STUDIA POLITOLOGICZNE VOL. 77
DOI: 10.33896/SPolit.2025.77.11

*Marcin Waszak**

Wymagania bezpieczeństwa w aplikacjach webowych dla sygnalistów

Security Requirements in Web Applications for Whistleblowers

Słowa kluczowe: *sygnalizowanie naruszeń, aplikacje webowe, standardy cyberbezpieczeństwa, platforma do zgłaszania, dyrektywa 2019/1937*

Key words: *whistleblowing, web applications, cybersecurity standards, reporting platform, directive 2019/1937*

Abstrakt: *Artykuł omawia wyzwania cyberbezpieczeństwa związane z wykorzystaniem narzędzi cyfrowych do wykrywania naruszeń w ramach procedur whistleblowing-u. Implementacja w Polsce dyrektywy o ochronie sygnalistów może doprowadzić do pojawienia się dedykowanych aplikacji webowych w masowej skali, tak w sektorze publicznym jak i prywatnym. Podmioty, które posłużą się nimi jak kanałem do przyjmowania zgłoszeń muszą brać pod uwagę ryzyka dla poufności, integralności i dostępności przetwarzanych w aplikacjach danych wrażliwych. Z punktu widzenia efektywnej obsługi zgłoszeń przez zobowiązane podmioty i organy publiczne pojawia się potrzeba wypracowania standardu minimum w zakresie wymagań bezpieczeństwa dla platform internetowych i ich weryfikacji, który będzie stosowany wobec dostawców.*

Abstract: *The article discusses the cybersecurity challenges of using digital tools to detect breaches under whistleblowing procedures. The implementation of the Whistleblower Protection Directive in Poland may lead to the emergence of dedicated web applications on a massive scale, both in the public and private sectors. Entities that will use them as*

* ORCID ID: https://orcid.org/0000-0002-9388-2051; doktorant na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. E-mail: marcin.waszak@uw.edu.pl.

a channel for receiving reports must take into account risks to the confidentiality, integrity and availability of sensitive data processed in the applications. From the point of view of effective handling of tips by obliged entities and public authorities, there is a need to develop a minimum standard for security requirements for online platforms and their verification to be applied to providers.

Wprowadzenie

Artykuł analizuje prawne i techniczne aspekty ochrony sygnalistów (ang. *whistleblowers*) w kontekście internetowych platform do zgłaszania naruszeń. Osoby dokonujące zgłoszeń w interesie publicznym mogą korzystać w tym celu m.in. z dostępu do aplikacji, które daje im pracodawca, formularzy udostępnianych przez organy publiczne oraz anonimowych platform służących do przekazywania informacji mediom. Podobne oprogramowanie należy zaliczyć do kategorii wymagających szczególnych gwarancji bezpieczeństwa. Przetwarzane z jego wykorzystaniem dane mogą być dowodami w postępowaniach dotyczących przestępstw, nadużyć władzy publicznej, zagrożeń dla bezpieczeństwa i zdrowia obywateli.

Celem artykułu jest omówienie standardów bezpieczeństwa dla aplikacji do *whistleblowing*-u, ich źródeł i znaczenia. Zagadnienie zaczęło budzić większe zainteresowanie polskich organizacji w 2024 r., kiedy Polska transponowała Dyrektywę 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dalej: Dyrektywa). Wcześniej aplikacje odpowiadające na wymagania prawa europejskiego zaczęły zyskiwać na popularności głównie w podmiotach prywatnych działających na innych rynkach[1]. Pierwszy impuls prawny dla wykorzystania anonimowych kanałów zgłaszania ryzyk naruszeń dotyczył sektora finansowego i było nim przyjęcie dyrektywy UE 2015/849 o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[2].

W reżimie regulacji o sygnalistach zobowiązującym do prowadzenia wewnętrznych i zewnętrznych ścieżek zgłaszania liczba podmiotów prywatnych i publicznych korzystających z aplikacji do sygnalizowania może w Polsce radykalnie wzrosnąć. Tym samym zostaną one postawione przed wyborem, czy skorzystać z oferty podmiotów komercyjnych, zaadaptować na swoje potrzeby

[1] M. Jenkins, *Overview of whistleblowing software*, Transparency International, 2020, s. 4–5, https://knowledgehub.transparency.org/helpdesk/overview-of-whistleblowing-software (4.11.2024).

[2] N. Colvin, V. Nad, C. Culnane, B. Galizzi, S. Dreyfus, *Expanding anonymous tipping technology in Europe*, Blueprint for Free Speech 2021, s. 22, https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/60fee180f7b25d77581c6f98/1627316617173/Expanding+Anonymous+Tipping+in+Europe_EAT.pdf (4.03.2025).

rozwiązania *open source* czy też zbudować w oparciu o własne zasoby autorskie aplikacje[3].

Ustawa o ochronie sygnalistów w 14 czerwca 2024 r. (dalej: Ustawa) nałożyła na podmioty publiczne i prywatne, na rzecz których pracuje co najmniej 50 osób, obowiązek wdrożenia wewnętrznych kanałów zgłaszania naruszeń[4]. Ustawa stanowi spóźnioną implementację Dyrektywy, której termin na wdrożenie minął 17 grudnia 2021 r.[5] Ochrona sygnalistów w Unii Europejskiej ma przyczynić się do poprawy skuteczności walki z korupcją i innymi naruszeniami prawa, pozwalając tym samym lepiej egzekwować prawo i polityki unijne.

Regulacja *whistleblowing*-u w Unii Europejskiej

Unijny model ochrony sygnalistów korzysta z koncepcji trzech poziomów zgłaszania (ang. *three-tiered model*), który wskazuje prawnie dozwolone ścieżki sygnalizowania. Pierwszą jest możliwość zgłoszenia wewnętrznego, do podmiotu, z którym sygnalista pozostaje w relacji zawodowej. Druga to kanał zewnętrzny, prowadzący do właściwego organu publicznego, który zgodnie z przepisami pozostaje kompetentny i uprawniony do zbadania zgłoszenia. W Polsce za dystrybucję zgłoszeń zewnętrznych ma odpowiadać Rzecznik Praw Obywatelskich, pośrednicząc w przekazaniu informacji od sygnalisty do właściwego organu. Trzecią ścieżką, dopuszczalną tylko w określonych okolicznościach, m.in., jeżeli powiadomienie organu publicznego nie przyniosło rezultatu albo z różnych przyczyn nie byłoby sensowne i bezpieczne dla sygnalisty, jest publiczne ujawnienie informacji. Polega na przekazaniu informacji do opinii publicznej m.in. za pośrednictwem prasy, organizacji społecznych, biur parlamentarnych czy mediów społecznościowych.

W każdym z trzech kroków sygnalista ma prawo skorzystać z innego kanału komunikacji, zapewnianego przez jego organizację, organ właściwy do przyjmowania zgłoszeń zewnętrznych, a także organizację społeczną czy platformę społecznościową, które umożliwią mu upublicznienie informacji. Sygnalista wybiera metodę zgłoszenia spośród trybów przewidzianych procedurą zgłoszeń wewnętrznych lub procedurą zgłoszeń zewnętrznych. Jego wybór pozostaje więc ograniczony do kanałów wdrożonych przez jego pracodawcę lub organ publiczny, zaś przy ujawnieniu publicznym zależy w praktyce od

[3] Tamże, s. 9–14.

[4] Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. 2024 poz. 928).

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305/17 z 26.11.2019).

dostępnych mu środków komunikacji, nietworzących barier kosztowych czy technologicznych, z których zdecyduje się skorzystać. Najbardziej wymagające kryteria Dyrektywa stawia kanałom wewnętrznym, narzucając w art. 9 ust. 1 ich zaprojektowanie, ustanowienie i wdrożenie w sposób bezpieczny, zapewniający ochronę poufności sygnaliście i osobom wymienionym w zgłoszeniu oraz uniemożliwiający dostęp do zgłoszeń osobom nieupoważnionym. Podmioty prawne przyjmujące zgłoszenia wewnętrzne i organy właściwie obsługujące zgłoszenia zewnętrzne w wyniku Dyrektywy zobowiązane zostały do prowadzenia rejestru wszystkich zgłoszeń zgodnie z zasadą poufności oraz do przechowywania ich nie dłużej niż jest to konieczne i proporcjonalne z punktu widzenia zapewnienia zgodności z prawem unijnym i krajowym (art. 18 ust. 1).

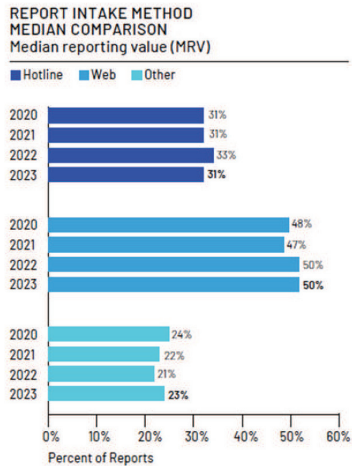
Dane globalnej korporacji NAVEX sprzedającej oprogramowanie do zgłaszania naruszeń wskazują, że aplikacja webowa to kanał najczęściej wybierany przez sygnalistów spośród im dostępnych (zob. rysunek 1). Jak sugerują Bartosz Jagura i Jacek Zdziarstek, aplikacje zapewniane przez zewnętrznych dostawców mają tę przewagę nad innymi metodami zgłoszeń, że działając poza systemem IT organizacji cieszą się większą wiarygodnością w aspekcie bezpieczeństwa i większym zaufaniem[6]. To wniosek zbieżny z tezą amerykańskich badaczy o tym, że upoważnienie do obsługi zgłoszeń certyfikowanego podmiotu trzeciego, w zakresie hostingu, zapewnienia bezpieczeństwa i dostarczanie narzędzia, często podnosi zaufanie do systemu i jest jakościowo lepsze niż rozwiązania tworzone *in-house*. Zewnętrzny dostawca jest w stanie dać bardziej wiarygodne zapewnienie, że informacje o adresach IP, dane geolokalizacyjne czy ogólne dane pozwalające na zidentyfikowanie sygnalisty nie są zbierane.[7]

Pracodawca albo zewnętrzny organ, który zastosuje narzędzie niesprawdzone pod względem bezpieczeństwa, bierze na siebie ryzyko niespełnienia prawnego obowiązku zachowania poufności danych sygnalisty i osób wymienionych w jego zgłoszeniu. Spowoduje to zagrożenie sankcjami karnymi dla zarządzających organizacją, jeżeli ich decyzje przyczynią się do ujawniania tożsamości sygnalisty, osoby pomagającej w dokonaniu zgłoszenia lub osoby powiązanej z sygnalistą. Wyciek danych może wymienione osoby narazić na działania odwetowe np. ze strony domniemanych sprawców, ale też osób z najbliższego otoczenia, jeżeli przejawiają niechęć wobec zachowań

6 B. Jagura, J. Zdziarstek, *Odpowiedź na występowanie naruszeń compliance, wewnętrzne postępowania wyjaśniające i whistleblowing*, [w:] B. Makowicz, B. Jagura (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*, Warszawa 2020, s. 217.

7 P. B. Lowry, G. D. Moody, D. Galletta, A. Vance, *The Drivers in the Use of Online Whistle-Blowing Reporting Systems*, «Journal of Management Information Systems» 2013, vol. 30(1), s. 37–38.

Rysunek 1. Mediana liczby zgłoszeń w zależności od kanału sygnalizowania (w ujęciu procentowym)



Źródło: *Whistleblowing & Incident Management Benchmark Report*, NAVEX 2024, s. 24.

polegających na informowaniu o nieprawidłowościach w miejscu pracy. Poza tym nieautoryzowany dostęp do informacji o zgłoszeniu daje możliwość zatuszowania śladów naruszenia.

