Bezpieczeństwo usług cloudowych

Prowadzący: Artur Cieślik
MBA, IRCA lead auditor ISO/IEC 27001 ISO 22301,CISA
redaktor naczelny „IT Professional”
artur.cieslik@politykabezpieczenstwa.com.pl

Artur Cieślik
politykabezpieczenstwa.com.pl

- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001 IRCA Certified Lead Auditor (nr w rejestrze: 6035034).
- Audytor wiodący normy ISO/IEC 22301 uzyskany zgodnie z IRCA.
- Certified Information Systems Auditor (CISA)
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.
- Współautor już drugiej publikacji „Dokumentacja ochrony danych osobowych ze wzorami” pod redakcją naukową dr hab. nauk prawnych Mariusza Jagielskiego

Problemy z bezpieczeństwem usług cloudowych

- Bezpieczeństwo usług zarządzanych przez usługodawcę
- Użytkownicy korzystający w ”własnych” usług cloudowych – Shadow IT

Shadow IT i cloud

- Admin – źródło najczęstszych problemów to użytkownicy
- User – jest petentem ciągle czekającym na obsługę ze departamentu IT

Shadow IT i cloud

- W głowach wielu użytkowników rodzi się w końcu pomysł pominięcia działu IT.
  - skomplikowane procedury bezpieczeństwa;
  - długotrwałe procesy akceptacji nowych narzędzi ;
  - niekończące się kolejki w helpdesku.

Shadow IT i cloud

- Rozwiązanie?
  - **Nie pytać IT i spróbować szybko stworzyć lub pozyskać aplikację, która ułatwi pracę – z cloudem to możliwe!**
  - **Wdrożyć zewnętrzne repozytorium danych dostępne tylko dla ludzi z mojego działu - tak, każdy teraz może założyć konto w usłudze dysku chmurowego.**

Shadow IT i cloud

- W ten sposób zaczyna się tworzyć się **szara strefa** zarządzania informatyką w przedsiębiorstwie lub instytucji niewidoczna na pierwszy rzut oka zarówno dla zarządzających, jak i samego działu IT.
- Forbes Insight wskazuje, że **więcej niż jedna na pięć organizacji** doświadczyła naruszenia bezpieczeństwa informatycznego z powodu użycia nieautoryzowanego zasobu IT.

Shadow IT i cloud

- Ryzyka:
  - prywatne skrzynki e-mail użytkowników,
  - **aplikacje instalowane na komputerze lub użytkowane w modelu SaaS**,
  - także prywatny sprzęt podłączany do sieci instytucji;

Shadow IT i cloud

- Powszechnym przykładem utraty danych z powodu praktyk shadow IT jest prywatne konto dysku cloudowego.

Dobre i złe strony własnej infrastruktury

- Dobre
  - Kontrola nad fizycznym dostępem do danych
  - Mniejsze obciążenie subskrypcjami za korzystanie z usług
  - Mniejsze uzależnienie od łącza internetowego
  - Możliwość osiągania wysokich wydajności dla lokalnych użytkowników
  - Szybkie lokalne odzyskanie danych w przypadku utraty
  - Brak lub mniejsze uzależnienie się od dostawcy usług cloudowych
  - Większa rozliczalność działań wykonawców
  - Większe możliwości migracji danych do innego środowiska
  - Brak konieczności transferu danych osobowych poza organizację

