Maciej PODSIADŁY, Dariusz PODSIADŁY

OTRS JAKO NARZĘDZIE WSPOMAGAJĄCE OBSŁUGĘ INCYDENTÓW BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

W artykule omówione zostały zalety i funkcjonalności systemu biletowego OTRS, wykorzystywanego między innymi do obsługi incydentów z zakresu bezpieczeństwa systemów, sieci czy teleinformatyki.

WSTĘP

Incydentem bezpieczeństwa teleinformatycznego nazywamy zaistniałe zdarzenie zagrażające cyberbezpieczeństwu, czyli każde działanie, które naruszyło przyjęte standardy i zasady bezpieczeństwa teleinformatycznego w organizacji. Każde zdarzenie może przekształcić się w incydent, które wymaga jego obsługi. Koniecznym aspektem przy obsłudze incydentów bezpieczeństwa teleinformatycznego jest jego klasyfikacja.

Jednym ze standardów jest klasyfikacja przedstawiona przez europejską organizację ENISA. Kategorie są oparte na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na dany system oraz jego ewentualnym wykorzystaniem. Taki podział przydatny jest zarówno dla działań operacyjnych jak i praktycznej analizy prowadzącej do osiągnięcia określonego celu.

Pierwszym typem klasyfikacji jest malware, czyli infekcje jednego lub wielu systemów specyficznym typem złośliwego oprogramowania. Następnie dostępność zasobów poprzez np. atak typu DoS / DDoS, który powoduje zakłócenie funkcjonowania systemów lub sieci, może nawet doprowadzić do ich uszkodzenia. Trzecią klasą incydentu jest zbieranie informacji poprzez wykorzystanie metod skanowania czy phishingu. Jest to próba zebrania informacji o użytkowniku lub systemie z wykorzystaniem metod socjotechnicznych. Kolejną kategorią jest próba włamania, która oznacza próbę ingerencji lub logowania w systemie przy wykorzystaniu jego podatności. Kolejną klasą jest potwierdzone włamanie, określone jako ingerencję w system, jego komponent lub sieć wykorzystując jego podatność lub skompromitowane konto. Następnym dużym typem incydentów jest bezpieczeństwo informacji. Jego zagrożenie może być spowodowane nieautoryzowanym dostępem, zmianą lub usunięciem danego zbioru informacji. Przedostatnią klasą jest fraud, czyli nielegalne lub nieautoryzowane użycie zasobów oraz np. użycia nazwy innego podmiotu bez zezwolenia. Ostatnią i zarazem największą kategorią jest nielegalna treść. Incydenty dotyczą przede wszystkim wszelkiego rodzaju spamu oraz praw autorskich, czyli dystrybucją materiałów chronionych prawem.

Dzięki wykorzystaniu standardu powyższej klasyfikacji, organizacja jest w stanie sprawnie zarządzać incydentami bezpieczeństwa teleinformatycznego. Jednak do obsługi potrzebne są źródła informacji o zagrożeniach oraz narzędzia wspomagające. Jednym z nich jest system OTRS.