Ochrona danych osobowych i inne wymogi prawne

Przetwarzanie danych osobowych w ramach systemu dla sygnalistów musi pozostawać co do zasady zgodne z unijnym rozporządzeniem 2016/679, czyli Ogólnym Rozporządzeniem o Ochronie Danych Osobowych (dalej: RODO). Wadliwe wdrożenie systemu grozi naruszeniem praw osób, których dane dotyczą oraz naraża podmioty na odpowiedzialność prawną z tego tytułu, w tym kary przyznawane przez regulatora. Relacje między regulacją sygnalizowania naruszeń a ochroną danych osobowych są bardzo ścisłe, a jednocześnie złożone i niewolne od odstępstw w zakresie wypełniania podstawowych obowiązków wynikających z RODO. Przy okazji wejścia w życie RODO i Dyrektywy ich wzajemnemu oddziaływaniu poświęcone zostały poradniki publikowane przez Europejskiego Inspektora Danych Osobowych[8] i Transparency International[9].

[8] *Guidelines on processing personal information within a whistleblowing procedure*, European Data Protection Supervisor, 2019 – https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf (11.05.2024).

[9] *The Impact of the General Data Protection Regulation on Whistleblowing*, Transparency International 2018 – https://knowledgehub.transparency.org/helpdesk/the-impact-of-the-general-data-protection-regulation-on-whistleblowing (11.05.2024).

Wymagania RODO trudno jest stosować do obszaru ochrony sygnalistów w sposób bezwzględny, choćby ze względu na konflikt między obowiązkiem zachowania w poufności tożsamości sygnalisty a prawem potencjalnego sprawcy, którego dane są przetwarzane, do poznania źródła pochodzenia danych[10]. Ustawa nadaje priorytetowe znaczenie ochronie poufności sygnalisty, pozwalając w tym celu ograniczyć zastosowanie obowiązku informacyjnego wobec osoby, której zgłoszenie dotyczy.

Przewidziane w art. 32 RODO środki technologiczne zabezpieczające dane, w tym szyfrowanie i pseudonimizacja, są zabezpieczeniami wykorzystywanymi też w aplikacjach do *whistleblowing*-u. O szyfrowaniu danych będzie jeszcze mowa w dalszej części artykułu. Co do pseudonimizacji natomiast należy wyjaśnić, że środek ten ma czynić niemożliwym przypisanie przechowywanych danych do osoby, o której informują, bez odpowiedniego klucza, który pozwoli je ze sobą połączyć[11]. Pseudonimizacja tym się różni od anonimizacji – polegającej na zgubieniu wszelkich zależności – że jest procesem odwracalnym. Aplikacje webowe mogą umożliwiać „zamazywanie" przez dostawcę podanych w zgłoszeniu szczegółów, jeżeli z ich kontekstu można odgadnąć tożsamość sygnalisty, jeżeli ten chciałby pozostać anonimowym. RODO w motywie 26 wskazuje, że nie obejmuje regulacją danych anonimowych, ale w przypadku zgłoszeń sygnalistów z taką sytuacją będziemy mieli do czynienia rzadko. Ustawa daje podstawę do przyjmowania zgłoszeń od anonimowego sygnalisty, jednak w treści tych zgłoszeń lub załącznikach do nich z dużym prawdopodobieństwem będą umieszczone nazwiska świadków, sprawcy i innych osób. Danymi osobowymi będą też informacje kontekstowe, które pozwolą na ich zidentyfikowanie, takie jak płeć, wiek, stanowisko czy dział, w którym pracują itp.

Techniczne środki zabezpieczania danych mogą być inspirowane m.in. normami ISO z zakresu zarządzania bezpieczeństwem informacji i zarządzania ryzykiem. Stosowanie norm technicznych podnoszących bezpieczeństwo przetwarzania jest w świetle obecnego stanu prawnego dobrowolne[12]. RODO kieruje się podejściem opartym na ryzyku (ang. *risk-based approach*), w ramach którego to administrator ma ocenić, jakie środki są niezbędne dla zapewnienia bezpieczeństwa danych. Działania administratora w tym zakresie

---

10 Por. K. Naumowicz, K. Pruszkiewicz-Słowińska, *Obowiązek informacyjny administratora danych osobowych wobec sygnalisty – klika uwag*, [w:] B. Baran, M. Ożóg (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021, s. 123–124.

11 Zob. *The Impact of the General…*, s. 4.

12 P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 409–410.

powinny wynikać z analizy ryzyka i oceny prawdopodobieństwa jego wystąpienia. Obsługa aplikacji dla sygnalistów, podobnie jak inne operacje przetwarzania danych, wymaga oceny ze względu na charakter, zakres, kontekst i cele przetwarzania. Zidentyfikowane ryzyko może się zmieniać w czasie, dlatego zabezpieczenie danych – tak jak wszelkie aktywności z obszaru cyberbezpieczeństwa – należy postrzegać nie w kategoriach produktu, ale procesu, który nie powinien ograniczać się do jednorazowej czynności[13].

W zakresie procesów przetwarzania, gdzie szacuje się wysokie ryzyko dla praw lub wolności osób fizycznych, administrator powinien przeprowadzić ocenę skutków dla ochrony danych (*Data Protection Impact Assessment*, DPIA). Paweł Fajgielski zauważa, że wskazanie na operacje przetwarzania z użyciem nowych technologii w art. 35 ust. 1 RODO jako jedną z przesłanek do przygotowania DPIA oznacza, że prawodawca traktuje je jako źródło niezbadanych jeszcze zagrożeń[14]. Urząd Ochrony Danych Osobowych (UODO) w komunikacie z 2019 r. identyfikuje systemy służące do zgłaszania nieprawidłowości jako przykład zastosowań operacji przetwarzania, dla których wymagane jest opracowanie DPIA[15]. Przy czym obowiązek ten występuje wg UODO przy odpowiedzialności administratora za co najmniej dwa obszary przetwarzania mieszczące się w grupie o podwyższonym ryzyku. Systemy *whistleblowing*-u, w szczególności przetwarzające dane pracowników, zostały wymienione w kryterium dotyczącym przetwarzania danych osób, których ocena i świadczone im usługi zależą od podmiotów dysponujących uprawnieniami nadzorczym i/lub ocennymi.

Wymagania dla aplikacji do *whistleblowing*-u w sektorze publicznym mogą być także determinowane minimalnymi wymaganiami dla systemów informatycznych, które zostały określone w rozporządzeniu w sprawie krajowych ram interoperacyjności. Znajdziemy w nim m.in. wskazania do korzystania z zabezpieczeń kryptograficznych w sposób adekwatny do zagrożeń lub wymogów prawa, w ramach zarządzania bezpieczeństwem informacji[16]. Pod względem zagrożeń szczególną grupą są podmioty zarządzające systemami i obiektami kluczowymi dla bezpieczeństwa państwa i jego obywateli, które pozwalają sprawnie funkcjonować administracji publicznej, instytucjom i przedsiębior-

---

13 F. Krzyżankiewicz, A. Mednis, *Ochrona danych osobowych*, [w:] C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023, s. 478.

14 P. Fajgielski, *Ogólne rozporządzenie*…, s. 438.

15 Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.

16 § 20 ust. 2 p.12d Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).

com. To podmioty zarządzające infrastrukturą krytyczną, scharakteryzowaną w ustawie o zarządzaniu kryzysowym[17], których luki w zabezpieczeniach narażają interes publiczny i mogą prowadzić np. do zakłócenia dostaw energii, wody, żywności czy braku łączności. Z ich strony dostawcy oprogramowania powinni spodziewać się surowszych kryteriów oceny bezpieczeństwa.

Uwarunkowania wynikające z Ustawy

W Ustawie uwzględniono szereg wymagań istotnych z punktu widzenia bezpieczeństwa przyjętego trybu zgłaszania. Za najbardziej krytyczne pod tym względem uznaję:

- zachowanie poufności danych sygnalisty i nieujawnianie ich bez jego wyraźnej zgody (art. 27 ust. 1);
- zachowanie poufności osoby, której dotyczy zgłoszenie (domniemanego sprawcy naruszenia) oraz osób trzecich występujących w zgłoszeniu (w tym świadków) (art. 27 ust. 1);
- gwarancje anonimowości osoby zgłaszającej, jeżeli podmiot prawny, Rzecznik Praw Obywatelskich lub organ publiczny podejmie decyzje o wdrożeniu anonimowych kanałów zgłaszania (art. 7 ust. 1);
- ograniczenia dostępu do informacji objętych zgłoszeniem wyłącznie do osób uprawnionych do ich odbioru i podejmowania działań następczych (art. 27 ust. 1). Jest to realizacja zasady *need to know*, według której udziela się upoważnień i daje dostęp do informacji w zakresie niezbędnym do wyjaśnienia zgłoszenia[18];
- dopuszczenie do prowadzenia rejestru zgłoszeń wewnętrznych wyłącznie upoważnioną osobę lub jednostkę wewnątrz organizacji (art. 29 ust. 2);
- nieprzechowywanie danych zbędnych, bez znaczenia dla rozpatrzenia zgłoszenia, i ich usuwanie w razie przypadkowego zebrania w ciągu 14 dni (art. 8 ust. 4). Jest to zgodne z zasadą adekwatności i minimalizacji przechowywania danych znaną z RODO[19].

Ustawa przewiduje możliwości odciążenia podmiotów w obsłudze zgłoszeń, ale tylko w ograniczonym stopniu. Średnie spółki prywatne zatrudniające między 50 a 249 osób mogą dzielić „zasoby" (art. 8 ust. 6 Dyrektywy) lub jak to zostało określone w polskim prawie „wspólne zasady" (art. 28 ust. 3 Ustawy) dotyczące przyjmowania zgłoszeń i podejmowania działań następczych. Przy

[17] Art. 3 ust. 2 Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007, Nr 89, poz. 509).

[18] *Guidelines on processing…*, s. 5.

[19] P. Fajgielski, *Ogólne rozporządzenie…*, s. 159–162.

czym podmioty korzystające ze wspólnego kanału zgłaszania nadal będą pozostawać osobnymi administratorami danych osobowych zawartych w zgłoszeniach, i jeżeli jeden podmiot pozyska informacje jego dotyczące na drodze zgłoszenia i postępowania wyjaśniającego, to dostępu do nich nie może mieć już inny administrator (art. 28 ust. 6 Ustawy). W rezultacie konieczna staje się separacja baz danych, jeżeli występują na współdzielonym środowisku, tak aby zgłoszenia nie zostały udostępnione podmiotowi, który nie jest właściwy do ich rozpatrzenia. Potrzeba prowadzenia w ramach jednego podmiotu niezależnych od siebie kanałów zgłaszania wystąpi w przypadków organów publicznych, które będę musiały wdrożyć jednocześnie własną wewnętrzną procedurę (lub wspólną procedurę wewnętrzną, którą mogą wdrożyć jednostki samorządu terytorialnego) oraz procedurę zgłoszeń zewnętrznych. Ustawa wskazuje też, że wspólną procedurę zgłoszeń mogą ustanowić podmioty należące do jednej grupy kapitałowej, bez względu na ich wielkość. W tym przypadku wydaje się dopuszczalne, aby istniał jeden rejestr zgłoszeń obsługiwany w ramach centralnego kanału, a podmioty w ramach grupy były jego współadministratorami. Natomiast to rozwiązanie nie zastępuje obowiązku wdrożenia własnych, osobnych kanałów zgłaszania przez podmioty, które wchodzą w skład grupy i są do tego zobowiązane[20]. Jeżeli sygnalista woli ominąć kanał centralny i udać się ścieżką lokalną do rodzimego podmiotu zgodnie z zasadą bliskości (ang. *proximity*), należy mu to umożliwić[21].

