CYBERSECURITY FOUNDATION

Porównanie rozwiązań dla Sygnalistów

pod względem zgodności z dobrymi praktykami bezpieczeństwa i ochroną danych osobowych

Październik 2022

na skróty

I Obowiązek wdrożenia procedur ochrony sygnalistów

Wdrożenie oprogramowania do ochrony sygnalistów jest obowiązkowe w sektorze publicznym, instytucjach finansowych, a także w firmach zatrudniających co najmniej 250 pracowników. Od roku 2023 obejmie dodatkowo wszystkich przedsiębiorców, którzy zatrudniają minimum 50 pracowników. Zatem podmioty te są zobowiązane do wdrożenia rozwiązania, które umożliwi zgłaszanie i rozstrzyganie nieprawidłowości. Tożsamość osób raportujących musi być chroniona prawnie[1] – należy im oraz osobom trzecim wymienionym w zgłoszeniu zapewnić poufność danych osobowych i dochować zasady minimalizacji tj. nie przetwarzać więcej danych osobowych niż jest to konieczne w danej sprawie.

Producenci rozwiązań dla sygnalistów, którzy zostali zaprezentowani w tym raporcie, muszą spełniać szereg nakładanych na nich regulacji, by zachować zgodność z unijną dyrektywą (2019/1937 [2]) i krajową ustawą, której zakres regulują indywidualnie państwa członkowskie Unii Europejskiej. Dyrektywę stosuje się do osób dokonujących zgłoszenia, które uzyskały informacje na temat naruszeń w kontekście związanym z pracą. Dyrektywę stosuje się także do osób, co do których ustał stosunek pracy lub zostanie dopiero zawiązany.

Państwa członkowskie, w kwestii zachowania poufności danych osobowych osób zgłaszających, będą ustalać czy podmioty prawne w sektorze prywatnymi publicznym oraz właściwe organy, mają obowiązek przyjmowania anonimowych zgłoszeń i podejmowania działań następczych. Dla osób, które dokonały anonimowego zgłoszenia, będzie obowiązywać zasada ochrony przed działaniami odwetowymi ze strony pracodawcyi pracowników (dyskryminacją i zwolnieniem).

Z założenia nieefektywne jest korzystanie z bezpiecznego oprogramowania, jeżeli będzie ono trudne we wdrożeniu i problematyczne w utrzymaniu. Zatem dodatkową wartością charakteryzują się systemy dla sygnalistów, które łączą bezpieczeństwo i produktywność – nie wymagają do obsługi wydelegowania pracownika o technicznych umiejętnościach. Najrozsądniejszy może być wybór oprogramowania w chmurze, ponieważ na producencie spoczywa odpowiedzialność za aktualizację, jak również zapewnienie dostępu do usługi i zabezpieczenie aplikacji.

Raport ten skierowany do osób decyzyjnych, które chciałyby dowiedzieć się więcej o spełnianiu podstawowych norm bezpieczeństwa uważanych w branży za niezbędne minimum w rozwiązaniach do obsługi sygnalistów. Zatem, jeśli to opracowanie czyta sygnalista, który chce pozostać anonimowy, to więcej pomocnych informacji może znaleźć na oficjalnej stronie internetowej [3] Unii Europejskiej poświęconej ochronie sygnalistów.

[1] https://www.parp.gov.pl/component/content/article/82333:sygnalisci-w-kontekscie-ochrony-danych-osobowych

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019L1937

[3] https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en

II Główne informacje o producentach systemów

Producentem systemu w chmurze (SaaS) jest SpecFile Project sp. z o.o. ze wsparciem języka polskiego, angielskiego, niemieckiego oraz 9 innych języków europejskich. Posiada szeroki zakres uprawnień i automatycznych odpowiedzi. System można testować przez 14 dni przed zakupem. Używa najbezpieczniejszej metody szyfrowania Client-Side Encryption, a jego cena zależy od ilości osób obsługujących zgłoszenia.

Producentem systemu jest BTC Sp. z o.o udostępnianego w modelach SaaS oraz On-premises. Zapewnia wsparcie serwisowe oraz język interfejsu w kilku językach z dostępnością kolejnych na zamówienie. System posiada API dla zewnętrznych usług, możliwość integracji z aplikacjami helpdeskowymi, a także z Microsoft Active Directory i Microsoft Azure Role-Based Access Control.

Aplikacja firmy E-nform sp. z o.o. jest dostępna w chmurze (SaaS) oraz do wdrożenia lokalnego (on-premises). Wspiera 12 języków obcych z możliwością zaimplementowania dowolnej wersji językowej. Dysponuje rozbudowanym procesem zaproszeń osób trzecich w roli eksperta, nadawaniem uprawnień koordynatorom oraz funkcjami zarządzania danymi osobowymi.

Rozwiązanie o publicznym kodzie jest finansowane z grantów amerykańskiego funduszu Open Technology Fund, holenderskiej fundacji Hivos oraz projektów ds. rozwoju demokracji Unii Europejskiej. Wspiera język angielski oraz inne tłumaczenia maszynowe. System jest dostępny do wdrożenia lokalnego (on-premises). Obsługuje sieć Tor, by zapewnić anonimowość i posiada certyfikat ISO 37002:2021.

Producent SafeLink Sp. z o.o. dostarcza oprogramowanie w chmurze (SaaS) w języku polskim oraz angielskim. W takim wdrożeniu klient końcowy nie ponosi odpowiedzialności za aktualizacje oraz zabezpieczenie serwera. System umożliwia przesyłanie anonimowego zgłoszenia poprzez e-mail i transkrypcję z połączenia telefonicznego.

Od 2013 roku rozwojem SecureDrop kieruje Freedom of the Press Foundation, a wcześniej projekt nosił nazwę DeadDrop. Wspierany jest tylko język angielski. Oprogramowanie zaprojektowano w modelu privacy-by-design do wdrożenia lokalnego (on-premises). Do obsługi wymagane jest połączenie przez sieć sieć Tor oraz dystrybucja systemu Linux Tails.

III Porównywane cechy oprogramowania

1. Model udostępniania oprogramowania.
2. Kanał sygnalizowania nieprawidłowości.
3. Zabezpieczenie przed intruzami logowania do systemu dla administratorów, osób nadzorujących, sygnalistów.
4. Wybrany przez producenta rodzaj szyfrowania kryptograficznego.
5. Metoda szyfrowania danych i zgłoszenia na serwerze.
6. Sposób uzyskiwania dostępu do zgłoszenia (deszyfrowania).
7. Ochrona tożsamości sygnalisty – analiza ryzyka dostępu do metadanych załączników przez producenta systemu.
8. Inne metody zapewnienia anonimowość sygnalisty dla pracodawcy i producenta aplikacji.
9. Ocena ryzyka cyberataku na infrastrukturę serwera systemu albo użytkownika aplikacji.
10. Maksymalna ilość osób nadzorujących zgłoszenia.
11. Delegowanie spraw pomiędzy odbiorcami zgłoszenia i zarządzanie uprawieniami w systemie.
12. Automatyzacja pracy: predefiniowane wzorce automatycznych odpowiedzi oraz komunikaty systemowe.
13. Zapewnienie generowania cyklicznych raportów.
14. Logi wszystkich operacji dokonywanych w zgłoszeniu (pełna historia).
15. Wybrane przez AVLab cechy unikatowe oprogramowania.

1. Model udostępniania oprogramowania

GLOBALEAKS

SECUREDROP

ehelpdesk

e-nform

Sygnanet

SafeLink

Oprogramowanie do wdrożenia lokalnego na serwerze (on-premises) niesie ze sobą konieczność wykonywania aktualizacji oraz dodatkowego zabezpieczenia serwera. Zwykle wymagana jest znajomość środowiska Linux / Windows oraz jego administrowanie: utrzymywanie aktualizacji oraz testowanie nowych wersji przed wdrożeniem na serwerze produkcyjnym.