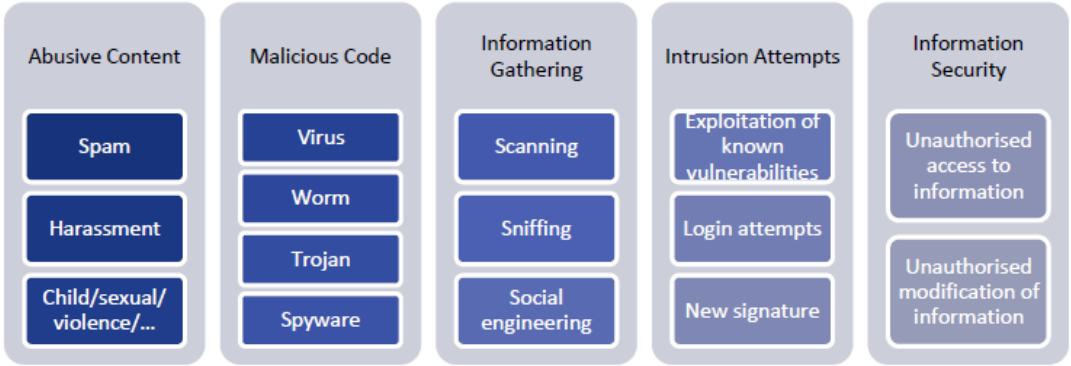
1. SYSTEM OTRS

1.1. Główne cechy systemu

Open-source Ticket Request System (OTRS) jest oprogramowaniem umożliwiającym obsługę przez organizację systemu biletowego, popularnie nazwanym Helpdesk lub Service Desk. System biletowy – ticket tracking, służy do odpowiadania na masowe zapytania wysyłane dowolnym sposobem i stanowi integralną część środowiska obsługi klientów wielu firm. Istotą systemu jest przypisanie każdemu zapytaniu statusu zgłoszenia zawierającego unikalny numer sprawy, całą jej historię oraz aktualny stan postępu.

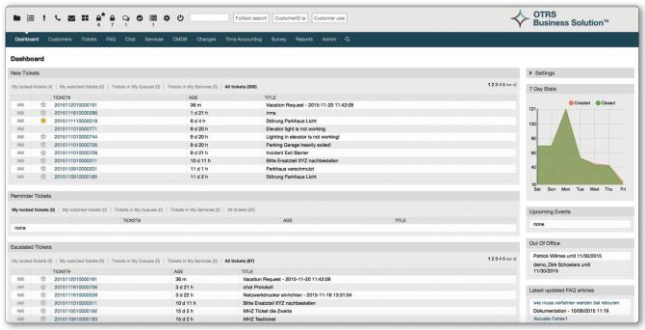
OTRS jest jednym z kilku systemów dostępnych na rynku do obsługi zgłoszeń, innymi znanymi są Mantis, RT czy Bugzilla. Historycznie OTRS był przeznaczony do obsługi klientów zgłoszeń telefonicznych, jednak w obecnych czasach środowisko udostępnione może być zarówno dla obsługującego dane zgłoszenie jak i klienta w celu jego śledzenia.

Pierwsza oficjalna wersja powstała w 2002 roku i została zaimplementowana w Perlu jako skrypt CGI. Po wielu poprawkach interfejs zyskał na jakości przy zastosowaniu JavaScriptu. Wewnętrzna



Rys.1. *Klasyfikacja typów incydentów według organizacji ENISA*

budowa systemu oparta jest na modelu modułowym, dzięki czemu nowe funkcjonalności można w łatwy sposób zaimplementować. Dodatkowo interfejs użytkownika można dostosować do własnych potrzeb przy pomocy wewnętrznego języka systemu zwanego Dynamic Template Language. OTRS współpracuje z wieloma bazami danych: DB2, MySQL czy Oracle, a środowisko unixowe jest dobrze zintegrowane z obsługą ruchu wiadomości elektronicznych jak Postfix czy procmail. Dodatkowo istnieje możliwość połączenia środowiska z innymi narzędziami np. ITSM, które służy do obsługi procesów w organizacji zgodnie z metodologią ITIL, uznawaną na całym świecie. Firma o tej samej nazwie skrótowej utworzyła również wersję komercyjną z wieloma zaprogramowanymi komponentami ułatwiającymi obsługę zgłoszeń. W 2013 roku kod źródłowy systemu został udostępniony publicznie na serwisie GitHub. Od tego czasu społeczność oprogramowania rozbudowuje moduły, które można wykorzystać i zaimplementować w swojej instancji. W roku 2017 firma pochwaliła się ponad 3mln pobraniem oprogramowania, dostępnego w 38 językach i pełnym wdrożeniem w ponad 170 tys. firmach i organizacjach.

