrowych) nakładają określone obowiązki dotyczące wykorzystania i przekazywania informacji.

33 Ponadto w unijnym **akcie o cyberbezpieczeństwie**[46] wprowadzono po raz pierwszy ramy certyfikacji cyberbezpieczeństwa na szczeblu unijnym dotyczące produktów, usług i procesów ICT. Oznacza to, że przedsiębiorstwa prowadzące działalność gospodarczą w UE będą musiały certyfikować swoje produkty, procesy i usługi ICT jedynie raz, a uzyskane certyfikaty będą uznawane w całej UE. W unijnym akcie o cyberbezpieczeństwie ustanowiono również **Agencję Unii Europejskiej ds. Cyberbezpieczeństwa** (ENISA, która zastąpiła dawną Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji). W akcie powierzono agencji zadanie zacieśniania współpracy operacyjnej na szczeblu unijnym przez udzielanie pomocy w zakresie reagowania na cyberincydenty tym państwom członkowskim UE, które się o taką

---

[45] 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).

[46] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych

pomoc zwrócą, oraz wspieranie koordynacji działań UE w przypadku transgranicznych cyberataków i cyberkryzysów na dużą skalę.

34 Ponadto w maju 2019 r. Rada ustanowiła instrument prawny, który pozwala UE nakładać ukierunkowane **środki ograniczające, by zapobiegać cyberatakom** stanowiącym zewnętrzne zagrożenie dla UE lub jej państw członkowskich i reagować na nie[47]. W rezultacie UE posiada uprawnienia do nakładania sankcji na osoby lub podmioty, które:

- są odpowiedzialne za cyberataki lub usiłowanie przeprowadzenia cyberataków;
- zapewniają w tym celu wsparcie finansowe, techniczne lub materialne lub są zamieszane w inny sposób.

W lipcu 2020 r. Rada po raz pierwszy skorzystała z tych nowych prerogatyw (zob. ***ramka 11***).

Ramka 11

Bardziej stanowcze działania – UE nakłada pierwsze w historii sankcje w związku z cyberatakami[48]

W lipcu 2020 r. Rada nałożyła środki ograniczające na sześć osób i trzy podmioty odpowiedzialne za cyberataki lub w nie zaangażowane. Chodzi m.in. o próbę cyberataku na Organizację ds. Zakazu Broni Chemicznej oraz ataki ogólnie znane pod nazwami WannaCry, NotPetya i Operation Cloud Hopper.

Sankcje polegają na zakazie wjazdu i zamrożeniu aktywów. Ponadto osoby i podmioty podlegające sankcjom nie mogą otrzymywać funduszy od osób i podmiotów z UE.

---

[47] Decyzja Rady (WPZiB) 2019/797 z 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim.

[48] Decyzja Rady (WPZiB) 2020/1127 z 30 lipca 2020 r. zmieniająca wspomnianą powyżej decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim.

Cyberbezpieczeństwo i cyberobrona

35 W ostatnich latach cyberprzestrzeń stawała się coraz bardziej zmilitaryzowana[49] i w coraz większym stopniu wykorzystywano ją w działaniach wojennych[50]. Obecnie postrzega się ją jako piątą sferę prowadzenia wojny obok lądu, morza, powietrza i przestrzeni kosmicznej. Unijne **ramy polityki w dziedzinie cyberobrony** przyjęto w 2014 r. i zaktualizowano w 2018 r.[51] W toku aktualizacji z 2018 r. wskazano priorytety obejmujące rozwój zdolności w zakresie cyberobrony oraz ochronę sieci komunikacyjnych i informacyjnych wspólnej polityki bezpieczeństwa i obrony UE. Cyberobrona stanowi również część ram stałej współpracy strukturalnej (PESCO) oraz współpracy między UE i NATO.

36 Powszechne stały się przypadki wykorzystywania cyberprzestrzeni do celów politycznych oraz agresywnego testowania i penetracji zabezpieczeń w zakresie cyberbezpieczeństwa w UE i państwach członkowskich. Te działania cyberszpiegowskie i hakerskie – wymierzone w rządy krajowe, podmioty polityczne i instytucje UE w celu pozyskiwania i gromadzenia informacji niejawnych – świadczą o tym, że przeciwko UE i jej państwom członkowskim prowadzone są wyrafinowane operacje w zakresie cyberszpiegostwa i manipulacji danymi. W unijnych **wspólnych ramach dotyczących przeciwdziałania zagrożeniom hybrydowym** z 2016 r. podjęto kwestię zagrożeń dla cyberbezpieczeństwa zarówno w odniesieniu do infrastruktury krytycznej, jak i do indywidualnych użytkowników, zwracając przy tym uwagę na fakt, że cyberataki mogą

---

[49] Centrum Studiów nad Polityką Europejską, „Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force", listopad 2018 r.

[50] Stany Zjednoczone, Zjednoczone Królestwo i Australia wskazały Koreę Północną jako miejsce pochodzenia złośliwego oprogramowania będącego przyczyną ataku typu ransomware Wannacry. Pierwotnie zostało ono jednak opracowane i było przechowywane przez amerykańską Narodową Agencję Bezpieczeństwa w celu wykorzystania luk w systemie Windows.
Źródło: A. Greenberg, Wired, 19 grudnia 2017 r. W następstwie ataków Microsoft potępił gromadzenie informacji na temat luk w oprogramowaniu i ponowił apel o ustanowienie „cyfrowej konwencji genewskiej".

[51] Ramy polityki UE w zakresie cyberobrony (aktualizacja 2018 r.) (14413/18) z 19 listopada 2018 r.

również przyjąć postać kampanii dezinformacyjnych w mediach społecznościowych[52]. W dokumencie zwrócono również uwagę na konieczność podniesienia poziomu świadomości i zacieśnienia współpracy między UE i NATO, co znalazło konkretny wyraz we wspólnych deklaracjach UE i NATO z 2016 i 2018 r.[53]

Wydatki związane z cyberbezpieczeństwem w UE – rozproszone i niewystarczające

Wydatki na cyberbezpieczeństwo w UE-27 są niższe niż w Stanach Zjednoczonych

37 Trudno oszacować wydatki publiczne na cyberbezpieczeństwo ze względu na przekrojowy charakter tej dziedziny, a także ponieważ często nie sposób rozróżnić wydatków ogólnych w obszarze IT i wydatków na potrzeby cyberbezpieczeństwa[54]. Niemniej z dostępnych danych wynika, że **wydatki publiczne na cyberbezpieczeństwo** w UE są stosunkowo niskie:

- W 2020 r. budżet rządu federalnego Stanów Zjednoczonych na samo cyberbezpieczeństwo wynosił około **17,4 mld dolarów**[55].

[52] Komisja Europejska i Europejska Służba Działań Zewnętrznych, „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej” (JOIN(2016) 18 final z 6.4.2016).

[53] Wspólne deklaracje przewodniczącego Rady Europejskiej, przewodniczącego Komisji oraz sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego z 8 lipca 2016 r. i z 10 lipca 2018 r.

[54] Komisja Europejska, COM(2018) 630 final z 12.9.2018.

[55] Biały Dom, „Cybersecurity spending fiscal year 2020”.

- Tytułem porównania, Komisja oszacowała, że wydatki publiczne na cyberbezpieczeństwo wynoszą **1–2 mld euro** rocznie we wszystkich państwach członkowskich UE (które łącznie mają prawie taki sam PKB jak USA)[56].

- Szacuje się, że w przypadku wielu państw członkowskich wydatki publiczne na cyberbezpieczeństwo wyrażone jako procent PKB wynoszą **jedną dziesiątą wydatków Stanów Zjednoczonych** lub jeszcze mniej[57].

Lata 2014–2020 – finansowanie unijne cyberbezpieczeństwa zostało rozproszone między kilka różnych instrumentów

38 Zgodnie z informacjami Komisji[58] w ramach budżetu ogólnego UE istnieje **co najmniej dziesięć różnych instrumentów**, za pomocą których można finansować przedsięwzięcia związane z cyberbezpieczeństwem (najistotniejsze programy w ujęciu finansowym przedstawiono w ***ramce 12***). Łączne finansowanie unijne na rzecz cyberbezpieczeństwa o charakterze innym niż wojskowy wynosiło w latach 2014–2020 **poniżej 200 mln euro rocznie**. Nie istnieje również żaden ogólnounijny instrument finansowania, który wspierałby państwa członkowskie w koordynacji działań w zakresie cyberbezpieczeństwa.

---

[56] Komisja Europejska, dokument roboczy służb Komisji pt. „Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program »Cyfrowa Europa« na lata 2021–2027” (SWD(2018) 305 final z 6.6.2018).

[57] The Hague Centre for Strategic Studies, „Dutch investments in ICT and cybersecurity: putting it in perspective”, grudzień 2016 r.

[58] Komisja Europejska, ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji (SWD(2018) 403 final z 12.9.2018).

Ramka 12

Programy unijne, w ramach których zapewnia się wsparcie na rzecz cyberbezpieczeństwa (okres 2014–2020)

- W ramach unijnych **programów badawczych „Horyzont 2020”** w latach 2014–2020 przeznaczono około 600 mln euro na projekty dotyczące cyberbezpieczeństwa i cyberprzestępczości. W kwocie tej uwzględniono 450 mln euro, które przydzielono w latach 2017–2020 na umowne partnerstwa publiczno-prywatne z myślą o przyciągnięciu dodatkowych środków na kwotę 1,8 mld euro z sektora prywatnego.

- Przewidziano wkład z **europejskich funduszy strukturalnych i inwestycyjnych (funduszy ESI)** w wysokości do 400 mln euro na inwestycje państw członkowskich w cyberbezpieczeństwo do końca 2020 r.

- Z **instrumentu „Łącząc Europę”** sfinansowano inwestycje w wysokości około 30 mln euro rocznie. Obejmują one współfinansowanie krajowych zespołów reagowania na incydenty komputerowe, które państwa członkowskie są zobowiązane ustanowić na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji, w kwocie około 13 mln euro rocznie w latach 2016–2018[59].

- W ramach **Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej** wspierane są badania, spotkania ekspertów i działania informacyjne, przy czym na te cele przeznaczono w latach 2014–2017 niemal 62 mln euro. Ponadto w ramach zarządzania dzielonego państwa członkowskie mogą otrzymywać dotacje na sprzęt, szkolenia, badania naukowe i gromadzenie danych. Łączna kwota tych dotacji wynosi 42 mln euro i skorzystało z nich już 19 państw członkowskich.

- W ramach **programu „Sprawiedliwość”** przeznaczono środki o wartości 9 mln euro na wsparcie współpracy sądowej i traktatów o wzajemnej pomocy prawnej, ze szczególnym uwzględnieniem wymiany danych elektronicznych i informacji finansowych.

[59] Art. 9 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji).

39 Ponadto przydzielono ponad 500 mln euro z budżetu UE na **Europejski program rozwoju przemysłu obronnego** w latach 2019 i 2020[60]. Program jest ukierunkowany na usprawnienie koordynacji i zwiększenie efektywności wydatkowania środków państw członkowskich na obronność dzięki zachętom na rzecz wspólnego rozwoju wyposażenia i technologii. Celem jest uruchomienie łącznych inwestycji w zdolności obronne na kwotę 13 mld euro po 2020 r. za pośrednictwem Europejskiego Funduszu Obronnego, przy czym część wydatków dotyczyć będzie cyberobrony. Ponadto w ramach **europejskiej inicjatywy na rzecz bezpieczeństwa** Europejski Bank Inwestycyjny zapewni 6 mld euro na finansowanie podwójnego zastosowania (badania i rozwój oraz cyberbezpieczeństwo i bezpieczeństwo cywilne) w latach 2018–2020[61].

Lata 2021–2027: nowy program „Cyfrowa Europa”

40 W konkluzjach z lipca 2020 r. w sprawie nowych wieloletnich ram finansowych (WRF) na lata 2021–2027 Rada postanowiła, że w ramach **programu „Cyfrowa Europa”**[62] należy zainwestować w kluczowe strategiczne zdolności cyfrowe, takie jak unijne systemy obliczeń wielkiej skali, sztuczna inteligencja i cyberbezpieczeństwo. Program będzie stanowił uzupełnienie innych instrumentów, w szczególności programu „Horyzont Europa” i instrumentu „Łącząc Europę”, wspierając transformację cyfrową Europy.

---

[60] Komisja Europejska, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1092 z dnia 18 lipca 2018 r. ustanawiające Europejski program rozwoju przemysłu obronnego mający na celu wspieranie konkurencyjności i zdolności innowacyjnych przemysłu obronnego Unii (Dz.U. L 200 z 7.8.2018, s. 30).

[61] Europejski Bank Inwestycyjny, „The EIB Group Operating Framework and Operational Plan 2018”, 12.12.2017.

[62] Komisja Europejska, „Europejskie inwestycje w dziedzinie cyfrowej: program «Cyfrowa Europa»”, wrzesień 2020 r.

41 Rada postanowiła ponadto przeznaczyć na program „Cyfrowa Europa” 6,8 mld euro w latach 2021–2027, czyli ok. **970 mln euro rocznie**. Stanowi to znaczny wzrost w porównaniu z latami 2014–2020, ale kwota jest wciąż mniejsza niż pierwotnie zaproponowana przez Komisję (8,2 mld euro na ten sam okres, z czego 2 mld euro przeznaczono na wzmocnienie unijnego sektora cyberbezpieczeństwa i ogólnej ochrony społeczeństwa, na przykład przez wspieranie wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji).

CZĘŚĆ II – Przegląd prac najwyższych organów kontroli

Wstęp

42 Cyberbezpieczeństwo i autonomia cyfrowa stały się kwestiami o strategicznym znaczeniu dla UE i jej państw członkowskich. Uchybienia w zarządzaniu w zakresie cyberbezpieczeństwa są powszechne w sektorach publicznym i prywatnym w UE, choć zakres stwierdzanych uchybień jest zróżnicowany. Taka sytuacja zmniejsza zdolność Unii do ograniczania cyberataków i reagowania na nie w razie potrzeby.

43 W 2018 r. w badaniu przeprowadzonym wśród najwyższych organów kontroli w UE wykazano jednak, że około połowa z nich nigdy nie prowadziła kontroli w obszarze cyberbezpieczeństwa. Od tego czasu najwyższe organy kontroli zintensyfikowały prace kontrolne w tym zakresie. Kontrolerzy położyli szczególny nacisk na kwestię ochrony danych, gotowość systemów na cyberataki oraz zabezpieczenie systemów zapewniających najważniejsze usługi użyteczności publicznej. Analizie poddano również inne bardzo istotne kwestie. Zrozumiałe jest, że nie wszystkie z tych kontroli można podać do publicznej wiadomości, ponieważ niektóre z nich mogą obejmować informacje szczególnie chronione (dotyczące bezpieczeństwa narodowego).

44 Z uwagi na znaczenie cyberbezpieczeństwa dla funkcjonowania europejskich społeczeństw i instytucji politycznych Komitet Kontaktowy postanowił poświęcić tegoroczne kompendium kontroli właśnie temu zagadnieniu. W części II kompendium przedstawiono podsumowanie wyników wybranych kontroli w zakresie cyberbezpieczeństwa przeprowadzonych przez NOK 12 państw członkowskich i Europejski Trybunał Obrachunkowy. Każdy z uczestniczących NOK przedstawił jedno wybrane sprawozdanie z kontroli, które omówiono bardziej szczegółowo w części III. Te wybrane kontrole stanowią jedynie małą część wszystkich kontroli przeprowadzonych w tej dziedzinie, o czym świadczy duża liczba innych sprawozdań wskazanych przez uczestniczące NOK.

Metodyka kontroli i tematy objęte zakresem kontroli

45 Jeśli chodzi o rodzaje kontroli stanowiących podstawę sprawozdań streszczonych w niniejszym kompendium, większość NOK uczestniczących w przygotowaniu publikacji przeprowadziła kontrole wykonania zadań odnoszące się do kwestii związanych z cyberbezpieczeństwem. Dwa organy (polski i węgierski) przeprowadziły kontrole zgodności, a jeden (Europejski Trybunał Obrachunkowy) przeprowadził przegląd polityki.

46 Przy określaniu podejścia kontrolnego większość NOK opracowało koncepcję kontroli w taki sposób, aby obejmowały one co najmniej dwa sposoby oceny przedmiotu kontroli. Do sposobów tych należały przykładowo przegląd strategicznych dokumentów wysokiego szczebla (np. krajowych) lub określonych strategii, przegląd procedur pod kątem oceny ich zgodności z ustaloną metodyką COBIT (zob. ***ramka 13***) lub przegląd skuteczności istniejących informatycznych systemów zarządzania. Jeden z NOK (niderlandzka Powszechna Izba Obrachunkowa) zaangażował nawet etycznych hakerów do zbadania skuteczności systemów cyberbezpieczeństwa wykorzystywanych na potrzeby kontroli granicznej i infrastruktury gospodarki wodnej o znaczeniu krytycznym. W ***ramce 14*** przedstawiono w postaci schematu zestawienie metod i technik stosowanych przez poszczególne NOK w prowadzonych pracach kontrolnych.

Ramka 13

Co to jest COBIT?

Cele kontroli w zakresie technologii informacyjnej i technologii pokrewnych (COBIT) to ramy uznanych najlepszych praktyk i procedur w zakresie zarządzania systemami informatycznymi i ładu informatycznego zdefiniowane przez stowarzyszenie do spraw audytu i kontroli systemów informacyjnych ISACA (ang. Information Systems Audit and Control Association). Za sprawą COBIT organizacja może łatwiej osiągać cele strategiczne dzięki skutecznemu wykorzystaniu dostępnych zasobów i minimalizacji ryzyka informatycznego. COBIT pozwala powiązać wzajemnie zarządzanie przedsiębiorstwem z ładem informatycznym dzięki połączeniu celów biznesowych i informatycznych, określeniu wskaźników i modeli dojrzałości na potrzeby pomiaru stopnia realizacji celów oraz określeniu zakresu odpowiedzialności właścicieli poszczególnych procesów biznesowych i informatycznych.

47 Kontrole dotyczące cyberbezpieczeństwa dotyczyły bardzo zróżnicowanych kwestii. Niektóre NOK przeprowadziły kontrolę bardzo konkretnych obszarów służących interesowi publicznemu – na przykład niderlandzki najwyższy organ kontroli przeprowadził kontrolę dotyczącą cyberbezpieczeństwa kluczowych obiektów chroniących wybrzeże i systemów gospodarki wodnej. Z kolei inne NOK, np. irlandzki i węgierski, zajęły się zagadnieniami o bardziej przekrojowym charakterze, takimi jak wdrożenie krajowej strategii cyberbezpieczeństwa oraz ochrona danych osobowych i krajowych zasobów danych. Niemniej wszystkie NOK zajmowały się problemami, które mogą negatywnie wpłynąć na usługi publiczne lub infrastrukturę.

48 Estoński i litewski NOK podkreśliły strategiczne znaczenie krajowych zasobów danych, które są kluczowe dla bezpieczeństwa narodowego, oraz ochrony integralności tych zasobów przed cyberatakami z zewnątrz. Duński NOK przeprowadził kontrolę poświęconą w szczególności ocenie zabezpieczenia czterech podmiotów publicznych przed atakami typu ransomware. Niderlandzki, polski i portugalski NOK skontrolowały skuteczność różnych systemów informatycznych wykorzystywanych do celów kontroli granicznych (odpowiednio w porcie lotniczym Schiphol, w Komendzie Głównej Straży Granicznej oraz w Ministerstwie Spraw Wewnętrznych i Administracji w Polsce oraz na granicach portugalskich). Kontrole te dotyczyły zatem również bezpieczeństwa wewnątrz UE.

Okres objęty kontrolą

49 Wybrane sprawozdania z kontroli zawarte w niniejszym kompendium opublikowano w latach 2014–2020. W przypadku większości z nich okres objęty kontrolą wynosił dwa lata lub więcej, chociaż w przypadku czterech (Dania, Estonia, Francja i Portugalia) okresy objęte kontrolą wynosiły jeden rok.

Cele kontroli

50 Poszczególne NOK uczestniczące w przygotowaniu niniejszego kompendium zajmowały się w prowadzonych pracach kontrolnych różnymi rodzajami ryzyka. Wśród czynników ryzyka przedstawionych w opisach kontroli można wymienić: zagrożenia dla praw indywidualnych obywateli Unii wynikające z niewłaściwego przetwarzania danych osobowych; ryzyko, że instytucje nie będą w stanie świadczyć istotnych usług publicznych lub będą działały mniej sprawnie; poważne konsekwencje dla bezpieczeństwa publicznego, dobrobytu i gospodarki w danym państwie członkowskim, a także dla cyberbezpieczeństwa w UE. Co najmniej cztery NOK (estoński, węgierski, niderlandzki i portugalski) uwzględniły co najmniej trzy wspomniane tematy w sprawozdaniach z kontroli omówionych w niniejszym kompendium.

51 Cyberbezpieczeństwo należy do kompetencji państw członkowskich. Niemniej ponieważ z czasem zwiększył się zakres i szczegółowość prawodawstwa UE, większość instytucji i organów kontrolowanych przez najwyższe organy kontroli już teraz przyczynia się do osiągania strategicznych celów UE w zakresie cyberbezpieczeństwa, choć w różnym stopniu. Na przykład irlandzki Urząd Kontrolera i Audytora Generalnego

przeprowadził kontrolę wdrożenia unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji, która ma na celu poprawę odporności kluczowych sieci i systemów informacyjnych, oraz doradził, w jaki sposób można usprawnić wdrożenie tej dyrektywy. Aspekt zgodności z obowiązującymi dyrektywami UE uwzględniono również w kontroli przeprowadzonej przez węgierską Państwową Izbę Obrachunkową.

52 W ***ramce 14*** wskazano także przypadki, w których wynik kontroli przyczynił się do zwiększenia cyberodporności jednostek kontrolowanych, do ograniczenia cyberprzestępczości albo pomógł w opracowaniu strategii w zakresie cyberobrony i zwiększeniu kompetencji, usprawnieniu rozwoju technologii i osiągnięciu postępów we współpracy na szczeblu międzynarodowym – elementy te stanowią w szczególności główne cele unijnej strategii w zakresie cyberbezpieczeństwa. Zalecenia przedstawione przez NOK w większości przypadków dotyczyły więcej niż dwóch celów strategicznych, do których osiągnięcia dąży UE.