W tym modelu (Software as a Service) odpowiedzialność za użytkowanie oprogramowania w chmurze jest przenoszona na producenta. Klient końcowy nie musi przejmować się aktualizacjami oraz zabezpieczeniem serwera, jak również dostępnością systemu przez przeglądarkę w połączeniu internetowym.

2. Kanał sygnalizowania nieprawidłowości

Sygnanet	Poprzez przeglądarkę z komentarzem oraz dodanymi załącznikami. Możliwość zdefiniowania adresu URL dedykowanego dla odbiorcy.
ehelpdesk	Poprzez przeglądarkę z komentarzem oraz dodanymi załącznikami. Możliwość zdefiniowania wielu różnych adresów URL, dowolnie definiowanych z personalizowaną zawartością strony docelowej np. w zależności od rodzaju i typu zgłoszenia. Możliwość uzupełniania zgłoszenia oraz korespondencji z organem.
e-nform	1. Poprzez przeglądarkę z komentarzem oraz dodanymi załącznikami. Możliwość zdefiniowania różnych adresów URL (dostarczonych przez E-nform lub Zamawiającego), personalizowane rodzaje i typy zgłoszeń w zakresie zależnym rodzaju licencji (predefiniowane typy lub dowolna konfiguracja ustalana z Zamawiającym) . 2. Możliwość zintegrowania adresu mailowego z systemem E-nform, co powoduje, że zgłoszenia wysłane na konkretny adres e-mail są przesyłane do bazy danych w systemie, a następnie kategoryzowane przez administratora z uwagi na powielanie/dublowanie elektronicznej formy zgłaszania naruszeń.
GLOBALEAKS	Poprzez przeglądarkę z komentarzem oraz dodanymi załącznikami.
SafeLink	1. Poprzez przeglądarkę z komentarzem oraz dodanymi załącznikami. 2. Poprzez transkrypt z nagrania telefonicznego pod specjalnym numerem telefonu (inny numer dla każdego wdrożenia). System nie przekaże pracodawcy informacji na temat numeru, z którego przyszło połączenie – informacje te nie są nigdzie ewidencjonowane. Aby otrzymać odpowiedź należy podać dane kontaktowe, które mogą zidentyfikować Sygnalistę, dlatego należy używać tego kanału w wyjątkowych okolicznościach. 3. Poprzez wiadomość na specjalny adres e-mail, podając swój identyfikator i hasło. Przekazywana jest tylko treść zgłoszenia. System nie przekazuje informacji na temat adresu e-mail, z którego przyszło zgłoszenie – informacje te nie są nigdzie ewidencjonowane. Podanie danych osobowych i preferowanej formy kontaktu w treści wiadomości pozwoli Osobom Nadzorującym na kontakt ze Zgłaszającym. Korzystając ze zgłoszenia przez e-mail brak jest możliwości monitorowania zgłoszenia. Korzystanie z tego kanału zgłoszeniowego zalecane jest w wyjątkowych przypadkach.

SECUREDROP	Poprzez przeglądarkę w wiadomości tekstowej wraz z załączonym komentarzem, opisem zgłoszenia oraz wypełnonym formularzem.	

3. Zabezpieczenie przed intruzami logowania do systemu dla administratorów, osób nadzorujących, sygnalistów.

Ocena aplikacji: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Sygnanet	1. Administrator i Osoba Nadzorująca – logowanie odbywa się po podaniu loginu oraz hasła. Logowanie dwuskładnikowe jest obsługiwane. 2. Sygnalista – po utworzeniu zgłoszenia generowany jest unikalny numer ID oraz tajne hasło przypisane do zgłoszenia.	+
ehelpdesk	Administrator oraz Osoba Nadzorująca – uwierzytelnienie dwuskładnikowe (login + hasło + certyfikat na bazie infrastruktury klucza publicznego). Sygnalista nie loguje się do systemu. Uzyskuje dostęp do zgłoszenia na bazie unikalnego identyfikatora	+

e-nform	Administrator i Osoba Nadzorująca – logowanie 2FA za pomocą aplikacji generujących jednorazowe tokeny np. Google Authenticator. Możliwe jest wykonanie integracji z korporacyjnymi systemami uwierzytelniania użytkowników: protokół LDAP lub framework OAuth. Sygnalista – uzyskuje dostęp do zgłoszenia poprzez identyfikator zgłoszenia (ID) oraz przypisany numer PIN. Dodatkowo sygnalista może założyć w systemie Anonimowe Konto, podając wybrany przez siebie login oraz hasło (wówczas dostępne jest 2FA). Przy zakładaniu konta może także dodać bezpieczny adres e-mail, który ewentualnie może pomóc w odzyskaniu hasła do swojego konta. Po założeniu takiego konta i zalogowaniu Sygnalista może przypisać do niego wcześniejsze zgłoszenia (podając ich ID i PIN).	
GLOBALEAKS	1. Aktywacja białej listy zaufanych adresów IP dla administratorów i wybranych ról użytkowników w systemie. 2. Możliwość aktywacji dostępności panelu dla Użytkowników systemu i Sygnalistów wyłącznie przez adres w sieci Tor (automatyczne generowanie domeny .onion). 3. Uprawnione Osoby Nadzorujące oraz Administratorzy mogą się logować do systemu za pomocą loginu, hasła oraz mechanizmu logowania 2FA za pomocą kodu TOTP (z aplikacji generującej jednorazowe kody np. Google Authenticator, Microsoft Authenticator, FreeOTP). 4. Sygnalista nie posiada swojego konta — uzyskuje dostęp do zgłoszeń dzięki wcześniej przypisanymu numerowi ID (16-cyfrowy kod).	
SafeLink	Administrator i Osoba Nadzorująca wykorzystuje login i hasło. Sygnalista po wysłaniu nieprawidłowości otrzymuje indywidualny login i hasło przypisany do zgłoszenia. Producent planuje wdrożyć dwuskładnikowe uwierzytelnienie.	
SECUREDROP	Administrator, Osoba Nadzorująca i Sygnalista: Logowanie do systemu musi być zabezpieczone loginem, hasłem oraz opcjonalnie tokenem HOTP z dwuskładnikowego uwierzytelnienia np. kluczem Yubikey albo tokenem z aplikacji generującej kody TOTP np. Microsoft Authenticator, Google Authenticator, FreeOTP.	

4. Wybrany przez producenta rodzaj szyfrowania kryptograficznego

Ocena aplikacji: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Sygnanet	Client-Side Encryption Szyfrowanie zgłoszenia jest realizowane kryptograficznie przed wysłaniem na serwer wszystkich danych oraz załączników w przeglądarce Sygnalisty kluczami generowanymi przez aplikację metodą end-to-end. Szyfrowanie na urządzeniu Sygnalisty jest bezpieczniejszą metodą, niż szyfrowanie na serwerze.	✚
ehelpdesk	Brak	!
e-nform	Server-Side Encryption Szyfrowanie danych odbywa się w pamięci serwera po ich dostarczeniu do aplikacji.	−
GLOBALEAKS	Server-Side Encryption Szyfrowanie danych odbywa się w pamięci serwera po ich dostarczeniu do aplikacji.	−
SafeLink	Server-Side Encryption Szyfrowanie danych odbywa się w pamięci serwera po ich dostarczeniu do aplikacji.	−
SECUREDROP	Server-Side-Encryption Szyfrowanie danych realizowane jest przy użyciu kluczy Sygnalistów i odbywa się w pamięci serwera po utworzeniu zgłoszenia.	−