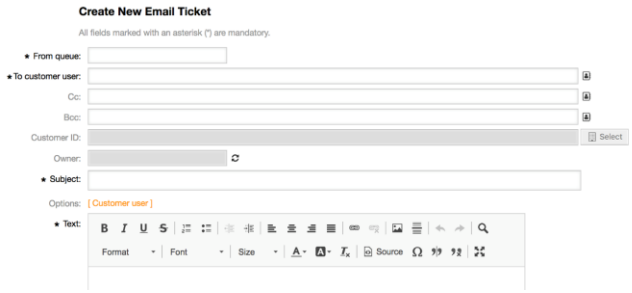


Rys.2 *Panel główny systemu OTRS*

1.2. Obsługa zgłoszeń w systemie

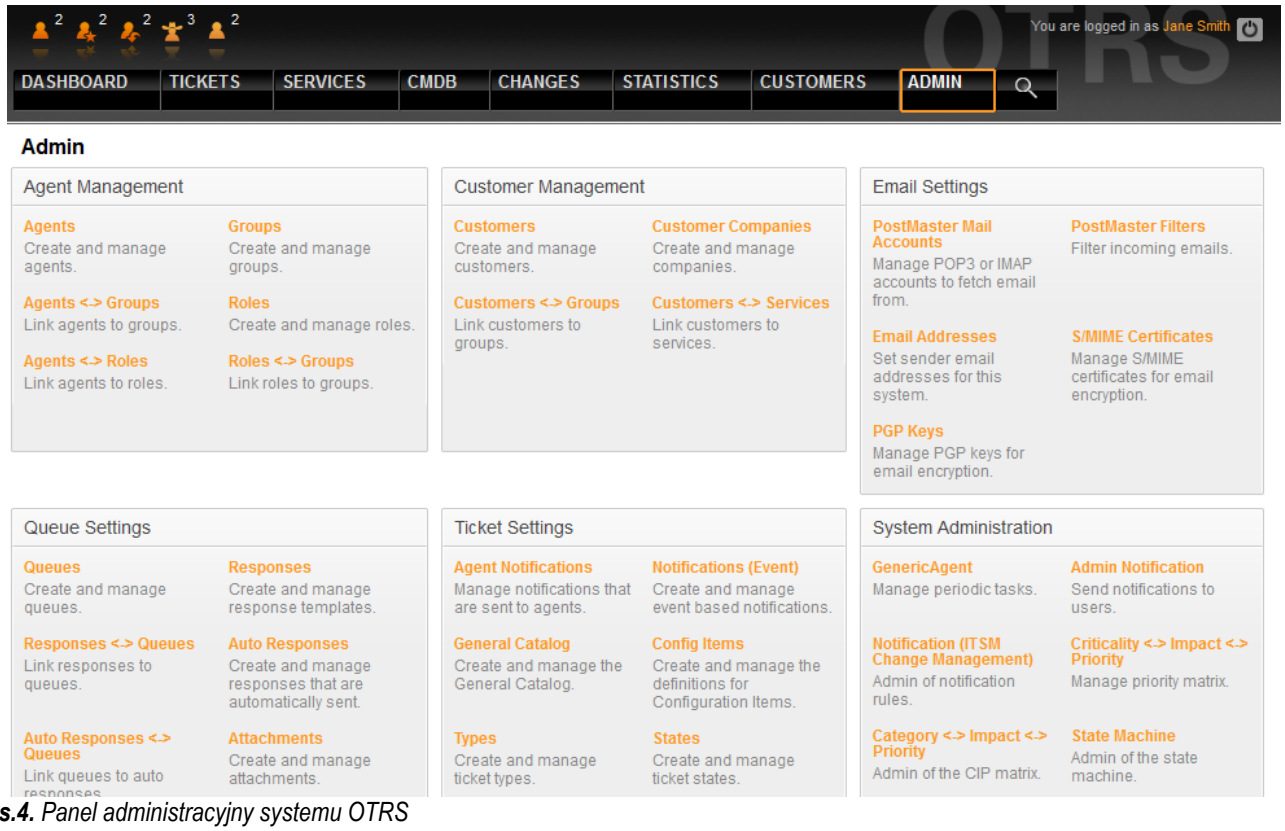
OTRS jest również narzędziem wspomagającym obsługę incydentów bezpieczeństwa teleinformatycznego wykorzystywanym w komórkach dużych organizacji sektorów np. telekomunikacji.

