openAudit

Bezpieczeństwo szyte na miarę

BEZPIECZNY KOMUNIKATOR DLA FIRM

PoC

Bezpieczeństwo biznesu każdej organizacji zależne jest od jej wizerunku w oczach klientów. Spektakularne włamania do systemów teleinformatycznych, ataki socjotechniczne, na które narażeni są pracownicy firm skutkują ogromnym ryzykiem, odpowiedzialnością karną oraz zaburzeniem stabilności prowadzonej firmy.

WPROWADZENIE

Komunikatory internetowe na dobre zagościły w przestrzeni ogólnoświatowej sieci Internet pod wieloma postaciami. Są to dedykowane aplikacje (takie jak wiele lat temu Gadu-Gady, czy obecnie Skype) ale również wersje wykorzystujące technologię WEB (np. Facebook Messenger). Korzystanie z komunikatorów usprawnia komunikację w życiu prywatnym po to, aby być na bieżąco z tym, co się dzieje u naszych przyjaciół czy rodziny?

Ale co w przypadku firm? Czy można sobie pozwolić na dowolny wybór narzędzi?

Przepisy dotyczące ochrony danych osobowych wymagają, aby przetwarzanie danych osobowych było zorganizowane w taki sposób, aby zminimalizować ryzyka dotyczące ich przetwarzania. Trudno zweryfikować jakie zabezpieczenia stosują światowi giganci jak Google, Facebook czy Microsoft gdyż chronią oni takie informacje przed konkurencją.

Nasze rozwiązanie jest przejrzyste. Zapewniamy funkcjonalność komunikowania się między pracownikami naszych klientów i jednocześnie chronimy prywatność użytkowników nie przechowując treści ich korespondencji oraz stosując kryptograficzne zabezpieczenia przesyłanych informacji.

WADY I ZALETY KORZYSTANIA Z KOMUNIKATORÓW WEWNĄTRZ ORGANIZACJI

ZALETY STOSOWANIA NASZEGO KOMUNIKATORA

1. Całość usługi **„Bezpieczny komunikator dla firm”** utrzymywana jest przez Open Audit bez dostępu dla dostawców zewnętrznych.
2. Klient w każdej chwili może zdecydować o przyszłości kont swoich użytkowników. W przypadku rezygnacji z usługi – usuwamy wszystkie konta użytkowników danego klienta bez możliwości ich odzyskania.
3. Ogromna liczba funkcji komunikatora, najważniejsze z nich:
   - możliwość ręcznego ustawiania statusu dostępności użytkownika (wolny do rozmowy, dostępny, zajęty, w trakcie rozmowy telefonicznej, nie przeszkadzać, niewidoczny). Ustawiony status jest widoczny dla innych użytkowników;
   - możliwość automatycznego ustawiania statusu (np. na niedostępny) użytkownika po określonym czasie jego nieaktywności przy komputerze, co pozwala szybko potwierdzić czy dany użytkownik pracuje przy komputerze;
   - możliwość przesyłania plików pomiędzy użytkownikami;
   - możliwość tworzenia stałych pokojów konferencyjnych dla poszczególnych zespołów (np. pokoje dedykowane dla kierownictwa firmy, pracowników poszczególnych komórek organizacyjnych lub dla powołanych zespołów roboczych);
   - możliwość tworzenia grupowych pokojów konferencyjnych samodzielne przez użytkowników dla wybranych użytkowników;
   - możliwość wysyłania wiadomości z serwera do wszystkich użytkowników (np. o awariach);
   - możliwość samodzielnej zmiany hasła z poziomu komunikatora;
4. Każdy użytkownik ma możliwość komunikowania się ze współpracownikami niezależnie czy są obecnie w biurze, w delegacji czy pracują w domu;
5. Zachowanie całkowitej poufności (nikt nie ma dostępu do treści przesyłanych wiadomości).
6. Wiadomości nie są przechowywane na serwerze, gdy uczestnicy konwersacji są dostępni „online” w komunikatorze. Wiadomości są przechowywane tylko w sytuacji, gdy jedna ze stron nie jest w danym momencie podłączona do komunikatora. Wiadomości są automatycznie usuwane po odczytaniu ich przez użytkownika po podłączeniu się do systemu.