53 Ponadto w wyniku prac kontrolnych przeprowadzonych przez NOK zidentyfikowano luki w zakresie bezpieczeństwa lub wdrażania, które skłoniły skontrolowane instytucje do dodatkowych wysiłków. Na przykład cztery skontrolowane duńskie instytucje już w trakcie prac kontrolnych rozpoczęły wdrażanie szeregu mechanizmów zabezpieczeń ukierunkowanych na przyszłe zagrożenia, tak aby znacznie zwiększyć poziom ochrony przed atakami typu ransomware. Zapoczątkowały również rozwijanie zdolności obronnych i zwiększanie odporności na cyberprzestępczość, tym samym zmniejszając swoją podatność na cyberprzestępczość w przyszłości.

54 Należy przy tym zauważyć, że zalecenia z kontroli przedstawiono w odniesieniu do różnych szczebli zarządzania i odpowiedzialności, kierując je do instytucji rządowych na szczeblu centralnym, ministerstw i agencji na szczeblu operacyjnym lub właścicieli systemów informatycznych.

Ramka 14

Przegląd prac kontrolnych NOK, których wyniki przedstawiono w kompendium (część 1)

Główny obszar tematyczny		Dania	Estonia	Irlandia	Francja	Łotwa	Litwa	Węgry	Niderlandy	Polska	Portugalia	Finlandia	Szwecja	UE (Trybunał Obrachunkowy)
Rodzaj kontroli	Kontrola wykonania zadań	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Kontrola zgodności							✓		✓				
	Przegląd													✓
Podejście kontrolne	Przegląd strategii	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Przegląd procedur	✓	✓		✓		✓	✓		✓	✓	✓		
	Przegląd systemów	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Ocena solidności za pomocą badania bezpośredniego								✓		✓			
Uwzględnione zagrożenia	Oddziaływanie na prawa indywidualne		✓		✓			✓			✓			✓
	Oddziaływanie na infrastrukturę lub usługi publiczne	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Oddziaływanie na bezpieczeństwo narodowe		✓	✓		✓	✓	✓	✓		✓			
	Oddziaływanie na bezpieczeństwo w UE	✓							✓		✓			✓

Przegląd prac kontrolnych NOK, których wyniki przedstawiono w kompendium (część 2)

Główny obszar tematyczny		Dania	Estonia	Irlandia	Francja	Łotwa	Litwa	Węgry	Niderlandy	Polska	Portugalia	Finlandia	Szwecja	UE (Trybunał Obrachunkowy)
Uwzględnione cele strategiczne UE w zakresie cyberbezpieczeństwa	Zwiększenie cyberodporności	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Ograniczenie cyberprzestępczości	✓					✓							✓
	Opracowanie polityki i rozbudowa zdolności w dziedzinie obrony	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Rozwój zasobów technologicznych				✓	✓			✓				✓	
	Poprawa współpracy międzynarodowej (strategie)			✓				✓						✓
Na jakim poziomie adresowane są zalecenia	Poziom instytucji rządowych na szczeblu centralnym	✓	✓				✓					✓	✓	✓
	Poziom operacyjny (ministerstwa i agencje)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Poziom właścicieli systemów informatycznych	✓			✓			✓	✓	✓				

Główne uwagi z kontroli

55 Poniżej streszczono główne uwagi z kontroli przedstawione przez NOK.

Kontrole wykonania zadań

56 **Duński organ *Rigsrevisionen*** ocenił, czy wybrane najważniejsze instytucje rządowe posiadają wystarczające zabezpieczenia przed atakami typu ransomware. Instytucje rządowe są częstym celem cyberataków, a ataki typu ransomware stanowią obecnie jedno z największych zagrożeń dla cyberbezpieczeństwa. Kontrolą objęto duński Urząd ds. Danych Dotyczących Zdrowia, duńskie Ministerstwo Spraw Zagranicznych, Banedanmark (duńską sieć kolejową) oraz duńską Agencję ds. Zarządzania Sytuacjami Wyjątkowymi. Te cztery instytucje wybrano, ponieważ są one odpowiedzialne za świadczenie usług kluczowych w dziedzinach zdrowia, spraw zagranicznych, transportu i gotowości na wypadek sytuacji wyjątkowych, a zapewnienie dostępu do danych w tych obszarach może mieć krytyczne znaczenie. W kontroli stwierdzono, że ochrona przed atakami typu ransomware w czterech wspomnianych instytucjach nie była zadowalająca. Jak wynika z prac kontrolnych, w instytucjach tych nie wdrożono szeregu powszechnie stosowanych mechanizmów zabezpieczeń służących ograniczeniu ataków. Na podstawie kontroli stwierdzono, że instytucje te stanowczo powinny rozważyć wdrożenie mechanizmów zabezpieczeń ukierunkowanych na przyszłe zagrożenia, aby zwiększyć swoją odporność na ataki typu ransomware.

57 **Estoński organ *Riigikontroll*** uznał, że zachowanie niepodległości Estonii wymaga nie tylko fizycznej obrony jej terytorium, ale również ochrony zasobów cyfrowych o kluczowym znaczeniu dla państwa. Zasobami cyfrowymi, które w największym stopniu wymagają ochrony, są dane dotyczące obywateli, terytorium i prawodawstwa. Zabezpieczenia wymagają również dane dotyczące własności, nieruchomości i praw mieszkańców Estonii. Estoński Urząd Kontroli Państwowej uwzględnił możliwość wystąpienia cyberzagrożeń w przypadku nasilenia się problemów w zakresie bezpieczeństwa. W razie urzeczywistnienia się tego ryzyka i wzrostu liczby incydentów związanych z bezpieczeństwem informacji, takich jak cyberataki i wycieki danych, może pojawić się zagrożenie dla danych i baz danych o największym znaczeniu dla państwa. W związku z tym podczas kontroli sprawdzono, w jaki sposób państwo określiło, które dane i bazy danych miały krytyczne znaczenie dla zagwarantowania bezpieczeństwa narodowego. W wyniku kontroli stwierdzono, że pomimo wdrożenia trzypoziomowego

podstawowego systemu bezpieczeństwa ISKE[63], obowiązkowego dla agencji państwowych, w kilku bazach danych o znaczeniu krytycznym istniały znaczne braki, jeśli chodzi o zagwarantowanie bezpieczeństwa informacji.

58 **Irlandzki *Office of the Comptroller and Auditor General*** dokonał przeglądu postępów poczynionych w zakresie działań na rzecz cyberbezpieczeństwa od momentu ustanowienia irlandzkiego Krajowego Centrum ds. Cyberbezpieczeństwa. Centrum powstało w 2011 r., a za jego prowadzenie odpowiada Departament Komunikacji, Działań w Dziedzinie Klimatu i Środowiska. Działalność Centrum koncentruje się przede wszystkim na zabezpieczaniu sieci rządowych, wspieraniu przemysłu i osób fizycznych w ochronie posiadanych przez nie systemów oraz zabezpieczaniu infrastruktury krajowej o znaczeniu krytycznym. Podczas kontroli stwierdzono, że choć Krajowe Centrum ds. Cyberbezpieczeństwa pełni funkcję o znaczeniu krytycznym, poziom zasobów w pierwszych czterech latach działania był znacznie niższy niż pierwotnie przewidziano i zabrakło planu strategicznego określającego ogólny strategiczny kierunek działalności Centrum. Ponadto należałoby jaśniej określić odpowiednie role organów zaangażowanych w prowadzenie dochodzeń w sprawie cyberprzestępstw i incydentów związanych z bezpieczeństwem narodowym. W dalszym ciągu nie wdrożono również wymogów unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji związanych z opracowaniem strategii krajowej.

59 **Francuski *Cour des comptes*** zbadał *Parcoursup* – nową platformę cyfrową będącą źródłem informacji na temat dostępnych kierunków studiów i wymagań wstępnych, której celem jest lepsze dopasowanie predyspozycji i wyników w nauce uczniów szkół średnich do treści studiów uniwersyteckich. Podczas kontroli stwierdzono, że rząd skutecznie scentralizował dostęp do wszystkich kierunków kształcenia pomaturalnego za pomocą platformy cyfrowej w odpowiedzi na upowszechnienie szkolnictwa wyższego. Platforma *Parcoursup* powstała jednak w wyniku pospiesznego przekształcenia poprzedniego systemu i nie dokonano żadnych znaczących zmian strukturalnych. W związku z tym nie wyeliminowano słabych punktów systemu informacyjnego w zakresie bezpieczeństwa, wydajności i solidności. Platforma jest nadal narażona na znaczne ryzyko, jeśli chodzi o jakość i ciągłość świadczenia usług publicznych oraz bezpieczeństwo danych osobowych.

---

[63] ISKE to norma bezpieczeństwa informacji opracowana na potrzeby estońskiego sektora publicznego. Jest ona wiążąca dla organizacji państwowych i samorządowych, które obsługują bazy danych i rejestry.

60 **Łotewski organ *Valsts Kontrole*** przeprowadził kontrolę wykonania zadań dotyczącą efektywności publicznej infrastruktury technologii informacyjno-komunikacyjnych (ICT). Celem tej kontroli było sprawdzenie, czy administracja publiczna stosowała jednolite podejście do efektywnego zarządzania infrastrukturą ICT oraz czy instytucje dokonały oceny korzyści związanych z centralizacją. W wyniku kontroli stwierdzono, że niechęć organów do centralizacji zarządzania infrastrukturą ICT skutkowała utworzeniem wielu serwerowni, co wiązało się ze znacznym zwiększeniem kosztów utrzymania. W większości serwerowni stwierdzono zagrożenia dla bezpieczeństwa – ośrodki przetwarzania danych nie były wystarczająco zabezpieczone przed fizycznym dostępem i ryzykiem środowiskowym. Ponadto w instytucjach nie wprowadzono żadnych praktyk zakładających regularną ocenę tego, czy taniej byłoby utrzymywać infrastrukturę ICT we własnym zakresie, współpracować z inną instytucją, czy też zlecać utrzymanie ICT podmiotom zewnętrznym. W wyniku kontroli zalecono wprowadzenie systemu stałego monitorowania, który umożliwiłby ocenę całej administracji publicznej jako jednego systemu.

61 **Litewski organ *Valstybės kontrolė*** zwrócił uwagę na znaczenie elektronicznych państwowych zasobów informacyjnych o znaczeniu krytycznym, np. związanych z zarządzaniem finansami publicznymi, administracją podatkową i ochroną zdrowia. Utrata informacji o znaczeniu krytycznym i niedostępność odnośnych systemów informacyjnych może mieć poważne konsekwencje dla bezpieczeństwa publicznego, dobrostanu i gospodarki. Przedmiotowa kontrola miała na celu ocenę zarządzania państwowymi zasobami informacyjnymi o znaczeniu krytycznym (ogólnej kontroli nad tymi zasobami) i odnośnej dojrzałości procesowej. Wykryto problemy systemowe zarówno w kształtowaniu, jak i wdrażaniu strategii w zakresie państwowych zasobów informacyjnych oraz w mechanizmie zarządzania nimi. W wyniku kontroli stwierdzono, że niski poziom dojrzałości procesowej państwowych zasobów informacyjnych o znaczeniu krytycznym wskazywał na uchybienia w kształtowaniu i wdrażaniu strategii w tej dziedzinie, w wyniku czego zasoby te były bardziej narażone na zagrożenia. Aby zwiększyć bezpieczeństwo tych państwowych zasobów informacyjnych, należało usprawnić mechanizm zarządzania nimi.

62 W 2018 r. **niderlandzka *Powszechna Izba Obrachunkowa*** postanowiła przeprowadzić kontrole w zakresie cyberbezpieczeństwa w sektorach o znaczeniu krytycznym dla społeczeństwa. Pierwszymi dwoma sektorami, w których przeprowadzono kontrole, były sektor gospodarki wodnej i sektor zautomatyzowanych kontroli granicznych. Pierwszy z nich ma podstawowe znaczenie ze względu na położenie kraju w dużej części poniżej poziomu morza, a drugi – ze względu na rangę

portu lotniczego Amsterdam Schiphol jako międzynarodowego lotniska przesiadkowego i przeładunkowego oraz punktu wjazdowego do kraju. Minister Infrastruktury i Gospodarki Wodnej wyznaczył szereg elementów infrastruktury gospodarki wodnej zarządzanych przez Dyrekcję Generalną ds. Robót Publicznych i Gospodarki Wodnej (kontrolowanego) jako elementy o znaczeniu krytycznym dla sektora gospodarki wodnej. Wiele systemów komputerowych wykorzystywanych do obsługi tych elementów infrastruktury pochodzi z lat 80. i 90. XX wieku – czasów, gdy kwestie dotyczące cyberbezpieczeństwa nie było powszechnie brane pod uwagę. Minister Obrony oraz Minister Sprawiedliwości i Bezpieczeństwa są wspólnie odpowiedzialni za kontrole graniczne przeprowadzane przez niderlandzkich strażników granicznych w porcie lotniczym Schiphol. Oba ministerstwa posiadają systemy informatyczne, na których polegają strażnicy graniczni. Systemy te mają zasadnicze znaczenie dla funkcjonowania portu lotniczego i są wykorzystywane do przetwarzania szczególnie wrażliwych danych. W związku z tym są one potencjalnym celem cyberataków ukierunkowanych na sabotaż, szpiegostwo lub manipulację w związku z kontrolami granicznymi. W toku kontroli powszechnej Izby Obrachunkowej zbadano, czy jednostki kontrolowane przygotowane były na radzenie sobie z zagrożeniami dla cyberbezpieczeństwa oraz czy działania w tym zakresie były skuteczne. W przypadku elementów infrastruktury gospodarki wodnej stwierdzono, że jednostka kontrolowana powinna podjąć jeszcze więcej działań, zarówno w zakresie wykrywania, jak i reagowania, aby osiągnąć własne cele dotyczące cyberbezpieczeństwa. W przypadku kontroli granicznych stwierdzono, że środki w zakresie cyberbezpieczeństwa nie były odpowiednie ani nie zapewniały ochrony przed przyszłymi zagrożeniami.

63 **Portugalski *Tribunal de Contas*** skontrolował systemy informacyjne wspierające przyznawanie i wydawanie portugalskiego paszportu elektronicznego (PEP) oraz korzystanie z niego, w szczególności w zakresie zautomatyzowanej kontroli pasażerów za pomocą odczytu danych biometrycznych na granicach Portugalii. W ramach kontroli zweryfikowano zgodność z prawem unijnym i krajowym, normami międzynarodowymi i wytycznymi dotyczącymi przyznawania i wydawania PEP oraz korzystania z niego, w tym adekwatności krajowych ram prawnych. Zbadano skuteczność kluczowych procesów związanych z cyklem życia PEP, w szczególności z przyznawaniem i wydawaniem PEP oraz korzystaniem z niego. Ponadto dokonano przeglądu najistotniejszych aspektów działania systemów informacyjnych, w szczególności spełniania wymogów bezpieczeństwa dotyczących systemów informacyjnych PEP (SIPEP).

64 **Fiński organ *Valtiontalouden tarkastusvirasto*** zbadał, czy cyberochrona w instytucjach rządowych na szczeblu centralnym była możliwie jak najbardziej skuteczna i opłacalna. Kontrola koncentrowała się na sposobie zarządzania cyberbezpieczeństwem w instytucjach rządowych na szczeblu centralnym. Wśród skontrolowanych jednostek znalazły się organy zarządzające cyberochroną w instytucjach rządowych na szczeblu centralnym (Kancelaria Premiera, Ministerstwo Finansów oraz Ministerstwo Transportu i Łączności) oraz organy odpowiedzialne za scentralizowane zadania w zakresie cyberochrony i scentralizowane usługi informatyczne w instytucjach rządowych na szczeblu centralnym. W fińskich instytucjach rządowych odpowiedzialność za cyberochronę jest zdecentralizowana, a każda jednostka instytucjonalna odpowiada za własne cyberbezpieczeństwo. W wyniku kontroli zalecono, aby Ministerstwo Finansów określiło i wdrożyło w odniesieniu do usług ICT instytucji rządowych na szczeblu centralnym szeroko zakrojony model zarządzania operacyjnego w przypadku wystąpienia cyberincydentów. Ministerstwo Finansów powinno również przeanalizować, w jaki sposób należy uwzględniać kwestię cyberbezpieczeństwa w ramach finansowania usług na wszystkich etapach ich świadczenia, a także pogłębić wiedzę na temat bieżącej sytuacji przez polecenie organom zgłaszania cyberincydentów do Centrum ds. Cyberbezpieczeństwa.

65 **Szwedzki organ *Riksrevisionen*** zajął się kwestią stosowania przestarzałych systemów informatycznych w administracji rządowej na szczeblu centralnym celem sprawdzenia, czy rząd i odpowiednie organy podjęły stosowne działania, aby zapobiec sytuacji, w której systemy te staną się przeszkodą dla skutecznej transformacji cyfrowej. W toku kontroli w wielu agencjach rządowych stwierdzono obecność przestarzałych systemów informatycznych. W wielu skontrolowanych agencjach stosowano co najmniej jeden przestarzały system informatyczny o krytycznym znaczeniu dla działalności, a w dużej części objętych kontrolą agencji nie stosowano właściwego podejścia do rozwoju wsparcia informatycznego i zarządzania nim. Znaczna część agencji nie dysponowała ogólnym opisem tego, w jaki sposób strategie, procesy operacyjne i systemy były ze sobą powiązane. Zgodnie z ogólnym wnioskiem z kontroli większości agencji nie udało się jeszcze skutecznie rozwiązać problemów związanych z przestarzałymi systemami informatycznymi. Szwedzki Urząd Kontroli Państwowej uważa, że problem jest na tyle poważny i powszechny, że stanowi przeszkodę dla dalszej skutecznej transformacji cyfrowej administracji państwa.

Kontrole zgodności przeprowadzone w odniesieniu do cyberbezpieczeństwa

66 **Węgierska *Państwowa Izba Obrachunkowa*** uznała, że bezpieczeństwo krajowych zasobów danych ma fundamentalne znaczenie dla społeczeństwa, jeśli chodzi o zachowanie i ochronę wartości narodowych. Zapewnienie zwiększonego bezpieczeństwa danych osobowych i publicznych w ramach krajowych zasobów danych Węgier jest niezwykle ważne dla wzmacniania zaufania obywateli do państwa oraz zapewniania ciągłego i płynnego funkcjonowania administracji publicznej. Kontrola zgodności w zakresie ochrony danych miała na celu ocenę, czy na Węgrzech ustanowiono regulacyjne i operacyjne ramy ochrony danych oraz czy główne organizacje zarządzające danymi przestrzegały wymogów dotyczących bezpiecznego zarządzania danymi i zlecenia podmiotom zewnętrznym przetwarzania danych. W wyniku kontroli stwierdzono, że wewnętrzne regulaminy organizacji zarządzających danymi dotyczące działań w zakresie zarządzania danymi zapewniły ochronę krajowych zasobów danych jako części zasobów krajowych, zgodnie z przepisami obowiązującymi w latach 2011–2015. Administratorzy danych prawidłowo zastosowali wymogi oraz odpowiednio wdrożono przekazywanie danych do osób trzecich.

67 **Polska *Najwyższa Izba Kontroli*** oceniła, czy zapewniono bezpieczeństwo danych gromadzonych w systemach wykorzystywanych do realizacji istotnych zadań publicznych. Kontrolą objęto sześć wybranych instytucji realizujących ważne zadania publiczne. Stopień przygotowania oraz wdrożenia Systemu Zapewnienia Bezpieczeństwa Informacji nie zapewniał akceptowalnego poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych. Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny. Spośród sześciu skontrolowanych jednostek tylko jedna wdrożyła System Zapewnienia Bezpieczeństwa Informacji, chociaż należy zauważyć, iż jego funkcjonowanie było również obarczone istotnymi nieprawidłowościami. W ramach kontroli stwierdzono, że konieczne jest opracowanie i wprowadzenie na szczeblu centralnym generalnych zaleceń i wymagań dotyczących zapewnienia bezpieczeństwa IT, obowiązujących wszystkie podmioty publiczne.

Przeglądy w zakresie cyberbezpieczeństwa

68 ***Europejski Trybunał Obrachunkowy*** dokonał przeglądu unijnej polityki cyberbezpieczeństwa oraz wskazał zasadnicze wyzwania związane ze skutecznym realizowaniem tej polityki. W przeglądzie poruszono kwestie bezpieczeństwa sieci i informacji, cyberprzestępczości, cyberobrony i dezinformacji. W dokumencie wskazano szereg luk w unijnym prawie dotyczącym cyberbezpieczeństwa i zauważono, że obowiązujące prawodawstwo nie zostało spójnie transponowane przez państwa członkowskie. Ponadto w przeglądzie zwrócono uwagę na fakt, że brakuje wiarygodnych danych dotyczących cyberincydentów na szczeblu unijnym, a także kompleksowego przeglądu wydatków na cyberbezpieczeństwo ponoszonych przez UE i jej państwa członkowskie. W przeglądzie odnotowano również ograniczenia pod względem zasobów, z jakimi borykają się unijne agencje zajmujące się cyberprzestrzenią, w tym trudności w przyciąganiu i zatrzymywaniu utalentowanych pracowników. Kolejnym wyzwaniem było niedostosowanie finansowania w dziedzinie cyberbezpieczeństwa do celów strategicznych UE.

CZĘŚĆ III – Streszczenie sprawozdań najwyższych organów kontroli

Dania
Rigsrevisionen

Ochrona przed atakami typu ransomware

Data publikacji: 2017 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: kwiecień – wrzesień 2017 r.

Streszczenie sprawozdania

Temat kontroli

W sprawozdaniu przeanalizowano, czy wybrane najważniejsze instytucje rządowe posiadają wystarczające zabezpieczenia przed atakami typu ransomware.

Instytucje rządowe są częstym celem cyberataków, a ataki typu ransomware są obecnie jednym z największych zagrożeń dla cyberbezpieczeństwa. Oprogramowanie typu ransomware to złośliwe oprogramowanie, które blokuje dostęp do danych. Ogólnie rzecz biorąc, oprogramowanie typu ransomware szyfruje dane i uniemożliwia zaatakowanym instytucjom korzystanie z nich. Hakerzy żądają okupu za odszyfrowanie danych i umożliwienie instytucjom odzyskania dostępu do nich. W związku z tym oprogramowanie typu ransomware stanowi szczególne zagrożenie dla dostępności danych.