5. Metoda szyfrowania danych na serwerze

Ocena aplikacji: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Sygnanet	Treść zgłoszenia oraz załączniki są umiejscowione w bazie danych aplikacji na serwerze w postaci zaszyfrowanej (zastosowano kryptografię klucza publicznego RSA o długości klucza 4096 bitów).	
ehelpdesk	Treść zgłoszenia oraz załączniki trafiają do bazy danych i nie są szyfrowane.	
e-nform	Treść zgłoszeń, wiadomości i załączniki są szyfrowane po stronie serwera aplikacji (AES-256).	
GLOBALEAKS	Szyfrowanie zgłoszenia realizowane jest za pomocą kryptografii krzywej eliptycznej (ECC Curve25519) i w takiej postaci jest zapisywane w bazie danych.	
SafeLink	Wszystko co znajduje się na serwerze jest szyfrowane: treść zgłoszenia, wiadomości od Sygnalisty i odpowiedzi pracodawcy, załączniki, notatki, dane osobowe Sygnalisty itp. Producent wykorzystuje do tego algorytm RSA-4096. W przypadku załączników do zgłoszeń wykorzystuje się AES-256.	
SECUREDROP	Do szyfrowania danych Sygnalisty zastosowano asymetryczny algorytm kryptograficzny z kluczem publicznym RSA. Zgłoszenie szyfrowane jest po wysłaniu na serwer. Dopuszczalne są długości klucza 2048 albo 4096 bitów.	

6. Sposób uzyskiwania dostępu do zgłoszenia (deszyfrowanie)

Ocena aplikacji: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Sygnanet	Deszyfracja następuje po wprowadzeniu hasła/ID zgłoszenia w przeglądarce przez Sygnalistę. Natomiast Osoba Nadzorująca uzyskuje dostęp do zaszyfrowanych zgłoszeń po wprowadzeniu swojego unikalnego hasła w panelu logowania.	+
ehelpdesk	Dane nie są zaszyfrowane w bazie danych, jednak dostęp do nich uwarunkowany jest uprawnieniami użytkownika (login, hasło + opcjonalnie klucz PKI). Dostęp do zgłoszenia następuje po zalogowaniu.	+
e-nform	Treść zgłoszeń, wiadomości i załączniki są odszyfrowywane wcześniej utworzonym kluczem po wysłaniu przez uwierzytelnionego użytkownika żądania na serwer aplikacji szyfrowanym protokołem HTTPS (TLS 1.2 lub TLS 1.3). W zależności od wdrożenia klucz szyfrowany jest na serwerze aplikacji (on-premise) lub w kontenerze Microsoft Azure Key Vault (SaaS).	+
GLOBALEAKS	1. Administrator i osoba nadzorująca zgłoszenie uzyskuje dostęp do systemu poprzez login i hasło, a także opcjonalne zabezpieczenie w postaci kodów TOPT (mechanizm logowania 2FA). 2. Sygnalista uzyskuje dostęp do zgłoszenia po wpisaniu wygenerowanego losowo wcześniej 16-cyfrowego numeru zgłoszenia. Nie ma możliwości odzyskania dostępu do zgłoszenia przez Sygnalistę. Potrzebny do deszyfracji zgłoszenia klucz symetryczny uzyskiwany jest automatycznie podczas podawania losowo wygenerowanego wcześniej 16-cyfrowego numeru zgłoszenia. W przypadku jego utraty ponowny dostęp do zgłoszenia nie jest możliwy.	+
SafeLink	1. Osoba uprawniona do odczytania zgłoszenia uzyskuje dostęp do systemu podając login i hasło. 2. Sygnalista uzyskuje dostęp do zgłoszenia, podając indywidualne dane dostępowe do konkretnego zgłoszenia.	+

SECUREDROP	Deszyfrowanie zgłoszenia następuje wyłącznie przez system Tails podłączony do komputera przez pendrive USB lub na maszynie wirtualnej. Sygnalista odwiedza adres .onion w sieci Tor i postępuje według instrukcji, uzyskując dostęp do swoich kluczy automatycznie i bez ręcznej ingerencji. Komunikacja jest dodatkowo szyfrowana siecią Tor. Klucze deszyfrujące znajdują się na serwerze niepodłączonym do Internetu i jest to jedyne miejsce, w którym zgłoszenia są odszyfrowywane i odczytywane.	

Enform: https://github.com/defuse/php-encryption/blob/master/docs/CryptoDetails.md

7. Ochrona tożsamości sygnalisty – analiza ryzyka dostępu do metadanych załączników przez producenta systemu.

Ocena aplikacji:  dostateczne zabezpieczenia są pewne braki w zabezpieczeniach  nieefektywne zabezpieczenia lub ich brak

Sygnanet	Producent wykorzystuje kryptograficzną technikę szyfrowania typu client-side encryption, która polega na szyfrowaniu całego zgłoszenia wraz z załącznikami na urządzeniu sygnalisty, dlatego technicznie rzecz ujmując, nie jest możliwe uzyskanie dostępu do metadanych przez system. Eliminuje to ryzyko potencjalnego odczytania metadanych.	
ehelpdesk	System pozwala na przesłanie w zgłoszeniu dowolnego formatu poza plikami wykonywalnymi (exe, com) oraz plikami zawierającymi skrypty Java. Skrypty z plików są automatycznie oczyszczane. Metadane z załączników można kasować automatycznie przed zapisem do bazy danych za pomocą odpowiedniej konfiguracji systemu.	
e-nform	Metadane załączników są usuwane podczas dodawania ich do systemu w celu uniknięcia przypadkowej identyfikacji Sygnalisty. W systemie nie są dostępne metadane załączników. Dodatkowo każdy załącznik jest sprawdzany komponentem antywirusowym.	
GLOBALEAKS	W rozwiązaniu GlobaLeaks domyślnie nie jest zaimplementowane czyszczenie metadanych z plików. Pomimo, że zgłoszenie wraz z załącznikami jest automatycznie szyfrowane po przesłaniu na serwer do aplikacji, to Sygnalista sam musi zadbać o usunięcie metadanych z załączników.	

SafeLink	Dostępny jest mechanizm automatycznego czyszczenia metadanych z załączników dodawanych do systemu przez Sygnalistę.	
SECUREDROP	System nie usuwa automatycznie metadanych z załączników. Należy zrobić to ręcznie przed wysłaniem pliku na serwer. Przypadkowe wysłanie załącznika może ujawnić tożsamość Sygnalisty. Każda strona internetowa aplikacji SecureDrop jest dostępna wyłącznie jako strona w sieci Tor, która utrudnia powiązanie tożsamości użytkownika (np. adresu IP jego komputera) z jego działaniem (np. przesyłaniem informacji do SecureDrop).	

8. Inne metody zapewnienia anonimowość sygnalisty dla pracodawcy i producenta aplikacji

Ocena aplikacji: dostateczne zabezpieczenia; są pewne braki w zabezpieczeniach; nieefektywne zabezpieczenia lub ich brak

Sygnanet	System nie zapisuje trwale żadnych informacji (IP, nazwy komputera, odcisku palca przeglądarki), które mogłyby ujawnić tożsamość Sygnalisty. Zastosowano tutaj usuwanie danych kontaktowych zawartych w transmisjach Sygnalisty z serwerem: maskowanie transmisji na serwerze anonimizującym proxy. Producent deklaruje, że stosuje się do zakazu tworzenia logów na serwerze.	
ehelpdesk	System zapewnia anonimizowanie adresów IP Sygnalistów. Sygnalista nie ma konta w systemie (nie ma więc loginu, hasła ani ID), co mogłoby zwiększyć ryzyko ujawnienia tożsamości. Sygnalista może przeglądać jedynie swoje zgłoszenia i proces ich obsługi, prowadzić też korespondencję wyłącznie po podaniu unikatowego identyfikatora oraz kodu generowanego każdorazowo dla zgłoszenia. System nie zapisuje w bazie danych informacji typu: IP, nazwa komputera, rodzaj i wersja przeglądarki, które mogłyby ujawnić tożsamość Sygnalisty. Po stronie serwera www prowadzone jest maskowanie transmisji.	

