COMARCH

Wymagania dot. bezpiecznego korzystania z Chmury Comarch Standard, Comarch Enterprise oraz Comarch Hosting ze stacji roboczych oraz urządzeń mobilnych dla Klientów i Partnerów Grupy Comarch

Spis treści

1 Wstęp

1.1 Postanowienia ogólne

Poniższy regulamin przedstawia zasady bezpiecznego korzystania z Chmury Comarch Standard, Comarch Enterprise oraz Comarch Hosting. Wytyczne zawarte w punkcie 4 dotyczą tylko usług Comarch Enterprise oraz Comarch Hosting, pozostałe punkty odnoszą się do wszystkich usług.

1.2 Definicja bezpieczeństwa IT

Bezpieczeństwo IT jest to zbiór reguł, określający metody ochrony informacji, a zwłaszcza sposoby ich przetwarzania. Ma to na celu zapobieganie manipulacji danymi i systemami przez nieuprawnione osoby trzecie. Bezpieczeństwo IT rozważa się w trzech kluczowych aspektach, które znane są jako triada CIA. W skład tych zagadnień wchodzi:

- dostępność – informacje powinny być spójne i łatwo dostępne dla upoważnionych stron w każdym żądanym przez użytkownika momencie;
- integralność – polega na utrzymaniu spójności, dokładności i wiarygodności danych w całym cyklu życia;
- poufność – polega na zapewnieniu, że próby dostępu do danych przez nieautoryzowanych użytkowników zakończą się niepowodzeniem.

1.3 Oznaczenie danych

Dane przetrzymywane przez Klienta/Partnera i poddawane do użytku przez produkty Grupy Comarch powinny być uprzednio sklasyfikowane. Ważne jest dokładne określenie danych poufnych. Informacje poufne stanowią w szczególności:

- Informacje dot. realizowanych kontraktów;
- informacje finansowe firmy;
- dane dostępowe do systemów IT;
- dane osobowe;
- inne informacje, które są uznawane przez ogół firmy jako „poufne”.

1.4 Metryki podatności

Podatności w zabezpieczeniach systemów komputerowych są klasyfikowane według istotności *(ang. Severity*) za pomocą otwartego branżowego standardu *Common Vulnerability Scoring System (CVSS).* CVSS klasyfikuje luki na czterech poziomach: Niskie *(ang. Low)*, Średnie *(ang. Medium)*, Wysokie *(ang. High)* oraz Krytyczne *(ang. Critical).* CVSS jest własnością FIRST.Org, Inc. (FIRST), amerykańskiej organizacji non-profit, której misją jest pomoc zespołom reagowania na incydenty bezpieczeństwa komputerowego na całym świecie. National Vulnerability Database (NVD), będąca amerykańskim rządowym repozytorium danych dotyczących zarządzania lukami w zabezpieczeniach opartych na standardach, reprezentowanych za pomocą protokołu Security Content Automation Protocol (SCAP), zawiera wyniki CVSS dla prawie wszystkich znanych luk w zabezpieczeniach oprogramowania związanych z bezpieczeństwem, błędami konfiguracji, nazwami produktów i metrykami wpływu.

Aktualna wersja CVSS (CVSSv3.1) została wydana w czerwcu 2019 i przedstawia sposób obliczania poziomu ważności podatności systemów, w oparciu o przyjęte przez organizację kryteria. CVSS składa się z trzech grup metryk: podstawowej (ang. *Base*), czasowej (ang. *Temporal*) i środowiskowej (ang. *Environmental*).

Metryki podstawowe dają wynik w zakresie od 0 do 10, który można następnie modyfikować, oceniając metryki czasowe i środowiskowe.

Metryki CVSS v3.1	
Istotność	**Ocena podstawowa**
Brak	0.0
Niska	0.1 – 3.9
Średni	4.0 – 6.9
Wysoka	7.0 – 8.9
Krytyczna	9.0 – 10.0

Poniższy Regulamin traktuje CVSS jako punkt odniesienia w klasyfikacji luk bezpieczeństwa. Pełna dokumentacja standardu wraz z kalkulatorem metryk dostępna jest pod adresem: *https://www.first.org/cvss/.*

2 Kontrola dostępu

2.1 Zasada najmniejszych uprawnień

Klient/Partner Grupy Comarch zobowiązany jest do przestrzegania zasady najmniejszych uprawnień (*ang. least privilege*) w całej swojej organizacji. Oznacza to, każdy pracownik Klienta/Partnera otrzymuje minimalne uprawnienia, jakie są niezbędne do wykonywania powierzonych zadań. Domyślne uprawnienia w systemach teleinformatycznych Klienta/Partnera mają być ustawione na zabronione (*ang. permission denied*), a dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator systemów IT Klienta/Partnera przyznaje stosowne uprawnienia. Cały proces przyznawania uprawnień powinien się odbywać po uprzednim poinformowaniu oraz akceptacji wniosku o nadanie uprawnień przez przełożonych w strukturze organizacji Klienta/Partnera.