Nagły brak dostępu do danych może utrudniać instytucjom świadczenie ważnych usług lub zupełnie im to uniemożliwić. Instytucje, które zostały zaatakowane takim oprogramowaniem, są zazwyczaj zmuszone do odłączenia części lub całej swojej sieci informatycznej w celu zbadania skali ataku. Ataki typu ransomware mogą mieć znaczne skutki gospodarcze, ponieważ narażają instytucje na ryzyko utraty zdolności

produkcyjnych, na przykład gdy nie mają one możliwości dostępu do swojej sieci informatycznej lub gdy tracą dane gromadzone i przetwarzane przez długi czas. W 2017 r. atak typu ransomware na brytyjską krajową służbę zdrowia spowodował odwołanie 19 000 operacji i wizyt. Kierownictwo instytucji powinno zatem skoncentrować się na ryzyku ataków typu ransomware i wdrożyć niezbędne mechanizmy zabezpieczeń w celu ochrony przed oprogramowaniem tego typu i ograniczenia skutków potencjalnego ataku.

Badaniem objęto duński Urząd ds. Danych Dotyczących Zdrowia, Ministerstwo Spraw Zagranicznych, Banedanmark (duńską sieć kolejową) oraz duńską Agencję ds. Zarządzania Sytuacjami Wyjątkowymi. Te cztery instytucje wybrano, ponieważ są one odpowiedzialne za świadczenie usług kluczowych w dziedzinach zdrowia, spraw zagranicznych, transportu i gotowości na wypadek sytuacji wyjątkowej, a zapewnienie dostępu do danych w tych obszarach może mieć krytyczne znaczenie. Urząd ds. Danych Dotyczących Zdrowia świadczy również scentralizowane usługi informatyczne na rzecz większości organów rządowych podlegających Ministerstwu Zdrowia.

Celem badania była ocena, czy wspomniane cztery instytucje posiadają wystarczające zabezpieczenia przed atakami typu ransomware za pośrednictwem poczty elektronicznej. Duński NOK zbadał zatem 20 powszechnie stosowanych mechanizmów zabezpieczeń, które zapewniają podstawową ochronę przed oprogramowaniem typu ransomware. Ponadto dokonał on przeglądu pięciu mechanizmów zabezpieczeń, które instytucje powinny uwzględnić w związku z przeprowadzanymi w przyszłości ocenami ryzyka. Mechanizmy zabezpieczeń ukierunkowane na przyszłe zagrożenia obejmują na przykład nową technologię, która może zmniejszyć liczbę fałszywych wiadomości elektronicznych odbieranych przez instytucje lub umożliwić wykrywanie nietypowej aktywności na komputerach i wysyłanie ostrzeżeń o takiej aktywności. Inicjatorem badania był najwyższy organ kontroli *Rigsrevisionen*. Zostało ono oparte na ustaleniach z czterech kontroli systemów informatycznych przeprowadzonych w okresie od kwietnia do września 2017 r. W wyniku badania pokrótce przedstawiono, w jakim stopniu instytucje były chronione przed atakami typu ransomware. Po zakończeniu kontroli systemów informatycznych instytucje miały możliwość wprowadzenia 20 powszechnie stosowanych mechanizmów zabezpieczeń. W związku z tym rezultaty badania dotyczą jedynie ochrony instytucji przed oprogramowaniem typu ransomware w czasie czterech kontroli systemów informatycznych. W badaniu przedstawiono wyniki czterech instytucji objętych kontrolą, ale nie zawiera ono analizy porównawczej ani rankingu uzyskanych przez nie wyników.

Ustalenia i wnioski

W ocenie *Rigsrevisionen* cztery instytucje objęte kontrolą nie dysponowały wystarczającymi zabezpieczeniami przed atakami typu ransomware. Z badania wynika, że w instytucjach tych nie wdrożono szeregu powszechnie stosowanych mechanizmów zabezpieczeń służących ograniczeniu ataków. W szczególności znaczne luki w zakresie bezpieczeństwa stwierdzono w Urzędzie ds. Danych Dotyczących Zdrowia i Banedanmark. Oznacza to, że wszystkie cztery instytucje były narażone na zwiększone ryzyko ataków typu ransomware za pośrednictwem poczty elektronicznej, które pozbawiłyby je możliwości świadczenia usług przez krótszy lub dłuższy czas. Wszystkie cztery instytucje poinformowały *Rigsrevisionen*, że od czasu ukończenia badania prowadziły działania na rzecz wdrożenia szeregu mechanizmów zabezpieczeń, tak aby zwiększyć poziom ochrony przed atakami typu ransomware.

Systemy zapobiegania atakom typu ransomware w instytucjach, w odniesieniu zarówno do zagrożeń wewnętrznych, jak i zewnętrznych, były nieodpowiednie. Szczególne zaniepokojenie wzbudza fakt, że żadna z tych instytucji nie dopilnowała, by przeprowadzano aktualizację łat oprogramowania zabezpieczającego, a trzy z nich nie wdrożyły technologii białej listy, aby zapobiec uruchamianiu złośliwego oprogramowania przez pracowników. Zwiększa to ryzyko zainfekowania części lub całej sieci informatycznej przez oprogramowanie typu ransomware i rozprzestrzenienia się tego oprogramowania.

W trzech z instytucji objętych kontrolą kierownictwo nie poświęciło wystarczającej uwagi zagrożeniu atakiem typu ransomware, a ocena ryzyka przeprowadzona przez kadrę kierowniczą w Urzędzie ds. Danych Dotyczących Zdrowia i w Banedanmark nie objęła wszystkich istotnych aspektów. W efekcie instytucje te nie dysponowały aktualną oceną zagrożenia atakiem typu ransomware i w związku z tym ich możliwości zapobieżenia nowym atakom i zmniejszenia skutków przyszłych ataków były ograniczone. Kierownictwo Urzędu ds. Danych Dotyczących Zdrowia i Banedanmark nie poświęciło wystarczającej uwagi ocenie ryzyka, w związku z czym bezpieczeństwo informatyczne w tych dwóch instytucjach nie opierało się na priorytetach określonych przez kierownictwo.

Trzy instytucje nie wprowadziły odpowiednich planów reagowania na incydenty, które pomogłyby im we wznowieniu działalności po ataku typu ransomware. Szczególnie znaczący jest fakt, że trzy z instytucji objętych kontrolą nie sprawdzały regularnie, czy byłyby w stanie przywrócić swoje dane i systemy, gdyby stały się one celem ataku typu ransomware. Zwiększa to ryzyko utraty danych posiadanych przez te instytucje

w związku z atakiem oraz ryzyko, że instytucje te będą niezdolne do świadczenia usług przez dłuższy czas.

Ponieważ nieustannie pojawiają się nowe czynniki ryzyka, ważne jest, aby w celu zwiększenia swojej odporności na ataki typu ransomware instytucje rozważyły wprowadzenie mechanizmów zabezpieczeń ukierunkowanych na przyszłe zagrożenia, tj. mechanizmów, które ułatwiają weryfikację tożsamości nadawców wiadomości elektronicznych oraz umożliwiają wykrycie i odrzucenie potencjalnie szkodliwych wiadomości. Wszystkie cztery instytucje objęte kontrolą prowadzą obecnie prace nad wdrożeniem niektórych mechanizmów zabezpieczeń ukierunkowanych na przyszłe zagrożenia, które mogą przyczynić się do wzmocnienia ochrony przed atakami typu ransomware.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Sprawozdanie dotyczące ochrony danych badawczych na duńskich uniwersytetach
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim)
Data publikacji:	2019 r.
Tytuł sprawozdania:	Sprawozdanie w sprawie ochrony systemów informatycznych i danych dotyczących zdrowia w trzech regionach Danii
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim)
Data publikacji:	2017 r.
Tytuł sprawozdania:	Sprawozdanie w sprawie zarządzania bezpieczeństwem informatycznym w przypadku systemów powierzonych dostawcom zewnętrznym
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim)
Data publikacji:	2016 r.
Tytuł sprawozdania:	Sprawozdanie w sprawie dostępu do systemów informatycznych, które wspierają świadczenie usług kluczowych na rzecz duńskiego społeczeństwa
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim)
Data publikacji:	2015 r.

Estonia
Riigikontroll

Zapewnienie bezpieczeństwa i ochrony estońskich państwowych baz danych o krytycznym znaczeniu

Data publikacji: maj 2018 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)
sprawozdanie (w j. estońskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: 2017 r.

Streszczenie sprawozdania

Temat kontroli

Zachowanie niepodległości Estonii wymaga nie tylko fizycznej obrony jej terytorium, ale również ochrony zasobów cyfrowych o kluczowym znaczeniu dla państwa w obliczu wydarzeń, które stanowią największe zagrożenie. Zasobami cyfrowymi, które wymagają największej ochrony, są dane dotyczące obywateli, terytorium i prawodawstwa. Zabezpieczenia wymagają również dane dotyczące własności, nieruchomości i praw mieszkańców Estonii.

Urząd Kontroli Państwowej sprawdził, w jaki sposób państwo określiło, które dane i bazy danych miały krytyczne znaczenie dla zagwarantowania bezpieczeństwa narodowego. Sprawdzono poziom ochrony bezpieczeństwa i ciągłości tych danych i baz danych, w tym dokonano przeglądu narzędzi wykorzystywanych do ochrony.

Ponieważ Estonia jest obecnie członkiem NATO i Unii Europejskiej, jej bezpieczeństwo fizyczne jest chronione w większym stopniu niż przed przystąpieniem do tych sojuszy. Estonia musi jednak uwzględniać możliwość wystąpienia cyberzagrożeń w przypadku

nasilenia się problemów w zakresie bezpieczeństwa. W razie urzeczywistnienia się takiego ryzyka i wzrostu liczby incydentów związanych z bezpieczeństwem informacji, takich jak cyberataki i wycieki danych, może pojawić się zagrożenie dla danych i baz danych o najważniejszym znaczeniu dla państwa. Gdyby dane o kluczowym znaczeniu dla państwa zostały zmodyfikowane bez zezwolenia, bądź w sytuacji ich wycieku lub utraty, państwo nie byłoby w stanie w dalszym ciągu pełnić niezbędnych funkcji, takich jak gwarantowanie bezpieczeństwa ludności, zapewnienie dostępu do podstawowych usług, tworzenie środowiska niezbędnego do prowadzenia działalności gospodarczej i wielu innych. Według pierwotnych planów Estonia zamierza wydać kwotę około miliona euro na przechowywanie danych o znaczeniu krytycznym poza granicami kraju.

Pytania kontrolne

- Czy ministerstwa zidentyfikowały wszystkie bazy danych o znaczeniu krytycznym i wymogi w zakresie ich obsługi?
- Czy bazy danych i rejestry o znaczeniu krytycznym są zabezpieczone?
- Czy zapewniono długoterminową ciągłość danych i baz danych o znaczeniu krytycznym?

Ustalenia

Urząd Kontroli Państwowej sformułował przedstawione poniżej uwagi na temat skontrolowanych baz danych o znaczeniu krytycznym.

- Nie ustanowiono żadnego planu działania ani wymagań dotyczących wdrażania koncepcji baz danych o znaczeniu krytycznym. Nie określono warunków wyboru baz danych o znaczeniu krytycznym i nie było pewności, że procesem tym objęto wszystkie niezbędne bazy danych. Dodatkowa ochrona baz danych została zorganizowana nieformalnie i nie była obowiązkowa dla właścicieli baz danych, a w rezultacie w przypadku pięciu baz danych o znaczeniu krytycznym nie utworzono kopii zapasowej danych za granicą.
- Dla baz danych o znaczeniu krytycznym nie ustanowiono dodatkowych zasad dotyczących bezpieczeństwa informacji. Ani system bezpieczeństwa informacji ISKE (norma bezpieczeństwa informacji opracowana dla estońskiego sektora publicznego, obowiązkowa dla organizacji państwowych i samorządowych, które

obsługują bazy danych / rejestry), ani żaden akt prawny czy norma nie zawierały dodatkowych wymogów dotyczących baz danych o znaczeniu krytycznym, dotyczących na przykład tworzenia kopii zapasowych danych poza terytorium Estonii. Kopie zapasowe skontrolowanych baz danych zostały zlokalizowane za granicą, ale nie przetestowano, w jaki sposób przebiegnie za ich pomocą przywracanie do pracy systemów informacyjnych.

- Wdrożenie ISKE i powiązane audyty były problematyczne w odniesieniu do baz danych o znaczeniu krytycznym. Do czasu przedmiotowej kontroli nie przeprowadzono żadnych audytów ISKE w przypadku dwóch z dziesięciu baz danych. Zorganizowano je dopiero pod koniec kontroli (30 listopada 2017 r.). Tylko dwie bazy danych o znaczeniu krytycznym były poddawane audytom tak często, jak wymagało tego prawo. Ponadto w niektórych przypadkach problemy uwydatnione przez audytora nie zostały rozwiązane w czasie pomiędzy dwoma audytami ISKE (dwa–trzy lata).

- W toku kontroli Urząd Kontroli Państwowej ustalił, że w przypadku niektórych baz danych o znaczeniu krytycznym nie wdrożono niektórych ważnych środków w zakresie bezpieczeństwa informacji. Na przykład w wytycznych dotyczących bezpieczeństwa informacji nie określono wymogów dotyczących regularnej oceny słabych punktów systemów informacyjnych, nie przeprowadzano regularnych kontroli lub analiz dzienników zdarzeń, nie wprowadzono planów szkoleń dotyczących bezpieczeństwa informacji ani nie przeprowadzono analizy wiedzy na temat bezpieczeństwa informacji w instytucjach rządowych, która stanowiłaby podstawę opracowywania takich planów szkoleń. Nie wykonano ponadto żadnych testów penetracyjnych z zewnątrz, a w niektórych przypadkach nie sprawdzono integralności plików.

Wnioski i zalecenia

Kontrola wykazała, że pomimo wdrożenia trzypoziomowego podstawowego systemu bezpieczeństwa ISKE, obowiązkowego dla agencji państwowych, także w odniesieniu do przeprowadzanych przez nie audytów, w szeregu baz danych o znaczeniu krytycznym występowały znaczne braki, jeśli chodzi o zapewnienie bezpieczeństwa informacji, na przykład w zakresie analizy dzienników, przeprowadzania testów penetracyjnych i ochrony urządzeń przenośnych. Do czasu przeprowadzenia kontroli nie ustanowiono specjalnych wymogów potrzebnych do ochrony danych o znaczeniu krytycznym.

Ministerstwo Spraw Gospodarczych i Komunikacji podjęło pierwsze działania niezbędne do zapewnienia ochrony danych o znaczeniu krytycznym, ale projekt dotyczący baz danych o znaczeniu krytycznym był na etapie, na którym konieczne było wprowadzenie prawnie wiążącego zestawu przepisów. Nie przeprowadzono ponadto szczegółowej analizy ryzyka ani nie opracowano planu działania na przyszłość.

W ambasadach w państwach trzecich przechowywano kopie zapasowe danych z pięciu baz danych o znaczeniu krytycznym, ale w przypadku fizycznego zniszczenia ośrodków przetwarzania danych zlokalizowanych w Estonii nie można byłoby zagwarantować zachowania danych o znaczeniu krytycznym w pozostałych pięciu bazach danych.

Sformułowano dwa następujące zalecenia ogólne:

- Należy określić zasady dotyczące dodatkowej ochrony baz danych o znaczeniu krytycznym, w tym wskazywania baz danych o znaczeniu krytycznym, przetwarzania danych w tych bazach i tworzenia kopii zapasowych danych o krytycznym znaczeniu dla państwa, a także przeanalizować, w jaki sposób zapewnić dodatkowe finansowanie tych działań.
- Należy przeanalizować poszczególne etapy ustanawiania baz danych, zarówno pod względem planowania finansowego, jak i bezpieczeństwa informacji, i wdrożyć na tych etapach najlepsze praktyki zarządzania projektami.

Irlandia
Office of the Comptroller and Auditor General

Działania dotyczące cyberbezpieczeństwa kraju

Data publikacji: wrzesień 2018 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2011–2018

Streszczenie sprawozdania

Temat kontroli

Za politykę cyberbezpieczeństwa w Irlandii odpowiada Departament Komunikacji, Działań w Dziedzinie Klimatu i Środowiska. Departament ten jest również odpowiedzialny – poprzez Krajowe Centrum ds. Cyberbezpieczeństwa – za koordynację reagowania kryzysowego instytucji rządowych na wszelkie cyberincydenty na szczeblu krajowym.

Krajowe Centrum ds. Cyberbezpieczeństwa ustanowiono w 2011 r. Koncentruje się ono przede wszystkim na zabezpieczaniu sieci rządowych, wspieraniu przemysłu i osób fizycznych w ochronie posiadanych przez nie systemów, a także na zabezpieczaniu infrastruktury krajowej o znaczeniu krytycznym.

Pytania kontrolne

W badaniu dokonano przeglądu postępów poczynionych w zakresie działań na rzecz cyberbezpieczeństwa od momentu ustanowienia Krajowego Centrum ds. Cyberbezpieczeństwa. W szczególności przeanalizowano kwestie związane z:

- mandatem Centrum i jego zasobami,
- krajową strategią cyberbezpieczeństwa (2015–2017),
- wdrożeniem unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji (dyrektywy NIS),
- rozwiązaniami w zakresie zarządzania i nadzoru.

Ustalenia i wnioski

Choć w decyzji rządu dotyczącej ustanowienia Krajowego Centrum ds. Cyberbezpieczeństwa zatwierdzono roczne finansowanie w wysokości 800 000 euro, rzeczywiste roczne finansowanie cyberbezpieczeństwa w latach 2012–2015 nie sięgnęło jednej trzeciej tej kwoty. W 2017 r. środki przeznaczone na ten cel zwiększono do 1,95 mln euro. W 2017 r. liczba pracowników Centrum zwiększyła się prawie dwukrotnie i stan zatrudnienia wyniósł 14,5 ekwiwalentu pełnego czasu pracy. W 2018 r. Centrum otrzymało zgodę na zatrudnienie dodatkowych 16 pracowników.

W krajowej strategii cyberbezpieczeństwa (2015–2017) określono 12 działań, które należało podjąć w perspektywie czasowej strategii. Do maja 2018 r. ukończono realizację czterech działań, cztery zostały wdrożone częściowo, a cztery kolejne – wcale.

Unijna dyrektywa w sprawie bezpieczeństwa sieci i informacji ma na celu zwiększenie odporności kluczowych sieci i systemów informatycznych. W wyniku oceny postępów poczynionych w Irlandii w odniesieniu do każdego z trzech filarów dyrektywy sformułowano następujące ustalenia:

- *Filar 1 – Zwiększanie zdolności państw członkowskich UE w zakresie cyberbezpieczeństwa.* Filar częściowo wdrożony – rozwiązano kwestię wymogów strukturalnych, ale pozostają luki w planowaniu strategicznym;

- Filar 2 – Ułatwianie współpracy w zakresie cyberbezpieczeństwa między państwami członkowskimi UE. Filar wdrożony;
- *Filar 3 – Wprowadzenie środków bezpieczeństwa i obowiązków w zakresie zgłaszania incydentów w odniesieniu do kluczowych sektorów.* Filar częściowo wdrożony – pozostają do wykonania prace związane z identyfikacją sieci i systemów informatycznych o znaczeniu krytycznym, formalnym wskazaniem, które podmioty są operatorami usług kluczowych, oraz zarządzaniem dostawcami usług cyfrowych.

Decyzją rządu (lipiec 2011 r.) w sprawie ustanowienia Krajowego Centrum ds. Cyberbezpieczeństwa zatwierdzono również powołanie międzydepartamentalnej komisji, której zadaniem będzie opracowanie i wdrożenie polityki mającej na celu sprostanie wyzwaniom związanym z cyberbezpieczeństwem w Irlandii. Choć w latach 2013–2015 odbyło się pięć posiedzeń komisji, tylko jeden protokół z posiedzenia był dostępny do wglądu. Od 2015 r. posiedzenia komisji nie odbywały się.

W planie wdrażania krajowej strategii cyberbezpieczeństwa zobowiązano się do opublikowania sprawozdania rocznego oraz do dokonania formalnej oceny skutków prowadzonych prac pod koniec 2017 r. Dokumentów tych w dalszym ciągu nie opracowano, jednak prace Centrum zostały przedstawione w sprawozdaniu rocznym Departamentu.

Do Departamentu wpłynął wniosek formalny o dokonanie oceny wyników Centrum, nie przedstawiono jednak żadnych dowodów na przeprowadzenie oceny. Departament stwierdził, że ocena wyników prac Krajowego Centrum ds. Cyberbezpieczeństwa stanowi część zwykłego zarządzania wynikami i ładu korporacyjnego w jego strukturach.

Wnioski z kontroli:

- Chociaż Krajowe Centrum ds. Cyberbezpieczeństwa pełni funkcję o znaczeniu krytycznym, poziom zasobów w pierwszych czterech latach jego działania był znacznie niższy niż pierwotnie przewidziano.
- Ogólny strategiczny kierunek działalności Centrum jest niejasny i nie przyjęto planu strategicznego.

- Konieczne jest jaśniejsze określenie odpowiednich ról organów zaangażowanych w prowadzenie dochodzeń w sprawie cyberprzestępstw i incydentów związanych z bezpieczeństwem narodowym.
- W dalszym ciągu nie wdrożono wymogów unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji związanych z opracowaniem strategii krajowej.
- Chociaż określono struktury zarządzania, nie jest jasne, jak rozwiązania w zakresie zarządzania funkcjonują w praktyce.

Brakuje przejrzystości co do dostępności i kosztów zasobów przeznaczonych na cyberbezpieczeństwo.

Francja
Cour des comptes

Dostęp do szkolnictwa wyższego – wstępna ocena ustawy o doradztwie zawodowym i zdawalności wśród studentów

Data publikacji: luty 2020 r.