e-nform	Dostęp do treści zgłoszeń możliwy jest za pomocą generowanych danych (ID, PIN), które nie są powiązane z konkretną osobą. Możliwe jest też utworzenie anonimowego konta (bez konieczności podawania adresu e-mail). System nie udostępnia też koordynatorom żadnych metadanych dotyczących autora zgłoszenia (poza datą utworzenia zgłoszenia czy wysłania wiadomości). System nie gromadzi numerów IP urządzeń, które nawiązują połączenie z serwerem. Aplikacja przechowuje jedynie tymczasowe dane, aby uniemożliwić enumerację danych dostępowych (przeciwdziałanie atakom słownikowym brute-force).	
GLOBALEAKS	System nie zapisuje adresu IP, informacji o przeglądarce, komputerze czy systemie operacyjnym użytkowników. Aplikacja nie zawiera żadnych treści należących do osób trzecich ani nie dostarcza trwałych plików cookie do przeglądarki użytkownika. Sygnalista może przeglądać jedynie swoje zgłoszenia (nie może utworzyć konta) i proces ich obsługi, prowadzić korespondencję wyłącznie po podaniu unikatowego kodu generowanego każdorazowo dla zgłoszenia. Identyfikator sygnalisty jest tworzony losowo i nie pozwala na identyfikację użytkownika. GlobaLeaks zaleca zgłaszanie nieprawidłowości przez sieć Tor, aby uzyskać lepszą ochronę prywatności.	
SafeLink	Jeśli sygnalista wybierze opcję anonimowości i w treści zgłoszenia nie wskaże swoich danych, to nie pojawią się one w panelu pracodawcy. Po dokonaniu zgłoszenia system generuje indywidualny login i hasło, które dają Sygnaliście możliwość monitorowania swojego zgłoszenia i utrzymywania kontaktu z pracodawcą przy zachowaniu anonimowości.	
SECUREDROP	SecureDrop nie zapisuje adresu IP, informacji o przeglądarce, komputerze czy systemie operacyjnym Sygnalisty. Ponadto aplikacja nie zawiera osadzanych skryptów firm trzecich, a dane przesyłane z przeglądarki Sygnalisty do serwera nie zawierają trwałych plików cookie. Serwer przechowuje jedynie datę i godzinę najnowszej wiadomości wysłanej. Po wysłaniu nowej wiadomości czas i data poprzedniej wiadomości są automatycznie usuwane. W przypadku Sygnalistów na serwerze rejestrowana jest tylko godzina i data wysłania wiadomości. Gdy Sygnalista wysyła nową wiadomość, czas i data ostatniej wiadomości są nadpisywane. Oznacza to, że nie ma śladu metadanych pokazujących, kiedy dokładnie Sygnalista oraz osoba nadzorująca korespondowali. Sygnaliści nie mogą utworzyć własnej nazwy użytkownika, która mogłaby ujawnić informacje o nich samych. Zamiast tego SecureDrop automatycznie generuje dwie losowe nazwy kodowe - jedną, którą pokazuje się osobie nadzorującej, a drugą Sygnaliście korzystającemu z systemu.	

9. Ocena ryzyka cyberataku na infrastrukturę serwera systemu albo użytkownika aplikacji

Ocena aplikacji: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Sygnanet	Klucze kryptograficzne potrzebne do deszyfracji treści i załączników są zaszyfrowane hasłem Sygnalisty, dlatego cyberatak na infrastrukturę producenta stanowi niskie ryzyko. Szyfrowanie klucza AES-256 odbywa się przy użyciu kryptografii klucza publicznego RSA-4096. Odszyfrowanie takich danych jest znacząco utrudnione, ponieważ spośród wszystkich aplikacji w Sygnanet zastosowano najbezpieczniejszą metodę szyfrowania Client-Side-Encryption.	
ehelpdesk	System korzysta z szyfrowanej transmisji klient-serwer w wersji TLS 1.3, co nie jest wystarczające, ponieważ nie zabezpiecza to danych na serwerze. Brak jest zabezpieczenia danych w przypadku luki w aplikacji, podatności na serwerze albo innego rodzaju uzyskania dostępu do serwera i uzyskania podwyższonych uprawnień. Zgłoszenia nie są szyfrowane na serwerze, dlatego ryzyko udanego ataku jest stosunkowo duże.	
e-nform	Dostęp do treści zgłoszeń możliwy jest za pomocą generowanych danych (ID, PIN), które nie są powiązane z konkretną osobą. Możliwe jest też utworzenie anonimowego konta bez konieczności podawania adresu e-mail. System nie udostępnia też koordynatorom żadnych metadanych dotyczących autora zgłoszenia poza datą utworzenia zgłoszenia czy wysłania wiadomości. Ponadto z załączników dodawanych przez Sygnalistę do systemu usuwane są metadane. System nie gromadzi numerów IP urządzeń oraz innych metadanych, które nawiązują połączenie z serwerem. Aplikacja przechowuje jedynie tymczasowe dane, aby uniemożliwić enumerację danych dostępowych (przeciwdziałanie atakom słownikowym brute-force).	

GLOBALEAKS	Zastosowanie szyfrowanego kanału komunikacyjnego klient-serwer TLS 1.3 jest tak skonfigurowane, aby uzyskać klasę A+ w testach SSLLabs. Dodatkowo administrator może wymusić dostęp do aplikacji tylko za pomocą sieci Tor, co zwiększa bezpieczeństwo przed atakami sieciowymi. Wszystkie klucze szyfrujące oraz loginy i hasła administratora, osób nadzorujących, są przechowywane w postaci zaszyfrowanej, ale bez kontroli Sygnalisty. System wykorzystuje zintegrowany iptables oraz AppArmor, a także mechanizm zapobiegania spamowaniu. Klucze szyfrujące zgłoszenie generowane są za pomocą kryptografii krzywej eliptycznej (ECC Curve25519) przez backend podczas zgłaszania informacji przez Sygnalistów. Zaszyfrowaniu ulegają komentarze, załączniki i związane z nimi metadane oraz inne dane przekazywane w zgłoszeniu po przesłaniu na serwer do bazy SQLite. Klucze są przypisane do poszczególnych użytkowników i zgłoszeń, dlatego dostępu do nich mają tylko Sygnaliści.	
SafeLink	Używany jest szyfrowany kanał komunikacyjny klient-serwer HTTPS (TLS 1.3), a treści, które są przechowywane na serwerze nie są jawne. System spełnia podstawowe zabezpieczenia przed cyberatakiem. Użycie znanej i bezpieczniejszej metody szyfrowania Client-Server Encryption pozwoliłoby uzyskać lepszą ocenę.	
SECUREDROP	Aplikacja centralna SecureDrop Administrator nie ma dostępu do Internetu, więc osoba atakująca musi najpierw wykonać kod w maszynie wirtualnej Qube OS. Można to osiągnąć za pomocą złośliwego zgłoszenia albo luki w kodzie aplikacji. Instancja serwera ma domyślnie zainstalowany firewall pfSense oraz odizolowane procesy interfejsów administratora, aplikacji oraz Sygnalisty. Wszystkie klucze deszyfrujące znajdują się na serwerze niepodłączonym do Internetu, więc dostęp do nich jest znacznie trudniejszy dla atakującego, co zmniejsza ryzyko, że osoba atakująca mogłaby wysłać złośliwe oprogramowanie przez SecureDrop, próbując zainfekować również normalną sieć organizacji prasowej. SecureDrop całkowicie oddziela swój ruch od sieci organizacji. Dostęp do materiałów i ich pobieranie odbywa się za pomocą systemu operacyjnego Tails, który jest uruchamiany z USB, nie dotyka dysku twardego komputera i kieruje cały ruch internetowy przez sieć Tor. Serwery SecureDrop są również poddawane znacznemu wzmocnieniu systemowemu (znajdziemy tutaj zabezpieczenie w postaci OSSEC IDS). Komunikacja za pośrednictwem SecureDrop jest szyfrowana, więc wiadomości nie mogą być łatwo przechwycone i odczytane w trakcie ich przesyłania przez Internet. Sieć Tor zapewnia szyfrowanie end-to-end w przeciwieństwie do protokołu HTTPS. Dodatkowo wiadomości oraz załączniki są szyfrowane na serwerze w pamięci (Server-Side Encryption) zanim zostaną zapisane na dysk, więc jeśli napastnikowi uda się włamać na serwer, nie będzie on w stanie odczytać żadnych danych albo będzie to bardzo trudne.	