7. Użytkownicy mają możliwość korzystania z komunikatora na komputerach osobistych (firmowych oraz prywatnych), oraz mobilnych (smartfonach).
8. Całkowite szyfrowanie komunikacji pomiędzy użytkownikiem komunikatora, a serwerami.
9. Możliwość zainstalowania komunikatora przez użytkownika bez konieczności działu informatyków.
10. Zapewniamy zgodność z dużą liczbą dostępnych komunikatorów na rynku (wiele z nich jest darmowych) za pomocą protokołu XMPP różnych producentów na różnych platformach (Windows, Linux, JAVA).

WADY STOSOWANIA OGÓLNODOSTĘPNYCH USŁUG KOMUNIKACJI INTERNETOWEJ

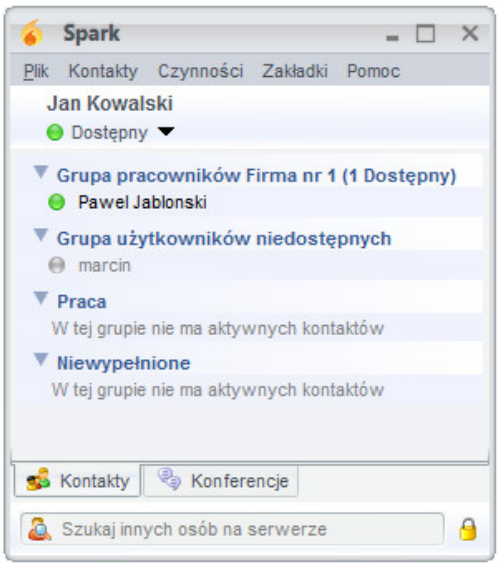
1. Brak kontroli nad informacjami o sesjach użytkowników oraz przesyłaną treścią wiadomości pomiędzy komunikatorem, a serwerem.
2. Brak kontroli nad przechowywanymi na serwerze informacjami (również treścią wiadomości).
3. Brak wpływu na politykę zabezpieczeń dla kont i wiadomości.
4. Wsparcie wyłącznie za pośrednictwem oficjalnych kanałów wsparcia (dla usług płatnych).
5. Brak pewności co tak naprawdę przechowują dostawcy usług oraz czy nie udostępniają danych użytkowników innym dostawcom usług.
6. Brak pewności co się dzieje z danymi użytkowników po zakończeniu świadczenia usługi.

INTERFEJS UŻYTKOWNIKA BEZPIECZNEGO KOMUNIKATORA

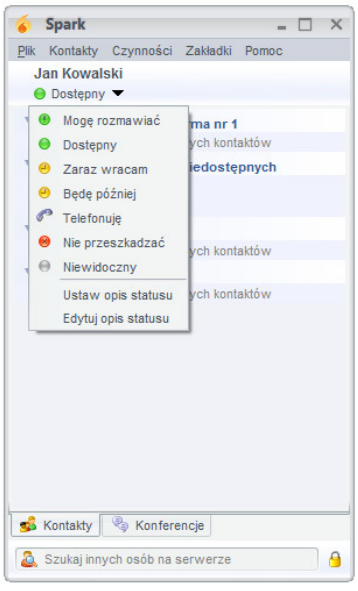
Interfejs użytkownika jest bardzo prosty. Został on zaprojektowany w taki sposób, aby jego obsługa nie sprawiała trudności użytkownikom w każdym wieku.

Podstawowe elementy interfejsu użytkownika, to:

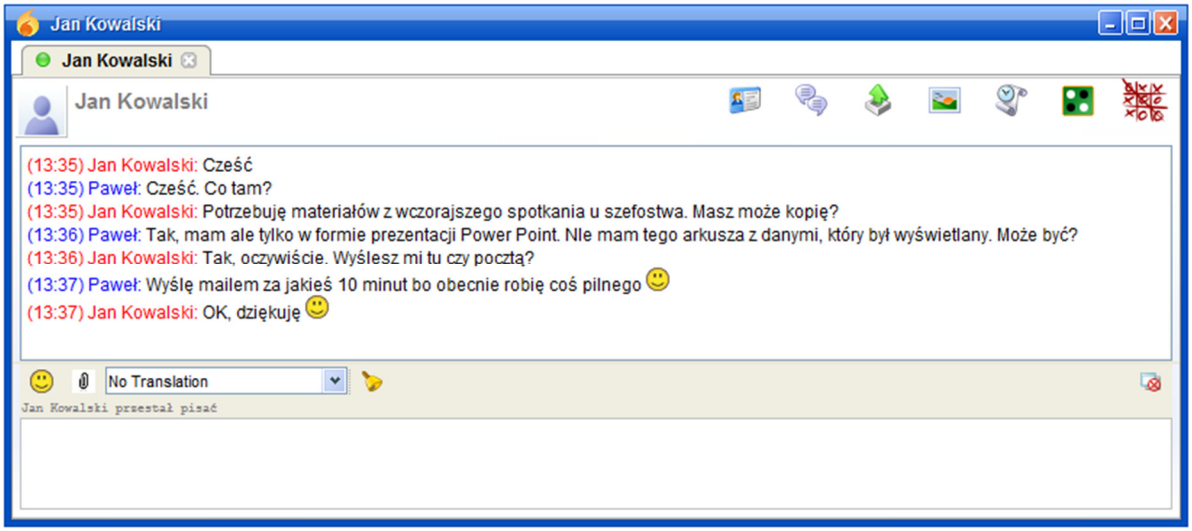
1. **Okno główne (rys. 1 i 2),** w którym wyświetlana jest lista dodanych kontaktów oraz ustawiany jest status obecności użytkownika. W zależności od ustawień aplikacji, użytkownicy mogą być wyświetlani w podziale na grupy (np. pracownicy działu ogólnego, księgowość, kadry itp.). W oknie głównym mogą być wyświetlane również dedykowane pokoje konferencyjne, w których może brać udział wiele osób.
2. **Okno konwersacji (rys. 3),** w którym poszczególni użytkownicy prowadzą rozmowy.



Rysunek 1 Widok listy kontaktów



Rysunek 2 Ustawianie statusu użytkownika



Rysunek 3 Widok okna konwersacji

PROOF OF CONCEPT (POC)

Proof of Concept jest próbnym (testowym) wdrożeniem danego rozwiązania w celu potwierdzenia czy sprawdzi się ono w danej organizacji. Metoda ta pozwala przetestować klientom narzędzie nie zawierając umowy na świadczenie usługi. Klient po zakończeniu okresu testowania podejmuje decyzję czy jest zainteresowany daną usługą, czy nie bez żadnych konsekwencji.

Umożliwiamy przeprowadzenie PoC w różnych wariantach:

1. **Wariant 1,** w którym utrzymujemy część serwerową po naszej stronie, a po stronie użytkowników (pracowników) klienta są instalowane na komputerach komunikatory komunikujące się z naszymi serwerami. Baza użytkowników po stronie serwerów jest lokalna (nie zintegrowana z Active Directory) i zarządzana przez nas lub przez wskazanego przez klienta pracownika.
2. **Wariant 2,** w którym utrzymujemy część serwerową po naszej stronie integrując ją przez Internet z usługą Active Directory klienta. Na komputerach użytkowników instalowane są komunikatory komunikujące się z naszymi serwerami.
3. **Wariant 3**, w którym instalowana jest infrastruktura serwerowa u klienta (np. w DMZ) wraz z komunikatorami na komputerach użytkowników. Serwery komunikacyjne w tej konfiguracji mogą być zintegrowane z Active Directory.

Niezależnie od wybranego wariantu, pracownicy IT otrzymują od nas szczegółową instrukcję instalacji oraz konfiguracji komunikatora internetowego na stacjach użytkowników.

Zakończenie okresu PoC wiąże się z usunięciem wszystkich danych przekazanych do tego zadania przez naszych klientów z naszych serwerów bez możliwości ich odzyskania.