System zintegrowany z serwerem poczty może w prosty sposób zarejestrować podejrzenie incydentu bezpieczeństwa poprzez wysłanie wiadomości elektronicznej na wskazany przez organizację adres e-mail. Może zostać on udostępniony zarówno pracownikom firmy, klientom komercyjnym jak i również klientom zewnętrznym w ramach współpracy centrum szybkiego reagowania. Następnie operator obsługujący zlecenie może je skategoryzować dodając je do odpowiedniej kolejki. Europejska agencja ENISA udostępniła klasyfikację wytycznych podziału incydentów bezpieczeństwa według których organizacje mogą je obsługiwać. Kolejnym krokiem jest wybór pól dynamicznych, które można w dowolny sposób skonfigurować w panelu administratora. Pola dynamiczne pomagają w obsłudze – rozróżnienie klientów, czasy reakcji czy późniejsze raportowanie zbiorcze. Dzięki temu, przy dużej liczbie zgłoszeń można w sposób przejrzysty sklasyfikować istotność incydentów bezpieczeństwa oraz ich wpływ na ciągłość działania organizacji.



Rys.3 *Panel tworzenia nowego zgłoszenia w systemie OTRS*

Ciekawym elementem systemu jest możliwość udostępnienia podglądu zdarzeń dla klientów komercyjnych. Środowisko posiada separację danych oraz dzięki odpowiedniej konfiguracji każdy z klientów może zapoznać się z obsługiwanymi zgłoszeniami przez dostawcę. Dodatkowo całość komunikacji może być szyfrowana, jak również dostęp do portalu wystawionego dla klienta udostępniona



Rys.4. *Panel administracyjny systemu OTRS*

przez bezpieczne połączenie. Generowanie raportów oraz ich podgląd w czasie rzeczywistym działa błyskawicznie, nawet za długi okres czasu. Istnieje możliwość zbiorczego podejrzenia incydentów w trybie edycji na portalu lub pobraniu go do pliku w różnych formatach.

Kolejnym ważnym aspektem jest zarządzanie procesem obsługi danego zgłoszenia oraz możliwość konfiguracji notyfikacji poprzez system pocztowy. Każdy nowy pracownik organizacji obsługujący dany incydent bezpieczeństwa w prosty sposób może wybrać z panelu głównego zakładkę f.a.q. gdzie znajdują się predefiniowane procesy obsługi przedstawione w sposób zarówno tekstowy jak i schematyczny. Przy dużej liczbie zgłoszeń notyfikacja na skrzynkę wiadomości elektronicznych jest pomocna i pozwoli w sposób przejrzysty nimi zarządzać.

Ciekawym rozwiązaniem dla usług komercyjnych jest generowanie dokumentów SLA – Service Level Agreement. Są to raporty zawierające czas reakcji na dane zgłoszenie, które może zostać zapisane w umowie w celu realizacji usługi w sposób odpowiedni i na wysokim poziomie.

Rysunek 4 przedstawia pełny panel administracyjny systemu OTRS. W pierwszej kategorii istnieje możliwość utworzenia agentów – obsługujących operatorów, grupy poziomu dostępu oraz ich relacje, dzięki czemu w pełni elastycznie można przydzielić dostępy do danej grupy osób.

Druga zakładka dotyczy zarządzania klientami. Utworzenie konta klientów, firm oraz usług pozwoli powiązać ich relacje z danymi zgłoszeniami i w pełni automatycznie wypełnić dane klienta.

Trzeci panel pozwala skonfigurować nie tylko serwer poczty elektronicznej i notyfikacji, ale również zarządzać kluczami PGP oraz certyfikatami S/MIME w celu szyfrowania i podpisu zgłoszeń. Dodatkowa opcja to filtracja zgłoszeń przychodzących, szczególnie przydatna funkcja do separacji prawdziwych incydentów od spamu, w momencie udostępnienia adresu w sieci Internet.

Czwartą kategorią jest zarządzanie kolejkami w systemie. Istnieje możliwość podziału kolejek na obsługę zgłoszeń według kategorii w danej organizacji lub np. przydzielenie danej kolejki do klienta komercyjnego. Relacje w tej części panelu służą do utworzenia automatycznych odpowiedzi wobec danej kolejki oraz zarządzania załącznikami.