10. Maksymalna ilość osób nadzorujących zgłoszenia

Sygnanet	Zależne od pakietu: Standard - 1 osoba, Premium - 3 osoby, Enterprise - 5 osób lub więcej.
ehelpdesk	Zależna jest od wykupionej licencji.
e-nform	Liczba koordynatorów uzależniona jest od wariantów aplikacji: SILVER - 3 koordynatorów, GOLD - 10 koordynatorów z możliwością zwiększenia wolumenu, PLATINUM - brak limitu. Liczba kont ekspertów (tj. osób wspierających koordynatora w wyjaśnianiu zgłoszenia) jest nieograniczona w każdym z wariantów.
GLOBALEAKS	Nieograniczona
SafeLink	Nieograniczona
SECUREDROP	Nieograniczona

11. Delegowanie spraw pomiędzy odbiorcami zgłoszenia i zarządzanie uprawieniami w systemie

Sygnanet	Aplikacja posiada rozbudowany system tworzenia uprawnień: Główny odbiorca zgłoszeń, Odbiorca zgłoszeń, Administrator oraz Audytor. Każde z nich ma określoną rolę w hierarchii oraz zakres uprawnień (powiadomienie o zgłoszeniu, odczytanie zgłoszenia, zmiana statusu zgłoszenia, korespondencja z sygnalistą, zarządzanie kategoriami, dodawanie i edycja użytkowników, usuwanie użytkowników).
ehelpdesk	System pozwala na automatyczne przydzielania spraw z uwagi na kanał zgłoszeń (profil reprezentowany przez adres URL portalu Sygnalisty), kategorię, podkategorię, grupy wsparcia lub jednostkowo. Zgłoszenie może być procesowane przez różne grupy wsparcia z odpowiednimi prawami dostępu. Oprogramowanie posiada rozbudowany system nadawania uprawnień – zarówno do zgłoszeń, jak i grup wsparcia obsługujących zgłoszenia.
e-nform	Od wariantu GOLD klient posiada rozbudowany panel administracyjny umożliwiający samodzielne zarządzanie kontami i uprawnieniami Koordynatorów (dostęp do wybranych typów zgłoszeń na poziomie odczytu, koordynacji i zarządzania danymi) i Ekspertów. W każdej chwili można zmienić gospodarza zgłoszenia. W wariancie SILVER, w okresie licencyjnym, możliwa jest także dowolna liczba zmian w zakresie kont koordynatorów.
GLOBALEAKS	Dostępne są dwie role: administrator i odbiorca zgłoszeń, który może uzyskać dostęp tylko do niewielu uprawnień.
SafeLink	Ze względu na profil klientów zazwyczaj są to dwie osoby, jedna nadzorująca, druga zastępcza lub do wykonywania czynności technicznych.
SECUREDROP	System pozwala wyłącznie na dodanie nowego użytkownika z rolą: Administrator Systemu albo Osoba Nadzorująca.

12. Automatyzacja pracy: predefiniowane wzorce automatycznych odpowiedzi oraz komunikaty systemowe

Sygnanet	Możliwość tworzenia dowolnych tekstów odpowiedzi powitalnych, w tym automatycznie wysyłanych oraz zamykających zgłoszenie.
ehelpdesk	Sygnalista po dokonaniu zgłoszenia otrzymuje dwa identyfikatory, które umożliwiają mu sprawdzenie statusu zgłoszenia oraz dwustronną komunikację z podmiotem przetwarzającym zgłoszenie. Osoby przetwarzające otrzymują powiadomienia w całym procesie przetwarzania zgłoszenia. Powiadomienia są w pełni definiowalne i uzależnione od zdefiniowanej grupy użytkowników, wykonanych akcji, zmiany statusu zgłoszenia.
e-nform	Aplikacja wysyła koordynatorom różnego rodzaju automatyczne powiadomienia systemowe pomagające w zarządzaniu zgłoszeniami. Powiadomienia mają postać m.in. przypomnień dotyczących okresów przetwarzania danych, upływu terminów wynikających z dyrektywy. W ramach konfiguracji aplikacji można wprowadzić ustandaryzowane szablony odpowiedzi.
GLOBALEAKS	System pozwala na przygotowania kwestionariusza dla Sygnalistów, aby lepiej dopasować kontekst zgłoszenia.
SafeLink	Brak
SECUREDROP	Brak

13. Zapewnienie generowania cyklicznych raportów

Sygnanet	System tworzy raport (w tym PDF) oraz zestawienia zgłoszeń z następującymi informacjami: ID zgłoszenia, czas dodania zgłoszenia, kategoria, kto ma dostęp do zgłoszenia (osoba uprawniona), status i tym podobne dane.
ehelpdesk	System pozwala na dodanie dowolnych raportów w standardzie Stimulsoft lub SAP Crystal Reports. Możliwy jest eksport raportów do kilkudziesięciu formatów.
e-nform	Aplikacja w każdym z wariantów posiada panel ze statystykami dotyczącymi zgłoszeń, w tym obciążenia poszczególnych koordynatorów. Raporty można generować w wybranych przez koordynatora lub administratora przedziałach czasowych oraz w formie pliku PDF lub Excel. Raporty rozbudowywane są bezpłatnie w ramach asysty rozwojowej w oparciu o sugestie klientów.
GLOBALEAKS	Raporty obejmują następujące dane zgłoszenia: data, ostatnia modyfikacja, czas wygaśnięcia, treść, status dostępności przez sieć Tor, komentarze, pliki, ostatni dostęp Sygnalisty.
SafeLink	Raporty dostępne są tylko w podstawowym zakresie.
SECUREDROP	Brak jest możliwości generowania jakichkolwiek raportów.

14. Logi wszystkich operacji dokonywanych w zgłoszeniu (pełna historia)

Sygnanet	System zawiera szczegółowe informacje m.in. o tym kiedy wysłano zgłoszenie, kiedy je odczytano oraz kiedy pobrano załączniki. Ponadto każda czynność wykonana przez zgłaszającego lub osobę obsługującą zostaje odnotowana: data i godzina utworzenia.
ehelpdesk	Dostępna jest pełna rozliczalność zgodna z wytycznymi.
e-nform	Każde zgłoszenie posiada szczegółowy audyt wszystkich operacji wykonanych w zgłoszeniu (ze wskazaniem daty, godziny i loginu użytkownika), dostępny Koordynatorowi zgłoszenia i Administratorowi. Dodatkowo Administrator systemu posiada odrębny, rozbudowany panel audytowy. W audycie nie pojawiają się informacje mogące zidentyfikować Sygnalistów.
GLOBALEAKS	Pełne logi audytowe (brak możliwości identyfikacji użytkowników).
SafeLink	Każda czynność wykonana przez zgłaszającego, czy osobę obsługującą zostaje odnotowana: data, godzina utworzenia (w module "Postępowanie wyjaśniające" również podpis osoby, która zostawiła notatkę lub dodała plik).
SECUREDROP	Brak