Współdzielenie jednego kanału sygnalizowania w formie aplikacji webowej jako wspólnego zasobu informatycznego to ważne zagadnienie prawne i techniczne zarazem. Wydaje się, że takie rozwiązanie wymaga przeprowadzenia w tym obszarze analizy ryzyka dla przetwarzania danych osobowych, czy, jak często i w jakich sytuacjach sygnaliści mogą przekazywać dane osobowe do podmiotu, który okaże się niewłaściwym administratorem do rozpatrzenia sprawy[22].

Ustawa nie przesądza, czy podmiot prawny ma wdrożyć tylko kanały pisemne, tylko ustne czy oba rodzaje. W przypadku, gdy zdecyduje się na zgłoszenia pisemne, może przyjmować je w formie papierowej lub elektronicznej

---

[20] Taka interpretacja Komisji Europejskiej została przedstawiona w pismach DG JUST z 2 czerwca 2021 r. JUST/C2/MM/rp/(2021)3939215 i 29 czerwca 2021 r. (JUST/C2/MM/rp/(2021)4667786).

[21] Por. M. Gumularz, *Sygnaliści: w grupie podmiotów jeden system zgłaszania naruszeń*, 07.03.2024, https://www.rp.pl/prawo-pracy/art39949501-sygnalisci-w-grupie-podmiotow-jeden-system-zglaszania-naruszen-prawa (19.05.2024).

[22] Ł. Mroczyński-Szmaj, *Nowe europejskie prawo sygnalizowania nieprawidłowości. Rozwiązania modelowe a polski projekt ustawy o ochronie osób zgłaszających naruszenia prawa*, «Prawo w Działaniu» 2022, nr 52, s. 216, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_32041_pwd_5209 (9.05.2024).

(art. 26 ust. 8). Ta sama zasada dotyczy organów publicznych, przy czym Ustawa precyzuje, że forma elektroniczna w przypadku zgłoszeń zewnętrznych może oznaczać m.in. skorzystanie z „formularza internetowego lub aplikacji wskazanej przez organ publiczny jako aplikacja właściwa do dokonywania zgłoszeń w postaci elektronicznej" (art. 36 ust. 2 p. 2). To przepis spójny z Dyrektywą, która dopuszcza przyjmowanie zgłoszenia za pośrednictwem aplikacji internetowych. Według jej motywu 54, do odbierania zgłoszeń o naruszeniach obsługiwanych wewnątrz podmiotu mogą zostać upoważnione osoby trzecie, w tym m.in. dostawcy platform internetowych. Z kolei motyw 45 stanowi, że sygnaliści mogą posługiwać się platformami online do zawiadamiania opinii publicznej o zagrożeniach. Z regulacji unijnej wynika zatem, że aplikacje mogą mieć co najmniej dwojakie przeznaczenie: z jednej strony zapewniać obsługę zgłoszeń wewnętrznych, z drugiej umożliwiać dokonanie tzw. ujawnienia publicznego. Grupa ekspercka przy Komisji Europejskiej odnotowała, że państwa członkowskie są zainteresowane wykorzystaniem platform dla sygnalistów, które będą zapewniać zgodność z RODO, m.in. pod względem szyfrowania i lokalizacji serwerów[23].

Ustawa wyłącza możliwość dokonania zgłoszenia kanałem dla sygnalistów treści objętych ochroną informacji niejawnych oraz niepodlegających ujawnieniu ze względu na bezpieczeństwo państwa, co nie oznacza, że w rzeczywistości takie zgłoszenia się nie pojawią. Tym bardziej, że w katalogu podmiotowym osób, które są uprawnione do korzystania z przepisów Ustawy, zostali wymieni także żołnierze, funkcjonariusze służb mundurowych i służb specjalnych.

Ewolucja platform dla sygnalistów

Dziesięć lat przed tym jak Unia Europejska wprowadziła prawną ochronę sygnalistów, ruch społeczny na rzecz radykalnej transparentności rządów i korporacji zainicjowany przez Juliana Assange'a, czyli projekt WikiLeaks, dał impuls do rozwoju platform internetowych w kierunku, który prowadził do przekazywania utajnionych dotąd danych opinii publicznej[24]. Na fali popularności inicjatywy WikiLeaks zaczęły powstawać kolejne, odwołujące się do tej samej misji oprogramowania, które stawiały sobie za cel ułatwienie anonimo-

[23] *Minutes of the seventh meeting of the Commission expert group on Directive (EU) 2019/1937*, 31.05.2022, s. 2, https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=44615&fromExpertGroups=3709 (5.11.2024).

[24] K. Gilsinan, *The Radical Evolution of WikiLeaks*, 17.11.2018, https://www.theatlantic.com/international/archive/2018/11/assange-wikileaks-trump-clinton-transparency-election-iraq/576115/ (5.11.2024).

wego przekazywania informacji od sygnalistów do dziennikarzy[25]. Platformy te miały chronić osoby ujawniające informacje przez Internet do mediów przed podsłuchiwaniem przez dostawców usług sieciowych, ale też przez służby specjalne czy policję analizujące ruch w sieci[26].

Dwa najczęściej stosowane dzisiaj oprogramowania, które pierwotnie miały spełniać potrzebę zapewnienia bezpieczeństwa dziennikarskim źródłom informacji, to GlobaLeaks (nawiązująca do dorobku WikiLeaks) i SecureDrop. Ich twórcy wyrośli ze środowiska etycznych hackerów i działań motywowanych *digital dissidence*, czyli cyfrowym sprzeciwem wobec inwigilacji w sieci. Aplikacje wyróżnia to, że tworzone są w modelu otwartego oprogramowania (ang. *open-source software*), co oznacza, że ich kod źródłowy jest udostępniany publicznie. To z kolei umożliwia bieżące monitorowanie błędów przez obywateli, użytkowników i osoby biorące udział w programach zgłaszania podatności bezpieczeństwa[27]. W przypadku aplikacji z zamkniętym kodem brakuje legalnych możliwości ich weryfikacji[28]. Nie jest to równoznaczne z tym, że aplikacje *open-source* cechuje wyższy poziom bezpieczeństwa niż te oparte na oprogramowaniu własnym (ang. *proprietary software*). Ich przewaga bierze się jednak stąd, że zapewniają zainteresowanym osobom w dowolnym momencie możliwość skontrolowania czy oprogramowanie jest zainfekowane i czy nie zawiera luk bezpieczeństwa (ang. *backdoors*).

GlobaLeaks od 2011 r. rozwijane jest przez włoską organizację pozarządową Hermes Center for Transparency and Digital Human Rights, tworzoną przez prawników, aktywistów i programistów. Z ich oprogramowania korzystają obecnie nie tylko media, ale też firmy prywatne, organizacje pozarządowe i instytucje publiczne takie jak włoski Krajowy Urząd Antykorupcyjny (ANAC)[29] czy Agencja ds. Zwalczania Nadużyć Finansowych i Korupcji Regionu Walencji (AFAV)[30]. Z GlobaLeaks korzystają też kolektywy podmiotów tak jak w przypadku holenderskiego PubLeaks, kanału do przyjmowania infor-

---

25 B. Brevini, G. Murdock, *Following the Money: WikiLeaks and the Political Economy Disclosure*, [w:] B. Brevini, A. Hintz, P. McCurdy (red.), *Beyond WikiLeaks. Implications for the Future of Communications, Journalism and Society*, Hampsire 2013, s. 49–50.

26 Zob. V. Roth, B. Güldenring, E. Rieffel, S. Dietrich, L. Ries, *A Secure Submission System for Online Whistleblowing Platforms*, 29.01.2013, http://arxiv.org/pdf/1301.6263 (17.05.2024).

27 M. Ahmed-Rengers, D. A. Vasile, D. Hugenroth, A. R. Beresfold, R. Anderson, *CoverDrop: Blowing the Whistle Through A News App*, «Proceedings on Privacy Enhancing Technologies» 2022, nr 2, https://petsymposium.org/popets/2022/popets-2022-0035.pdf (8.05.2024).

28 *The Pitfalls of Closed-Source Whistleblowing Software*, 05.08.2022, whistleblowingnetwork.org/Our-Work/Spotlight/Stories/The-Pitfalls-of-Closed-Source-Whistleblowing-Softw (8.05.2024).

29 https://whistleblowing.anticorruzione.it/#/ (27.05.2024).

30 https://bustiadenuncies.antifraucv.es/#/ (27.05.2024).

macji od sygnalistów założonego przez 15 holenderskich organizacji związanych z mediami[31]. SecureDrop z kolei to oprogramowanie częściej spotykane w Stanach Zjednoczonych[32]. Obie platformy przeznaczone są do wdrożenia lokalnego na serwerze w modelu *On Premises*. Obie korzystają z dostępu do anonimowej sieci TOR, które zaciemnia pochodzenie danych.

Rozwiązania oferowane przez GlobaLeaks i SecureDrop stały się inspiracją dla powstania prototypów kolejnych aplikacji, których twórcy, dostrzegając deficyty obu platform, proponują autorskie rozwiązania. Ich krytyka dotyczy m.in. braku możliwości uwiarygodnienia, że źródłem informacji jest sygnalista, a nie osoba, która się pod niego podszywa[33]. U osób obsługujących wewnętrzną procedurę może pojawić się potrzeba upewnienia się, czy anonimowy zgłaszający to osoba, która ma jakikolwiek związek z ich organizacją i czy są podstawy do rozpatrzenia zgłoszenia. Ponadto wyzwaniem dla aplikacji jest ochrona treści zgłoszenia, tak, żeby nie można było jej zmodyfikować bez wiedzy i zgody sygnalisty[34].

Odpowiedzią na te problemy była m.in. propozycja *blockchain*-a, wcielającego w życie filozofię cyfrowego zaufania (ang. *digital trust*)[35]. Jest to system, który pozwala dzielić się wybranymi informacjami, przy zachowaniu prywatności innych danych[36]. Wykorzystanie w nim grupowych podpisów ma dowodzić przynależności do organizacji. Daje pewność, że ten kto zgłasza informacje o naruszeniu wszedł w ich posiadanie w kontekście związanym z pracą. Dzięki czemu można odrzucić obawy, że zgłoszenia dokonuje ktoś niezwiązany z organizacją czy osoba, która poprzez wykradzenie poufnych danych próbuje zrzucić winę za popełnione naruszenie na pracownika.

Niezaprzeczalną zaletą omawianego konceptu jest pełne zaufanie do integralności danych w *blockchain*. Prywatny *blockchain* ma być kontrolo-

31 https://www.publeaks.nl/ (5.11.2024).

32 Przykładową listę organizacji stosujących oba oprogramowania można znaleźć w raporcie przygotowanym z grantu Funduszu Bezpieczeństwa Wewnętrznego Unii Europejskiej: N. Colvin, V. Nad, C. Culnane, B. Galizzi, S. Dreyfus, *Expanding*…, s. 48–57.

33 S. Chica, A. Marin, D. Arroyo, J. Diaz, F. Almenares, D. Diaz, *Enhancing the Anonymity and Auditability of Whistleblowers Protection*, [w:] J. Preto, F. L. B. Martinez, S. Ferretti, D. A. Guardeño, P. T. Nevado-Batalla (red.), *Blockchain and Applications, 4th International Congress*, «Lecture Notes in Networks and Systems» 2023, vol. 595, s. 415.

34 Istnieją aplikacje, które zapewniają o niezmienności zgłoszenia wysyłając zahashowany, cyfrowy „odcisk palca" sygnalisty na jego adres e-mail. Zob.: https://www.whistleblowing.software/en/security-whistleblowing-system/ (28.05.2024).

35 P. M. Asprion, H. Grieder, F. Grimberg, *Building Digital Trust to Protect Whistleblowers – A blockchain-based Reporting Channel*, „Proceedings of the 56th Hawaii International Conference on System Sciences", 2023, s. 4328, https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/cce23d75-65ac-4c6f-9104-f800bfcc58ff/content (8.05.2024).