Link do sprawozdania: sprawozdanie (w j. francuskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2019–2020

Streszczenie sprawozdania

Temat kontroli

Celem ustawy o doradztwie zawodowym i zdawalności wśród studentów z 2018 r. (*loi relative à l'orientation et à la réussite des étudiants*, tzw. ustawa ORE) było usprawnienie trzech głównych etapów ścieżki edukacyjnej, którą podążają młodzi ludzie rozpoczynający studia wyższe: doradztwa zawodowego i wsparcia dla uczniów szkół średnich II stopnia, wyboru kierunku studiów i zdawalności w pierwszych latach studiów. Na podstawie ustawy wprowadzono *Parcoursup*, nową platformę cyfrową będącą źródłem informacji na temat dostępnych kierunków studiów i wymagań wstępnych, której celem było lepsze dopasowanie umiejętności i wyników w nauce uczniów szkół średnich do programów studiów uniwersyteckich.

W pierwszych dwóch latach stosowania ORE poczyniono pierwsze kroki w kierunku zmiany systemu dostępu do szkolnictwa wyższego. Pomimo licznych ograniczeń wprowadzenie *Parcoursup* przebiegło bardzo sprawnie, choć platforma nadal nie posiadała odpowiednich zabezpieczeń i nie gwarantowała trwałości, a dane mogły zostać lepiej wykorzystane, biorąc pod uwagę ich istotność.

Ustawa ORE została przyjęta w celu rozwiązania dwóch głównych problemów w polityce edukacyjnej. Pierwszym z nich była duża liczba studentów niekończących studiów. Drugi problem wynikał z narastającego przez lata głębokiego niezadowolenia z poprzedniej platformy cyfrowej, na której etap końcowy przeprowadzano w drodze losowania.

Na reformę przewidzianą w ustawie ORE w ciągu pięciu lat przyznano finansowanie w wysokości 867 mln euro. Reforma ta była oparta na ciągłości między różnymi etapami edukacji „-3/+3", a jej podstawową zasadą było założenie, że im więcej uczniowie szkół średnich II stopnia wiedzą na temat programów kierunków studiów, tym większe będą ich szanse powodzenia na egzaminach, ponieważ wybiorą te kierunki, które najlepiej odpowiadają ich umiejętnościom i ambicjom. Celem reformy było rozwiązanie problemu braku doradztwa zawodowego dostępnego dla uczniów szkół średnich II stopnia, a tym samym ograniczenie przypadków zmiany kierunku studiów. Według szacunków *Cour des comptes* koszt tych zmian wyniósł prawie 550 mln euro rocznie tylko po uwzględnieniu pierwszego roku szkolnictwa wyższego.

Kontrolerzy przeprowadzili wstępną ocenę dostępu do szkolnictwa wyższego w kontekście ustawy ORE, biorąc pod uwagę kwestie bezpieczeństwa informatycznego związane z platformą.

Obciążenie systemu informacyjnego znacznie się zwiększyło (w 2020 r. włączono do systemu wszystkie kierunki studiów, a liczba użytkowników szybko wzrosła w ciągu zaledwie kilku lat). Wynikało to z pospiesznego przejścia z poprzedniej platformy na platformę *Parcoursup* bez zmiany jej struktury, co spowodowało znaczne ryzyko w zakresie jakości, ciągłości, możliwości dostosowania i dalszego doskonalenia funkcjonowania platformy. Uchybienia w systemie w obszarach bezpieczeństwa, wydajności i solidności nie zostały wyeliminowane. Szybkie utworzenie *Parcoursup* było możliwe, ponieważ platforma ta była zarządzana w trybie beta przez niewielką grupę zmotywowanych osób o wysokich umiejętnościach, ale takie podejście świadczy o tym, że przyjęte rozwiązanie nie obejmowało strategicznego ukierunkowania i odpowiedniego zarządzania.

Kontrolerzy ocenili jakość systemu informacyjnego i wydajność nowej platformy *Parcoursup*. Platformę tę utworzono na podstawie ustawy ORE w celu poprawy jakości procesu przypisywania maturzystów do kierunków studiów, a tym samym podwyższenia wskaźnika ukończenia studiów.

Ustalenia

Choć platforma *Parcoursup* działała zadowalająco, była narażona na ryzyko informatyczne, które należało zmniejszyć. Konieczne jest zagwarantowanie bezpieczeństwa i trwałości platformy. Dane można było wykorzystać w większym stopniu.

Poprzedni system informatyczny

Platforma *Parcoursup* nie zawierała wielu nowych funkcji i była tak samo nieintuicyjna i wadliwa jak poprzednia platforma o nazwie *Admission Post-Bac* (APB). Była ponadto obarczona wieloma czynnikami ryzyka, których nie wyeliminowano. System informacyjny stanowiący podstawę strukturalną platformy *Parcoursup* pochodził bezpośrednio z wcześniejszej platformy. Mimo zapowiedzi, że system informacyjny będzie stanowił nowe narzędzie do przypisywania maturzystów, jego rdzeń został tylko nieznacznie zmodyfikowany w porównaniu z APB. W rzeczywistości ponad 72% infrastruktury informacyjnej pozostało bez zmian, ponieważ zaledwie niespełna 30% kodu APB zostało napisane od nowa.

Podstawy informatyczne platformy zostały zaprojektowane na samym początku XXI wieku w taki sposób, aby w skali roku mogła ona obsłużyć około 1 mln zgłoszeń na około 100 000 miejsc. Rozszerzono jednak zakres systemu informacyjnego, tak aby mógł on obsłużyć roczny napływ około 10 mln wniosków na około 1 mln miejsc. Platforma *Parcoursup* okazała się starym narzędziem pod nową nazwą. Wzrost obciążenia sprawił, że pojawiły się wątpliwości co do tego, czy platforma zapewni osiągnięcie wyznaczonego jej celu.

Nieodpowiednio udokumentowany system informacyjny

Pomimo starań ministerstwa na rzecz zapewnienia przejrzystości nadal nie ujawniono 99% kodu źródłowego *Parcoursup*. To, co zostało upublicznione, w ograniczonym stopniu przyczyniło się do zrozumienia, analizy i oceny procesu przypisywania kandydatów do kierunków studiów.

Tak jak poprzednia platforma *Parcoursup* był nieodpowiednio udokumentowanym operacyjnym systemem informacyjnym. W wyniku kontroli kodu uznano, że charakteryzował się on niską jakością i wysokim poziomem ryzyka. Stwierdzono również występowanie licznych błędów krytycznych. System ten był gorszej jakości niż inne rodzaje oprogramowania tworzone w podobnym czasie i wiązał się z dużym ryzykiem awarii.

Platforma *Parcoursup* korzystała zarówno z dostępnego publicznie, jak i z zamkniętego kodu źródłowego. Kod otwarty charakteryzował się znacznie wyższym wskaźnikiem błędów krytycznych niż kod zamknięty, co świadczy o istnieniu ryzyka zakłócenia funkcjonowania platformy. Platforma nie była ponadto zabezpieczona przed atakami hakerów (według kontroli bezpieczeństwa kodu źródłowego z lipca 2018 r.). Pod koniec 2019 r. ministerstwo ogłosiło jednak, że rozpoczęto procedurę certyfikacji kodu platformy *Parcoursup*.

Istniejąca dokumentacja kodu źródłowego nie była ani spójna, ani wyczerpująca. Kod *Parcoursup* był wyjątkowo skomplikowany. Kontrolerzy stwierdzili, że należałoby przebudować kod źródłowy, aby zmniejszyć liczbę skomplikowanych elementów.

Struktura systemu informacyjnego *Parcoursup* była obarczona wysokim ryzykiem, a bazą danych zarządzano ręcznie, co stanowi przestarzałe rozwiązanie. Słabość systemu polegała na dużej zależności od dostępności i czujności operatora. Ministerstwo przyznało, że jego struktura pociągała za sobą duże ryzyko oraz że ryzyka tego nie da się zmniejszyć bez udoskonalenia aplikacji.

System informacyjny *Parcoursup* był nieodpowiednio udokumentowany i opierał się zasadniczo na wiedzy fachowej pracowników krajowej agencji rządowej (*Service à Compétence Nationale*, SCN). Dokumentacja miała postać komentarzy zapisanych w bazie danych, która stanowiła rdzeń systemu, co utrudniało utrzymanie i rozwój systemu informacyjnego oraz wykorzystanie danych. Bez szczegółowego badania nie można było łatwo pozyskać i ocenić przechowywanych na platformie informacji o użytkownikach. Biorąc pod uwagę brak ustrukturyzowanej dokumentacji technicznej, zdolność agencji SCN do realizacji przypisanych jej zadań strategicznych zależała w zupełności od dyrektora centrum informatycznego.

Strategia bezpieczeństwa – konieczne są udoskonalenia

Ze względu na wrażliwość danych osobowych przechowywanych w systemie platforma *Parcoursup* stanowi znaczne wyzwanie pod względem bezpieczeństwa. Zasadniczo wszystkie organizacje zarządzające jakimkolwiek systemem informacyjnym muszą stosować formalną politykę bezpieczeństwa systemów informacyjnych przedstawioną w formie pisemnej. Mimo że decyzją premiera platforma *Parcoursup* została uznany za kluczowego dostawcę usług, nie przyjęto dla niej polityki bezpieczeństwa systemów informacyjnych. Konieczne jest niezwłoczne podjęcie działań w celu wprowadzenia takiej polityki.

W każdym zespole ds. *Parcoursup* wyznaczono urzędnika ds. bezpieczeństwa systemów informacyjnych podlegającego centrum informatycznemu. Dobrą praktyką byłoby wyznaczenie urzędników ds. bezpieczeństwa systemów informacyjnych podlegających bezpośrednio dyrektorowi SCN w celu zagwarantowania ich niezależności.

W połowie 2019 r. nadal trwały prace nad dostosowaniem platformy *Parcoursup* do przepisów RODO. Niektóre środki w dalszym ciągu nie zostały wdrożone, w szczególności konieczne było formalne ustanowienie różnych procedur stosowanych w odniesieniu do przetwarzania danych. Wciąż nie zapewniono odpowiedniego bezpieczeństwa danych osobowych i przechowywano zbyt wiele kompletnych danych jednostkowych.

Jednostka ds. *Parcoursup* podlegała zarówno kierownikowi projektu *Parcoursup* przydzielonemu z Biura Ministra, jak i Departamentowi Strategii Szkoleniowej i Spraw Studenckich w ramach Dyrekcji Generalnej ds. Szkolnictwa Wyższego i Integracji Zawodowej, co powodowało konflikt lojalności. Kwestie praktyczne związane z systemem informacyjnym *Parcoursup* były rozwiązywane na cotygodniowych spotkaniach. Chociaż zaletą tej formy organizacji był szybki czas reakcji w zakresie codziennego zarządzania przepływami studentów, w efekcie platformie *Parcoursup* brakowało jednak strategicznego ukierunkowania.

Ponadto system nie był wystarczająco przejrzysty. Pomimo ogromnego potencjału nie umożliwiał on optymalnego wykorzystania danych przechowywanych na platformie. Uruchomienie tego potencjału niemal na pewno przyniosłoby poprawę wydajności.

Wnioski i zalecenia

Rząd skutecznie scentralizował dostęp do szkolnictwa wyższego za pomocą platformy cyfrowej łączącej wszystkie programy kształcenia. Działania te podjęto w celu reakcji na upowszechnienie szkolnictwa wyższego. Poprzedni system pospiesznie przekształcono w *Parcoursup*, nie dokonano jednak żadnych znaczących zmian strukturalnych. W związku z tym nie wyeliminowano jego słabych punktów w zakresie bezpieczeństwa, wydajności i solidności, mimo że spodziewano się dalszego wzrostu obciążenia, biorąc pod uwagę ostateczny cel zakładający uwzględnienie wszystkich kierunków studiów pierwszego stopnia. System był ponadto nieodpowiednio udokumentowany. Zastosowano dość uproszczone podejście do programowania, przy czym niezwykle rozbudowany charakter systemu zwiększył ryzyko błędu w przypadku

jakichkolwiek zmian operacyjnych. W związku z tym platforma była narażona na znaczne ryzyko, jeśli chodzi o jakość i ciągłość świadczenia usług publicznych oraz bezpieczeństwo danych osobowych.

Cour des comptes sformułował następujące zalecenia:

- W zespole informatycznym SCN należy zatrudnić więcej pracowników, a finansowanie reformy ORE powinno zostać ukierunkowane na zwiększenie zasobów kadrowych i finansowych w Poddyrekcji ds. Systemów Informacyjnych i Badań Statystycznych.
- System informacyjny powinien zostać ustanowiony z myślą o długoterminowym funkcjonowaniu poprzez skorygowanie najpilniejszych błędów, modernizację lub zmianę struktury oraz udokumentowanie w sposób systematyczny i ustrukturyzowany podstawowych baz danych zarówno z poprzedniego systemu, jak i z *Parcoursup*.
- Należy opracować politykę bezpieczeństwa systemu informacyjnego *Parcoursup*.
- Należy ustanowić wspólny organ sterujący dla Ministerstwa Edukacji i Młodzieży oraz Ministerstwa Szkolnictwa Wyższego, Badań Naukowych i Innowacji, który nadzorowałby platformę *Parcoursup*, i skierować środki z finansowania reformy ORE na działania w zakresie doradztwa zawodowego.

Łotwa
Valsts Kontrole

Czy administracja publiczna wykorzystała wszystkie możliwości, aby efektywnie zarządzać infrastrukturą ICT?

Data publikacji: czerwiec 2019 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2017–2019

Streszczenie sprawozdania

Temat kontroli

Łotewski Urząd Kontroli Państwowej przeprowadził kontrolę wykonania zadań dotyczącą efektywności publicznej infrastruktury ICT. Celem kontroli było sprawdzenie, czy administracja publiczna stosowała jednolite podejście do efektywnego zarządzania infrastrukturą ICT oraz czy instytucje dokonały oceny korzyści związanych z centralizacją. Ponadto uznano, że bezpieczeństwo ośrodków przetwarzania danych stanowi ważną kwestię w ramach oceny możliwości dalszego planowania optymalizacji.

Niechęć organów do centralnego zarządzania infrastrukturą ICT, przejawiana na szczeblu co najmniej jednego z ministerstw, poskutkowała utworzeniem szeregu serwerowni, co wiązało się ze znacznym zwiększeniem kosztów utrzymania. W ramach kontroli czterech ministerstw ustalono, że działające w nich 22 podjednostki korzystają z 38 ośrodków przetwarzania danych. Podczas kontroli Urząd Kontroli Państwowej zaobserwował, że w niektórych przypadkach systemy informacyjne o istotnym znaczeniu, w tym znaczeniu krajowym, były zlokalizowane w pomieszczeniach

o niewystarczającym poziomie bezpieczeństwa. Optymalizacja liczby serwerowni umożliwiłaby nie tylko zmniejszenie wydatków na ICT, ale również zapewnienie wystarczającego poziomu bezpieczeństwa przy niższych kosztach. Tymczasem serwerownie o wysokim poziomie bezpieczeństwa były już dostępne w instytucjach, ale nie wykorzystywano w pełni ich potencjału.

Główny przedmiot kontroli

Kontrola miała na celu sprawdzenie, czy stworzono i wdrożono wszystkie warunki konieczne do jednolitego zarządzania infrastrukturą ICT, tak aby promować bardziej efektywne i bezpieczne wykorzystanie zasobów ICT.

Ustalenia i wnioski

Zarządzanie infrastrukturą ICT i jej optymalizacja

- Zarówno na szczeblu krajowym, jak i w ministerstwach brakowało długoterminowej wizji rozwoju i optymalizacji ICT. Ministerstwa i ich podjednostki optymalizowały infrastrukturę ICT zgodnie z własną wiedzą i możliwościami.

W latach 2011–2017 całkowite koszty utrzymania ICT w skontrolowanych instytucjach wzrosły z 17 do 20 mln euro rocznie. W instytucjach nie wprowadzono żadnych praktyk zakładających regularną ocenę tego, czy taniej byłoby utrzymywać infrastrukturę ICT we własnym zakresie, współpracować z inną instytucją, czy też zlecać utrzymanie ICT podmiotom zewnętrznym. Ani centralizacja ICT, ani ich decentralizacja nie są same w sobie postrzegane jako cel. Aby uzyskać jasność co do istniejących kosztów i możliwych rozwiązań alternatywnych, należy jednak przeprowadzić analizę konkretnej sytuacji i takich rozwiązań.

Bezpieczeństwo ICT

- W ramach prawnych nie określono w jasny sposób wymogów bezpieczeństwa infrastruktury ICT w ramach logicznego systemu w zależności od istotności informacji, które mają być przetwarzane. Nie określono szczegółowych wymogów technicznych w zakresie ochrony ośrodków przetwarzania danych ICT.

- Niedociągnięcia w zakresie wymogów bezpieczeństwa doprowadziły do wysokich kosztów ochrony lub wręcz przeciwnie – do braku ochrony informacji o znaczeniu

krajowym. Ważne systemy informacyjne były nawet hostowane w ośrodkach przetwarzania danych o niskim poziomie bezpieczeństwa.

- W większości serwerowni stwierdzono zagrożenia dla bezpieczeństwa – ośrodki przetwarzania danych nie były wystarczająco zabezpieczone przed fizycznym dostępem i ryzykiem środowiskowym. Na zapobieganie zagrożeniom dla bezpieczeństwa potrzebne były środki w kwocie co najmniej 247 000–765 000 euro, w zależności od przyjętego podejścia. Obejmowały one: 1) ulepszenie serwerowni zawierających systemy informacyjne o większym znaczeniu i zapewnienie przechowywania istotnych zasobów ICT w ośrodkach przetwarzania danych o wyższym poziomie bezpieczeństwa; lub 2) ulepszenie wszystkich istniejących serwerowni. Działania te wymagałyby jednak kwoty inwestycji, której kontrolerzy nie mogliby uzasadnić, chyba że zminimalizowano by liczbę ośrodków przetwarzania danych.

Ramy prawne były niepełne, ponieważ nie określały szczegółowych wymogów bezpieczeństwa dotyczących infrastruktury ICT, na przykład zawierały one wymogi dotyczące różnych kryteriów odnoszących się do bezpieczeństwa logicznego, ale nie przewidziano w nich kryteriów odnoszących się do fizycznego i środowiskowego bezpieczeństwa infrastruktury, które również wpływa na dostępność systemów i ochronę danych. Chociaż w dokumentach dotyczących planowania polityki publicznej podkreślono znaczenie bezpieczeństwa infrastruktury ICT i potrzebę jego wzmocnienia, nie zaplanowano konkretnych działań w tym obszarze. Brak jasnego, identyfikowalnego i logicznego zróżnicowania wymogów bezpieczeństwa stwarzał ryzyko, że w różnych częściach kraju wymogi bezpieczeństwa dotyczące przetwarzania informacji o takiej samej wadze i znaczeniu mogą być różne.

Państwo centralnie monitorowało bezpieczeństwo w przestrzeni cyfrowej i reagowało na incydenty występujące w tej przestrzeni, ale odpowiedzialność za wdrażanie środków bezpieczeństwa dotyczących infrastruktury ICT pozostawiono osobom stojącym na czele poszczególnych instytucji. W związku z powyższym panowało bardzo duże zróżnicowanie pod względem zrozumienia przez instytucje kwestii związanych z bezpieczeństwem ICT, oceny wagi przetwarzanych informacji oraz zasobów, jakimi dysponowały instytucje w celu rozwiązywania problemów dotyczących bezpieczeństwa ICT.

Potrzebny był stały system monitorowania tych procesów w celu przeprowadzenia oceny – niezależnie i z wykorzystaniem standardowych kryteriów – całej administracji

publicznej jako jednego systemu, tak aby zidentyfikować różne podejścia i zapobiec temu zróżnicowaniu poprzez wskazanie wspólnych czynników ryzyka, oraz aby zaplanować działania zapobiegawcze mające na celu zmniejszenie tego ryzyka.

Litwa
Valstybės Kontrolė

Zarządzanie państwowymi zasobami informacyjnymi o znaczeniu krytycznym

Data publikacji: czerwiec 2018 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)
sprawozdanie (w j. litewskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2014–2017

Streszczenie sprawozdania

Temat kontroli

Z wykorzystaniem państwowych zasobów informacyjnych o znaczeniu krytycznym – informacji elektronicznych o znaczeniu krytycznym – pełnione są ważne funkcje instytucji rządowych, takie jak zarządzanie finansami publicznymi, administracja podatkowa i ochrona zdrowia. Każda utrata informacji o znaczeniu krytycznym lub niedostępność odnośnych systemów informacyjnych może mieć poważne konsekwencje dla bezpieczeństwa publicznego, dobrostanu i gospodarki. W wyniku przeprowadzonej przez litewską Kontrolę Państwową w latach 2006–2016 oceny mechanizmów ogólnej kontroli systemów informatycznych ujawniono powtarzające się problemy w zarządzaniu systemami informatycznymi (planowaniu, określaniu struktury informacyjnej, strukturze organizacyjnej, zmianach, zapewnianiu ciągłości działania, bezpieczeństwie danych, monitorowaniu i ocenie zarządzania systemami informatycznymi). Litewska Kontrola Państwowa przeprowadziła kontrolę państwowych zasobów informacyjnych o znaczeniu krytycznym, aby ocenić zarządzanie tymi zasobami i ich bezpieczeństwo oraz aby zapewnić usprawnienia w tym zakresie.

Kontrola miała na celu ocenę zarządzania państwowymi zasobami informacyjnymi o znaczeniu krytycznym (ogólnej kontroli nad tymi zasobami) i odnośnej dojrzałości procesowej oraz określenie problemów systemowych.

Litewska Kontrola Państwowa oceniła dojrzałość zarządzania systemami informatycznymi w dwunastu organizacjach sektora publicznego[64], które zarządzają 44 państwowymi systemami informacyjnymi kategorii pierwszej. Kontrolę przeprowadzono zgodnie z wymogami w zakresie kontroli publicznej oraz Międzynarodowymi Standardami Najwyższych Organów Kontroli. Oceny dokonano zgodnie z metodyką COBIT[65] w następujących obszarach obarczonych największym ryzykiem: planowanie strategiczne w obszarze IT, określanie struktury informacyjnej, zarządzanie ryzykiem w obszarze IT, zarządzanie zmianą, zapewnianie niezakłóconego świadczenia usług, bezpieczeństwo systemów, zarządzanie danymi, monitorowanie i ocena działań informatycznych, zapewnienie pewności co do zarządzania systemami informatycznymi. Ocena procesów obejmowała zarówno zarządzanie systemami informatycznymi na szczeblu organizacji i na szczeblu krajowym, jak i interakcje między tymi szczeblami zarządzania.