15. Wybrane przez AVLab cechy unikatowe oprogramowania

Sygnanet

- System używa najbezpieczniejszej metody szyfrowania zgłoszenia treści i załączników zanim zostaną wysłane na serwer (Client-Side Encryption).
- Sygnanet używa biblioteki System.Security.Cryptography zgodnej z zaleceniem OWASP i posiadającej certyfikację FIPS.
- Dostępne są tutoriale jak korzystać z panelu Sygnanet, instrukcja PDF dla pracowników oraz ulotki, plakaty, poradniki i materiały wideo.
- System uprawnień: dany użytkownik może mieć dostęp tylko do określonych czynności – na przykład nie może zarządzać całym systemem albo ma dostęp jedynie do wybranych zgłoszeń (co chroni treść zgłoszeń i załączniki przed niepowołanym dostępem).
- System automatycznych wzorców odpowiedzi: predefiniowane przez producenta oraz możliwość tworzenia własnych.
- Możliwość testowania serwisu przez 14 dni przed zakupem.
- Cena zależna tylko od ilości osób obsługujących zgłoszenia sygnalistów.
- System posiada analizę ryzyka (DPIA), dokument jest udostępniany klientom. Aplikacja przechodzi cykliczne testy bezpieczeństwa.

ehelpdesk

- Rozbudowany system uprawnień.
- System przeszedł pozytywnie testy bezpieczeństwa (podatności) obejmujące aplikację oraz bazę danych.
- Dostępne jest API do systemów zewnętrznych. Wbudowany importer danych dowolnego formatu wraz z harmonogramem importu.
- Integracja z systemami helpdeskowymi, integracja z Microsoft Active Directory, Microsoft Azure Role-Based Access Control.
- Automatyczne aktualizacje z portalu producenta nie wymagają ingerencji użytkownika.
- Systematyczny rozwój aplikacji, w tym także na życzenie użytkownika.
- Filmy instruktażowe. Pełne wsparcie wdrożenia.
- Wsparcie gwarancyjne i serwisowe w języku polskim. Korzystne SLA.

e-nform

- Proces wdrożenia systemu obejmuje m.in. instruktaż (1h) dla Koordynatorów z obsługi systemu oraz okres testowania skonfigurowanego systemu przed jego produkcyjnym uruchomieniem.
- Możliwość założenia przez Sygnalistę anonimowego konta i zarządzania swoimi zgłoszeniami.
- Rozbudowany proces nadawania uprawnień koordynatorom (dostęp do poszczególnych typów zgłoszeń oraz TAGów na poziomie odczytu, koordynacji oraz zarzadzania danymi).
- Rozbudowane funkcje zarządzania danymi osobowymi przez koordynatora zgłoszenia (m.in. oznaczanie typu danych w zgłoszeniu, anonimizacja danych, liczenie okresu przetwarzania danych, automatyczne powiadomienia systemowe).
- Rozbudowany proces zapraszania do zgłoszenia tzw. ekspertów (osoby pomagające w wyjaśnianiu zgłoszenia) z określeniem uprawnień dostępu do poszczególnych elementów zgłoszenia.
- Aplikacja przechodzi cykliczne testy bezpieczeństwa oraz pogłębione analizy ryzyka (DPIA, TIA), które są udostępniane klientom.
- System zgodny z WCAG 2.0 (trwają prace nad dostosowaniem do WCAG 3.0).

GLOBALEAKS

- System używa sieci Tor do wspierania anonimowości użytkowników.
- Posiada certyfikat ISO 37002:2021.
- Traktuje prywatność w najwyższych kategoriach, tzn. privacy-by-design.
- Zawiera dodatkowe szyfrowanie asymetryczne (kryptografia krzywej eliptycznej ECC Curve25519).
- Na licencji Free Software OSI Approved AGPL 3.0 License.
- Wspiera szyfrowanie PGP powiadomień e-mail oraz pobieranych plików przez użytkowników.
- Dostępna jest szczegółowa dokumentacja.
- Dostępne jest DEMO online.

SafeLink

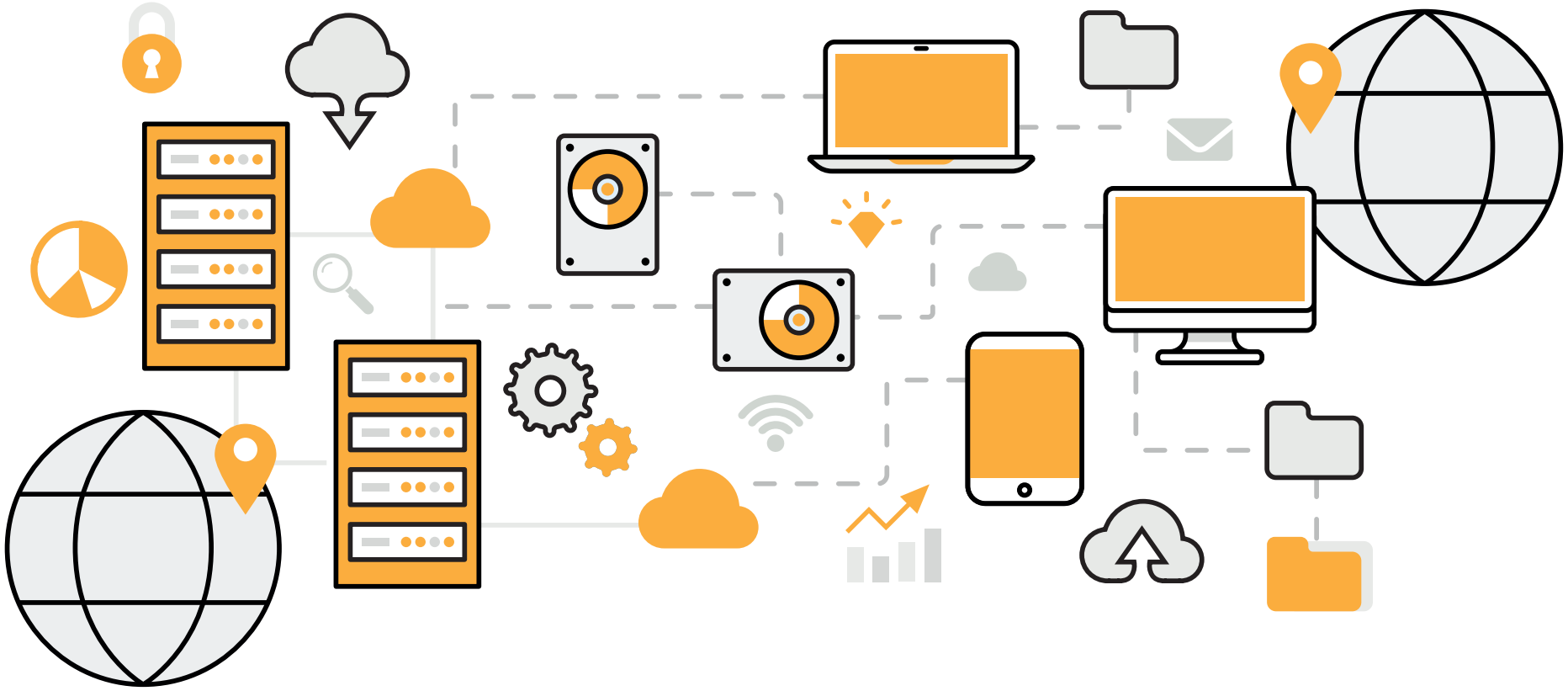
- Przesyłanie anonimowego zgłoszenia poprzez e-mail i transkrypcję z połączenia telefonicznego.
- Procedura wewnętrzna dokonywania zgłoszeń i podejmowania działań następczych.
- Szkolenia dla osób obsługujących z prowadzenia postępowań wyjaśniających.
- Indywidulane przygotowane materiały edukacyjne dla pracowników.
- Możliwość dodania zgłoszenia własnego przez obsługujących zgłoszenia: w przypadku otrzymania zgłoszenia poza systemem np. podczas spotkania osobistego z Sygnalistą. Opcja ta pozwala też wygenerować dane dostępowe dla Sygnalisty (nr zgłoszenia i PIN), które pozwalają sygnaliście monitorować sprawę i prowadzić dalszy kontakt przez system.