36 S. Chica, A. Marin, D. Arroyo, J. Diaz, F. Almenares, D. Diaz, *Enhancing the Anonymity*…, s. 414.

wany przez konsorcjum godnych zaufania osób. Operatorzy decydują w nim, kto może dołączyć do sieci, przeczytać i napisać *blockchain* oraz zatrzymać rekord. To zapewnia bezpieczeństwo *blockchain*-a bez dzielenia się treścią na zewnątrz organizacji. Zdecentralizowana architektura systemu umożliwia tworzenie różnych grup interesariuszy, którzy niezależnie od siebie za pomocą osobnych węzłów sieci (ang. *nodes*) i kopii rejestrów (ang. *ledger*) mogą odbierać zgłoszenia. Jako odbiorców można wskazać zarząd, związki zawodowe czy przedstawicieli spółki matki w grupie kapitałowej. Nie ma w tym systemie możliwości zafałszowania prawdziwych danych zgłoszenia i manipulowania treściami, jeżeli ktoś chciałby zniszczyć niewygodne informacje lub ukryć je przed kontrolerami[37]. Każdy z węzłów jest audytowany przez inne strony. Rozliczalność systemu zostaje zapewniona poprzez dostęp do logów audytowych, bez uszczerbku dla ochrony poufności sygnalistów.

To, co jest zaletą z punktu widzenia cyberbezpieczeństwa, staje się wyzwaniem, gdy chcemy zachować zgodność działania systemu z prawem. Omawiana koncepcja zapewnia niepodważalność rejestrów. Zapisy w *blockchain* są przechowywane w rozproszonych księgach, co oznacza, że ich retencja nie może być też w pełni kontrolowalna przez władze organizacji[38]. Jest to oczywiście z korzyścią dla przejrzystości transakcji i dostępności informacji. Jednak niezmienność raz wprowadzonych danych, a przede wszystkim brak możliwości ich usunięcia nie pozwalają realizować obowiązków prawnych związanych z wymaganym okresem przechowywania danych i bieżącym czyszczeniem z rejestru danych zbędnych[39].

Twórcy prototypu innej aplikacji CoverDrop zwrócili z kolei uwagę na zagrożenie dla poufności tożsamości sygnalisty związane z analizą ruchu sieciowego i wnioskowaniem na jego podstawie o połączeniach, np. z dziennikarzem w sytuacji sygnalizowania do mediów. Adwersarze mają możliwość instalowania śledzącego oprogramowania na telefonach dziennikarzy i sygnalistów, mogą też monitorować ruch wewnątrz redakcji. Nawet jeżeli nie są w stanie rozszyfrować treści wiadomości i jej zmienić, mogą ustalić, kto jest jej nadawcą. Twórcy CoverDrop powołali się na przykład wysokiego urzędnika państwowego, który może być łatwo rozpoznany jako źródło przecieku do mediów informacji obciążających polityków, jeżeli jako jedyny z kilkudziesięciu osób w otoczeniu rządu instalował wcześniej przeglądarkę TOR lub oprogramowanie typu SecureDrop[40]. W zamyśle autorów CoverDrop czyn-

[37] P. M. Asprion, H. Grieder, F. Grimberg, *Building Digital Trust*…, s. 4334–4335.
[38] Tamże, s. 4335.
[39] Tamże, s. 4330.
[40] M. Ahmed-Rengers, D. A. Vasile, D. Hugenroth, A. R. Beresfold, R. Anderson, *CoverDrop: Blowing the Whistle Through A News App*, «Proceedings on Privacy Enhancing Technolo-

ności te nie powinny być wymagane przez użytkownika. Odnotowywano już zresztą przypadki, że za używanie TOR-a sygnaliści byli umieszczani na listach obserwacyjnych amerykańskiej agencji wywiadowczej NSA[41]. W dyskusji nad zasadnością wykorzystania trasowania cebulowego w oprogramowaniu dla sygnalistów pojawiają się argumenty uzasadniające, że jest to kłopotliwa forma zgłaszania, zniechęcająca osoby bez kompetencji cyfrowych mało przyjaznym sposobem obsługi[42].

Rozwój narzędzi takich jak GlobaLeaks i SecureDrop, testowanych i okresowo weryfikowanych pod względem bezpieczeństwa, odegrał ważną rolę standaryzacyjną na rynku platform dla sygnalistów[43]. Ich pierwotnym przeznaczeniem nie była jednak obsługa wewnętrznych ścieżek sygnalizowania, ale dokonywanie zgłoszeń do mediów lub organów zewnętrznych, poza organizację, w której doszło do naruszenia. Tymczasem poufny mechanizm, który umożliwi przekazywanie informacji o naruszeniach w miejscu pracy i zminimalizuje ryzyka po obu stronach – sygnalisty i jego organizacji – powinien objąć też inne aspekty przetwarzania danych[44]. Dlatego sposób obsługi i zakres funkcjonalności omówionej kategorii platform nie zawsze musi być adekwatny do warunków rozpatrywania zgłoszeń wewnętrznych.

Badania pokazują, że sygnaliści w zdecydowanej większości w pierwszym kroku wybierają dostępną im ścieżkę raportowania wewnątrz organizacji – a jeżeli już dokonują ujawnienia publicznego, to częściej poprzez związki zawodowe, stowarzyszenia zawodowe lub organizacje branżowe, aniżeli bezpośrednio do mediów[45]. W tym kontekście utrzymanie bezpieczeństwa aplikacji dla sygnalistów będzie mieć coraz większy związek z błędami i zaniechaniami użytkowników obsługujących zgłoszenia po stronie organizacji.

---

gies» 2022, nr 2, s. 51, https://petsymposium.org/popets/2022/popets-2022-0035.pdf (8.05.2024).

41 S. Rosenblatt, *NSA likely targets anybody who's "Tor-curious"*, 03.07.2013, https://www.cnet.com/news/privacy/nsa-likely-targets-anybody-whos-tor-curious/ (20.05.2024).

42 H. Javakrishnan, R. Murali, *A Simple and Robust End-to-End Encryption Architecture for Anonymous and Secure Whistleblowing*, Twelfth International Conference on Contemporary Computing (IC3), 2019, https://ieeexplore.ieee.org/document/8844917 (8.05.2024).

43 P. Di Salvo, *Digital Whistleblowing Platforms in Journalism. Encrypting Leaks*, Cham 2020, s. 72–74.

44 P. M. Asprion, H. Grieder, F. Grimberg, *Building Digital Trust*…, s. 4330.

45 A. J. Brown et al., *Clean as a whistle: a five step guide to better whistleblowing policy and practice in business and government*, Brisbane 2019, s. 47–48, http://www.whistlingwhiletheywork.edu.au/wp-content/uploads/2019/08/Clean-as-a-whistle_A-five-step-guide-to-better-whistleblowing-policy_Key-findings-and-actions-WWTW2-August-2019.pdf (19.05.2024).

Podstawowe zabezpieczenia techniczne

Polska firma ODO 24 działająca w obszarze ochrony danych osobowych zainicjowała ranking oceniający aplikacje webowe dla sygnalistów według zaproponowanych i konsultowanych z branżą kryteriów. Do tej pory przeprowadzono trzy jego edycje w 2022 r., 2023 i 2024 r.[46] W ciągu dwóch lat liczba aplikacji zidentyfikowanych przez twórców rankingu wzrosła na polskim rynku z 34 do 49. Obecnie ranking posługuje się zestawem 30 kryteriów, które mają mierzyć bezpieczeństwo danych, jednak ma on charakter poglądowy i nie stanowi uniwersalnego, obowiązującego wszystkich dostawców standardu. Niektórzy dostawcy, chcąc wyróżnić się na rynku, swoją przewagę konkurencyjną budują właśnie na technicznych gwarancjach poufności danych sygnalisty, takich jak szyfrowanie *end-to-end* czy wykorzystanie przeglądarki TOR.

Jeżeli bierzemy pod uwagę zabezpieczenia architektury aplikacji, ważne jest, aby rozróżnić dwa podstawowe modele, w których swoje usługi oferują dostawcy aplikacji dla sygnalistów: *On Premises* oraz *SaaS* (*Software as a Service*)[47]. W pierwszym przypadku oprogramowanie jest instalowane lokalnie u klienta, w drugim utrzymywane w oparciu o infrastrukturę i zasoby należące do dostawcy. W modelu *SaaS* to na dostawcy spoczywa odpowiedzialność za utrzymanie bezpieczeństwa architektury aplikacji, którą zobrazowano na rysunku 2. Dostawca będzie musiał zatem m.in. zapewnić bezpieczeństwo własnych serwerów (lub wybór bezpiecznych pod tym względem serwerów chmurowych), ich aktualizację, aplikacyjne zapory ogniowej (ang. *Web Application Firewall*, WAF), stałą dostępność kanału zgłoszeniowego przez przeglądarkę w połączeniu internetowym. W przypadku aplikacji *On Premises* poziom ich bezpieczeństwa będzie natomiast warunkowany tym, jak zostały zabezpieczone sieć i zasoby klienta, u którego oprogramowanie działa lokalnie. Do zabezpieczenia architektury aplikacji nie wystarczy jeden z opisanych elementów. Przykładowo *firewall* oczywiście zmniejsza ryzyko ataku, ale nie zawsze będzie skuteczny[48].

Jedną z czynności koniecznych do wykonania jest odpowiednia konfiguracja serwera, tak, aby zminimalizować powierzchnię wrażliwą na ataki, zwana też hartowaniem (ang. *hardening*) serwera. Minimalizację szkód w razie ataku

---

46 Więcej: https://odo24.pl/ranking-aplikacji-dla-sygnalistow#ranking-aplikacji (3.03.2025).

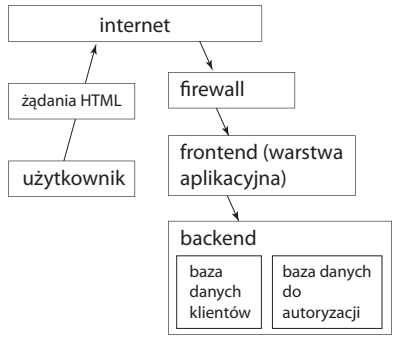
47 *Porównanie rozwiązań dla sygnalistów pod względem zgodności z dobrymi praktykami bezpieczeństwa i ochroną danych osobowych*, AVLab Cybersecurity Foundation 2022, s. 6, https://app.sygnanet.pl/pdf/AVLab_report.pdf (9.05.2024).

48 M. Sajdak, *Co każdy administrator powinien wiedzieć o bezpieczeństwie aplikacji webowych?*, [w:] M. Sajdak (red.), *Wprowadzenie do bezpieczeństwa IT*, Kraków 2023, s. 113.

typu SQL Injection można osiągnąć poprzez separację użytkowników na poziomie bazy danych i separację baz danych należących do różnych klientów dostawcy[49]. W ramach konfiguracji serwera aplikacyjnego należy uwzględnić ochronę poufności, poprzez unikanie rejestrowania wraz z treścią zgłoszenia danych, które mogłyby sygnalistę identyfikować. Z tego względu dane w logach serwera zbierające informacje o adresie IP i szczegółach przeglądarki użytkownika, nie powinny być możliwe do połączenia ze zgłoszeniami.

W obliczu wymogów prawnych związanych z retencją danych tym bardziej uzasadnione staje się wykonywanie możliwie częstych i regularnych kopii zapasowych, które w razie awarii będą łatwe do odtworzenia, ale też do odszyfrowania. Taka operacja może stać się konieczna, jeżeli służby państwa zażądają dostępu do danych zgromadzonych na serwerze na potrzeby prowadzonego postępowania, na co Ustawa w uzasadnionych przypadkach pozwala.