2.2 Zarządzanie dostępem użytkowników

W celu zapobiegania nieuprawnionemu dostępowi do systemów IT należy:

- przestrzegać zasady najmniejszych uprawnień;
- zapewniać zgodności zasad kontroli dostępu z klasyfikacją informacji;
- nadawać użytkownikom unikalnych identyfikatorów oraz nazw użytkowników, które zapewniają jednoznaczną identyfikację;
- wprowadzać mechanizm rozliczalności działań dla kont administratora;
- ograniczać tylko do uzasadnionych przypadków zgody na używanie kont grupowych;
- przeprowadzania okresowych przeglądów przyznanych praw dostępu.

2.3 Zabezpieczenie stacji roboczych oraz dostęp do danych poufnych

Stacje robocze powinny być zabezpieczone przed nieautoryzowanym dostępem osób trzecich, zaś dostęp do danych poufnych powinien być ograniczony do minimum. W tym celu Klient/Partner zobowiązany jest:

- dostęp do danych poufnych realizować tylko na przeznaczonych do tego celu serwerach;
- logować każdą próbę uzyskania dostępu do serwerów zwierających dane poufne (zarówno udaną jak i nieudaną);
- szyfrować dyski twarde przenośnych stacji roboczych;
- zapewnić dostęp do sieci wewnętrznej z zewnątrz za pomocą bezpiecznego kanału szyfrowanego;

- zainstalować oprogramowanie antywirusowe na każdej stacji roboczej;
- zabezpieczyć sieć firmową za pomocą systemu typu firewall;
- regularnie aktualizować swoje systemy;
- wymagać podania hasła przed uzyskaniem dostępu do infrastruktury teleinformatycznej Klienta/Partnera;
- nie otwierać załączników/linków pochodzących z nieznanych źródeł;
- nie pozostawiać niezablokowanych stacji roboczych bez nadzoru.

2.4 Urządzenia mobilne

Urządzenia mobilne, na których Klient/Partner korzysta z usług Grupy Comarch powinny być odpowiednio zabezpieczone. W tym celu Klient/Partner zobowiązuje się do:

- niepozostawiania urządzeń mobilnych bez nadzoru oraz blokowania ekranu na czas, gdy nie korzysta się z urządzenia;
- korzystania z kodu bądź hasła, znanego tylko użytkownikowi urządzenia, które służy do odblokowania ekranu;
- regularnego aktualizowania systemu operacyjnego oraz aplikacji znajdujących się na urządzeniu mobilnym;
- wyłączenia Wi-Fi oraz Bluetooth, jeśli w danym momencie nie jest wykorzystywane;
- niełączenia się z niezaufanymi (publicznymi) sieciami bezprzewodowymi;
- niełączenia się z niezabezpieczonymi, otwartymi sieciami bezprzewodowymi, chyba że Klient/Partner zestawi bezpieczne połączenie z zaufaną siecią za pomocą tunelu VPN;
- nieotwierania załączników/linków pochodzących z nieznanych źródeł;
- pobierania aplikacji tylko z zaufanych źródeł (Google Play lub App Store);
- udzielania instalowanym aplikacjom najniższych możliwych uprawnień, jakie pozwolą na poprawne jej działanie;
- niełączenia przewodowo urządzeń mobilnych z niezaufanymi stacjami.