SECUREDROP

- Sygnalista może zalogować się do SecureDrop tylko przez przeglądarkę Tor, która maskuje adres IP źródła. Nie jest też rejestrowany adres IP sieci Tor, komputer ani rodzaj przeglądarki.
- Na serwerze rejestrowana jest tylko godzina i data wysłania wiadomości. Gdy Sygnalista wysyła nową wiadomość, czas i data ostatniej wiadomości są nadpisywane.
- Sygnaliści nie mogą utworzyć własnej nazwy użytkownika, która mogłaby ujawnić informacje o nich samych.
- Klucze deszyfrujące znajdują się na komputerze niepodłączonym do Internetu.
- Dostęp do materiałów i ich pobieranie odbywa się za pomocą systemu operacyjnego Tails, który jest uruchamiany z USB, nie dotyka dysku twardego komputera i kieruje cały ruch internetowy przez sieć Tor.
- Serwery SecureDrop są poddawane hardeningowi według zapotrzebowania organizacji, aby maksymalnie utrudnić hakerom włamanie.
- Dostępne jest DEMO online rozwiązania.

IV Nieuwzględnione atrybuty oprogramowania

Po konsultacjach z producentami zdecydowaliśmy, aby do końcowej oceny nie uwzględniać niektórych atrybutów oprogramowania. Możemy tutaj wymienić np. „zdolność do szyfrowania kanału komunikacyjnego typu klient-serwer” (TLS1.2+, HTTPS), które zostało spełnione przez wszystkich producentów. Inną cechą jest „cena rozwiązania”, która zależy od wielu czynników. Jeszcze inną jest „personalizacja strony internetowej” dla sygnalisty (podmiana logo, stylów szablonu strony itp.), a także „awaryjne odzyskiwanie dostępu do zgłoszenia” (resetowanie poświadczeń logowania 2FA).



Nie braliśmy pod uwagę następujących cech:

Szyfrowanie wymiany danych typu klient-serwer.

Szyfrowanie ruchu danych między serwerem a przeglądarką użytkownika jest spełnione przez wszystkich producentów minimalną wersją protokołu TLS 1.2.

Awaryjne odzyskiwanie dostępu do zgłoszenia przez sygnalistę.

Każdy z producentów systemów przewidział utratę informacji o zgłoszeniu. Zwykle polega to na przypisaniu ID, hasła, PIN-u do zgłoszenia, a w przypadku zgubienia przez sygnalistę indywidualnego numeru zgłoszenia, odzyskanie dostępu nie jest możliwe.

Ocena bezpieczeństwa kodu aplikacji.

Bezpieczeństwo kodu aplikacji opiera się na zaufaniu do producenta, dlatego trudno było wystawiać ocenę na podstawie deklaracji przyznanych certyfikatów. Część przekazanych nam publicznych audytów jest już nieaktualna, a nawet ich ważność nie gwarantuje całkowitego bezpieczeństwa kodu aplikacji. Szczegółowe informacje może dostarczyć producent każdego rozwiązania.

Personalizacja strony zgłoszeniowej.

Cecha ta może być istotna dla organizacji i sygnalistów, jednak nie była poddawana ocenie.

Całkowity koszt systemu.

Cena uwarunkowana jest rodzajem pakietu. Bardziej rozszerzone plany zależą np. od liczby osób przypisanych do obsługi systemu, liczby sygnalistów, funkcji tworzonych na potrzeby klienta, dodatkowych języków w systemie dla sygnalisty i wielu innych.

Czas wdrożenia systemu.

Wdrożenie typu SaaS z natychmiastowym dostępem do panelu graficznego aplikacji nie oznacza, że sygnalista, administrator, koordynator, będą mieć dostęp do usługi, ponieważ czas wdrożenia zależy np. od wybranego przez klienta wariantu aplikacji oraz przekazania przez niego wszystkich danych konfiguracyjnych – jeżeli producent tego wymaga. Niektórzy dostawcy systemów umożliwiają testowe wdrożenie aplikacji, szkolenie dla przedsiębiorstwa, następnie po testach następuje czyszczenie bazy danych ze zgłoszeń oraz formalny odbiór i rozpoczęcie okresu licencyjnego. Dodatkowo czas wdrożenia rozwiązań w modelu on-premises wymaga obsługi technicznej i późniejszego testowania aktualizacji przed udostępnieniem nowej wersji dla sygnalistów.

V Zestawienie modelu bezpieczeństwa systemów dla sygnalistów

Analiza została opracowana w oparciu o wcześniejsze deklaracje producentów oraz ocenę ryzyka cyberataku na system dla sygnalisty. Wyszliśmy od modelu bezpieczeństwa opartego na braku zaufania (zero-trust) i założyliśmy, że (1)atakujący już znajduje się w sieci organizacji, gdzie zainstalowany jest system dla sygnalisty (wdrożenie lokalne) albo haker (2)miał dostęp do systemu operacyjnego pracownika, gdzie przez przeglądarkę następuje łączenie się do aplikacji. W zależności od wariantu, cyberatak może przebiegać inaczej, ale efekt końcowy będzie ten sam – potencjalne ryzyko odczytania informacji (również danych osobowych) od sygnalisty lub dostęp do całego (albo części) systemu operacyjnego na skutek wykorzystania podatności 0-day. Zatem na ogólną ocenę miał wpływ rodzaj zastosowanego szyfrowania kryptograficznego, ponieważ prawie wszystkie systemy przekazują plik z jawną treścią zgłoszenia na serwer, gdzie tworzony jest nowy plik zaszyfrowany i w niejawnej postaci jest przechowywany. Należy się zastanowić, co się dzieje z plikiem przekazanym przez sygnalistę i czy jest pewność, że oryginalny plik zostanie skasowany i nie będzie przechwycony w cyberataku?

Należy maksymalnie ograniczyć zaufanie do serwera, aby zminimalizować ryzyko, dlatego najmocniejszym wariantem szyfrowania jest Client-Side Encryption – szyfrowanie zgłoszenia na urządzeniu sygnalisty – zanim jakiekolwiek dane opuszczą komputer pracownika. Ten rodzaj szyfrowania jest obsługiwany wyłącznie przez system Sygnanet. Zaletą szyfrowania Client-Side Encryption jest pełne bezpieczeństwo danych, ponieważ serwer nie ma dostępu do kluczy szyfrowania i nie może odszyfrować danych bez udziału sygnalisty – do tego niezbędne jest hasło, które odbiorca zgłoszenia ustala podczas rejestracji w systemie (hasło jest kodowane w wyniku działania funkcji jednokierunkowej). Podobnie koordynator zgłoszenia – aby odczytać zaraportowane naruszenie, musi podać własne hasło użytkownika systemu, które jest niezbędne do odszyfrowania klucza prywatnego sygnalisty. Serwer producenta nie bierze udziału w szyfrowaniu i deszyfrowaniu zgłoszeń. Operacje kryptograficzne odbywają się na komputerach pracowników, koordynatorów i innych użytkowników, którzy mają dostęp do systemu sygnalisty.

Ważną cechą jest zapewnienie anonimowości sygnalisty oraz ochrona danych osobowych, które mogą uniemożliwić rozpoznanie użytkownika przez osoby nadzorujące oraz przez serwer producenta. Dlatego ciągle pamiętając o zasadzie ograniczonego zaufania do serwera, niezbędne jest, aby oprogramowanie po zastosowaniu szyfrowania typu client-side encryption, w ogóle nie miało dostępu do załączników, dzięki czemu możliwe będzie zachowanie pełnej anonimowości sygnalisty.