Ustalenia kontroli

Tendencje zmian poziomów dojrzałości w zakresie zarządzania państwowymi zasobami informacyjnymi o znaczeniu krytycznym były pozytywne. Biorąc jednak pod uwagę rosnący poziom zagrożeń dla cyberbezpieczeństwa, zaobserwowane postępy były zbyt

[64] Krajowy Inspektorat Podatkowy, Przedsiębiorstwo Państwowe Centrum Rejestrów, Departament Technologii Informatycznych i Komunikacji, Zakład Państwowego Funduszu Ubezpieczeń Społecznych, Przedsiębiorstwo Państwowe Centrum Informacji i Przedsiębiorczości Rolnej, Centrum Systemów Informacji Celnej, Państwowe Służby Żywności i Weterynaryjne, Kancelaria Sejmu Republiki Litewskiej, Ministerstwo Finansów, Komitet Rozwoju Społeczeństwa Informacyjnego, Państwowy Fundusz Pacjentów, Państwowa Służba Leśna.

[65] COBIT (cele kontroli w zakresie technologii informacyjnej i technologii pokrewnych) to norma międzynarodowej organizacji ISACA określającej najlepsze praktyki w dziedzinie zarządzania systemami informatycznymi.

wolne i należałoby zwiększyć bezpieczeństwo tych zasobów, co wynikało z uchybień przedstawionych poniżej.

- System identyfikacji państwowych zasobów informacyjnych o znaczeniu krytycznym nie był wystarczająco skuteczny, aby umożliwić wdrożenie rozwiązań w zakresie bezpieczeństwa zaspokajających rzeczywiste potrzeby:
  - Oceny opracowane w celu wykazania krytycznego znaczenia państwowych zasobów informacyjnych nie były wystarczająco obiektywne, zmiany nie zawsze były uwzględniane w ponownej ocenie, cały proces nie był monitorowany na poziomie krajowym, a wytyczne dotyczące określania krytycznego znaczenia nie zapewniały skutecznego wdrażania.
  - System identyfikacji państwowych zasobów informacyjnych o znaczeniu krytycznym i infrastruktury informacyjnej o znaczeniu krytycznym nie był ustandaryzowany; zasoby i infrastruktura były identyfikowane w różny sposób na podstawie wagi informacji i usług, co komplikowało ten proces.
  - Nie opracowano krajowej struktury informacyjnej, która stanowiłaby odzwierciedlenie państwowych systemów informacyjnych i ich wzajemnych połączeń, ukazywałaby skalę państwowych zasobów informacyjnych o znaczeniu krytycznym i umożliwiała podejmowanie przemyślanych decyzji dotyczących znaczenia tych zasobów.
- Konieczne było zapewnienie większej zgodności zarządzania państwowymi zasobami informacyjnymi z najlepszymi praktykami i normami w zakresie zarządzania systemami informatycznymi w celu osiągnięcia zintegrowanej poprawy w dziedzinie technologii informacyjnej, która przyczyniłaby się do większych postępów w zakresie zarządzania państwowymi zasobami informacyjnymi o znaczeniu krytycznym:
  - Planowanie w obszarze IT nie było zrównoważone: planowane narzędzia informatyczne zostały przedstawione w różnych dokumentach, brakowało jakiegokolwiek systematycznego podejścia ze względu na zbyt dużą liczbę dokumentów strategicznych, co utrudniało określenie kluczowych priorytetów i ukierunkowanie zasobów w celu zarządzania największymi zagrożeniami.

- Monitorowanie systemów informatycznych nie zapewniało mierzenia przez organizacje skuteczności operacji informatycznych oraz tego, aby kontrole przeprowadzane przez kierownictwo państwowych zasobów informacyjnych o znaczeniu krytycznym ukazywały faktyczny poziom dojrzałości zarządzania systemami informatycznymi. Państwowe zarządzanie systemami informatycznymi nie było kontrolowane na szczeblu krajowym, a kwestie zarządzania systemami informatycznymi nie były systematycznie analizowane. Utworzono system monitorowania zgodności państwowych zasobów informacyjnych z wymogami w zakresie bezpieczeństwa informacji elektronicznych, który miał służyć jedynie do ułatwiania monitorowania zgodności w zakresie bezpieczeństwa, ale jego funkcjonalność nie była wystarczająco wykorzystywana.

- Środki mające zapewnić odporność zasobów informacyjnych o znaczeniu krytycznym odpowiadającą poziomowi zagrożeń dla cyberbezpieczeństwa nie były wystarczająco skuteczne, w związku z czym nadal istniało ryzyko, że zasoby te były narażone na zagrożenia:

  - Należało zwiększyć skuteczność oceny ryzyka w zakresie bezpieczeństwa informatycznego, ponieważ nie określono wszystkich istotnych zagrożeń, a metodyka ich oceny nie była zgodna z najnowszymi praktykami w zakresie zarządzania systemami informatycznymi. Nie zapewniono też terminowego zarządzania niedopuszczalnym ryzykiem.

  - Środki w zakresie bezpieczeństwa organizacyjnego mogące ograniczyć zagrożenia dla cyberbezpieczeństwa nie były systematycznie wykorzystywane. Nie przeprowadzano wystarczających testów bezpieczeństwa, nie zapewniono pełnego przeszkolenia pracowników podczas opracowywania, aktualizacji i modyfikacji systemów informacyjnych, nie zarządzano bezpiecznymi konfiguracjami i aktualizacjami oprogramowania. Niewłaściwe zarządzanie ciągłością działania systemów informatycznych i plikami kopii zapasowych zagrażały odtworzeniu ciągłości działania. Pomiary wydajności bezpieczeństwa były niewystarczające i nie przyczyniały się do poprawy bezpieczeństwa.

Wnioski

Zarządzanie systemami informatycznymi przez podmioty sektora publicznego skontrolowane w ostatnich dziesięciu latach osiągnęło średnio pierwszy poziom dojrzałości z pięciu[66], a w czasie sporządzania niniejszego dokumentu było na poziomie 1,7. Ten niski poziom dojrzałości w zakresie zarządzania państwowymi zasobami informacyjnymi o znaczeniu krytycznym wskazywał na uchybienia w kształtowaniu i wdrażaniu polityki dotyczącej państwowych zasobów informacyjnych, przez co były one bardziej narażone na zagrożenia. Aby zwiększyć bezpieczeństwo tych zasobów, należy usprawnić mechanizm zarządzania nimi, tak aby w możliwie największym stopniu odpowiadał on najlepszym praktykom. Kontrolerzy zauważyli również, że środki mające na celu zagwarantowanie odporności zasobów informacyjnych o znaczeniu krytycznym na zagrożenia dla cyberbezpieczeństwa nie były wystarczająco skuteczne. W związku z tym należy zwiększyć skuteczność oceny zagrożeń dla bezpieczeństwa informatycznego, kładąc większy nacisk na testowanie bezpieczeństwa podczas tworzenia i modernizowania systemów informacyjnych i szkolenie pracowników.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Czy cyberprzestępczość jest skutecznie zwalczana?
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. litewskim)
Data publikacji:	2020 r.

Tytuł sprawozdania:	Środowisko cyberbezpieczeństwa na Litwie
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. litewskim)
Data publikacji:	2015 r.

[66] Zgodnie z metodyką COBIT.

Węgry
Państwowa Izba Obrachunkowa

Kontrola ochrony danych – kontrola krajowych ram ochrony danych i niektórych rejestrów danych priorytetowych w kontekście współpracy międzynarodowej

Data publikacji: marzec 2017 r.

Link do sprawozdania: sprawozdanie (w j. węgierskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola zgodności

Okres objęty kontrolą: lata 2011–2015

Streszczenie sprawozdania

Temat kontroli

Bezpieczeństwo krajowych zasobów danych ma fundamentalne znaczenie dla społeczeństwa w każdym kraju w odniesieniu do zachowania i ochrony wartości narodowych. W związku z tym zapewnienie zwiększonego bezpieczeństwa danych osobowych i publicznych w ramach krajowych zasobów danych Węgier jest niezwykle ważne dla wzmacniania zaufania obywateli do państwa oraz zapewniania ciągłego i płynnego funkcjonowania administracji publicznej. Ochrona danych i sieć bezpieczeństwa zapewniana przez ramy prawne w celu jej egzekwowania mają kluczowe znaczenie dla społeczeństwa.

Jeśli chodzi o ochronę danych, administracja publiczna odgrywa zasadniczą rolę w zarządzaniu największymi i najbardziej wrażliwymi rejestrami danych należących do krajowych zasobów danych. Administratorzy danych odpowiedzialni za te rejestry ściśle ze sobą współpracują przy wykonywaniu swoich zadań. Regularnie przekazują oni rejestry zawierające duże ilości danych i są zobowiązani zwracać uwagę na ustawowe wymogi w zakresie ochrony danych. Wykorzystanie elektronicznych systemów informacyjnych do zarządzania danymi i ich przetwarzania ma w obecnych czasach

kluczowe znaczenie, dlatego należy zagwarantować odpowiednią i niezawodną obsługę tych systemów poprzez odpowiednio zaprojektowane i obsługiwane mechanizmy kontroli.

Podczas swoich kontroli węgierska Państwowa Izba Obrachunkowa kładzie duży nacisk na ochronę danych. Przeprowadziła ona w latach 2011–2015 kompleksowe kontrole ochrony danych, a w pierwszym kwartale 2017 r. opublikowała odnośne sprawozdanie. Kontrola obejmowała również aspekty kontroli międzynarodowych przeprowadzonych równolegle we współpracy z grupą roboczą ds. systemów informatycznych EUROSAI, które dotyczyły przede wszystkim zgodności z istniejącymi dyrektywami Unii Europejskiej.

Kontrola zgodności w zakresie ochrony danych na Węgrzech miała na celu ocenę, czy w kraju tym ustanowiono regulacyjne i operacyjne ramy ochrony danych oraz czy główne organizacje zarządzające danymi przestrzegały wymogów dotyczących bezpiecznego zarządzania danymi i zlecania podmiotom zewnętrznym ich przetwarzania. Podczas kontroli skoncentrowano się w szczególności na ochronie danych osobowych i krajowych zasobów danych.

W kontekście kontroli Państwowa Izba Obrachunkowa oceniła zarządzanie danymi w sześciu organizacjach zarządzających danymi (przykładowo organ podatkowy, skarb państwa, ubezpieczenia zdrowotne, wypłaty emerytur, urząd ds. edukacji, dane osobowe i rejestry adresów, rejestry pojazdów i dane transportowe oraz agencje administracyjne zajmujące się zarządzaniem danymi w sprawach karnych) oraz działalność organu ochrony danych i organu bezpieczeństwa informacji.

W kontroli położono szczególny nacisk na uprawnienia organizacji zarządzających danymi, w szczególności w przypadku przekazywania danych osobom trzecim. Podczas badania mechanizmów kontroli wewnętrznych w zakresie zarządzania danymi oraz ich przetwarzania oceniono, czy istnieją aktualne regulacje dotyczące obowiązków, zakresu odpowiedzialności i kompetencji, a także zarządzania zasobami ludzkimi i procesów.

Jeśli chodzi o systemy elektroniczne wykorzystywane w zarządzaniu danymi, Państwowa Izba Obrachunkowa oceniła powiązane z nimi środki bezpieczeństwa, w tym obszary ochrony fizycznej, prawa dostępu, logowanie, procedury oceny bezpieczeństwa, bezpieczeństwo systemów i komunikacji oraz zgodność klasyfikacji bezpieczeństwa w całej organizacji.

Zlecanie przetwarzania danych podmiotom zewnętrznym skontrolowano na podstawie zawartych umów, przyglądając się temu, czy organizacje zarządzające danymi zobowiązały organizacje przetwarzające dane do spełniania wymogów związanych z działalnością w zakresie przetwarzania danych zgodnie z regulacjami ustawowymi.

Ustalenia i wnioski

Na podstawie kontroli węgierska Państwowa Izba Obrachunkowa ustaliła, że wewnętrzne regulaminy organizacji zarządzających danymi dotyczące działań w zakresie zarządzania danymi zapewniły ochronę krajowych zasobów danych jako części zasobów krajowych, zgodnie z przepisami obowiązującymi w latach 2011–2015. Administratorzy danych prawidłowo zastosowali w praktyce wymogi w zakresie bezpiecznego zarządzania danymi i zlecania przetwarzania danych podmiotom zewnętrznym. Przekazywanie danych osobom trzecim realizowano na podstawie odpowiedniego mandatu i w oparciu o jasne rozgraniczenie obowiązków i uprawnień.

W odniesieniu do niektórych administratorów danych ustalono, że klasyfikacja bezpieczeństwa systemów elektronicznych i całej organizacji nie zawsze była zgodna z wymogami prawnymi, ale zakres niedociągnięć nie wpływał znacząco na bezpieczeństwo przetwarzanych danych. Na podstawie zaleceń zawartych w sprawozdaniu z kontroli organizacje zarządzające danymi zlikwidowały te niedociągnięcia w ramach planów działania zatwierdzonych przez najwyższy organ kontroli.

W związku z kontrolą międzynarodową przeprowadzoną równolegle we współpracy z grupą roboczą ds. systemów informatycznych EUROSAI Państwowa Izba Obrachunkowa ustaliła, że węgierskie ustawodawstwo w zakresie ochrony danych było zgodne z istniejącą dyrektywą UE.

Podsumowując, poprzez kontrolę ochrony danych węgierska Państwowa Izba Obrachunkowa przyczyniła się do zapewnienia dobrego zarządzania krajowymi zasobami danych i ich ochrony.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Sprawozdanie – kontrole następcze – kontrola ochrony danych – kontrola krajowych ram ochrony danych i niektórych rejestrów danych kluczowych w kontekście współpracy międzynarodowej
Link do sprawozdania:	sprawozdanie (w j. węgierskim)
Data publikacji:	2020 r.

Niderlandy
Powszechna Izba Obrachunkowa

Cyberbezpieczeństwo infrastruktury gospodarki wodnej o znaczeniu krytycznym i kontroli granicznych w Niderlandach

Data publikacji: marzec 2019 r. i kwiecień 2020 r.

Link do sprawozdań: streszczenie sprawozdania dotyczącego cyberbezpieczeństwa i infrastruktury gospodarki wodnej o znaczeniu krytycznym (w j. angielskim)

streszczenie sprawozdania dotyczącego cyberbezpieczeństwa i zautomatyzowanych kontroli granicznych (w j. angielskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2018–2020

Streszczenie sprawozdania

Temat kontroli

W 2018 r. niderlandzka Powszechna Izba Obrachunkowa postanowiła przeprowadzić kontrole w zakresie cyberbezpieczeństwa w sektorach o znaczeniu krytycznym dla społeczeństwa. Na podstawie wieloletniego doświadczenia w kontrolowaniu zgodności w zakresie bezpieczeństwa informacji w instytucjach rządowych na szczeblu centralnym Powszechna Izba Obrachunkowa dostrzegła wartość dodaną w kontroli *wyników* strategii politycznych i środków w praktyce. Pierwszymi dwoma sektorami, w których przeprowadzono kontrole, były sektor gospodarki wodnej i sektor zautomatyzowanych kontroli granicznych. Pierwszy z nich ma podstawowe znaczenie ze względu na położenie kraju w dużej części poniżej poziomu morza, a drugi – ze względu na rangę portu lotniczego Amsterdam Schiphol jako międzynarodowego lotniska przesiadkowego i przeładunkowego oraz bramy wjazdowej do kraju.

Minister Infrastruktury i Gospodarki Wodnej określił szereg elementów infrastruktury gospodarki wodnej zarządzanych przez Dyrekcję Generalną ds. Robót Publicznych i Gospodarki Wodnej (jednostkę kontrolowaną) jako „części o znaczeniu krytycznym" sektora gospodarki wodnej. Wiele systemów komputerowych wykorzystywanych do obsługi infrastruktury gospodarki wodnej o znaczeniu krytycznym pochodzi z lat 80. i 90. XX wieku – czasów, w których „cyberbezpieczeństwo" nie było powszechnie brane pod uwagę. Systemy te zostały pierwotnie zaprojektowane z myślą o samodzielnym funkcjonowaniu, ale następnie były stopniowo łączone z większymi sieciami komputerowymi, na przykład w celu ułatwienia ich zdalnej obsługi. Tendencja ta sprawiła, że systemy te stały się bardziej narażone na zagrożenia dla cyberbezpieczeństwa.

Minister Obrony oraz Minister Sprawiedliwości i Bezpieczeństwa są wspólnie odpowiedzialni za kontrole graniczne przeprowadzane przez funkcjonariuszy niderlandzkiej straży granicznej w porcie lotniczym Schiphol. Oba ministerstwa (jednostki kontrolowane) posiadają systemy informatyczne, na których polega straż graniczna. Systemy te mają krytyczne znaczenie dla funkcjonowania portu lotniczego i są wykorzystywane do przetwarzania bardzo wrażliwych danych. W związku z tym są one potencjalnym celem do przeprowadzania cyberataków ukierunkowanych na sabotaż, szpiegostwo lub manipulację w związku z kontrolami granicznymi.

Podczas kontroli zbadano, w jaki sposób jednostki kontrolowane były przygotowane na radzenie sobie z zagrożeniami dla cyberbezpieczeństwa oraz czy ich działania w tym zakresie były skuteczne.

- Pytania kontrolne miały na celu udzielenie odpowiedzi na poniższe pytania: W jaki sposób jednostki kontrolowane *chronią* systemy przed zagrożeniami dla cyberbezpieczeństwa i *zapobiegają* cyberatakom?
- W jaki sposób jednostki kontrolowane *wykrywają* zagrożenia dla cyberbezpieczeństwa i cyberataki?
- W jaki sposób jednostki kontrolowane *reagują* w sytuacji wystąpienia cyberataku?

Obie kontrole skupiały się w głównej mierze na skuteczności. W ścisłej współpracy z jednostkami kontrolowanymi etyczni hakerzy przeprowadzili prace w zakresie infrastruktury gospodarki wodnej o znaczeniu krytycznym i jednego z systemów kontroli granicznej. Przed ukazaniem się sprawozdań podjęto, rzecz jasna, działania

w związku ze wszystkimi ustaleniami z testów, a w publikacjach nie ujawniono żadnych szczegółów technicznych.

Główna różnica między tymi dwiema kontrolami polegała na tym, że podczas kontroli infrastruktury gospodarki wodnej skoncentrowano się na osiągnięciu celów przez jednostkę kontrolowaną, podczas gdy kontrola dotycząca kontroli granicznych opierała się na ramach cyberbezpieczeństwa opracowane przez NIST.

Ustalenia

W ramach obu kontroli ustalono przede wszystkim, że jednostki kontrolowane zdawały sobie sprawę z zagrożeń dla cyberbezpieczeństwa i były w trakcie procesu wdrażania profesjonalnego podejścia do tej kwestii.

W przypadku infrastruktury gospodarki wodnej stwierdzono jednak, że aby osiągnąć wyznaczone jej cele dotyczące cyberbezpieczeństwa, jednostka kontrolowana powinna podjąć więcej działań, zarówno w zakresie wykrywania zagrożeń, jak i reagowania na nie. Jednostka kontrolowana ustanowiła wprawdzie centrum działań w zakresie bezpieczeństwa w celu wykrywania cyberataków i reagowania na nie, do jesieni 2018 r. nie osiągnięto jednak wyznaczonego na koniec 2017 r. celu polegającego na natychmiastowym wykrywaniu wszelkich cyberataków wymierzonych w infrastrukturę gospodarki wodnej o znaczeniu krytycznym. Oznacza to, że istniało ryzyko niewykrycia cyberataku wymierzonego w element infrastruktury wodnej o znaczeniu krytycznym lub zbyt późnego wykrycia takiego ataku. Ponadto w teście, którym objęto jeden z elementów tej infrastruktury, wykazano, że możliwe było uzyskanie do niej fizycznego dostępu. Hakerzy zdołali uzyskać dostęp do pokoju kontrolnego, w którym znaleźli się sami, a stanowiska pracy były niezabezpieczone. Co więcej, jednostka kontrolowana nie sporządziła scenariusza na wypadek kryzysu spowodowanego przez cyberatak, a informacje dotyczące reagowania były niepełne lub nieaktualne. Dostępność aktualnych informacji może mieć kluczowe znaczenie dla szybkiego i skutecznego reagowania w sytuacji kryzysowej.

W przypadku kontroli granicznych środki w zakresie cyberbezpieczeństwa nie były odpowiednie ani dostosowane do przyszłych wyzwań. Po pierwsze, aby zapewnić wdrożenie wszystkich środków w zakresie cyberbezpieczeństwa, ważne systemy kontroli granicznej musiały być formalnie zatwierdzone przed rozpoczęciem funkcjonowania. Powszechna Izba Obrachunkowa ustaliła, że dwa z trzech systemów wykorzystywano, choć nie zostały one zatwierdzone, nie było zatem żadnej gwarancji,

że wprowadzono niezbędne środki w zakresie bezpieczeństwa. Po drugie, funkcjonowało jedno centrum działań w zakresie bezpieczeństwa, ale żaden z systemów nie był z nim bezpośrednio połączony. Choć ogólna infrastruktura była połączona z tym centrum, nadal istniało ryzyko, że cyberataki nie zostaną zauważone lub zostaną wykryte zbyt późno. Po trzecie, nie przeprowadzano regularnie testów bezpieczeństwa. W gruncie rzeczy tylko jeden z trzech systemów poddanych kontroli był testowany w przeszłości i tylko w ograniczonym zakresie. Ponadto, tak jak w przypadku pierwszej kontroli, nie sporządzono konkretnego scenariusza na wypadek kryzysu spowodowanego cyberatakiem.

Podczas testu bezpieczeństwa jednego z systemów, który nigdy wcześniej nie był testowany, etyczni hakerzy natrafili na wiele luk. Nieuprawniona osoba z wewnątrz działająca w złych zamiarach mogłaby je zbiorowo wykorzystać w celu przeprowadzenia cyberataku, który umożliwiłby dostęp do informacji w systemie, ich kopiowanie, a nawet manipulowanie nimi. Wyniki te świadczą o tym, jak ważne jest regularne testowanie bezpieczeństwa.