2.5 Hasła

Z powodu konieczności zabezpieczania infrastruktury teleinformatycznej za pomocą haseł, wymaga się od Klienta/Partnera:

- wymuszenia okresowej zmiany haseł;
- wdrożenia logowania dwuetapowego do newralgicznych systemów;
- tworzenia bezpiecznych haseł (minimum 8 znaków, w tym małe i wielkie litery, minimum jedna cyfra i jeden znak specjalny);
- tworzenia haseł w sposób losowy, tzn. hasła nie mogą być częściowo lub w pełni wyrażeniami słownikowymi;
- nieprzechowywania haseł w postaci otwartej (*ang. plaintext*);
- stosowania przez jednego użytkownika różnych haseł do różnych elementów infrastruktury IT Klienta/Partnera;
- opracowania wewnętrznej polityki tworzenia bezpiecznych haseł;
- zalecane jest korzystanie z menedżera haseł.

3 Specyfika Chmury Comarch Standard, Comarch Enterprise oraz Comarch Hosting

Specyfika Chmury Comarch Enterprise, Comarch Hosting oraz Chmury Standard dostępna jest pod poniższym linkiem: *https://www.comarch-cloud.pl/charakterystyka-chmury/*

4 Chmura Comarch Enterprise oraz Comarch Hosting

4.1 Warunki bezpiecznego korzystania z Chmury Comarch Enterprise/Comarch Hosting

- Klient/Partner:
  - powinien posiadać wiedzę techniczną niezbędną do zapewnienia poprawnej administracji zasobami udostępnionymi w ramach Chmury Comarch Enterprise/ Hosting;
  - może instalować oraz aktualizować usługi firm trzecich na Chmurze Enterprise/Hosting, jednakże bierze pełną odpowiedzialność za posiadanie wymaganych przez te produkty licencji;
  - potwierdza, że instalowane przez niego oprogramowanie na Chmurze Enterprise/Hosting, niebędące produktem firmy Comarch, pochodzi z zaufanych źródeł;
  - zobowiązuje się nie korzystać z sieci TOR (trasowanie cebulowe) oraz innych narzędzi służących do anonimizacji ruchu na serwerach Chmury Enterprise/Hosting;
  - zobowiązuje się nie wysyłać niechcianej poczty elektronicznej oraz nie przełamywać zabezpieczeń oraz nie podejmować prób przedostania się (np. skanowanie portów, sniffing, itp.) na infrastrukturę osób trzecich z wykorzystaniem Chmury Enterprise/Hosting;
  - zobowiązuje się nie pozyskiwać kryptowalut z wykorzystaniem Chmury Comarch Enterprise/Hosting;
  - zobowiązany jest do wykonywania okresowych kopii zapasowych swoich danych przetrzymywanych na Chmurze Enterprise/Hosting;
  - akceptuje fakt, że niektóre dostępne w Internecie usługi, które są niebezpieczne, zabronione przez przepisy prawa i ich regulaminy, są z góry zablokowane ze względu na bezpieczeństwo Chmury Enterprise/Hosting;
  - akceptuje fakt, że ze względu bezpieczeństwa komunikacja wykorzystująca protokół UDP oraz ICMP może być z góry zablokowana;
  - zobowiązuje się do niewyłączania oraz nieusuwania programu antywirusowego, jaki jest zainstalowany na Chmurze Enterprise/Hosting.
  - zobowiązuje się nie łączyć z systemami Chmury Enterprise/Hosting z krajów posiadających wzmożoną aktywność cyberprzestępczą;
  - akceptuje fakt, iż jego lokalizacja podczas łączenia się z Chmurą Enterprise/Hosting może być śledzona przy pomocy systemów korzystających z GeoIP;
  - zobowiązuje się nie instalować na systemach Chmury Enterprise/Hosting oprogramowania pozwalającego na korzystanie z tuneli wirtualnej sieci prywatnej (VPN);