W przeciwnym wypadku zachodzi ryzyko, że producent systemu ma dostęp do plików podczas procedury czyszczeniu metadanych. Dodatkowo należy uwzględnić brak możliwości zapisywania informacji o urządzeniu pracownika (tzw. odcisk palca przeglądarki i np. adres IP). Część producentów doskonale realizuje zgodność z dobrymi praktykami anonimowości, kierując się zasadą, że „im mniej wiemy" o stronie trzeciej, tym lepiej. Zwracamy też uwagę, że tylko dwa systemy obsługują sieć Tor: GlobaLeaks oraz SecureDrop. Pierwsze rozwiązanie zezwala na wybór, czy system ma być dostępy przez sieć Tor w domenie ".onion". Drugie rozwiązanie obowiązkowo wymaga do obsługi sieci Tor, co już znacząco utrudnia stworzenie konkretnego profilu osoby zgłaszającej naruszenia. Ponadto wszystkie produkty cechują funkcjonalności, które nie sposób wymienić w krótkim podsumowaniu, dlatego zachęcamy do zapoznania się z pełnymi opisami w poszczególnych tabelach.

	Sygnanet	ehelpdesk	e-nform	GLOBALEAKS	SafeLink	SECUREDROP
Zabezpieczenie logowania do systemu	+	+	+	+	−	+
Wybrany przez producenta rodzaj szyfrowania kryptograficznego	+	!	−	−	−	−
Metoda szyfrowania danych na serwerze	+	!	+	+	+	+
Dostęp do zgłoszenia przez Sygnalistę i Użytkowników Systemu (metoda deszyfrowania)	+	+	+	+	+	+
Dostępne metody ochrony tożsamości Sygnalisty	+	−	−	−	−	−
Anonimowość Sygnalisty dla pracodawcy i producenta aplikacji	+	+	+	+	+	+
Cyberatak na infrastrukturę serwera systemu albo użytkownika aplikacji	+	!	−	−	−	−

Ocena aplikacji: + dostateczne zabezpieczenia − są pewne braki w zabezpieczeniach ! nieefektywne zabezpieczenia lub ich brak

VI Wnioski z badania

Wybierając system dla sygnalistów warto zwrócić szczególną uwagę na poniższe kwestie:

A.

System powinien zapewniać szyfrowanie zgłoszenia metodą end-to-end (zero-knowledge service) kluczem kryptograficznym generowanym na komputerze pracownika[1]. Niedopuszczalne jest używanie marketingowego opisu producenta dla „szyfrowania TLS" w architekturze systemu komputerowego typu klient-serwer, gdyż nie można mówić o zatajeniu istotnych danych sygnalisty, a jedynie o szyfrowaniu informacji przesyłanych z formularza webowego z przeglądarki do serwera. W ostatecznym rozrachunku nie oznacza to, że dane będą szyfrowane na serwerze, jeżeli system dla sygnalisty tego nie obsługuje. Szyfrowanie warstwy aplikacyjnej spełnia każdy producent protokołem w minimalnej wersji TLS 1.2 lub TLS 1.3.

[1] https://www.eenewseurope.com/en/client-side-vs-server-side-encryption-who-holds-the-key/

B.

System powinien zapewniać szyfrowanie zgłoszenia (w tym plików), aby lepiej wypełniał regulacje dotyczące RODO. Szyfrowanie jest najbezpieczniejszym sposobem zachowania zgodności z niektórymi aspektami unijnego rozporządzenia o ochronie danych osobowych i jest metodą zapewniającą „pseudoanimizację". Dane sygnalisty podlegają ochronie prawnej, dlatego ich ujawnienie na przykład w następstwie cyberataku, może mieć negatywne konsekwencje dla zaatakowanej organizacji.

C.

System należy zabezpieczyć przed dostępem osób przypadkowych. Zatem logowanie powinno być chronione dodatkowym kodem pochodzącym z aplikacji generującej jednorazowe tokeny np. Google Authenticator. W bardziej rozbudowanych środowiskach roboczych mogą to być wspierane protokoły LDAP lub framework OAuth do integracji z korporacyjnymi systemami uwierzytelniania użytkowników.

D.

Maksymalnie bezpieczny system nie powinien mieć możliwości odczytywania metadanych z załączników, które są przesyłane przez sygnalistów. Ograniczenie zaufania do serwera minimalizuje ryzyko związane z przypadkowym lub celowym ujawnieniem (np. w wyniku cyberataku lub podatności aplikacji) tożsamości sygnalisty.

E. Jeżeli mimo wszystko producent zezwala na wysyłanie załączników i jednocześnie nie stosuje szyfrowania po stronie użytkownika, to należy zwrócić uwagę na implementację funkcji, która zablokuje przesyłanie potencjalnie niebezpiecznych formatów plików. Przeglądarka może interpretować plik „jako do uruchomienia" podczas próby odczytywania, dlatego nie należy zezwalać na przesyłanie potencjalnie groźnych plików wykonywalnych oraz plików zawierających skrypty – a jeżeli tak, skrypty z plików powinny być automatycznie oczyszczane lub archiwizowane.

F. Jednocześnie system powinien zapewniać anonimizowanie adresów IP sygnalistów: nie może zapisywać trwale żadnych informacji (numeru IP, nazwy komputera, odcisku palca przeglądarki), które mógłby ujawnić tożsamość sygnalisty. System nie powinien też pozostawiać śladów na komputerze osoby dokonującej zgłoszenia.

G. Ochrona anonimowości sygnalisty to ważna cecha, ale nie zawsze idzie w parze z bezpieczeństwem. Przykładowo kiedy pracownik korzysta z sieci Tor w firmowej sieci tworzy wąski profil użytkowników, którzy mogliby dokonać zgłoszenia.

H. Nawet najbezpieczniejszy system będzie nieprzyjazny w obsłudze, jeśli nie zapewni automatyzacji czynności dokonywanych przez osoby nadzorujące i koordynujące.

VII Metodologia

Raport został przygotowany na zlecenie firmy SpecFile Project Sp.z o.o. biorącej udział w porównaniu. Niezbędnym minimum doboru systemu była ugruntowana pozycja producenta na rynku polskim. Nie pobierano żadnych dodatkowych opłat od pozostałych producentów.

Metodologia i opracowanie raportu jest autorskim dziełem Fundacji AVLab dla Cyberbezpieczeństwa.

Polski przedstawiciel systemu Keeper (business-keeper.com) odmówił udziału w porównaniu.

Nie uzyskaliśmy odpowiedzi na liczne próby kontaktu od producentów systemów: Whistlink (whistlink.com), WhistleB (whistleb.com), Sygnalista Online (sygnalista.online).

Niektóre cechy ważne dla bezpieczeństwa zostały wyraźnie otagowane trzystopniową kalkulacją oceny ryzyka aplikacji:

- dostateczne zabezpieczenia
- są pewne braki w zabezpieczeniach
- nieefektywne zabezpieczenia lub ich brak

Opracowano dla: specfile.pl

AVLAB
CYBERSECURITY FOUNDATION

Jako niezależni pasjonaci stoimy na straży ochrony prywatności i cyfrowego bezpieczeństwa w Internecie.

Zajmujemy się dostarczaniem informacji z branży zagrożeń internetowych i zabezpieczeń w artykułach, relacjach ze szkoleń, konferencjach i materiałach edukacyjnych.

Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, w których wykorzystujemy szkodliwe oprogramowanie, narzędzia oraz techniki obchodzenia zabezpieczeń, które są używane w prawdziwych atakach przez hakerów.