Ustalenia kontroli są niepokojące ze względu na trwającą automatyzację procedur na granicach. W niedalekiej przyszłości coraz więcej systemów kontroli granicznej będzie przetwarzało coraz więcej danych z wykorzystaniem coraz większej liczby połączeń, co zwiększa ryzyko cyberataków. Przyjęte podejście nie było zatem dostosowane do przyszłych wyzwań.

Wnioski

W przypadku infrastruktury gospodarki wodnej niektóre kluczowe elementy uniemożliwiały jednostce kontrolowanej podjęcie ostatecznych działań w zakresie cyberbezpieczeństwa. Na przykład poziom zagrożenia nie był jasny, co utrudniało ocenę, czy podjęte działania i przydzielony budżet były wystarczające. Ponadto departament na szczeblu centralnym odpowiedzialny za kwestie cyberbezpieczeństwa nie miał uprawnień do wdrażania niezbędnych środków w zakresie cyberbezpieczeństwa w zdecentralizowanych elementach infrastruktury gospodarki wodnej. Zalecenia z kontroli dotyczące tej kwestii zostały zrealizowane, co pomogło organizacji w poczynieniu postępów w tym obszarze.

W odniesieniu do kontroli granicznych nie było wyraźnej przyczyny niewystarczającego poziomu cyberbezpieczeństwa. Badania przeprowadzone w ramach kontroli wykazały istnienie kompletnych i szczegółowych procedur i strategii w zakresie

cyberbezpieczeństwa, a także gwarancję wystarczającej wiedzy fachowej oraz wykwalifikowanych pracowników. W związku z tym zalecenia z kontroli skoncentrowano głównie na zapewnieniu, aby faktycznie podjęto wszystkie możliwe działania.

Obie kontrole wzbudziły duże zainteresowanie w parlamencie i mediach. Przyczyniły się one do zwiększenia świadomości w zakresie cyberbezpieczeństwa w odniesieniu do kluczowej infrastruktury oraz zapewniły jednostkom kontrolowanym wskazówki na temat tego, jak mogą poprawić cyberbezpieczeństwo. Ścisła współpraca z jednostkami kontrolowanymi była niezbędna do dogłębnego zrozumienia ich sytuacji i podjęcia ryzyka związanego z weryfikowaniem i testowaniem cyberbezpieczeństwa.

Planuje się również przeprowadzenie trzeciej kontroli tego typu. Ponadto poziom bezpieczeństwa informacji na szczeblu rządu krajowego w Niderlandach jest kluczowym elementem rocznego cyklu kontroli zgodności. Na przestrzeni lat najwyższy organ kontroli Niderlandów zaobserwował, że wiele resortów nie stosuje odpowiednich środków zapewniających bezpieczeństwo informacji. Powszechna Izba Obrachunkowa wykorzystuje obecnie doświadczenie zdobyte podczas kontroli cyberbezpieczeństwa do poszerzenia swojej perspektywy w zakresie kontroli bezpieczeństwa informacji, z zamiarem wyjścia poza analizę dokumentów oraz strategii politycznych i testowania rzeczywistej skuteczności podjętych środków.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Rozdział 3 dokumentu pt. „Staat van de rijksverantwoording 2019”
Link do sprawozdania:	sprawozdanie (w j. niderlandzkim)
Data publikacji:	2020 r.

Tytuł sprawozdania:	Analiza pracy zdalnej z domu
Link do sprawozdania:	sprawozdanie (w j. niderlandzkim)
Data publikacji:	2020 r.

Polska
Najwyższa Izba Kontroli

Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych

Data publikacji: 2016 r.

Link do sprawozdania: sprawozdanie (w j. polskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola zgodności

Okres objęty kontrolą: lata 2014–2015

Streszczenie sprawozdania

Temat kontroli

Celem kontroli była ocena, czy w kontrolowanych jednostkach zapewnione jest bezpieczeństwo danych gromadzonych w systemach przeznaczonych do realizacji istotnych zadań publicznych. Kontrolą objęto sześć wybranych instytucji realizujących ważne zadania publiczne. W każdej z powyższych instytucji wybrano po analizie jeden z istotnych systemów informatycznych i objęto go szczegółowym badaniem. W kontroli wykorzystano metodę COBIT (cele kontroli w zakresie technologii informacyjnej i technologii pokrewnych) w wersji 4.1.

Kontrola ta została podjęta po przeprowadzonej w 2015 r. kontroli „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej”[67], w której dokonano ustaleń wskazujących na problemy o charakterze systemowym. Wykazała ona między innymi, że administracja państwowa nie podjęła do tego czasu działań mających na celu zapewnienie bezpieczeństwa

[67] https://www.nik.gov.pl/kontrole/P/14/043/

teleinformatycznego na poziomie krajowym. Stwierdzono, że działania podmiotów publicznych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez wizji systemowej. W sytuacji braku centralnych rozwiązań zapewniających warunki bezpieczeństwa konkretnych systemów informatycznych istotnych dla funkcjonowania państwa podjęto próbę szczegółowego zbadania, czy instytucje administrujące systemami informatycznymi służącymi do realizacji istotnych zadań publicznych zapewniają warunki dla bezpiecznego ich działania.

W 2019 r. zatwierdzono ustalenia kolejnej systemowej kontroli dotyczącej cyberbezpieczeństwa „Bezpieczeństwo teleinformatyczne RP ", lecz jej wyniki są niejawne.

Pytania kontrolne

Cele cząstkowe zostały podzielone na dwa obszary poddane ocenie, w ramach których dążono do uzyskania odpowiedzi na pytania szczegółowe.

W obszarze wspierania bezpieczeństwa IT na poziomie całej organizacji badano między innymi, czy:

- prowadzone jest zarządzanie bezpieczeństwem IT;
- wdrożono plany zapewnienia bezpieczeństwa IT;
- testuje się, nadzoruje i monitoruje bezpieczeństwo IT;
- zdefiniowano incydenty związane z bezpieczeństwem IT;
- zarządza się kluczami kryptograficznymi;
- wdrożono ochronę przed złośliwym oprogramowaniem, jego wykrywanie i dystrybucję poprawek;
- zapewniono bezpieczeństwo sieciowe.

W obszarze wspierania bezpieczeństwa na poziomie wybranego systemu badano między innymi, czy:

- zarządza się tożsamościami i kontami użytkowników;
- chroni się technologie zabezpieczeń i dane wrażliwe.

Ustalenia i wnioski

Stopień przygotowania oraz wdrożenia Systemu Zapewnienia Bezpieczeństwa Informacji nie zapewniał akceptowalnego poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych. Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny. Spośród sześciu skontrolowanych jednostek tylko jedna wdrożyła System Zapewnienia Bezpieczeństwa Informacji, chociaż należy zauważyć, iż jego funkcjonowanie było również obarczone istotnymi nieprawidłowościami. W większości zbadanych jednostek (wszystkich poza jedną) prace nad zapewnieniem odpowiednich warunków bezpieczeństwa informacji przetwarzanych w systemach informatycznych nie osiągnęły właściwego poziomu – zostały niedawno rozpoczęte i znajdowały się na wstępnym etapie, obejmującym opracowanie niezbędnych podstaw formalnych. Opierano się na uproszczonych lub nieformalnych zasadach wynikających z dobrych praktyk lub dotychczasowych doświadczeń pracowników działów IT.

Zgodnie z metodyką COBIT 4.1 poziom zarządzania procesem zapewnienia bezpieczeństwa w poszczególnych jednostkach kontrolowanych wahał się pomiędzy „początkowy/doraźny” (1) a „zdefiniowany” (3), w skali od zera do pięciu, gdzie pięć stanowi wartość maksymalną.

Główny ciężar zapewnienia bezpieczeństwa IT w jednostkach kontrolowanych spoczywał na koordynatorze ds. bezpieczeństwa, który jednak nie posiadał w praktyce kompetencji w zakresie zarządzania całym procesem. Często też zadania te były realizowane jednoosobowo. Powoływano wprawdzie zespoły specjalistów lub zawierano umowy z wykonawcami zewnętrznymi, jednakże nie sporządzano niezbędnych analiz, czy usługi świadczone przez nich zaspakajają potrzeby jednostki w zakresie bezpieczeństwa. Świadomość potrzeby zapewnienia bezpieczeństwa informatycznego była w jednostkach kontrolowanych fragmentaryczna i ograniczona. Bezpieczeństwo danych było postrzegane głównie jako przedmiot odpowiedzialności i domena działu IT, a nie wszystkich komórek realizujących zadania statutowe, co w dużej mierze utrudniało wypracowanie spójnych dla całej instytucji systemów zarządzania bezpieczeństwem informatycznym.

Porównując jakość realizacji obowiązków dotyczących zapewnienia bezpieczeństwa informacji z punktu widzenia całych organizacji i wybranych systemów, stwierdzić należy, że w tym drugim obszarze realizacja zadań była na nieco wyższym poziomie. Może to wynikać z wpływu, jaki na zapewnienie bezpieczeństwa miały praktyczna

wiedza i zaangażowanie średniego personelu technicznego, oraz z coraz powszechniejszego wykorzystywania w administracji państwowej komercyjnych systemów informatycznych, opartych o standardowe na rynku, nowoczesne rozwiązania wspierające zapewnianie bezpieczeństwa. Dzięki wykorzystaniu tych rozwiązań oraz dotychczasowych doświadczeń i dobrych praktyk możliwe było utrzymywanie pewnego poziomu bezpieczeństwa funkcjonowania poszczególnych systemów w warunkach ograniczonych zasobów, braków organizacyjnych lub niefunkcjonujących regulacji. Nie może to jednak stanowić rozwiązania docelowego, bowiem w dobie dynamicznego wzrostu zagrożeń zapewnienie bezpieczeństwa systemów IT nie może być oparte na chaotycznie zarządzanych działaniach ukierunkowanych jedynie na przezwyciężanie aktualnych trudności.

Wnioski z kontroli

Konieczne jest opracowanie i wprowadzenie na szczeblu centralnym generalnych zaleceń i wymagań dotyczących zapewnienia bezpieczeństwa IT obowiązujących wszystkie podmioty publiczne. Istnieje potrzeba systemowego rozwiązania ujawniania wyników audytów dotyczących bezpieczeństwa IT, w sposób zapewniający dostęp obywateli do informacji o działalności podmiotów publicznych, z jednoczesnym zachowaniem ograniczeń w dostępie do wiedzy o stosowanych środkach i metodach zapewniających bezpieczeństwo przetwarzanych informacji.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego
Link do sprawozdania:	sprawozdanie (w j. polskim)
Data publikacji:	2019 r.

Tytuł sprawozdania:	Bezpieczeństwo teleinformatyczne RP (informacja niejawna)
Link do sprawozdania:	*dokument nie został udostępniony do publicznej wiadomości*
Data zatwierdzenia:	2019 r.

Tytuł sprawozdania:	Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Link do sprawozdania:	sprawozdanie (w j. polskim)
Data publikacji:	2018 r.

Tytuł sprawozdania:	Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży
Link do sprawozdania:	sprawozdanie (w j. polskim)
Data publikacji:	2017 r.

Tytuł sprawozdania:	Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP
Link do sprawozdania:	sprawozdanie (w j. polskim)
Data publikacji:	2015 r.

Tytuł sprawozdania:	Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu
Link do sprawozdania:	sprawozdanie (w j. polskim)
Data publikacji:	2015 r.

Portugalia
Tribunal de Contas

Kontrola dotycząca portugalskiego paszportu elektronicznego

Data publikacji: 2014 r.

Link do sprawozdania: sprawozdanie (w j. portugalskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: 2013 r.

Streszczenie sprawozdania

Temat kontroli

Kontrola procesów dotycząca portugalskiego paszportu elektronicznego (PEP) była ukierunkowana na kwestię skuteczności systemów informacyjnych wspierających przyznawanie i wydawanie paszportu oraz korzystanie z niego, w szczególności w zakresie zautomatyzowanej kontroli pasażerów przeprowadzanej poprzez odczyt danych biometrycznych na granicach Portugalii[68].

Główne cele kontroli były następujące:

- weryfikacja zgodności z prawem unijnym i krajowym, normami międzynarodowymi i wytycznymi dotyczącymi przyznawania i wydawania PEP oraz korzystania z niego, w tym adekwatności krajowych ram prawnych;

[68] Chodzi o zautomatyzowany system kontroli granicznej w ramach Frontexu (Europejskiej Agencji Straży Granicznej i Przybrzeżnej).

- zbadanie skuteczności kluczowych procesów związanych z cyklem życia PEP, w szczególności związanych z przyznawaniem i wydawaniem PEP oraz korzystaniem z niego;
- zbadanie najistotniejszych aspektów działania systemów informacyjnych, w szczególności spełniania wymogów bezpieczeństwa dotyczących systemów informacyjnych PEP (SIPEP).

Kluczowe obszary ryzyka obejmowały:

- utratę/kradzież środków trwałych lub informacji elektronicznych;
- niewłaściwe wykorzystywanie informacji poufnych;
- ryzyko braku zgodności (niespełnienie wymogów prawnych i regulacyjnych).

Okres objęty kontrolą: 1 stycznia 2013 r. – 31 grudnia 2013 r. (w stosownych przypadkach rozszerzony na lata wcześniejsze i późniejsze).

Ustalenia i wnioski

Wyróżnia się trzy kategorie portugalskiego paszportu elektronicznego (PEP): paszport zwykły[69], dyplomatyczny lub specjalny. Wydawany jest również paszport dla cudzoziemców, przyznający ograniczone przywileje.

System koncesji obejmuje różnorodne wnioski i szereg podmiotów zajmujących się gromadzeniem danych oraz podmiotów przyznających paszporty, ale tylko jeden podmiot wydający paszporty (zajmujący się ich produkcją, personalizacją i dostarczeniem).

[69] Około 99% wszystkich wydawanych paszportów.

W procesie tym bierze udział wiele podmiotów (podmiotów PEP). Następujące podmioty gromadzą dane i przyznają paszporty:

- w kontynentalnej części Portugalii: Serviço de Estrangeiros e Fronteiras (SEF)[70] oraz służby zajmujące się rejestracją w Instituto dos Registos e do Notariado (IRN)[71];
- Regiony Autonomiczne Azorów[72] i Madery: służby działające przy odpowiednim *Vice-Presidência do Governo Regional*[73]; za granicą: konsulaty portugalskie;
- Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] wydaje i dostarcza paszporty.

Główne procesy są w większości obsługiwane przez SIPEP (centralny system obsługi wniosków na potrzeby wydawania paszportów portugalskich). SIPEP umożliwia rejestrowanie, przechowywanie, przetwarzanie, zatwierdzanie i dostarczanie wymaganych informacji związanych z przyznaniem PEP, uruchamia proces personalizacji realizowany przez INCM i zapewnia wzajemne połączenie z innymi wnioskami w systemie, koordynując pracę wszystkich podmiotów PEP uczestniczących w działaniach fizycznych i logistycznych związanych z rejestracją zgromadzonych danych.

Struktura organizacyjna podmiotów PEP umożliwia im realizację celów prawnych związanych z PEP. Na poziomie składania wniosków i gromadzenia danych system nadal w dużym stopniu opiera się na zasobach kadrowych. SIPEP obejmuje jednak szereg automatycznych funkcji przetwarzania i kontroli zatwierdzania.

Ponieważ procedury zapewniają funkcje kontrolne i procesy obsługi danych, z których część może być prowadzona niezależnie, bez interwencji człowieka, SIPEP ma znaczący wpływ na organizację i system informacyjny, w szczególności w zakresie: (i)

---

[70] Służby imigracyjne i graniczne.

[71] Urząd rejestracji i notariat (tylko gromadzenie danych).

[72] A także punkty obsługi w *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – w Agencji Modernizacji i Jakości Usług na rzecz Obywateli, będącej instytutem publicznym (tylko gromadzenie danych).

[73] Wiceprzewodniczący rządu regionalnego.

[74] Oficjalna Drukarnia i Mennica, przedsiębiorstwo publiczne.

zrozumienia i określenia norm, procesów i wymaganych danych; (ii) określenia własnych wymogów systemu informacyjnego.

Efektywność i skuteczność procesu gromadzenia danych jest zapewniona poprzez interakcję SIPEP z innymi systemami informacyjnymi[75] zgodnie z przepisami prawa.

Ustanowiono ramy ogólnej kontroli działań informatycznych (zarządzanie, rozwój i pozyskiwanie, operacje informatyczne, ciągłość działania i przywrócenie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, bezpieczeństwo informacji) i, choć nie są one obszernie udokumentowane, zapewniają rozwój, funkcjonowanie i utrzymanie systemu SIPEP oraz zarządzanie nim.

Wskaźniki dotyczące działalności (2013 r.):

- Przyznano około 500 000 PEP, z czego około 63% zostało przyznanych przez SEF, 33% przez konsulaty portugalskie i 4% przez rządy regionalne.
- Dochód z wydawania PEP wyniósł ogółem około 37 mln euro, głównie z INCM (43%), SEF (32%) oraz z *Ministério dos Negócios Estrangeiros (MNE)*[76] (17%).

W odniesieniu do 2013 r. testy przeprowadzone w SIPEP nie potwierdziły, że dochowywano ustawowo określonego maksymalnego terminu dostarczenia paszportu (od daty złożenia wniosku do daty udostępnienia PEP do odbioru w miejscu jego dostarczenia), ponieważ rzeczywista data dostarczenia paszportu nie zawsze była rejestrowana terminowo.

SEF, MNE, RIAC i INCM podjęły inwestycje związane z nabyciem sprzętu do gromadzenia danych biometrycznych i podpisów (punktów samoobsługi), wyposażenia na potrzeby systemów zautomatyzowanej kontroli granicznej oraz zakupem i utrzymaniem systemów informatycznych, usług i pomocy technicznej na łączną kwotę 11 mln euro, przy czym najwięcej wydały służby SEF.

[75] Należą do nich: Zintegrowany System Informacyjny SEF (SIISEF); krajowy moduł Systemu Informacyjnego Schengen (NSIS); baza danych dotyczących identyfikacji osób cywilnych, baza danych rejestrów karnych.

[76] Ministerstwo Spraw Zagranicznych.

Przed wprowadzeniem PEP cena paszportu Republiki Portugalskiej (bez cech biometrycznych) wynosiła 22,44 euro; w 2006 r. wydanie zwykłego (biometrycznego) PEP kosztowało 60 euro, a w 2011 r. 65 euro.

Wnioski o wydanie PEP

Wnioski o wydanie PEP są przetwarzane osobiście przez właściwe służby, które przyjmują wniosek wraz z towarzyszącymi mu dokumentami, gromadzą dane personalizacyjne i biometryczne wnioskodawców, pobierają opłaty, a następnie dostarczają wydane PEP.

System (SIPEP) sprawdza poprawność i jakość danych poprzez wirtualne kontrole i porównania z innymi systemami informacyjnymi, w szczególności z bazą danych dotyczących identyfikacji osób cywilnych, w celu zapewnienia, aby wniosek był zgodny z wymogami i odpowiedni na potrzeby przyznania i wydania PEP.

Powiązane zmiany statusu są rejestrowane w plikach dziennika, co zapewnia możliwość kontroli, a także gwarantuje integralność i niezaprzeczalność transakcji.

Przekazywanie danych między organami gromadzącymi dane (w Portugalii i za granicą) a SEF odbywa się za pośrednictwem VPN (wirtualnej sieci prywatnej), w oparciu o zarządzanie dostępem zgodnie z danymi uwierzytelniającymi kontrolowane przez SEF[77].

W inny sposób przetwarza się wniosek o wydanie zwykłego PEP, jeżeli jest on składany przez obywateli, których prawa są ograniczone, w tym: (i) osoby, które nie mogą wykonywać swoich praw (małoletni, osoby ubezwłasnowolnione lub osoby pozbawione praw); (ii) osoby objęte zakazem wykonywania przysługujących im praw przez wymiar sprawiedliwości lub policję (wpis do rejestru karnego, toczący się proces sądowy lub zajęcie dokumentów); (iii) gdy wnioskodawca ubiegający się o wydanie drugiego PEP powołuje się na interes krajowy lub prawnie uzasadniony.

[77] SIPEP jest dostępny (przez internet) na poziomie krajowym/regionalnym i międzynarodowym dla służb zlokalizowanych na kontynencie, w Regionach Autonomicznych Azorów i Madery oraz za granicą (w konsulatach portugalskich).

Przyznanie PEP

Decyzja o przyznaniu zwykłego PEP może być wydana:

- automatycznie – poprzez automatyczne zatwierdzenie wniosku przez system składania wniosków SIPEP po weryfikacji tożsamości wnioskodawcy i ustaleniu braku wpisu w rejestrze karnym (w wyniku porównania z prowadzonymi przez IRN bazami danych dotyczącymi identyfikacji osób cywilnych i rejestrami karnymi) oraz braku toczących się postępowań sądowych. Dotyczy tylko SEF w odniesieniu do wniosków o PEP składanych w kontynentalnej części państwa[78];
- po wyrażeniu indywidualnej zgody / zatwierdzeniu wniosku przez inne podmioty (rządy regionalne i urzędy konsularne) lub – w przypadku SEF – na podstawie wymogów nieobjętych automatycznym wydawaniem decyzji[79].

Wydawanie PEP

Wydawanie PEP, obejmujące jego produkcję, personalizację i dostarczenie – należy do kompetencji INCM. Po zarejestrowaniu w SIPEP, że dostarczono PEP, status paszportu zostaje zmieniony na „ważny".

Koszt wydania PEP różni się w zależności od poziomu wymaganej usługi. Aby zmierzyć poziom usług, SIPEP musi uwzględnić rzeczywisty termin dostarczenia PEP.

PEP są dostarczane w ramach zleconej usługi transportowej.

---

[78] Jest to zautomatyzowana funkcja systemu wniosków SIPEP służąca do zatwierdzania (wewnętrznie proces ten nazywany jest „autoryzacją") wniosków (z wyjątkiem drugiego PEP) złożonych przez obywateli pełnoletnich, posiadających ważną kartę obywatela, wobec których nie toczą się postępowania sądowe i którzy nie są objęci zakazem lub pozbawieni prawa do uzyskania PEP. Zwykłe PEP przyznawane przez SEF (około 60% PEP) były objęte automatycznymi procedurami zatwierdzania i wydawania decyzji, natomiast przyznanie pozostałych rodzajów paszportów podlegało kontroli i zatwierdzeniu przez *Direção Central de Imigração e Documentação (DCID)*.