NASZE KOMPETENCJE

OBSZAR PROCESOWEGO ZARZĄDZANIA BEZPIECZEŃSTWEM

- Organizujemy i przeprowadzamy audyty bezpieczeństwa informacji pod kątem zgodności systemów zarządzania bezpieczeństwem informacji z normami grupy ISO/IEC 27000 (w szczególności ISO/IEC 27001);
- Organizujemy i przeprowadzamy audyty bezpieczeństwa systemów informatycznych według standardów COBIT i CISA;
- Organizujemy i przeprowadzamy audyty systemów zarządzania bezpieczeństwem pod kątem zgodności z obowiązującymi regulacjami prawnymi [PL], w szczególności, zgodnie z zapisami:
  - Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne i związanego z nią rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
  - Ustawy o ochronie danych osobowych.
- Projektujemy i budujemy Systemy Zarządzania Bezpieczeństwem Informacji (SZBI);
- Wykonujemy analizy i projektujemy procesy zarządzania bezpieczeństwem w modelu usługowym opartym o:
  - Normę ISO/IEC 20000-1 i ISO/IEC 20000-2;
  - Information Technology Infrastructure Library (ITIL).

Posiadamy wiedzę i doświadczenie związane z regulacjami prawnymi, w tym realizując zadania:

- **Pełnomocników ds. Bezpieczeństwa Cyberprzestrzeni działając na rzecz podmiotu zlecającego (kontrakt);**
- **Architektów i wdrożeniowców wymagań Krajowych Ram Interoperacyjności;**
- **Inspektorów Ochrony Danych**

Osoby kierujące jednostkami administracji publicznej zapewniamy iż nasze pracę są całkowicie zgodne z rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

OBSZAR ZABEZPIECZEŃ TECHNICZNYCH

- Prowadzimy techniczne audyty bezpieczeństwa systemów teleinformatycznych pod kątem wykrycia podatności na ataki (wykonujemy również testy penetracyjne);
- Projektujemy i wdrażamy zabezpieczenia sieci, systemów operacyjnych oraz systemów aplikacyjnych opartych na technologiach WEB;
- Wykonujemy analizę po-włamaniową (w jaki sposób doszło do przełamania zabezpieczeń);
- Wykonujemy analizę bezpieczeństwa systemów teleinformatycznych;
- Odtwarzamy systemy informatyczne po awarii (po kompromitacji systemu).

OBSZAR ANALITYCZNY

- Współpracujemy z zespołami CERT w imieniu naszych klientów;
- Projektujemy i dokumentujemy procesy z wykorzystaniem notacji BPMN;
- Świadczymy usługi konsultacyjne (consulting), podczas:
  - Opracowywania założeń do Specyfikacji Istotnych Warunków Zamówienia. W takiej sytuacji, nasi eksperci pomagają organizacji w przygotowaniu dokumentacji przetargowej. Sami nie bierzemy wówczas udziału w postępowaniu;
  - Negocjacji z innymi dostawcami usług, gdy dochodzi do sytuacji spornych, w których trudno jest wypracować kompromis.

Nasze zespoły są dedykowane dla każdego kontraktu, a klient nie ma problemu z dostępnością konsultantów. Współpracujemy również na podstawie średnio i długo terminowych kontraktów. Wizytówką naszych Kierowników Projektów w czasie spotkań biznesowych jest wiedza, doświadczenie oraz wysoki poziom kultury osobistej. Naszą misją jest popularyzacja mechanizmów zabezpieczających uniemożliwiających kradzież danych z systemów teleinformatycznych. Nie jesteśmy dostawcami technologii, ale w ramach prowadzonych projektów współpracujemy z naszymi partnerami dostarczającymi technologiczne rozwiązania bezpieczeństwa.

MIĘDZYNARODOWE CERTYFIKATY POTWIERDZAJĄCE KWALIFIKACJE BRANŻOWE

- **C|EH (Certified Ethical Hacker / Etyczny Hacker);**
- **CompTIA Security+;**
- **ITILv3;**
- **PRINCE2;**
- **ISO 27001 (audytor wiodący);**
- **ISO 27001 (audytor wewnętrzny);**
- **Zarządzanie ryzykiem w oparciu o standard M_o_R;**
- **RHCE (inżynier systemowy Red Hat Enterprise Linux).**

DANE KONTAKTOWE

OPEN AUDIT MARCIN KURPIEWSKI

ul. Marii Konopnickiej 10, 05-230 Kobyłka

Biuro: 22 535 33 51, office@open-audit.eu

NIP: 758-174-63-18

Osoba bezpośrednio odpowiedzialna:
Marcin Kurpiewski tel. 784 335 380, mk@open-audit.eu