Dobre i złe strony własnej infrastruktury

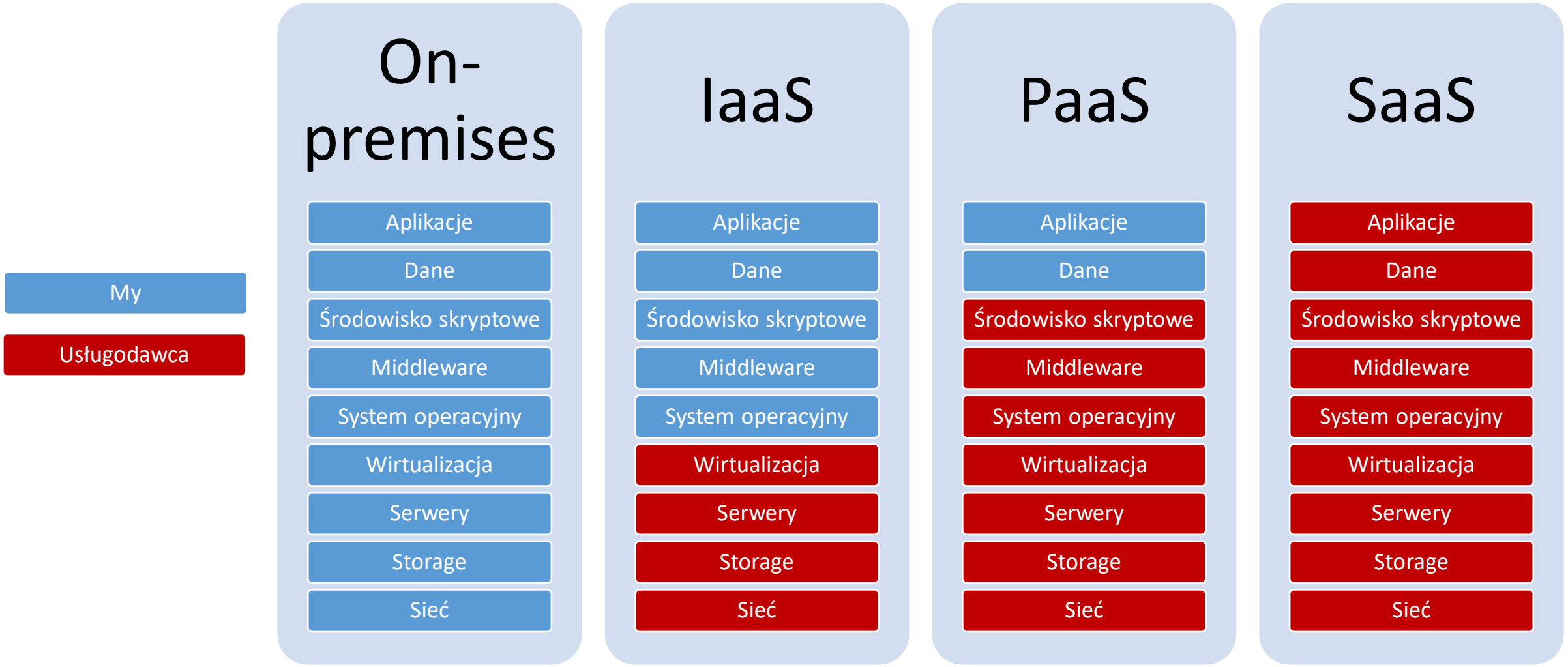
- Złe
  - Koszty rozbudowy i wymiany przestarzałych urządzeń
  - Trudne do osiągnięcia bezpieczeństwo datacenter fizyczne i środowiskowe na poziomie TIER III, TIER IV
  - Utrzymanie i aktualizacja urządzeń oraz oprogramowania
  - Utworzenie i utrzymanie niezależnego od IT zespołu SOC
  - Utrzymanie wysokiego poziomu redundancji
  - Może utrudniać działania dla użytkowników mobilnych
  - Mniejsze możliwości skalowania środowiska w przypadku zwiększenia zapotrzebowania na pojemność

Rodzaje usług cloudowych

- Niewątpliwe zalety usług chmurowych:
  - niezawodność
  - wysoka dostępność przetwarzania
  - użytkownicy mogą uzyskiwać dostęp do danych i aplikacji w chmurze bez względu na to, gdzie się znajdują i z jakiego urządzenia korzystają