[79] W szczególności w przypadku wnioskodawców, którzy nie mogą wykonywać przysługujących im praw (małoletni, osoby ubezwłasnowolnione lub osoby pozbawione praw), wnioskodawców objętych zakazem wykonywania przysługujących im praw przez wymiar sprawiedliwości lub policję lub – w przypadku drugiego PEP – wnioskodawców, których wnioski są rozpatrywane indywidualnie przez DCID.

Utrata ważności PEP

W przypadku gdy wnioskodawca dostarczy poprzedni, nadal ważny PEP, należy go unieważnić, aby zapobiec jego dalszemu wykorzystywaniu, co odbywa się poprzez zmianę statusu dokumentu paszportowego w systemie SIPEP na „nieważny”.

Finlandia
Valtiontalouden tarkastusvirasto

Rozwiązania w zakresie cyberochrony

Data publikacji: 2017 r.

Link do sprawozdania: sprawozdanie (w j. fińskim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2016–2017

Streszczenie sprawozdania

Temat kontroli

Celem kontroli było zbadanie, czy cyberochrona w instytucjach rządowych na szczeblu centralnym została zorganizowana w możliwie skuteczny i opłacalny sposób. Kontrola koncentrowała się na sposobie organizacji i zarządzania cyberbezpieczeństwem w instytucjach rządowych na szczeblu centralnym. Wyniki kontroli mogły zostać wykorzystane do zwiększenia efektywności i skuteczności cyberbezpieczeństwa w tych instytucjach. Kontrola została przeprowadzona w okresie od 22 września 2016 r. do 4 września 2017 r. Kontrolę następczą przeprowadzono jesienią 2019 r. W jej ramach Urząd Kontroli Państwowej zbadał działania podjęte w związku z ustaleniami i zaleceniami z kontroli.

Wśród skontrolowanych jednostek znalazły się organy odpowiedzialne za cyberochronę w instytucjach rządowych na szczeblu centralnym (Kancelaria Premiera, Ministerstwo Finansów, Ministerstwo Transportu i Łączności) oraz organy odpowiedzialne za scentralizowane zadania w zakresie cyberochrony i scentralizowane usługi informatyczne w instytucjach rządowych na szczeblu centralnym (Krajowe Centrum ds. Cyberbezpieczeństwa Fińskiej Agencji Transportu i Łączności, Rządowe

Centrum ds. ICT Valtori, Agencja Usług ds. Danych Cyfrowych i Demograficznych). Skuteczność wytycznych oceniono również poprzez zbadanie jednostek instytucji rządowych na szczeblu centralnym świadczących e-usługi (Agencja Usług ds. Danych Cyfrowych i Demograficznych, Fińska Agencja Transportu i Łączności Traficom, Krajowy Urząd Administracyjny ds. Egzekwowania Prawa i jego organ nadzorczy Ministerstwo Sprawiedliwości oraz Centrum Usług Teleinformatycznych Ministerstwa Sprawiedliwości).

Pytania kontrolne

Podczas kontroli organizacji cyberbezpieczeństwa postawiono następujące pytania kontrolne:

- Czy jednostka kontrolowana w wystarczającym stopniu uwzględniła aspekt ekonomiczny przy organizowaniu cyberbezpieczeństwa?
- Czy wiedza jednostki kontrolowanej na temat sytuacji w zakresie cyberbezpieczeństwa przyczynia się do zapewnienia cyberbezpieczeństwa systemów?
- Czy zdolność jednostki kontrolowanej do reagowania na cyberincydenty jest wystarczająca?

Temat kontroli dotyczący rozwiązań w zakresie cyberochrony był częścią tematyki kontroli określonej w planie kontroli Urzędu Kontroli Państwowej Finlandii na lata 2016–2020 jako „Zapewnienie niezawodności działania społeczeństwa informacyjnego”. Z punktu widzenia znaczenia dla finansów instytucji rządowych na szczeblu centralnym temat kontroli można uzasadnić utrudnieniami związanymi z przerwami w świadczeniu usług i naruszeniami ochrony danych, a także negatywnym wpływem niedostatecznego poziomu cyberbezpieczeństwa na działalność gospodarczą. Kontrola została przeprowadzona równolegle z kontrolą „Kierowanie niezawodnością działania e-usług”, która należy do tej samej tematyki. Na kluczowe materiały kontrolne składały się dokumenty i wywiady z przedstawicielami organów odpowiedzialnych za daną działalność.

Ustalenia i wnioski

W strategii cyberbezpieczeństwa Finlandii określono główne cele i strategie polityczne służące sprostaniu wyzwaniom stojącym przed cyberprzestrzenią i zapewnieniu jej funkcjonowania. Podjęto działania w celu wdrożenia strategii cyberbezpieczeństwa w ramach programu wdrożeniowego, którego postępy są corocznie oceniane. Komitet ds. Bezpieczeństwa jest organem współpracy w Ministerstwie Obrony, który monitoruje i koordynuje wdrażanie strategii cyberbezpieczeństwa.

Skuteczna organizacja cyberbezpieczeństwa opiera się na zarządzaniu ryzykiem, którego powodzenie wymaga wprowadzenia skutecznych struktur i rozwiązań zarządczych umożliwiających zintegrowanie zarządzania ryzykiem z działaniami na wszystkich szczeblach organizacji. Podobnie jak wiele innych krajów Finlandia i jej instytucje rządowe na szczeblu centralnym nie są samowystarczalne pod względem zasobów w zakresie cyberochrony. Prawodawstwo Unii Europejskiej na przestrzeni czasu uległo rozszerzeniu i coraz więcej przepisów staje się wiążących. W fińskich instytucjach rządowych odpowiedzialność za cyberochronę jest zdecentralizowana, a każda jednostka instytucjonalna odpowiada za własne cyberbezpieczeństwo. W instytucjach rządowych na szczeblu centralnym przydział obowiązków w odniesieniu do charakteru, zakresu i przebiegu ewentualnych cyberincydentów jest złożony.

Ze względu na wspomnianą złożoność reakcja na incydenty może być zbyt powolna, a niedostateczne finansowanie ograniczyło wdrażanie fińskiej strategii cyberbezpieczeństwa. W oparciu o ustalenia kontroli Urząd Kontroli Państwowej sformułował następujące wnioski i zalecenia dotyczące organizacji cyberbezpieczeństwa w instytucjach rządowych na szczeblu centralnym:

Nie określono sposobu zarządzania operacyjnego w przypadku poważnego naruszenia cyberbezpieczeństwa

Planowanie zarządzania operacyjnego w przypadku poważnego naruszenia cyberbezpieczeństwa oraz podział związanych z nim obowiązków mogłyby pozwolić na szybsze reagowanie i odpowiednią koordynację oraz przydział zasobów na środki zapobiegające. W obecnym modelu operacyjnym każda agencja jest odpowiedzialna za własną cyberochronę. Brakuje jednak wystarczającej wiedzy eksperckiej w tym zakresie, co utrudnia tworzenie systemów cyberbezpieczeństwa zarówno wewnętrznie, jak i poprzez zlecenie go podmiotom zewnętrznym.

Niektóre cele strategii cyberbezpieczeństwa nie zostały osiągnięte

Program wdrożeniowy fińskiej strategii cyberbezpieczeństwa przyczynił się do poprawy cyberochrony. Niektóre z celów pierwszego programu wdrożeniowego nie zostały osiągnięte, ponieważ poziom zaangażowania w działania był zróżnicowany i nie można było go podwyższyć w sposób scentralizowany. Nowy program wdrożeniowy obejmował jedynie działania, do których realizacji zobowiązały się właściwe organy i inne podmioty. Istniała wzajemna zależność między poziomem zaangażowania a dostępnymi zasobami.

Stosowność rozwiązań w zakresie finansowania cyberochrony była niejasna

Różnice w stopniu rozwoju systemu cyberochrony wynikały częściowo z różnic w wysokości zasobów przeznaczonych na ten cel, jakimi dysponowały organizacje. W regulacjach dotyczących przygotowania budżetu państwa ani w ramach procesu przygotowawczego nie określono żadnych procedur zapewniających przeznaczenie środków na najważniejsze cele cyberochrony. Agencje i instytucje przewidziały w swoich budżetach środki na cyberbezpieczeństwo jako nieokreśloną część wydatków operacyjnych. Działania określone w strategii cyberbezpieczeństwa Finlandii zostały wdrożone tylko w zakresie, w jakim pozwalały na to przyznane środki.

Cyberochronę należy uwzględniać również przy wprowadzaniu zmian w organizacji ICT

Zmiany w organizacji ICT instytucji rządowych na szczeblu centralnym miały wpływ na rozwiązania w zakresie cyberochrony. Rozwój cyberbezpieczeństwa zarządzany centralnie przez Valtori okazał się trudnym zadaniem. Wystąpiły niedociągnięcia w ocenie adekwatności praktycznych procedur cyberochrony oraz we wdrażaniu nowych rozwiązań.

Należy pogłębić wiedzę na temat bieżących działań w zakresie cyberbezpieczeństwa

Za wiedzę na temat sytuacji w zakresie cyberbezpieczeństwa w skali całego kraju odpowiadało Centrum ds. Cyberbezpieczeństwa. W czasie, gdy przeprowadzano kontrolę, nie było obowiązku zgłaszania przypadków naruszenia cyberbezpieczeństwa do Centrum ds. Cyberbezpieczeństwa. Zobowiązanie organizacji rządowych do zgłaszania takich incydentów poprawiłoby sytuację, podobnie jak zwiększenie zasięgu scentralizowanych procedur wykrywania cyberincydentów.

W oparciu o powyższe stwierdzenia Urząd Kontroli Państwowej zaleca, aby Ministerstwo Finansów określiło i wdrożyło szeroko zakrojony model zarządzania operacyjnego w przypadku wystąpienia cyberincydentów w usługach ICT instytucji rządowych na szczeblu centralnym. Ministerstwo Finansów powinno również przeanalizować, w jaki sposób należy uwzględniać kwestię cyberbezpieczeństwa w ramach finansowania usług na wszystkich etapach ich świadczenia, a także pogłębić wiedzę na temat bieżącej sytuacji przez polecenie organom zgłaszania cyberincydentów do Centrum ds. Cyberbezpieczeństwa. Zalecono, aby Valtori usprawniło wdrażanie, ocenę i rozwój procedur cyberbezpieczeństwa oraz wykrywanie cyberincydentów.

W ramach kontroli następczej zbadano, w jaki sposób zostały wdrożone zalecenia wydane podczas kontroli. Urząd Kontroli Państwowej uznał, że Ministerstwo Finansów, jako właściwy organ do wdrażania zaleceń, nie podjęło wystarczających działań w odpowiedzi na sformułowane zalecenia. Cyberbezpieczeństwo w Finlandii zostało jednak zwiększone również poprzez działania podjęte przez inne organy. Wprowadzano właśnie zmianę w zarządzaniu strategicznym cyberbezpieczeństwem polegającą na przejściu na model dyrektora ds. cyberbezpieczeństwa. W projekcie budżetu na 2020 r. rząd zwiększył pulę środków dla instytucji rządowych na szczeblu centralnym, które odgrywają kluczową rolę we wzmacnianiu cyberbezpieczeństwa. Ponadto Valtori podejmowało działania zgodne z zaleceniem Urzędu Kontroli Państwowej. Podsumowując, Urząd Kontroli Państwowej stwierdził, że ze względu na niewdrożone zalecenia konieczne jest przeprowadzenie kontroli uzupełniającej. Ponadto zupełnie nowa kontrola w tym obszarze jest uzasadniona wprowadzanymi zmianami w rozwiązaniach w zakresie cyberbezpieczeństwa i środowiska cyfrowego oraz związanym z nimi ryzykiem, jak również znaczeniem cyberbezpieczeństwa dla finansów instytucji rządowych na szczeblu centralnym oraz społeczeństwa.

Szwecja
Riksrevisionen

Przestarzałe systemy informatyczne – przeszkoda na drodze do skutecznej transformacji cyfrowej

Data publikacji: 2019 r.

Link do sprawozdania: streszczenie sprawozdania (w j. angielskim)
sprawozdanie (w j. szwedzkim)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: kontrola wykonania zadań

Okres objęty kontrolą: lata 2018–2019

Streszczenie sprawozdania

Temat kontroli

Przestarzałe systemy informatyczne o krytycznym znaczeniu dla działalności wiążą się z dużym ryzykiem wystąpienia problemów z efektywnością, ponieważ organizacje są zmuszone do przeznaczania odpowiednio większych zasobów na utrzymanie systemu. Istnieją zatem podstawy, aby zakładać, że przestarzałe systemy informatyczne niosą za sobą wysokie ryzyko niewłaściwego gospodarowania funduszami publicznymi. Utrzymanie takich systemów pochłania zasoby z uszczerbkiem dla zdolności agencji do innowacyjnego rozwoju nowych systemów informatycznych. Przestarzałe systemy informatyczne stwarzają jednak nie tylko ryzyko dla poszczególnych agencji – problemy w jednej agencji mogą oznaczać poważne konsekwencje dla jej zdolności do koordynowania działań z inną agencją lub zainteresowaną stroną z sektora prywatnego. Systemy te wiążą się również z ryzykiem w zakresie bezpieczeństwa informacji.

Określenie głównego przedmiotu kontroli / Pytania kontrolne / Kontekst

Celem kontroli było zbadanie, czy w administracji rządowej na szczeblu centralnym stosuje się przestarzałe systemy informatyczne oraz czy organy i rząd podjęły odpowiednie działania, aby zapobiec sytuacji, w której systemy te staną na przeszkodzie skutecznej transformacji cyfrowej. Postawiono następujące pytania kontrolne:

- Czy organy podjęły odpowiednie środki w celu rozwiązania problemów związanych z przestarzałymi systemami informatycznymi?
- Czy rząd podjął odpowiednie środki w celu rozwiązania problemów związanych z przestarzałymi systemami informatycznymi?

Ustalenia i wnioski

- Kontrola wykazała, że w wielu agencjach rządowych systemy informatyczne były przestarzałe. Ponadto w wielu agencjach przestarzały był co najmniej jeden system informatyczny o krytycznym znaczeniu dla działalności. Z wiedzy szwedzkiego Urzędu Kontroli Państwowej wynika, że są to nowe informacje i nikt wcześniej nie zdawał sobie sprawy ze skali problemu występującego w administracji rządowej na szczeblu centralnym. Około 80% agencji stwierdziło, że ma trudności z utrzymaniem poziomu bezpieczeństwa informacji w co najmniej jednym systemie o krytycznym znaczeniu dla działalności. Ponad 10% organów udzieliło odpowiedzi, że dotyczy to wszystkich lub większości systemów.
- W dużej części objętych kontrolą agencji nie stosowano właściwego podejścia do rozwoju wsparcia informatycznego i zarządzania nim. Nie wykorzystywały one istniejących narzędzi do rozwoju operacyjnego, aby określić, w jaki sposób wsparcie informatyczne mogłoby najskuteczniej przyczynić się do osiągnięcia celów ich podstawowej działalności. Znaczna część objętych kontrolą agencji nie dysponowała zatem ogólnym opisem tego, w jaki sposób strategie, procesy operacyjne i systemy były ze sobą powiązane. To z kolei oznaczało, że miały one trudności z analizą i zrozumieniem tego, jak zmiany wpływają na cele organizacji, dlatego trudniej było im określić pożądaną sytuację w przyszłości.
- Ponad połowa organów stwierdziła, że nie ma zatwierdzonego modelu postępowania z systemami informatycznymi i podejmowania decyzji dotyczących tych systemów począwszy od etapu rozwoju systemu do jego stopniowego

wycofywania, co zwykle określa się mianem zarządzania cyklem życia. Zdaniem szwedzkiego Urzędu Kontroli Państwowej oznacza to, że zarządzanie cyklem życia nie zostało przeprowadzone w sposób ustrukturyzowany i metodyczny. Wykryto również niedociągnięcia w pracach związanych z analizą ryzyka oraz w zakresie zdolności do szczegółowego podziału kosztów informatycznych niezbędnego do podejmowania właściwych decyzji.

- Prawie 60% organów nie opracowało planów dotyczących cyklu rozwoju systemu z wyjątkiem planu dla jednego lub kilku systemów o krytycznym znaczeniu dla działalności. Wobec braku planów dotyczących cyklu życia systemów i innej dokumentacji planistycznej w wielu agencjach oraz niedociągnięć w faktycznie przeprowadzanym zarządzaniu cyklem życia zasadniczo nie można było uznać, że agencje wypracowały świadome, jednoznaczne stanowisko w sprawie swoich systemów informatycznych.

- W opinii szwedzkiego Urzędu Kontroli Państwowej odnośne ministerstwa, a tym samym również rząd, nie posiadały wystarczającej wiedzy ani na temat przypadków stosowania przestarzałych systemów informatycznych, ani związanych z tym skutków.

Wyciągnięto ogólny wniosek, że do czasu przeprowadzenia kontroli większość agencji nie rozwiązała skutecznie problemów związanych z przestarzałymi systemami informatycznymi. Szwedzki Urząd Kontroli Państwowej uznał, że problem jest na tyle poważny i powszechny, iż stanowi przeszkodę na drodze do dalszej efektywnej transformacji cyfrowej administracji państwa. Kontrola wykazała również, że rząd nie miał wiedzy na temat występowania problemów związanych z przestarzałymi systemami informatycznymi i skutków tych problemów. Ponadto nie wprowadził on żadnych środków w celu bardziej bezpośredniego rozwiązania problemu przestarzałych systemów informatycznych. W związku z tym w ocenie szwedzkiego Urzędu Kontroli Państwowej nie można było uznać, że rząd podjął wystarczające środki, aby zapewnić ograniczenie lub wyeliminowanie istniejących problemów.

Inne sprawozdania w tym obszarze

Tytuł sprawozdania:	Ułatwienie rozpoczęcia działalności gospodarczej – działania rządu na rzecz promowania procesu transformacji cyfrowej (RiR 2019:14)
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. szwedzkim)
Data publikacji:	2019 r.
Tytuł sprawozdania:	Transformacja cyfrowa administracji publicznej – prostsza, bardziej przejrzysta i skuteczna administracja (RiR 2016:14)
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. szwedzkim)
Data publikacji:	2016 r.
Tytuł sprawozdania:	Działania w zakresie bezpieczeństwa informacji w dziewięciu agencjach (RiR 2016:8)
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. szwedzkim)
Data publikacji:	2016 r.
Tytuł sprawozdania:	Cyberprzestępczość – działania policji i prokuratury mogą być skuteczniejsze (RiR 2015:21)
Link do sprawozdania:	streszczenie sprawozdania (w j. angielskim) sprawozdanie (w j. szwedzkim)
Data publikacji:	2015 r.

Unia Europejska
Europejski Trybunał Obrachunkowy

Dokument analityczny pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją”

Data publikacji: 2018 r.

Link do sprawozdania: sprawozdanie (w 23 językach)

Rodzaj kontroli i okres objęty kontrolą

Rodzaj kontroli: przegląd polityki

Okres objęty kontrolą: kwiecień – wrzesień 2018 r.

Streszczenie sprawozdania

Temat przeglądu

Cel tego dokumentu analitycznego – niebędącego sprawozdaniem z kontroli – polegał na przedstawieniu w zarysie złożonych warunków, w jakich prowadzona jest unijna polityka cyberbezpieczeństwa, oraz wskazaniu zasadniczych wyzwań związanych ze skutecznym realizowaniem tej polityki. W dokumencie poruszono kwestie bezpieczeństwa sieci i informacji, cyberprzestępczości, cyberobrony i dezinformacji.

Trybunał przeanalizował wybrane ogólnodostępne oficjalne dokumenty, stanowiska i opracowania zewnętrzne. Prace przeprowadzono w okresie od kwietnia do września 2018 r., przy czym w dokumencie uwzględniono rozwój sytuacji aż do grudnia 2018 r. Uzupełniono je ankietą rozesłaną do krajowych organów kontroli państw członkowskich oraz wywiadami z przedstawicielami kluczowych zainteresowanych stron z unijnych instytucji oraz sektora prywatnego.

Nie ma standardowej definicji cyberbezpieczeństwa. Ogólnie rzecz biorąc, są to wszystkie zabezpieczenia i środki przyjęte w celu ochrony systemów informacyjnych i ich użytkowników przed nieuprawnionym dostępem, atakiem lub szkodą, tak aby zapewnić poufność, integralność i dostępność informacji. Na cyberbezpieczeństwo

składa się zapobieganie cyberincydentom, ich wykrywanie, reagowanie na nie oraz przywracanie działalności po takich incydentach. Incydenty mogą być wywoływane umyślnie lub nieumyślne i obejmują np. niezamierzone ujawnienie informacji, ataki na przedsiębiorstwa i infrastrukturę krytyczną, kradzieże danych osobowych, a nawet zakłócanie przebiegu procesów demokratycznych.

Podstawą unijnej polityki w tej dziedzinie jest strategia w zakresie cyberbezpieczeństwa z 2013 r. Ambicją strategii jest uczynienie środowiska cyfrowego w UE najbezpieczniejszym na świecie, a jednocześnie zapewnienie ochrony podstawowych wartości i wolności. Przyświeca jej pięć podstawowych celów: (i) zwiększenie cyberodporności; (ii) ograniczenie cyberprzestępczości; (iii) opracowanie polityki i zdolności w dziedzinie cyberobrony; (iv) rozbudowa zasobów przemysłowych i technologicznych w zakresie cyberbezpieczeństwa; (v) ustanowienie międzynarodowej polityki w zakresie cyberprzestrzeni zgodnej z podstawowymi wartościami UE.