Przedostatnią kategorią są ustawienia ticketów – zgłoszeń. Każdy obsługujący – agent ma możliwość ustawienia notyfikacji zarówno w formie wiadomości elektronicznej jak i również na głównej stronie środowiska. Ważnym elementem jest również konfiguracja typów oraz statusów zgłoszeń. Poprzez odpowiednie statusy agent jest w stanie na bieżąco weryfikować progres obsługi incydentu bezpieczeństwa oraz wykonać w razie potrzeby odpowiednie eskalacje.

Ostatnią sekcją w panelu jest administracja systemu, gdzie zarządzający środowiskiem może sprawdzić stan uruchomionych usług czy skonfigurować notyfikację zdarzeń systemowych dotyczących ewentualnych błędów. Jedną z ciekawych funkcji w tej części jest utworzenie generycznego agenta, który w sposób programowalny jest w stanie wykonać określone zadanie na bazie danych zawierających zbiór obsłużonych lub obsługiwanych zgłoszeń.

1.3. Integracja z innymi systemami

Wydajna i wieloprocesowa obsługa incydentów bezpieczeństwa teleinformatycznego wymaga, aby rozwiązania oprogramowania OTRS były wysoce zintegrowane z komponentami innych systemów. Generyczny interfejs środowiska zwiększa zdolność do łatwej integracji z istniejącymi na rynku rozwiązania systemowymi w oparciu o usługi sieciowe. Dodatkowo umożliwia jej personalizację przy jednoczesnym zmniejszeniu ryzyka, czasu, kosztu budowy i utrzymania dodatkowego interfejsu.

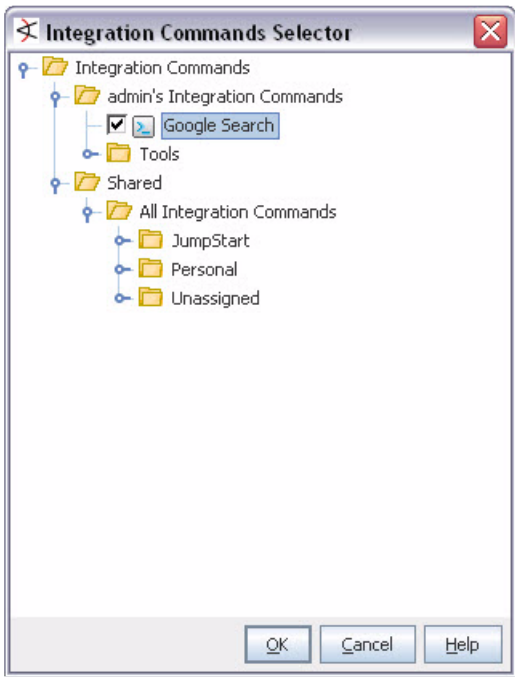
Główne zalety generycznego interfejsu OTRS:
- Modułowy, konfigurowalny i łatwo rozszerzalny framework
- Brak dodatkowych kosztów dostosowania przy zmianie wersji oprogramowania
- Mapowanie połączeń przychodzących i wychodzących
- Kolejkowanie i debugowanie oraz obsługa błędów
- Łatwe połączenie istniejących usług internetowych
- Możliwość wykorzystania istniejących connectorów innych systemów
- SOAP/HTTP jako standard protokołu transmisji
- Możliwość wykorzystania też skryptów klasy REST i JSON
- Graficzny interfejs agent – użytkownika do mapowania danych
- Łatwa i przejrzysta konfiguracja kolejnych serwisów usług sieciowych poprzez wykorzystanie obecnych modułów OTRS

Wiele systemów będących źródłami generującymi lub dostarczającymi incydenty bezpieczeństwa teleinformatycznego można zintegrować z systemem OTRS. Dzięki temu stanowczo skróci się czas obsługi danego incydentu oraz wyeliminuje potencjalne błędy agenta – operatora.