Rodzaje usług cloudowych

- Odpowiedzialność za bezpieczeństwo danych jest zarówno po stronie dostawcy usługi chmurowej, jak i usługobiorcy.
- Zakres odpowiedzialności usługobiorcy zależy od rodzaju usług:
  - **SaaS** – Software as a Service (np. Microsoft 365 lub Salesforce) — odpowiedzialność za zabezpieczenie danych oraz dostęp użytkowników.
  - **PaaS** – Platform as a Service (np. Microsoft Azure, cloud SAP lub Heroku)— odpowiedzialność za zabezpieczenie danych, dostęp użytkowników i zabezpieczenie aplikacji.
  - **IaaS** – Infrastracture as a Service (np. Amazon Web Services (AWS) lub Microsoft Azure) — odpowiedzialność za zabezpieczenie danych, dostępu użytkowników, aplikacji, systemów operacyjnych i ruchu w sieci wirtualnej


My
Usługodawca
On-premises
Aplikacje
Dane
Środowisko skryptowe
Middleware
System operacyjny
Wirtualizacja
Serwery
Storage
Sieć
IaaS
Aplikacje
Dane
Środowisko skryptowe
Middleware
System operacyjny
Wirtualizacja
Serwery
Storage
Sieć
PaaS
Aplikacje
Dane
Środowisko skryptowe
Middleware
System operacyjny
Wirtualizacja
Serwery
Storage
Sieć
SaaS
Aplikacje
Dane
Środowisko skryptowe
Middleware
System operacyjny
Wirtualizacja
Serwery
Storage
Sieć

Za co zatem odpowiada dostawca usług chmurowej?

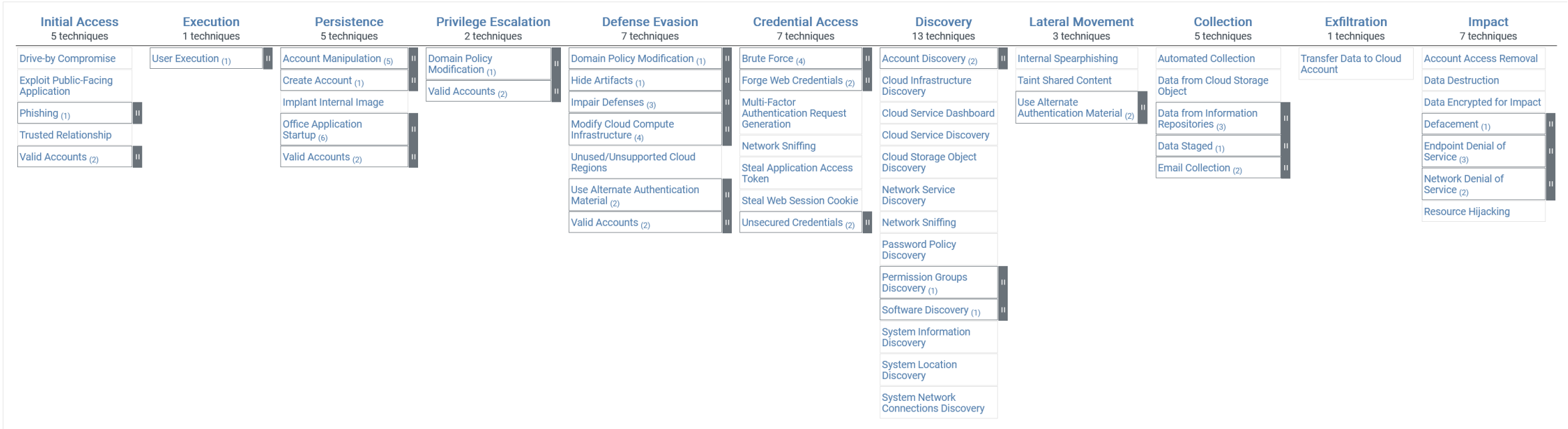
- Zazwyczaj dostawca usługi chmurowej odpowiada:
  - ciągłość działania usługi;
  - bezpieczeństwo fizyczne infrastruktury serwerowej;
  - procedury odtwarzania po katastrofie;
  - aktualizacje systemów;
  - kopie zapasowe.
- Najwięksi dostawcy usług chmurowych oferują funkcje bezpieczeństwa co najmniej na poziomie tradycyjnego modelu bezpieczeństwa IT. Ponadto zapewniają spełnienie wymagań dotyczących bezpieczeństwa informacji i ochrony danych osobowych.