Ustalenia

Trudno było zmierzyć wpływ niedostatecznego przygotowania na cyberataki ze względu na brak wiarygodnych danych. Gospodarcze skutki cyberprzestępczości zwiększyły się pięciokrotnie w latach 2013–2017. Dotknęła ona zarówno rządy, jak i przedsiębiorstwa – i te małe, i duże. Znajduje to odbicie w przewidywanym wzroście składek na ubezpieczenia w dziedzinie cyberbezpieczeństwa, z 3 mld euro w 2018 r. do 8,9 mld euro w 2020 r. Choć 80% europejskich przedsiębiorstw spotkało się z co najmniej jednym incydentem w dziedzinie cyberbezpieczeństwa w 2016 r., świadomość istnienia zagrożeń jest wciąż niepokojąco niska. Wśród przedsiębiorstw w UE 69% nie posiada żadnej wiedzy na temat własnego narażenia na zagrożenia dla cyberbezpieczeństwa lub posiada taką wiedzę jedynie w podstawowym zakresie, a 60% nigdy nie szacowało potencjalnych strat finansowych. Jak wynika z globalnego badania ankietowego, jedna trzecia podmiotów zapłaciłaby raczej hakerom okup niż inwestowała w bezpieczeństwo informacji.

Ustalenia Trybunału były następujące:

- Unijne cyberśrodowisko jest złożone i wielowarstwowe. Uczestniczy w nim wiele zainteresowanych stron. Koordynowanie wszystkich tych rozbieżnych elementów stanowi spore wyzwanie.

- UE dąży do tego, by stać się najbezpieczniejszym środowiskiem cyfrowym na świecie. Do osiągnięcia tego celu konieczne są znaczne wysiłki wszystkich zainteresowanych stron, a ponadto solidne podstawy finansowe i należyte zarządzanie finansami. Trudno uzyskać rzetelne dane liczbowe, ale szacuje się, że ze środków publicznych na cyberbezpieczeństwo w UE każdego roku wydaje się od 1 do 2 mld euro. Dla porównania przewidziane w budżecie amerykańskiego rządu federalnego na 2019 r. wydatki na ten cel wynoszą ok. 21 mld dolarów.

- Zarządzanie w zakresie bezpieczeństwa informacji polega na wprowadzaniu struktur i strategii mających na celu zapewnienie poufności, integralności i dostępności danych. Wykracza ono poza kwestie czysto techniczne i wymaga zapewnienia skutecznego przywództwa, solidnych procesów i strategii dostosowanych do celów organizacyjnych.

- Modele zarządzania w zakresie cyberbezpieczeństwa są różne w poszczególnych państwach członkowskich, przy czym często w obrębie jednego państwa odpowiedzialność za cyberbezpieczeństwo spoczywa na wielu podmiotach. Różnice te mogą utrudniać współpracę konieczną, by reagować na transgraniczne incydenty o dużej skali oraz wymieniać informacje wywiadowcze na temat zagrożeń na szczeblu krajowym, nie wspominając o szczeblu unijnym.

- Opracowanie skutecznej reakcji na cyberataki ma zasadnicze znaczenie dla możliwie jak najwcześniejszego powstrzymania takich działań. Jest szczególnie istotne, by sektory o krytycznym znaczeniu, państwa członkowskie i instytucje UE były w stanie reagować w sposób szybki i skoordynowany. W tym kontekście bardzo ważne jest wczesne wykrywanie.

Zalecenia

Przeprowadzony przez Trybunał przegląd wskazuje, że do zapewnienia rzetelnej rozliczalności i oceny konieczne jest przejście na kulturę organizacyjną ukierunkowaną na wyniki i powiązaną z ugruntowanymi praktykami oceny. Wciąż utrzymują się pewne luki w prawie, a obowiązujące przepisy nie są transponowane w sposób spójny przez państwa członkowskie. Utrudnia to wykorzystanie pełnego potencjału tkwiącego w prawodawstwie.

Inne rozpoznane wyzwanie dotyczy dostosowania poziomów inwestycji do celów strategicznych, co wymaga podniesienia poziomów inwestycji i zwiększenia ich

oddziaływania. Zadanie to jest jeszcze trudniejsze w sytuacji, gdy UE i państwa członkowskie nie posiadają jasnego obrazu wydatków unijnych w dziedzinie cyberbezpieczeństwa. Odnotowano również niedostatki odpowiednich zasobów w unijnych agencjach zajmujących się cyberprzestrzenią, w tym trudności w przyciąganiu i zatrzymywaniu utalentowanych pracowników.

Wykaz akronimów i skrótów

APT – zaawansowane, trwałe zagrożenie

CEF – instrument „Łącząc Europę”

CERT-UE – zespół reagowania na incydenty komputerowe

COBIT – cele kontroli w zakresie technologii informacyjnej i technologii pokrewnych

COVID-19 – choroba koronawirusowa z 2019 r.

cPPP – umowne partnerstwo publiczno-prywatne

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego

DDoS – rozproszony atak typu „odmowa usługi”

Dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) – dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

EC3 – Europejskie Centrum ds. Walki z Cyberprzestępczością działające przy Europolu

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

ERRS – Europejska Rada ds. Ryzyka Systemowego

ESDZ – Europejska Służba Działań Zewnętrznych

Europol – Agencja Unii Europejskiej ds. Współpracy Organów Ścigania

Fundusze ESI – europejskie fundusze strukturalne i inwestycyjne

ICT – technologie informacyjno-komunikacyjne

ISACA – stowarzyszenie Information Systems Audit and Control Association

IT – technologia informacyjna

MERS – bliskowschodni zespół niewydolności oddechowej

NATO – Organizacja Traktatu Północnoatlantyckiego

NOK – najwyższe organy kontroli

PESCO – stała współpraca strukturalna

PKB – produkt krajowy brutto

RDP – protokół *Remote Desktop Protocol*

RODO – ogólne rozporządzenie o ochronie danych

SARS – zespół ostrej niewydolności oddechowej

Trybunał – Europejski Trybunał Obrachunkowy

UE – Unia Europejska

URL – ujednolicony format adresowania zasobów

USA – Stany Zjednoczone Ameryki

WPBiO – wspólna polityka bezpieczeństwa i obrony

WRF – wieloletnie ramy finansowe

Glosariusz

5G – standard technologiczny piątej generacji dla komórkowych sieci szerokopasmowych, który przedsiębiorstwa z branży telefonii komórkowej zaczęły wdrażać na całym świecie w 2019 r. Jest on planowanym następcą sieci 4G zapewniających łączność większości obecnych telefonów komórkowych. Zwiększoną prędkość osiąga się częściowo dzięki wykorzystaniu fal radiowych o wyższej częstotliwości niż w poprzednich sieciach komórkowych.

Ataki sieciowe – zarejestrowani użytkownicy są przekonani, że wrażliwe dane osobowe, które ujawniają na stronie internetowej, będą przechowywane w sposób poufny i bezpieczny. Wtargnięcie (atak) może oznaczać, że podane przez nich dane karty kredytowej, informacje dotyczące zabezpieczenia społecznego lub informacje medyczne mogą stać się jawne, co może wywołać poważne konsekwencje.

Bezpieczeństwo informacji – zestaw procesów i narzędzi chroniących dane fizyczne i cyfrowe przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, naruszeniem, modyfikacją, rejestracją lub zniszczeniem.

Bezpieczeństwo sieci – poddziedzina cyberbezpieczeństwa dotycząca ochrony danych przesyłanych za pomocą urządzeń w ramach tej samej sieci w celu zagwarantowania, że informacja nie zostanie przechwycona ani zmodyfikowana.

Bitcoin – waluta cyfrowa lub wirtualna stworzona w 2009 r., która wykorzystuje technologię typu P2P w celu ułatwienia płatności natychmiastowych.

Cyberatak – próba naruszenia lub zniszczenia poufności, integralności lub dostępności danych lub systemów komputerowych z wykorzystaniem cyberprzestrzeni.

Cyberbezpieczeństwo (cyberochrona) – wszystkie zabezpieczenia i środki przyjęte w celu ochrony systemów informacyjnych i powiązanych danych przed nieuprawnionym dostępem, atakiem lub szkodą, tak aby zapewnić poufność, integralność i dostępność informacji.

Cyberdyplomacja – wykorzystanie zasobów dyplomatycznych i pełnienie funkcji dyplomatycznych w celu zabezpieczenia interesów narodowych w odniesieniu do cyberprzestrzeni. Prowadzona jest w całości lub częściowo przez dyplomatów, w ramach spotkań dwustronnych (takich jak dialog Stany Zjednoczone–Chiny) lub na forach wielostronnych (takich jak ONZ). Oprócz pełnienia tradycyjnych funkcji dyplomatycznych dyplomaci współpracują również z różnymi podmiotami niepaństwowymi, takimi jak liderzy przedsiębiorstw internetowych (np. Facebook lub Google), przedsiębiorstwa technologiczne lub organizacje społeczeństwa

obywatelskiego. Dyplomacja może również wiązać się ze wzmacnianiem pozycji osób uciśnionych w innych krajach za pośrednictwem technologii.

Cyberincydent – wydarzenie, które w sposób pośredni lub bezpośredni szkodzi lub zagraża odporności lub bezpieczeństwu danego systemu informatycznego i danym przetwarzanym, przechowywanym lub przesyłanym przez ten system.

Cyberobrona – poddziedzina cyberbezpieczeństwa, która ma na celu obronę cyberprzestrzeni środkami wojskowymi i za pomocą innych odpowiednich działań, aby osiągnąć cele strategiczno-wojskowe.

Cyberodporność – zdolność do zapobiegania cyberatakom i incydentom, przygotowania się do nich, przetrwania ich, a także do przywrócenia działalności po cyberatakach i incydentach.

Cyberprzestępczość – różne rodzaje działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Obejmuje ona: tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług, złośliwe oprogramowanie lub oprogramowanie typu ransomware).

Cyberprzestrzeń – niematerialne globalne środowisko, w którym za pośrednictwem sieci komputerowych i urządzeń technicznych odbywa się sieciowa komunikacja między ludźmi, oprogramowaniem i usługami.

Cyberszpiegostwo – działanie lub praktyka polegające na pozyskiwaniu tajemnic i informacji bez zgody lub wiedzy posiadacza informacji od osób fizycznych, konkurentów, rywali, grup, rządów i wrogów w celu osiągnięcia korzyści osobistych, ekonomicznych, politycznych lub wojskowych przy użyciu internetu, sieci lub pojedynczych komputerów.

Cyberśrodowisko – złożony zbiór współdziałających urządzeń, danych, sieci, osób, procesów i podmiotów oraz środowisko złożone z procesów i technologii wpływających na to współdziałanie i je wspierających.

Cyberzagrożenie – czyn dokonany w złym zamiarze, który ma na celu uszkodzenie danych, kradzież danych lub ogólne zakłócenie funkcjonowania świata cyfrowego.

Cyfryzacja – proces przekształcania informacji na format cyfrowy, w którym informacje są zapisane w formie bitów. Wynikiem tego procesu jest stworzenie reprezentacji obiektu, obrazu, dźwięku, dokumentu lub sygnału przez wygenerowanie serii liczb opisujących zbiór dyskretny punktów lub prób.

Dane biometryczne (biometria) – przedstawione w formie liczbowej cechy fizyczne (takich jak odciski palców i cechy tęczówki oka) lub behawioralne człowieka. W informatyce jako formę identyfikacji i kontroli dostępu stosuje się uwierzytelnianie.

Dane na temat dostępu – informacje na temat czynności logowania się i wylogowania się użytkownika w związku z dostępem do usługi, takie jak data, godzina i adres IP.

Dane osobowe – informacje dotyczące możliwej do zidentyfikowania osoby fizycznej.

Dezinformacja – możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną.

Dostawca usług cyfrowych – każdy, kto świadczy co najmniej jeden z następujących trzech rodzajów usług cyfrowych: internetowa platforma handlowa, wyszukiwarka internetowa, usługi w chmurze.

Dostępność – zapewnienie terminowego i wiarygodnego dostępu do informacji i korzystania z informacji.

Etyczny haker – osoba (ekspert ds. bezpieczeństwa komputerowego), która przenika do sieci komputerowej w celu przetestowania lub oceny jej bezpieczeństwa, a nie w złym celu lub z zamiarem popełnienia czynu zabronionego.

Haker – osoba, która wykorzystuje umiejętności komputerowe, umiejętności tworzenia sieci kontaktów lub inne umiejętności w celu uzyskania nieuprawnionego dostępu do danych, systemu komputerowego lub sieci.

Infrastruktura krytyczna – obiekty, usługi i zasoby fizyczne, w przypadku których zaburzenie funkcjonowania lub zniszczenia poważnie wpłynęłoby na funkcjonowanie gospodarki i społeczeństwa.

Infrastruktura wyborcza – obejmuje systemy informatyczne i bazy danych na potrzeby kampanii wyborczych, szczególnie chronione informacje na temat kandydatów, systemy rejestracji wyborców i systemy zarządcze.

Instalacje użyteczności publicznej – wszelkie słupy, wieże, przewody napowietrzne lub podziemne, wszelkie inne konstrukcje nośne lub podtrzymujące oraz wszelkie wykopy wraz z osprzętem, które mogą być wykorzystywane do dostarczania lub dystrybucji usług elektrycznych, telefonicznych, telegraficznych, prowadzenia kabli, usług sygnalizacyjnych lub wszelkich innych podobnych usług.

Integralność – ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji oraz zagwarantowanie jej autentyczności.

Internet rzeczy – sieć przedmiotów codziennego użytku wyposażonych w układy elektroniczne, oprogramowanie i czujniki, tak że mogą one łączyć się i wymieniać dane za pośrednictwem internetu.

Kryptowaluta – zasób cyfrowy, który jest wytwarzany i wymieniany z wykorzystaniem technik szyfrowania, niezależnie od banku centralnego. Kryptowaluty są akceptowalnym środkiem płatniczym wśród członków społeczności internetowych.

Krytyczny system informacyjny – każdy system informacyjny, istniejący lub przewidywany, który uznaje się za niezbędny do zapewnienia sprawnego i skutecznego funkcjonowania organizacji.

Łatka na oprogramowanie – zestaw zmian w oprogramowaniu mający na celu aktualizację, naprawę lub usprawnienie działania, w tym usunięcie luk w zakresie bezpieczeństwa.

Manipulacje z zakresu inżynierii społecznej – w dziedzinie bezpieczeństwa informacji oznaczają one psychologiczną manipulację mającą sprawić, że użytkownicy wykonają określoną czynność lub ujawnią poufne informacje.

Naruszenie ochrony danych – zamierzone lub niezamierzone ujawnienie zabezpieczonych bądź prywatnych lub poufnych informacji w środowisku niezaufanym.

Obliczenia wielkiej skali – zdolność do przetwarzania danych i wykonywania skomplikowanych obliczeń z dużą prędkością.

Operator usług kluczowych – podmiot publiczny lub prywatny świadczący usługę, która ma kluczowe znaczenie dla utrzymania istotnej działalności społecznej lub gospodarczej.

Oprogramowanie reklamowe – złośliwe oprogramowanie wyświetlające banery reklamowe lub wyskakujące okienka, w których zamieszcza się kod śledzący zachowania zainfekowanych użytkowników w internecie.

Oprogramowanie szpiegujące – złośliwe oprogramowanie, które ma na celu gromadzenie informacji o osobie lub organizacji i przesyłanie takich informacji do innego podmiotu w sposób, który szkodzi użytkownikowi, na przykład naruszając prywatność lub zagrażając bezpieczeństwu urządzenia stosowanego przez użytkownika.

Oprogramowanie typu ransomware – złośliwe oprogramowanie, które uniemożliwia ofierze dostęp do systemu komputerowego lub sprawia, że nie można odczytać plików, zazwyczaj za sprawą szyfrowania. Atakujący szantażuje następnie ofiarę, uzależniając przywrócenie dostępu do systemu od opłacenia przez ofiarę okupu.

Phishing – praktyka polegająca na wysyłaniu pocztą elektroniczną wiadomości, które sprawiają wrażenie wiadomości pochodzących z wiarygodnego źródła, tak aby skłonić odbiorców do kliknięcia w łącza, za którymi kryje się złośliwe oprogramowanie, lub do udostępnienia danych osobowych.

Platforma cyfrowa – środowisko umożliwiające interakcję między co najmniej dwiema różnymi grupami, z których jedną są zazwyczaj dostawcy, a drugą – konsumenci lub użytkownicy. Platforma może oznaczać sprzęt lub system operacyjny, a nawet przeglądarkę internetową i powiązane z nią interfejsy aplikacji lub inne oprogramowanie bazowe, o ile za jego pomocą wykonywany jest kod programu.

Poufność – ochrona informacji, danych i zasobów przed nieuprawnionym dostępem lub ujawnieniem.

Protokół RDP (ang. *Remote Desktop Protocol*) – norma techniczna (wydana przez Microsoft) dotycząca zdalnego korzystania z komputera stacjonarnego. Użytkownicy pulpitu zdalnego mogą uzyskać dostęp do własnego pulpitu, otwierać i edytować pliki oraz korzystać z aplikacji tak, jakby rzeczywiście siedzieli przy swoim komputerze stacjonarnym.

Przetwarzanie danych – wykonywanie operacji na danych – szczególnie z wykorzystaniem komputera – w celu wyszukania, przekształcenia lub sklasyfikowania informacji.

Przetwarzanie w chmurze – zapewnienie zasobów informatycznych i zasobów na żądanie – takich jak zdolność przechowywania, moce obliczeniowe lub zdolności do wymiany danych – za pośrednictwem sieci dzięki usługom hostingowym na zdalnych serwerach.

Robaki – robak komputerowy jest samodzielnym złośliwym programem komputerowym, który powiela się, aby rozprzestrzenić się na inne komputery. W tym

celu często wykorzystuje sieć komputerową, korzystając z luk w zakresie bezpieczeństwa na komputerze docelowym, aby uzyskać do niego dostęp.

Rozproszony atak typu „odmowa usługi" (atak typu DDoS) – cyberatak uniemożliwiający właściwym użytkownikom dostęp do sieciowej usługi lub zasobu przez zalanie systemu ogromną ilością zapytań, których nie sposób obsłużyć.

Sabotaż – działanie mające na celu zamierzone zniszczenie, uszkodzenie lub utrudnienie, szczególnie z myślą o osiągnięciu korzyści politycznych lub wojskowych.

Sztuczna inteligencja – symulacja ludzkiej inteligencji za pomocą maszyn, które są zaprogramowane tak, aby myśleć jak ludzie i naśladować ich działania. Pojęcie to obejmuje każdą maszynę, która wykazuje cechy przypisywane ludzkiemu umysłowi, takie jak uczenie się i rozwiązywanie problemów.

Szyfrowanie – przekształcenie informacji gotowych do odczytu w niemożliwy do odczytania kod w celu ochrony danych. Aby odczytać informacje, użytkownik musi mieć dostęp do tajnego kodu lub hasła.

Treści cyfrowe – wszelkie dane – takie jak tekst, dźwięk, obraz lub wideo – przechowywane w formacie cyfrowym.

Trojan – rodzaj złośliwego kodu lub oprogramowania, które wydają się wiarygodne, ale mogą przejąć kontrolę nad komputerem użytkownika. Trojan jest zaprojektowany z myślą o uszkadzaniu, zakłócaniu, kradzieży danych lub sieci lub ogólnie wyrządzaniu innych szkód w odniesieniu do danych lub w sieci.

Wektoryzacja tekstu – proces zamierzający do przekształcenia słów, zdań lub całych dokumentów w wektory cyfrowe, tak aby nadawały się one do wykorzystania w uczeniu się maszyn.

Zaawansowane, trwałe zagrożenia – atak, podczas którego nieuprawniony użytkownik uzyskuje dostęp do systemu lub sieci i przez dłuższy czas pozostaje w tym systemie lub w tej sieci niewykryty. Takie ataki są szczególnie niebezpieczne dla przedsiębiorstw, ponieważ hakerzy mają stały dostęp do danych wrażliwych przedsiębiorstw. Z reguły nie powodują one jednak uszkodzeń sieci firmowej ani lokalnych urządzeń. Celem tych ataków jest kradzież danych.

Zagrożenie hybrydowe – wrogie działania, w których przeciwnik wykorzystuje połączenie tradycyjnych i nietradycyjnych technik prowadzenia wojny (tj. metod wojskowych, politycznych, gospodarczych i technologicznych) do osiągnięcia siłowo własnych celów.

Zasoby cyfrowe – wszystkie elementy w formacie cyfrowym w posiadaniu osoby fizycznej lub przedsiębiorstwa, które są związane z prawem do wykorzystania (np. obrazy, zdjęcia, materiały wideo, pliki zawierające tekst itp.).

Złośliwe oprogramowanie – program komputerowy, który ma na celu uszkodzenie komputera, serwera lub sieci.

Jak skontaktować się z UE

Osobiście
W całej Unii Europejskiej istnieje kilkaset centrów informacyjnych Europe Direct. Adres najbliższego centrum można znaleźć na stronie: https://europa.eu/european-union/contact_pl.

Telefonicznie lub drogą mailową
Europe Direct to serwis informacyjny, który udziela odpowiedzi na pytania na temat Unii Europejskiej. Można się z nim skontaktować:
— dzwoniąc pod bezpłatny numer telefonu: 00 800 6 7 8 9 10 11 (niektórzy operatorzy mogą naliczać opłaty za te połączenia),
— dzwoniąc pod standardowy numer telefonu: +32 22999696,
— drogą mailową: https://europa.eu/european-union/contact_pl.

Wyszukiwanie informacji o UE

Online
Informacje o Unii Europejskiej są dostępne we wszystkich językach urzędowych UE w portalu Europa: https://europa.eu/european-union/index_pl.

Publikacje UE
Bezpłatne i odpłatne publikacje UE można pobrać lub zamówić na stronie: https://publications.europa.eu/pl/publications. Większą liczbę egzemplarzy bezpłatnych publikacji można otrzymać, kontaktując się z serwisem Europe Direct lub z lokalnym centrum informacyjnym (zob. https://europa.eu/european-union/contact_pl).

Prawo UE i powiązane dokumenty
Informacje prawne dotyczące UE, w tym wszystkie unijne akty prawne od 1952 r., są dostępne we wszystkich językach urzędowych UE w portalu EUR-Lex: https://eur-lex.europa.eu.

Portal Otwartych Danych UE
Unijny portal otwartych danych (http://data.europa.eu/euodp/pl) umożliwia dostęp do zbiorów danych pochodzących z instytucji i innych organów UE. Dane można pobierać i wykorzystywać bezpłatnie, zarówno do celów komercyjnych, jak i niekomercyjnych.

Contact Committee

Komitet Kontaktowy

Najwyższych Organów Kontroli Państw Unii Europejskiej