Rysunek 2. Uproszczony schemat architektury aplikacji webowej



Źródło: opracowanie własne.

Aby rzetelnie ocenić bezpieczeństwo architektury aplikacji webowej konieczne są jeszcze informacje na temat szyfrowania. Zapewnienie od dostawcy, że aplikacja jest szyfrowana niewiele mówi, jeżeli nie zostanie uzupełniona o dodatkowe informacje. Po pierwsze na temat tego, co jest realnie szyfrowane. Większość aplikacji, jak sugerują raporty na ich temat, będzie spełniać warunek szyfrowanego kanału komunikacji między przeglądarką użytkownika a serwerem aplikacyjnym poprzez protokół HTTPS przy użyciu protokołu szyfrowanego TLS (ang. *Transport Layer Security*) w wersji 1.2 (przy czym obecnie dąży się do używania wersji 1.3)[50]. Certyfikat SSL jest nieodzowny dla zapewnienia bezpieczeństwa, ponieważ potwierdza komu sygnalista powierza dane.

[49] M. Bentkowski, *Podatność SQL Injection*, [w:] M. Sajdak (red.), *Bezpieczeństwo aplikacji webowych*, Kraków 2021, s. 475.

[50] *Porównanie rozwiązań…*, s. 37.

Poza kanałem komunikacji użytkownik – serwer aplikacyjny trzeba pamiętać o konieczności szyfrowania transportu danych z serwera aplikacyjnego do bazy, a na koniec o szyfrowaniu serwera bazowego. Inaczej w przypadku nieuprawnionego dostępu do serwera, luki bezpieczeństwa lub innej podatności samego serwera zachodzi duże ryzyko, że zgłoszenie sygnalisty odczyta ktoś nieupoważniony. Luka w zabezpieczeniach może polegać np. na publicznym dostępie do portu internetowego poprzez nieszyfrowane połączenie. Aplikacje webowe nie są wyjątkiem od znanej zasady cyberbezpieczeństwa, że dane szyfrujemy zawsze w obu możliwych stanach: tak „w locie" (ang. *in transit*) jak i „w spoczynku" (ang. *at rest*). Szyfrowane powinny być nie tylko wiadomości wysyłane przez sygnalistę lub do sygnalisty, ale też dodawane do zgłoszenia załączniki: zeskanowane dokumenty, fragmenty nagrań czy zdjęcia.

Inna ważna informacja dotyczy sposobu generowania klucza szyfrującego. Możemy mieć do czynienia z *client-side encryption*, czyli sytuacją, kiedy szyfrowanie realizowane jest kryptograficznie przed wysłaniem na serwer wszystkich danych oraz załączników poprzez przeglądarkę użytkownika. Tymczasowy klucz generowany jest przy pierwszej interakcji przeglądarki z aplikacją. Uniemożliwia to podsłuchanie (ang. *sniffing*) i przechwycenie treści zgłoszenia. W przypadku *server-side encryption* mamy natomiast do czynienia z szyfrowaniem danych odbywającym się w pamięci serwera po ich dostarczeniu do aplikacji. To szyfrowanie bazodanowe odbywające się wg innego klucza, który jest rzadko zmieniany. Szyfrowanie i deszyfrowanie na „końcówkach" (ang. *end-to-end*), czyli urządzeniu lokalnym użytkownika jest rozwiązaniem bezpieczniejszym, gdyż nie ma tymczasowego stanu niezaszyfrowania informacji jak w systemach chmurowych, gdzie procesy szyfrowania i deszyfrowania odbywają się na serwerach.

Nie niweluje to zagrożenia przy wprowadzaniu czystych danych do aplikacji, jeżeli użytkownik padnie ofiarą podatności XSS (ang. *Cross-Site Scripting*), czyli osadzeniu przez atakującego własnego kodu HTML/JavaScript. Skutki ataku XSS mogą być brzemienne w skutkach, gdyż prowadzą do przejęcia sesji zalogowanego użytkownika i odczytania przez atakującego w tym kontekście dowolnych danych[51]. Użytkownik aplikacji staje się ofiarą ataku m.in. po kontakcie ze złośliwym linkiem, który będzie prowadził do wykonania ukrytego kodu JavaScript, co nazywa się też „atakiem z wodopoju" (ang. *watering hole attacks*)[52]. Możliwe scenariusze ataku XSS pokazują, że niezbędne jest zapro-

[51] Zob. M. Bentkowski, *Podatność Cross-Site Scripting* (XSS), [w:] M. Sajdak (red.), *Bezpieczeństwo…*, s. 281–287.

[52] *OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks*, The OWASP Foundation 2017, s. 13, https://raw.githubusercontent.com/OWASP/Top10/master/2017/OWASP%20Top%2010-2017%20(en).pdf (12.05.2024).

jektowanie w formularzu dla sygnalistów odpowiednich mechanizmów walidacyjnych.

Kolejna informacja na temat szyfrowania dotyczy algorytmów kryptograficznych i ich zastosowania do szyfrowania symetrycznego, asymetrycznego czy hybrydowego. W aplikacjach dla sygnalistów to szyfrowanie asymetryczne jest najbardziej popularne, często oparte o algorytm krzywej eliptycznej[53]. Wraz z dynamicznym rozwojem technologii kwantowej wymagania w tej materii stawiane aplikacjom webowym mogą jeszcze wzrosnąć. Kamienie milowe w dziedzinie cyberbezpieczeństwa, czyli klucze szyfrujące RSA i AES, staną się podatne na dekryptaż kwantowy. Jak wskazuje Włodzimierz Nowak, już w 2025 r. najpopularniejszy klucz publiczny RSA, czyli algorytm Rivesta-Shamira-Adlemana ma zostać złamany przez komputer kwantowy, co stanie się realnym zagrożeniem nie tylko dla aplikacji do zgłaszania naruszeń, ale też np. dla systemów bankowych[54]. Zatem klienci aplikacji coraz większą uwagę powinni zwracać na to, czy stosowane w niej algorytmy szyfrujące nie zostały skompromitowane. Odpowiedzią na przewidywane zagrożenia związane z rozwojem technologii kwantowej jest stosowanie postkwantowych protokołów szyfrujących, które zaczęły być już wprowadzane do komunikatorów internetowych[55].

Z myślą o sygnalistach, którzy działają w reżimach niedemokratycznych i narażeni są na represje władzy, niektórzy twórcy niektórych aplikacji starają się wdrożyć w życie koncepcję „wiarygodnego zaprzeczenia" (ang. *plausible deniability*). W cyberbezpieczeństwie jest to realizowane przez sposób dzielenia i szyfrowania danych w wielu różnych warstwach, tak aby adwersarze nie byli w stanie odnaleźć pewnych wolumenów danych, zorientować się, które z nich zostały zaszyfrowane i czy istnieje do nich klucz deszyfrujący[56]. Wszystko po to, aby ukryć ślady po dokonaniu zgłoszenia oraz dowody, które świadczyłyby o przekazaniu konkretnych danych. W ten sposób sygnalista ma szanse uniknąć sytuacji, w której organy władzy będą wymuszały na nim ujawnienie, jakie informacje przekazywał.

---

53 https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html#algorithms (13.05.2024).

54 W. Nowak, *Ochrona infrastruktury krytycznej w cyberprzestrzeni*, [w:] C. Banasiński (red.), *Cyberbezpieczeństwo…*, s. 231–232.

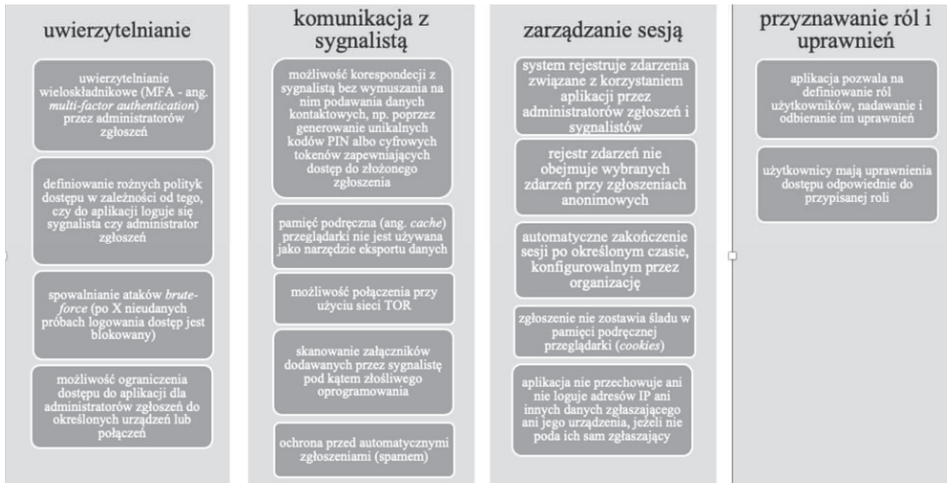
55 Zob. *iMessage with PQ3: The new state of the art in quantum-secure messaging at scale*, security.apple.com/blog/imessage-pq3/ (26.02.2024).

56 J. Lake, *What is plausible deniability (in encryption) and does it really work?*, 08.01.2024, https://www.comparitech.com/blog/information-security/plausible-deniability-encryption/ (18.05.2024).

Bezpieczeństwo procesów przetwarzania zgłoszeń

Producenci aplikacji dla sygnalistów mają dawać gwarancje bezpieczeństwa procesów przetwarzania danych. Na rysunku 3 przedstawiono najbardziej podstawowe procesy, do których przypisano przykładowe środki zabezpieczające.

Rysunek 3. Wybrane wymogi bezpieczeństwa dla procesów obsługiwanych przez aplikacje dla sygnalistów



Źródło: Wybrane kryteria bezpieczeństwa pochodzące m.in. z rankingu ODO 24 i wskazywane w ofertach dostawców aplikacji.

Wśród podanych kryteriów w zakresie uwierzytelniania warto wyróżnić coraz częściej pojawiający się wymóg uwierzytelniania wieloskładnikowego, w praktyce często dwuskładnikowego (ang. *two factor authentication*, 2FA). To zabezpieczenie ma przeciwdziałać nieuprawnionemu dostępowi do panelu administratora przez osobę, której np. udało się wykraść albo zgadnąć hasło innego użytkownika. Działa według zasady „coś wiesz i coś masz", czyli użytkownik musi pamiętać hasło, a jednocześnie mieć przy sobie inne urządzenie, np. telefon, który umożliwi dokonanie uwierzytelnienia.

Sposób uwierzytelniania loginem i hasłem użytkownika musi wykazywać też odporność na ataki siłowe (ang. *brute-force*). Polityka tworzenia haseł dla aplikacji może służyć do zminimalizowania tego ryzyka poprzez zdefiniowanie wymaganej długości haseł, które jednocześnie nie będą hasłami słownikowymi[57].

[57] Według zaleceń CERT Polska minimalna długość hasła to 12 znaków, https://cert.pl/posts/2022/01/kompleksowo-o-haslach/ (4.06.2024).