Za co zatem odpowiada dostawca usług chmurowej?

- Dostawcy usług chmurowych starają się zapewnić wysokiej jakości bezpieczeństwo danych. Jednym rozwiązań jest wdrożenie kompleksowych polityk bezpieczeństwa.
- Główni dostawcy usług chmurowych są w stanie wykazać się certyfikatami: ISO/IEC 27001, ISO 22301, ISO/IEC 27017, ISO/IEC 27018 czy ISO/IEC 27701.
- Przykład: AWS, Microsoft Office 365

Zagrożenia dla usług cloudowych wg MITRE ATT&CK

- https://attack.mitre.org/matrices/enterprise/cloud/



Zagrożenia dla usług cloudowych wg Cloud Security Alliance

- https://cloudsecurityalliance.org/

- Niewystarczająca zarządzanie tożsamością, poświadczeniami, dostępem i kluczami
- Niezabezpieczone interfejsy i API
- Błędna konfiguracja i nieodpowiednia kontrola zmian
- Brak architektury i strategii bezpieczeństwa w chmurze
- Niebezpieczny rozwój oprogramowania
- Niezabezpieczone zasoby stron trzecich
- Luki w systemie
- Przypadkowe ujawnienie/ujawnienie danych w chmurze
- Błędna konfiguracja i wykorzystywanie obciążeń bezserwerowych i kontenerowych
- Przestępczość zorganizowana/hakerzy/APT
- Eksfiltracja danych w chmurze

Zagrożenia dla usług cloudowych

- Przykład z 26.08.2022. Haker kradnie kod źródłowy, i zastrzeżone dane z usługi LastPass

- Firma twierdzi, że nieautoryzowany użytkownik włamał się na jedno konto programisty, aby ukraść części środowiska programistycznego LastPass. „Nie ma dowodów na to, że atakujący uzyskał dostęp do danych klientów lub zaszyfrowanych sejfów haseł”, powiedział rzecznik LastPass, Nikolett Bacso-Albaum, Information Security Media Group. Incydent miał miejsce dwa tygodnie temu.
- Zgodnie z informacją na stronie internetowej LastPass ilość użytkowników usługi do przeszło **33 mln**.

Bezpieczeństwo informacji dla usług cloudowych

- Zgodnie z normą ISO/IEC 27017 zaleca się uwzględnić następujące aspekty bezpieczeństwa informacji dla usługi cloudowej:
  - Należy założyć, że informacje przechowywane w usłudze są dostępne dla dostawcy usługi, stąd wymagane jest podpisanie umowy powierzenia przetwarzania danych osobowych.
  - Należy wskazać geograficzne lokalizacji naszych danych w umowach i zapewnić spełnienie wymagań ochrony danych osobowych obowiązujących w EU.
  - Zasoby usługi chmurowej powinny zostać uwzględnione w wymaganiach polityki bezpieczeństwa usługobiorcy.
  - Role i odpowiedzialność za bezpieczeństwo informacji powinny być uzgodnione pomiędzy stronami i zapisane w umowie.