Przykłady aplikacji zintegrowanych z systemem ticketowym:
- System klasy SIEM, np. ArcSight
- Antymalware, np. Fireeye
- Inne systemy obsługi zgłoszeń, np. ITSM Remedy
- antyDDoS, np. Arbor
- serwer pocztowy, np. Exchange
- oprogramowanie SAP
- baza danych zarządzania konfiguracją, np. CMDB
- zarządzanie relacjami z klientami CRM
- system weryfikacji reguł na urządzeniach sieciowych, np. Tufin

Najciekawszą integracją jest na pewno wykorzystanie połączenia między systemami klasy SIEM a OTRS. Cechuje się on centralizacją logów z wielu systemów, ich skorelowaniem poprzez reguły oraz przedstawieniem zdarzeń końcowych gotowych do obsługi jako potencjalne incydenty bezpieczeństwa teleinformatycznego. Obecnie na rynku istnieje wiele systemów klasy SIEM, jednak jednym z liderów jest ArcSight, dzięki silnikowi ESM służącego do analizy w czasie rzeczywistym, profilowaniu aktywności oraz elastycznej wizualizacji danych. Dzięki flexconnectorom system jest w stanie obsłużyć miliardy zdarzeń praktycznie z każdego środowiska / urządzenia dostępnego na rynku. Odebrane zdarzenia należy skorelować i znormalizować poprzez utworzenie specjalnych reguł przypadków użycia. Następnym krokiem jest obsługa takiego eventu przez agenta – operatora poprzez wykonanie kroków odpowiedniej procedury lub instrukcji. Aby przyspieszyć proces i zminimalizować błędy istnieje możliwość integracji systemu ArcSight z OTRS. Wykorzystuje się do tego celu funkcji Integration Commands. Utworzenie takiej komendy na bazie wewnętrznego języka skryptowego spowoduje:
- otworzenie przeglądarki
- wklejenie w pasek adresu wygenerowanego URL
- URL zawiera adres docelowy naszego systemu OTRS
- Utworzenie nowego zgłoszenia z wypełnionymi polami, które są zmapowane z danymi w zdarzeniu systemu ArcSight

Takie zaawansowane połączenie jest możliwe, dzięki wykorzystaniu zmiennych oraz pól dynamicznych zarówno w systemie OTRS jak i ArcSight. Mapowanie tych zmiennych spowoduje ich powiązanie podczas korzystania z komendy zintegrowanej klikając na wygenerowany incydent w systemie monitorowania.



Rys.5. *Funkcja Integration Commands w systemie ArcSight*

PODSUMOWANIE

Podsumowując, system obsługi zgłoszeń OTRS jest bardzo dobrym narzędziem, prostym do wdrożenia, z darmową instancją do późniejszej konfiguracji. Posiada szereg funkcjonalności ułatwiających pracę oraz możliwościami integracji z innymi aplikacjami. Poprzez skalowalność rozwiązania, OTRS jest w stanie funkcjonować stabilnie i spełniać swoją rolę nawet w bardzo dużej organizacji, zarówno w formie obsługi klientów detalicznych czy specjalistycznych incydentów bezpieczeństwa teleinformatycznego. Dodatkowo społeczność środowiska systemowego cały czas rozwija narzędzie i przy odpowiednich, okresowych aktualizacjach, dana firma czy organizacja może posiadać potężne narzędzie usprawniające pracę, zadania czy procesy.

BIBLIOGRAFIA

1. OTRS Group, OTRS Admin Manual, online 2015
2. Strona internetowa firmy OTRS - https://www.otrs.com
3. Strona internetowa społeczności GitHub https://github.com/OTRS/otrs
4. Strona internetowa organizacji ENISA https://www.enisa.europa.eu/
5. Doświadczenie własne – wdrożenie, konfiguracja, obsługa

OTRS as a tool supporting the handling of IT Security incidents

Paper discussed the advantages and functionalities of the OTRS ticketing systems, used to handle incidents in the field of security systems, network or ICT.

Autorzy:
mgr inż. **Maciej Podsiadły** - COMP S.A. Warszawa, maciej.podsiadly@safecomp.com.pl
mgr inż. **Dariusz Podsiadły** – Uniwersytet Technologiczno-Humanistyczny w Radomiu, d.podsiadly@uthrad.pl

JEL: L96 **DOI**: 10.24136/atest.2018.067
Data zgłoszenia: 2018.05.21 **Data akceptacji**: 2018.06.15