Po kilku nieudanych próbach logowania jako pierwszą linię obrony przed próbą ataku siłowego wykorzystuje się mechanizm CAPTCHA, którego zaimplementowanie w ramach dodatkowej funkcji wiąże się zarazem ze zwiększeniem powierzchni ataku. Jeszcze prostszym zabezpieczeniem jest czasowa blokada konta użytkownika w aplikacji po określonej liczbie nieudanych prób logowania. Aby mechanizm ten był skuteczny, informacja o wprowadzeniu niepoprawnego hasła powinna być rejestrowana w bazie danych, a nie w sesji na stronie internetowej, co atakujący może obejść. Uwierzytelnianie jest niezwykle istotne w aplikacjach do *whistleblowing*-u, gdyż dokonują go nie tylko użytkownicy mający konta, ale też sygnaliści, którzy kont nie zakładają. Twórcy oprogramowania pozostawiają im jednak możliwość anonimowego komunikowania się z organizacją z użyciem panelu, do którego dostęp mają pod wskazanym adresem www, np. po wpisaniu przypisanego im unikalnego kodu PIN. Anonimowy sygnalista nie będzie miał możliwości skorzystania z uwierzytelnienia 2FA, a jego panel może zostać zhakowany nawet łatwiej, gdyż atakujący nie musi zgadywać loginu. Może stać się tak w szczególności, jeśli kod dostępu nie jest generowany losowo, ale polega na łatwym do odczytania algorytmie. Dlatego należy zwracać uwagę na zwiększenie bezpieczeństwa uwierzytelniania także od strony dostępu sygnalisty do treści swojego zgłoszenia.

Jak sugerują dane zbierane przez NAVEX, zgłaszanie naruszeń z użyciem aplikacji webowych na tle innych kanałów zdecydowanie najbardziej sprzyja zgłoszeniom anonimowym[58]. Wydaje się oczywiste, że ma to bezpośredni związek z możliwościami anonimizowania zgłoszeń, którymi chwalą się dostawcy takich aplikacji. Połączenie z serwerem aplikacyjnym musi wtedy dawać gwarancje, że adres IP, nazwa komputera, system operacyjny, rodzaj i „odcisk palca" przeglądarki oraz dane geolokalizacyjne nie są zbierane, zaś *cookies* nie są używane do śledzenia tego, co sygnalista robi w oknie przeglądarki[59]. W przypadku plików, które mają być dowodem w sprawie albo uzupełniają przekazane przez sygnalistę informacje, zachodzi też potrzeba wyczyszczenia ich z metadanych zawierających informacje identyfikujące właściciela załączników. Poza tym aplikacja powinna brać pod uwagę, że zgłaszający intencjonalnie lub nie może załączać pliki zainfekowane złośliwym kodem, stąd istnieje potrzeba ich skanowania i niezałączania niebezpiecznych załączników lub automatycznego oczyszczania ich ze skryptów.

---

58 *Whistleblowing & Incident Management Benchmark Report*, NAVEX 2024, s. 42.

59 B. Berendt, S. Schniffer, *Whistleblower protection in the digital age – why „anonymous" is not enough? From technology to a wider view of governance*, «International Review of Information Ethics» 2022, vol. 31, s. 7, https://informationethics.ca/index.php/irie/article/view/479/440 (28.05.2024).

Gwarancje poufności dla sygnalisty nie są przeszkodą dla rozliczalności systemu. Aplikacja musi dawać możliwość monitorowania, kto z administratorów zgłoszeń miał dostęp do systemu, kiedy oraz jakie operacje w nim wykonał. W celu ochrony przed cyberatakami powinna pozwalać na wykrycie nieautoryzowanych połączeń i działań. To ryzyko może zostać zminimalizowane z wykorzystaniem panelu zarządzania rolami i uprawnieniami w aplikacji. Ma on służyć do takiej konfiguracji dostępów, w której żaden z użytkowników nie będzie miał przyznanych nadmiarowych uprawnień, ale wyłącznie te, które pozwolą mu wykonywać zadania, do jakich został powołany. Ze względów prawnych pożądane jest też, aby aplikacja posiadała repozytorium upoważnień dotyczących systemu wraz z potwierdzeniem ich akceptacji.

Przywołane kryteria bezpieczeństwa aplikacji webowych dla sygnalistów wpisują się w perspektywę ogólnych standardów, które opracowała Fundacja OWASP (*The Open Worldwide Application Security Project*). Najbardziej aktualne standardy OWASP dotyczące weryfikacji zabezpieczeń aplikacji (*Application Security Verification Standard*, ASVS) pochodzą z 2021 r. To narzędzie do samooceny, które może służyć jako przewodnik, co powinno być weryfikowane w ramach zapewnienia bezpieczeństwa aplikacji. Standardy OWASP nadają się też do wykorzystania przy przygotowaniu dokumentacji zamówieniowej na aplikacje, pomogą ustalić kryteria ich wyboru i poziom, w jakim kryteria te powinny zostać spełnione[60]. OWASP ASVS w formie zaleceń i zestawu dobrych praktyk podpowiada, co warto zweryfikować i wdrożyć, aby prewencyjnie unikać zagrożeń i podatności. Opracowanie obejmuje wszystkie zabezpieczenia i procesy, które zostały wspomniane wcześniej jako szczególnie istotne z perspektywy aplikacji dla sygnalistów: kryptografię, komunikację z użytkownikiem, uwierzytelnianie, zarządzanie sesją czy kontrolę dostępu.

W części poświęconej bezpieczeństwu danych OWASP ASVS streszcza cele ich ochrony w akronimie CIA, za którym kryje się poufność, integralność i dostępność (ang. *Confidentiality*, *Integrity*, *Availability*)[61]. Poufność oznacza, że dane są chronione przed nieautoryzowaną obserwacją lub ujawnieniem, zarówno kiedy znajdują się w trakcie przesyłania jak i podczas przechowywania. Integralność ma zapewniać o tym, żeby dane nie są złośliwie modyfikowane, zmieniane lub usuwane przez nieautoryzowane osoby. Dostępność natomiast polega na tym, że dane pozostają dostępne dla osób upoważnionych za każdym razem, gdy jest to wymagane. OWASP uczula w tym zakresie m.in., żeby minimalizować liczbę parametrów, które pojawiają się w żądaniu

[60] *OWASP Application Security Verification Standard 4.0.3.*, The OWASP Foundation 2021, s. 15–16, https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf (12.05.2024).

[61] Tamże, s. 47.

aplikacji i wykrywać anomalie, które mogą przejawiać się w nietypowej liczbie żądań pochodzących z jednego adresu IP czy od jednego użytkownika oraz tym jak długo i kiedy były wysyłane.

Monitoring podatności

Źródłami ryzyk dla elektronicznych zgłoszeń mogą być zarówno zewnętrzni adwersarze jak i jej użytkownicy. Joakim Uddholm wymienia jako słabe ogniwa w tym kontekście władzę organizacji, której może zależeć, żeby zgłoszenie nie zostało wysłane na zewnątrz, odbiorcę informacji, który może intencjonalnie lub nie ujawnić dane zgłaszającego, administratora serwera śledzącego adresy IP, zewnętrznego obserwatora, zdolnego m.in. monitorować ruch sieciowy oraz samego sygnalistę, który może m.in. przekazać złośliwe pliki[62].

Specjalistom ds. cyberbezpieczeństwa w identyfikacji zagrożeń pomagają dokumenty ramowe (ang. *frameworks*). Poddając aplikacje dla sygnalistów przeglądowi, niezastąpionym punktem wyjścia do modelowania zagrożeń jest OWASP Top 10, czyli ranking najbardziej krytycznych ryzyk bezpieczeństwa dla aplikacji webowych. Zbiór kluczowych podatności aplikacji to narzędzie, które pomaga organizacji priorytetyzować działania i wydatki związane z zapewnieniem bezpieczeństwa. OWASP Top 10 może być użyteczny jako miernik podatności aplikacji webowych i jako punkt odniesienia do oceny zgodności bezpieczeństwa oprogramowania organizacji m.in. z normami ISO 27001[63].

OWASP korzysta z bardziej rozbudowanej listy podatności CWE (ang. *Common Weakness Enumeration*) stworzonej przez MITRE (*Massachusetts Institute of Technology Research and Engineering*), która obecnie zawiera 940 opisanych słabości, w tym 399 z zakresu rozwoju oprogramowania[64]. CWE podobnie jak OWASP stara się je porządkować publikując własną listę 25 najbardziej niebezpiecznych słabości oprogramowania[65]. Badawczy ośrodek MITRE znany jest też z tego, że doprowadził w 1999 r. do powstania listy publicznie ogłoszonych podatności CVE (ang. *Common Vulnerabilities and Exposures*)[66], które są używane przez OWASP i do której odwołuje się amerykański NIST (*National Institute*

62 J. Uddholm, *Anonymous Javascript Cryptography and Cover Traffic in Whistleblowing Applications*, 2016, s. 7–9, http://www.diva-portal.org/smash/get/diva2:953534/FULLTEXT01.pdf (5.22.2024).

63 Norma międzynarodowa ISO-IEC 27001 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

64 https://cwe.mitre.org/ (4.03.2025).

65 cwe.mitre.org/top25/archive/2023/2023_top25_list.html (13.05.2024).

66 www.cve.org/ (4.03.2025).

of Standard and Technology), prowadząc krajową bazę podatności NVD (*National Vulnerability Database*)[67]. Każdej nowo zgłoszonej podatności przypisuje się w bazie unikalny identyfikator. Lista CVE ma umożliwić szybkie łatanie (ang. *patching*) i aktualizowanie aplikacji w odpowiedzi na zagrożenia, zanim te same informacje zostaną wykorzystane w złej wierze przez adwersarzy[68].

Usługi takie jak platformy dla sygnalistów, zwłaszcza jeżeli służą do wykrywania naruszeń na szkodę interesu publicznego, mogą przyciągać uwagę etycznych hackerów, którzy chcieliby np. sprawdzić czy oprogramowanie nie grozi wyciekiem danych o sygnaliście. W przeciwieństwie do cyberprzestępców, hakerzy w białych kapeluszach (ang. *white-hat hackers*) pomagają wykrywać luki w oprogramowaniu i podatności, kierując się motywacjami finansowymi, uznaniem, możliwością zatrudnienia, ale też działając z wyższych pobudek, z myślą o bezpieczeństwie i prywatności obywateli[69]. Mogą to robić m.in. w ramach skoordynowanego ujawnienia podatności (ang. *Coordinated Vulnerability Disclosure* – CVD), polegającego na bezpośrednim informowaniu producenta oprogramowania o znalezionej w nim wadzie, zanim informacja zostanie ujawniona publicznie. W niektórych przypadkach właściciele systemów IT sami do tego zachęcają, ogłaszając własne polityki CVD, które dzieli się na *Vulnerability Disclosure Programmes* (VDP) oraz *Bug Bounty Programmes* (BBP) – te ostatnie związane z wypłacaniem nagród. Badacze bezpieczeństwa spoza organizacji uzupełniają pracę pentesterów, a ich odkrycia prowadzą do zmiany specyfikacji wymagań bezpieczeństwa lub narzędzi i metod do testowania bezpieczeństwa[70]. Innym rozwiązaniem dostępnym dla białych hakerów, jeżeli dostawcy oprogramowania nie odpowiadają na zgłoszenia, jest zwrócenie się do zaufanej trzeciej strony, która będzie pośredniczyć w kontakcie między badaczami bezpieczeństwa a twórcami aplikacji, tak jak robi to np. CERT Polska[71]. NASK Polska we współpracy z Narodowym Centrum Bezpieczeństwa Holandii wydał poradnik, zawierający m.in. założenia dla krajowej polityki CVD mającej wspierać zgłaszanie podatności[72].

---

67 *Weaknesses in the 2024 CWE Top 25 Most Dangerous Software Weaknesses*, https://cwe.mitre.org/data/definitions/1430.html (4.03.2025).

68 D. G. Graham, *Ethical Hacking. A Hands-on Introduction to Breaking In*, San Francisco 2021, s. 146–147.

69 T. Walshe, A. C. Simpson, *Coordinated Vulnerability Disclosure programme effectiveness: Issues and recommendations*, «Computers & Security» 2022, vol. 123, s. 1, https://www.sciencedirect.com/science/article/pii/S0167404822003285 (10.05.2024).

70 Tamże.

71 https://cert.pl/en/cvd/ (8.05.2024).