Bezpieczeństwo informacji dla usług cloudowych

- Zgodnie z normą ISO/IEC 27017 zaleca się uwzględnić następujące aspekty bezpieczeństwa informacji dla usługi cloudowej:
  - Usługobiorca powinien uwzględnić ryzyka w swojej analizie zgodnie z normą ISO/IEC 27001 np. zgodnie z ENISA 2009, *Cloud Computing Security Risk Assessment.*
  - Usługobiorca powinien określić sposób kontaktu z władzami adekwatnie do usług chmurowej.
  - Kontrola dostępu do usług powinna zapewnić spełnienie wymagań:
    - Wskazania zasad rejestracji i wyrejestrowania użytkowników.
    - Określenie poziomu uprawnień dla dostępu poszczególnych grup użytkowników.
    - Określenie metod uwierzytelnienia ze wskazaniem ilości składników.
    - Określenie polityki haseł spełniającej wymagania przepisów o ochronie danych osobowych.
    - Zapewnienie ograniczenia dostępu do danych w usłudze.

Bezpieczeństwo informacji dla usług cloudowych

- Zgodnie z normą ISO/IEC 27017 zaleca się uwzględnić następujące aspekty bezpieczeństwa informacji dla usługi cloudowej:
  - Stosowanie kryptografii stosowanie do wyników analizy ryzyka. Należy uwzględni szyfrowanie danych przechowywanych w usłudze oraz przesyłane do i z usługi.
  - W przypadku stosowani kluczy kryptograficznych, należy uzyskać informacji o rodzaju kluczy, sposobie zarządzania kluczami.
  - Usługodawca powinien zapewnić, ze posiada polityki i procedury pozwalające na bezpiecznie przekazywanie oraz ponownie użycie zasobów usługi.
  - Należy monitorować zmiany w usłudze i uwzględnić w procedurach nadzoru nad zmianami.

Bezpieczeństwo informacji dla usług cloudowych

- Zgodnie z normą ISO/IEC 27017 zaleca się uwzględnić następujące aspekty bezpieczeństwa informacji dla usługi cloudowej:
  - Należy zapewnić monitorowanie pojemności usługi.
  - Usługodawca powinien zapewnić sposób wykonywania kopii zapasowych danych przechowywanych w usłudze oraz programów służących do ich przetwarzania.
  - Strony powinny uzgodnić sposób logowania zdarzeń w usłudze i archiwizowania logów.
  - Usługa powinna zapewniać logowanie działań użytkowników uprzywilejowanych.
  - Usługobiorca powinien uzgodnić wzorzec czasu wykorzystywany w usłudze.
  - Usługodawca powinien dostarczyć informacje o sposobie zarządzania podatnościami technicznymi.

Bezpieczeństwo informacji dla usług cloudowych

- Zgodnie z normą ISO/IEC 27017 zaleca się uwzględnić następujące aspekty bezpieczeństwa informacji dla usługi cloudowej:
  - Należy regularnie oceniać spełnienie wymagań bezpieczeństwa informacji przez usługodawcę.
  - Usługobiorca powinien żądać od usługodawcy informacji o stosowanych procedurach i praktykach związanych z rozwojem usługi.
  - Usługodawca powinien zapewnić procedury zarządzania incydentami.
  - Usługodawca i usługobiorca powinni zapewnić spełnienie wymagań w zakresie ciągłości działania usługi.

Bezpieczeństwo informacji dla usług cloudowych – zapisy umowy

- Umowa na usługę cloudową może zawierać odpowiedzialność i sposób:
  - Zabezpieczenia przed malware.
  - Kopie zapasowe.
  - Wykorzystania kryptografii.
  - Zarządzania podatnościami.
  - Zarządzania incydentami.
  - Zapewnienia zgodności z wymaganiami technicznymi.
  - Testowania zabezpieczeń.
  - Audytowania.
  - Zarządzania logami, zabezpieczania dowodów oraz śladów audytowych.
  - Zabezpieczenia informacji po zakończeniu umowy.
  - Sposób kontroli dostępu i uwierzytelniania.
  - Sposób identyfikacji użytkownika.

Dziękuję za uwagę