72 *Skoordynowane ujawnianie podatności (Coordinated Vulnerability Disclosure, CVD). Poradnik*, s. 26–27, https://cyberpolicy.nask.pl/coordinated-vulnerability-disclosure-cvd-poradnik/ (5.11.2024).

Subkultura hakerska nagradza dzielenie się wiedzą pomiędzy jej członkami, ale już niekoniecznie przekazywanie informacji o podatnościach komercyjnym podmiotom, które nie posługują się rozwiązaniami *open source*[73]. Ma to związek z różnymi reakcjami dużych korporacji na niezlecone testowanie zamkniętego oprogramowania i niekonsekwentnym stosowaniem prawa, które również w Polsce mogą prowadzić do odpowiedzialności karnej etycznych hakerów, jeżeli np. organy ścigania wykażą, że ich działalność przyniosła niedozwolony efekt[74].

Znana jest publicznie historia zgłoszenia błędu na platformie dla sygnalistów[75], z której Komisja Europejska korzysta na potrzeby identyfikowania przypadków obchodzenia sankcji nakładanych w ramach wspólnej polityki zagranicznej i bezpieczeństwa UE[76]. Podatność została zgłoszona przez haktywistę i współzałożyciela GlobaLeaks Giovanniego Pellerano do dostawcy w formie raportu z audytu[77]. Pellerano powiadomił też o niej MITRE, które potwierdziło istnienie podatności XSS polegającej na możliwości wstrzyknięcia złośliwego kodu JavaScript w formularzu aplikacji webowej. W efekcie nadano jej też unikalny kod CVE[78]. Dostawca dzięki zgłoszeniu szybko załatał podatność i w celu poprawy zabezpieczeń zaimplementował dla aplikacji nagłówek HTTP „Content-Security-Policy" (CSP).

Jak pokazano na rysunku 4 sama podatność XSS w ostatnim rankingu OWASP została zaliczona do trzeciej, najczęściej pojawiającej się, klasy błędów bezpieczeństwa. Nierozwijanie aplikacji webowych pod względem zabezpieczeń przed cyberatakami jest też widocznym znakiem braku świadomości o podatnościach, które zostały sklasyfikowane w rankingu OWASP na innych pozycjach. Moim zdaniem w szczególności należy w tym kontekście zwrócić uwagę na błędy przy stosowaniu technik kryptograficznych lub zupełne ich pomijanie, np. przechowywanie haseł użytkowników w formie jawnego tekstu[79]. Pozycja siódma związana z wadliwym mechanizmem identyfikacji

---

73 M. Weulen Kranenbarg, T. J. Holt, J. van der Ham, *Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure*, «Crime Science» 2018, nr 7, s. 4, https://research.utwente.nl/en/publications/dont-shoot-the-messenger-a-criminological-and-computer-science-pe (16.05.2024).

74 *Skoordynowane ujawienie podatności (Coordinated Vulnerability Disclosure, CVD). Poradnik*, NASK 2022, s. 10–12, https://cyberpolicy.nask.pl/wp-content/uploads/2022/09/CyberPolicy_Poradnik_CVD.pdf (3.06.2024).

75 https://eusanctions.integrityline.com/frontpage (8.05.2024).

76 *The Pitfalls of Closed-Source…*

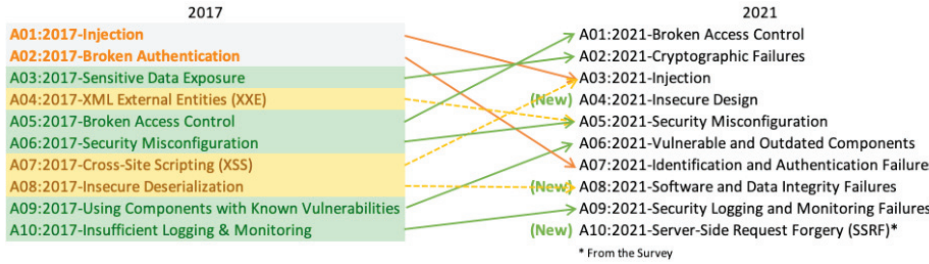
77 https://www.ush.it/team/ush/advisory-eqs-integrity-line/eqs_integrity_line.txt (20.05.2024).

78 https://nvd.nist.gov/vuln/detail/CVE-2022-34007 (1.06.2024).

79 Zob. Ł. Basa, W. Sędkowski, *Modelowanie zagrożeń i analiza ryzyka aplikacji*, [w:] M. Sajdak (red.), *Wprowadzenie…*, s. 383–384.

i uwierzytelniania użytkowników także wydaje się kluczowa, gdyż obszar ataku w aplikacjach dla sygnalistów jest szczególnie duży, a konsekwencje dla poufności niezwykle groźne. Nie zmienia to faktu, że programiści tworzący kod aplikacji dla sygnalistów, a później dostawcy odpowiadający za ich rozwój i wdrożenie powinni brać pod uwagę wszystkie dziesięć najczęstszych kategorii błędów według OWASP.

Rysunek 4. Zmiany w rankingu OWASP Top 10 pomiędzy edycjami z lat 2017 i 2021



Źródło: https://owasp.org/Top10/ (28.05.2024).

Formułowanie wymagań dla dostawców aplikacji

Ustawa dopuszcza upoważnienie podmiotu trzeciego do obsługi zgłoszeń wewnętrznych w organizacji na podstawie osobnej umowy o świadczeniu usług. Nie uchyla to jednak odpowiedzialności podmiotu zobowiązanego za wdrożenie procedury zgodnie z Ustawą, w tym za zachowanie poufności zgłoszeń. Dlatego decydując się na subskrybowanie platformy dla sygnalistów organizacja najlepiej zadba o swój interes prawny, jeżeli w kryteriach wyboru dostawcy znajdą się odpowiednie wymagania bezpieczeństwa i sposoby ich rozliczalności. Do podobnych wniosków dojdziemy odwołując się do regulacji o ochronie danych osobowych. To na administratorze spoczywa obowiązek wcześniejszej weryfikacji dostawcy aplikacji, który staje się w tym układzie procesorem danych[80].

Organizacje często dokonują sprawdzenia dostawców za pomocą ankiet bezpieczeństwa przetwarzania danych osobowych. Innym sposobem jest zaufanie certyfikatom, opisującym działalność dostawców w zakresie wytworzenia i utrzymania aplikacji. Najbardziej adekwatne w tym kontekście są certyfikaty ISO 27001 (zarządzanie bezpieczeństwem informacji), ISO 27018 (bezpieczeństwo danych w chmurze), ISAE 3000 (atestacja niefinansowych danych

[80] Zob. P. Kawczyński, *Ocena podmiotu przetwarzającego jako podstawa do powierzenia przetwarzania danych osobowych*, «Magazyn ODO» 2023, nr 23, s. 13.

przedsiębiorstw) lub SOC 2 (amerykański standard bezpieczeństwa informacji). Choć nie stanowią jeszcze gwarancji, że żaden incydent bezpieczeństwa się nie wydarzy, to z pewnością podnoszą wiarygodność dostawców, a przez to budują zaufanie cyfrowe i pomagają przekonać pracowników do korzystania z bezpiecznych narzędzi[81]. Twórców aplikacji webowej będzie też uwiarygadniała dodatkowa techniczna certyfikacja obejmująca jej elementy takie jak biblioteki kryptograficzne. W tym aspekcie możliwe jest uzyskanie certyfikacji FIPS (*Federal Information Processing Standards*) na normy zabezpieczeń technologii informatycznych i komputerów, które prowadzi NIST i które zostały zatwierdzone przez amerykański rząd. Komisja Europejska, która w 2024 r. uruchomiła kolejne dwa kanały dla sygnalistów do zgłaszania naruszeń w zakresie nowych rozporządzeń: aktu o usługach cyfrowych i aktu o rynkach cyfrowych, może wyznaczyć kolejne trendy w certyfikacji. Ogłoszono bowiem, że nowe kanały są nie tylko szyfrowane, ale też certyfikowane przez niezależną trzecią stronę[82]. Z komunikatu nie wynika, co to dokładnie oznacza. Wybór dostawcy aplikacji do *whistleblowing*-u dla podmiotów administracji publicznej ze względu na ochronę publicznego interesu będzie wymagać co najmniej zapewnienia, że zbierane dane są przechowywane na serwerach w Polsce. Dodatkowo należałoby wyeliminować zagrożenie, że podmioty, które świadczą takie usługi, w szczególności w modelu *SaaS*, nie znajdują się pod kontrolą wrogich państw.

Koniecznym elementem do ustalenia między dostawcą a klientem aplikacji w wypadku usługi chmurowej jest SLA (*Service Level Agreement*). Porozumienie to najczęściej definiuje zakres czasowej niedostępności aplikacji, która jest akceptowalna przez obie strony, przyczyny usprawiedliwionej niedostępności, informowanie i reagowanie w sytuacji planowanego i nieplanowanego braku dostępu. Dochowanie tych ustaleń jest w interesie sygnalistów, gdyż aplikacja co do zasady powinna umożliwiać im dokonanie zgłoszenia przez całą dobę siedem dni w tygodniu. W sytuacjach skrajnych, nawet krótki problem z dostępem do aplikacji spowoduje, że sygnalista zrezygnuje ze zgłoszenia lub nadane zgłoszenie nie dotrze do administratora. W interesie klientów aplikacji jest z kolei, aby poszerzyć zakres SLA o zarządzanie incydentami lub ryzykami dla bezpieczeństwa, np. poprzez wymóg wcześniejszego informowania przez dostawcę o planowanych modyfikacjach aplikacji, które mogą wpłynąć na jej bezpieczeństwo[83].

---

81 P. M. Asprion, H. Grieder, F. Grimberg, *Building Digital Trust*…, s. 4329.

82 *Commission launches Whistleblower Tools for Digital Services Act and Digital Markets Act*, 30.04.2024, https://digital-strategy.ec.europa.eu/en/news/commission-launches-whistleblower-tools-digital-services-act-and-digital-markets-act (20.05.2024).

83 Por. E. Hansen, *Internal SLA (Service Level Agreement) for Information Security*, SANS Institute 2001, https://sansorg.egnyte.com/dl/ROZN7Fbvrb (5.06.2024).

Ważne jest, czy i komu dostawca aplikacji będzie podpowierzał dane osobowe w celu zapewnienia hostingu, utrzymania serwerów czy prac programistycznych[84]. Subprocesorzy mogą okazać się słabym ogniwem w łańcuchu bezpieczeństwa, dlatego klient aplikacji powinien być poinformowany, w jaki sposób bezpieczeństwo przetwarzania danych jest przez nich gwarantowane i czy istnieje możliwość wycofania się dostawcy ze współpracy z podwykonawcą, który doprowadził do incydentu.

Na podstawie motywu 81 RODO w wytycznych Europejskiej Rady Ochrony Danych (EROD) wskazuje się, że w wyborze procesora administrator powinien kierować się jego wiedzą fachową, w tym wiedzą techniczną w zakresie środków bezpieczeństwa i naruszeń ochrony danych, wiarygodnością podmiotu przetwarzającego i jego zasobami. EROD jako dodatkowe kryterium wskazuje też reputację procesora na rynku[85].

Rozliczalność wymogów

Zgodnie z wytycznymi EROD administrator nie powinien poprzestawać na jednorazowym zweryfikowaniu podmiotu przetwarzającego przed zawarciem umowy, ale ponawiać audyty i inspekcje już w trakcie jej trwania w odpowiednich odstępach czasu[86]. Audytu strony drugiej klient może dokonywać samodzielnie lub zlecając podmiotowi zewnętrznemu przeprowadzenie czynności audytowych u dostawcy. Dostawcy mogą podlegać też audytowi strony trzeciej przez niezależną jednostkę certyfikującą. Jeżeli taki audyt traktować jako poświadczenie wiarygodności danej aplikacji, w szczególności istotne jest, żeby był realizowany przez organizację audytorską lub ośrodek rządowy, któremu nie można postawić zarzutu konfliktu interesów. Jeszcze inną formą weryfikowania, czy korzystanie z aplikacji nie powoduje ryzyka naruszeń prawa, może być skontrolowanie dostawcy przez regulatora albo inny organ publiczny, np. UODO, który na lata 2023–2024 zapowiadał kontrole wobec podmiotów przetwarzających dane osobowe przy użyciu aplikacji internetowych[87].

Po stronie dostawcy aplikacji jest zadbanie o to, żeby przechodziła regularne testy penetracyjne. Jason Andress zwraca uwagę, że testy penetracyjne

84 P. Kawczyński, *Ocena podmiotu*…, s. 14.

85 *Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO*, European Data Protection Supervisor, 2021, s. 35, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf (13.05.2024).

86 Tamże, s. 35.

87 *Plan kontroli sektorowych UODO na 2024 r.*, https://uodo.gov.pl/pl/138/2986 (15.05.2024).

aplikacji są bardziej wymagające aniżeli testy penetracyjne sieci, gdyż do ich przeprowadzenia potrzeba bardziej wyspecjalizowanych narzędzi i umiejętności[88]. Wymienia też dwie możliwe techniki przeprowadzania takich testów. Pierwszą jest analiza statyczna (ang. *static analysis*), która polega na analizie kodu źródłowego w celu znalezienia luk i podatności przez pentesterów biegłych w językach programowania. Druga to analiza dynamiczna (ang. *dynamic analysis*), czyli testowanie aplikacji w działaniu, z wykorzystaniem oprogramowania znajdującego luki w zabezpieczeniach (ang. *exploit*). W przypadku aplikacji *open source* testowanie kodu źródłowego jest w zasadzie opcją domyślną.

Podobnie jak w przypadku audytów, o wiarygodności pentestów świadczyć będzie informacja, czy ich wykonawca potrafi wykazać niezbędne kompetencje oraz czy udzielenie mu dostępu do infrastruktury aplikacji nie rodzi ryzyka skompromitowania informacji o zgłaszanych naruszeniach. Inny dylemat może dotyczyć tego, czy w każdej sytuacji za bezstronnego kontrolera należy uznać np. ośrodek rządowy lub inny zależny od władzy politycznej, który poddawałby testom oprogramowanie wykorzystywane w podmiotach publicznych.

Na koniec należy dodać, że choć odpowiedzialność za dostarczenie bezpiecznego i rozliczalnego systemu leży po stronie dostawcy, to edukowanie pracowników, w jaki sposób korzystać z dostępnych narzędzi jest zadaniem ich macierzystej organizacji. W jej interesie jest prowadzić działania zwiększające zaufanie do platform internetowych dla sygnalistów i tłumaczenie w jaki sposób chronią informacje. Niektóre projekty ustawy o ochronie osób zgłaszających naruszenia prawa zachęcały do uświadamiania pracowników na temat zasad korzystania z systemów informatycznych, które zabezpieczą poufność ich zgłoszenia[89]. Zapis, który uzasadniał podejmowanie akcji informacyjnych na temat ochrony tożsamości sygnalistów w sieci, finalnie nie znalazł się w Ustawie[90]. Jednakże patrząc od strony interesu organizacji jest to cenna podpowiedź, gdyż cykliczna edukacja pomaga pracowników nabierać przekonania do narzędzi wdrażanych przez pracodawcę i redukuje potrzebę poszukiwania alternatywnych, czasem dużo mniej bezpiecznych ścieżek zgłaszania naruszeń w miejscu pracy.

---

88 J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Gliwice 2022, s. 227–238.

89 Art. 25 ust. 2 p. 4 projektu ustawy o ochronie osób zgłaszających naruszenia prawa z dnia 6 lutego 2023 r., https://www.legislacja.gov.pl/projekt/12352401/katalog/12822845#12822845 (13.05.2024).

90 Z podobnych kampanii znane były do tej pory organizacje pozarządowe. Zob. *Cybersecurity: Whistleblower Best Practices*, National Whistleblower Center, https://www.whistleblowers.org/wp-content/uploads/2019/05/Cybersecurity-Best-Practices.pdf (13.05.2024).

Zakończenie

Aplikacje do zgłaszania naruszeń nie doczekały się do tej pory jednego standardu bezpieczeństwa, który mógłby być obowiązujący dla wszystkich dostawców. Wpływ na to ma z pewnością stosunkowo krótki okres rozwoju takiego oprogramowania i to dodatkowo w nie zawsze spójnych kierunkach – z jednej strony jako narzędzia do dokonywania ujawnień naruszeń do opinii publicznych, z drugiej jako kanału zgłaszania wewnątrz organizacji. Intensywny rozwój technologii kwantowej i nowe podatności rozpoznawane w aplikacjach webowych stawiają przed twórcami kolejne dylematy bezpieczeństwa. Uwarunkowania te sprzyjają dużemu zróżnicowaniu oferty dostawców pod względem zakresu usług, poziomu bezpieczeństwa i mechanizmów, które mają je zapewniać.

Autorzy aplikacji deklarują wykorzystywanie najbardziej zaawansowanych technologii, w tym autorskich protokołów kryptograficznych, blockhaina i algorytmów postkwantowych. Należy podchodzić do takich deklaracji z pewną ostrożnością, gdyż zdarza się, że dotyczą nigdy niewdrożonych prototypów aplikacji lub ofert, które nie zostały do tej pory zweryfikowane przez rynek. Dlatego niezwykle ważnym aspektem standardów bezpieczeństwa dla aplikacji jest wymóg ich rozliczalności. W oprogramowaniu, które nie jest regularnie poddawane testom lub dostawca nie przedstawia na to żadnych dowodów, może nie udać się w porę wykryć i usunąć wszystkich luk bezpieczeństwa. Przytrafiło się to już w przypadku kanału obsługiwanego przez Komisję Europejską. W interesie dostawców, odbiorców aplikacji, ich użytkowników i samych sygnalistów jest to, żeby narzędzia te służyły minimalizowaniu ryzyka naruszeń i same nie stawały się dodatkowym, dobrze nierozpoznanym jeszcze źródłem ryzyk.

Bibliografia

Ahmed-Rengers M., Vasile D. A., Hugenroth D., Beresfold A. R., Anderson R., *CoverDrop: Blowing the Whistle Through A News App*, «Proceedings on Privacy Enhancing Technologies» 2022, nr 2 – https://petsymposium.org/popets/2022/popets-2022-0035.pdf (8.05.2024).

Andress J., *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Gliwice 2022.

Asprion P. M., Grieder H., Grimberg F., *Building Digital Trust to Protect Whistleblowers – A blockchain-based Reporting Channel*, "Proceedings of the 56th Hawaii International Conference on System Sciences" 2023, https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/cce23d75-65ac-4c6f-9104-f800bfcc58ff/content (8.05.2024).

Baran B., Ożóg M. (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021.

Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszaw 2023.

Berendt B., Schniffer S., *Whistleblower protection in the digital age – why "anonymous" is not enough? From technology to a wider view of governance*, «International Review of Information Ethics» 2022, vol. 31, https://informationethics.ca/index.php/irie/article/view/479/440 (28.05.2024).

Brevini B., Hintz A., McCurdy P. (red.), *Beyond WikiLeaks. Implications for the Future of Communications, Journalism and Society*, Hampsire 2013.

Brown A. J. et al., *Clean as a whistle: a five step guide to better whistleblowing policy and practice in business and government*, Brisbane 2019, http://www.whistlingwhiletheywork.edu.au/wp-content/uploads/2019/08/Clean-as-a-whistle_A-five-step-guide-to-better-whistleblowing-policy_Key-findings-and-actions-WWTW2-August-2019.pdf (19.05.2024).

Colvin N., Nad V., Culnane C., Galizzi B., Dreyfus S., *Expanding anonymous tipping technology in Europe*, Blueprint for Free Speech 2021, https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/60fee180f7b25d77581c6f98/1627316617173/Expanding+Anonymous+Tipping+in+Europe_EAT.pdf (4.03.2025).

Di Salvo P., *Digital Whistleblowing Platforms in Journalism. Encrypting Leaks*, Cham 2020.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

Graham D. G., *Ethical Hacking. A Hands-on Introduction to Breaking In*, San Francisco 2021.

Gumularz M., *Sygnaliści: w grupie podmiotów jeden system zgłaszania naruszeń*, 07.03.2024, https://www.rp.pl/prawo-pracy/art39949501-sygnalisci-w-grupie-podmiotow-jeden-system-zglaszania-naruszen-prawa (19.05.2024).

Hansen E., *Internal SLA (Service Level Agreement) for Information Security*, SANS Institute 2001, https://sansorg.egnyte.com/dl/ROZN7Fbvrb (5.06.2024).

Javakrishnan H., Murali R., *A Simple and Robust End-to-End Encryption Architecture for Anonymous and Secure Whistleblowing*, Twelfth International Conference on Contemporary Computing (IC3), 2019, https://ieeexplore.ieee.org/document/8844917 (8.05.2024).

Jenkins M., *Overview of whistleblowing software*, Transparency International, 2020, https://knowledgehub.transparency.org/helpdesk/overview-of-whistleblowing-software (4.11.2024).

Kawczyński P., *Ocena podmiotu przetwarzającego jako podstawa do powierzenia przetwarzania danych osobowych*, «Magazyn ODO» 2023, nr 23.

Lake J., *What is plausible deniability (in encryption) and does it really work?*, 08.01.2024, https://www.comparitech.com/blog/information-security/plausible-deniability-encryption/ (18.05.2024).

Lowry P. B., Moody G. D., Galletta D., Vance A., *The Drivers in the Use of Online Whistle-Blowing Reporting Systems*, «Journal of Management Information Systems» 2013, vol. 30(1).

Makowicz B., Jagura B. (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*, Warszawa 2020.

Mroczyński-Szmaj Ł., *Nowe europejskie prawo sygnalizowania nieprawidłowości. Rozwiązania modelowe a polski projekt ustawy o ochronie osób zgłaszających naruszenia prawa*, «Prawo w działaniu» 2022, nr 52, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_32041_pwd_5209 (9.05.2024).

Rosenblatt S., *NSA likely targets anybody who's "Tor-curious"*, 03.07.2013, https://www.cnet.com/news/privacy/nsa-likely-targets-anybody-whos-tor-curious/ (20.05.2024).

Roth V., Güldenring B., Rieffel E., Dietrich S., Ries L., *A Secure Submission System for Online Whistleblowing Platforms*, 29.01.2013, http://arxiv.org/pdf/1301.6263 (17.05.2024).

Sajdak M. (red.), *Bezpieczeństwo aplikacji webowych*, Kraków 2021.

Sajdak M. (red.), *Wprowadzenie do bezpieczeństwa IT*, Kraków 2023.

Uddholm J., *Anonymous Javascript Cryptography and Cover Traffic in Whistleblowing Applications*, 2016, http://www.diva-portal.org/smash/get/diva2:953534/FULLTEXT01.pdf (5.11.2024).

Walshe T., Simpson A. C., *Coordinated Vulnerability Disclosure programme effectiveness: Issues and recommendations*, «Computers & Security» 2022, vol. 123, https://www.sciencedirect.com/science/article/pii/S0167404822003285 (10.05.2024).

Weulen Kranenbarg M., Holt T. J., van der Ham J., *Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure*, «Crime Science» 2018, nr 7, https://research.utwente.nl/en/publications/dont-shoot-the-messenger-a-criminological-and-computer-science-pe (16.05.2024).