- zobowiązuje się do korzystania z uprawnień administratorskich tylko w sytuacji, gdy będzie do tego uzasadniona potrzeba, zaś podczas codziennego korzystania z usług w ramach Chmury Enterprise/Hosting będzie wykorzystywał konto nieuprzywilejowanego użytkownika;
- akceptuje fakt, iż dostęp do stron o charakterze rasistowskim, homofobicznym, pornograficznym, hackerskim oraz do stron zawierających treści nielegalne może być z góry zablokowany;
- jeśli dotyczy to danego Klienta, zobowiązuje się do przestrzegania normy PCI DSS (ang. *Payment Card Industry Data Security Standard*), a dane przechowywane w ramach tego standardu oraz pliki konfiguracyjne zawierające dane logowania muszą być szyfrowane;
- zobowiązuje się do hostowania na Chmurze Enterprise/Hosting tylko takich witryn, które są stworzone za pomocą frameworków uznanych w świecie IT za bezpieczne;
- jest odpowiedzialny za serwisy oraz strony internetowe wraz z wszystkimi plikami do nich należącymi, jakie tworzy w Chmurze Enterprise/Hosting;
- w przypadku wykrycia podatności zobowiązuje się do niezwłocznego poinformowania firmy Comarch oraz podjęcia odpowiednich działań w celu ich usunięcia;
- jest świadomy, że w przypadku, gdy konieczne będzie odzyskanie danych oraz systemów z wykorzystaniem kopii zapasowych, proces ponownego uruchomienia usługi z pełną jej funkcjonalnością może trwać około 2 tygodni. W tym czasie nie obowiązują ustalenia związane z SLA;
- przyjmuje do wiadomości, iż w sytuacji, gdy jest to konieczne, (np. atak DDOS lub atak na aplikację Klienta/Partnera, który wpływa na pozostałe części Chmury Enterprise/Hosting lub uniemożliwia pracę pozostałym Klientom/Partnerom), firma Comarch, w celu podjęcia odpowiednich działań zapobiegawczych, może dokonać czasowej blokady dostępu do Chmury Enterprise/Hosting, bądź jej modyfikacji w niezbędnym zakresie (w tym modyfikacji materiałów Klienta/Partnera, które stanowią zagrożenie), o czym niezwłocznie zawiadamia Klienta/Partnera.
  Z uwagi na to, iż czynność ta podejmowana jest w interesie Klienta/Partnera, Klient/Partner wyraża na to zgodę i nie jest wówczas uprawniony do zwrotu jakichkolwiek opłat z tytułu Usług.

- Mając na uwadze bezpieczeństwo Chmury Enterprise/Hosting poniższe działania należy uznać za niedozwolone:
  - prowadzenia badań oraz tworzenia złośliwego oprogramowania na środowisku Comarch Enterprise/Hosting; tworzenie aplikacji internetowych, które maja na celu przechowywanie, udostępnianie i synchronizację danych;
  - tworzenie maszyn wirtualnych na Chmurze Enterprise/Hosting;
  - podłączanie maszyn Chmury Enterprise/Hosting do botnetu;
  - współdzielenie kont na Chmurze Enterprise/Hosting;
  - korzystanie z domyślnych haseł oraz haseł tworzonych niezgodnie z pkt 2.5
  - skanowanie oraz wykonywania audytów bezpieczeństwa wewnętrznej sieci firmy Comarch z wykorzystaniem Chmury Enterprise/Hosting;
  - łączenie z maszynami Chmury Enterprise/Hosting z sieci publicznej, chyba że Klient/Partner zestawi bezpieczne połączenie z zaufaną siecią za pomocą tunelu VPN;
  - udostępnianie publicznie baz danych, które są podpięte pod usługi hostowane na Chmurze Enterprise/Hosting;
  - mapowanie dysków lokalnych z dyskami maszyn Chmury Enterprise/Hosting;

- omijanie firewallu firmy Comarch podczas korzystania z Chmury Enterprise/Hosting;
- zamieszczanie przez Klienta/Partnera treści:
  - obraźliwych, stanowiących groźbę skierowaną do innych osób;
  - naruszających w inny sposób dobre obyczaje - na przykład erotyka, przepisy obowiązującego prawa, normy społeczne lub obyczajowe;
  - propagujących poglądy nazistowskie, faszystowskie i im pokrewne.

- Firma Comarch nie ponosi odpowiedzialności za treść danych, jakie Klient/Partner przetrzymuje w Chmurze Enterprise/Hosting;
- W przypadku wykrycia ruchu, który może świadczyć o ingerencji osób trzecich, firma Comarch zastrzega sobie prawo do czasowego wyłączenia Usługi. Klient/Partner zobowiązuje się do dostarczenia informacji o wykrytym ruchu, jeśli był jego źródłem;
- W przypadku otrzymania powiadomienia przez osobę trzecią, uprawnioną, bądź organ władzy państwowej, Comarch zastrzega sobie prawo do modyfikowania lub usuwania treści zamieszczanych przez Klienta, w sytuacji stwierdzenia, że mogą one stanowić naruszenie niniejszego Regulaminu lub obowiązujących przepisów prawa. Firma Comarch nie kontroluje na bieżąco zamieszczanych treści;
- Firma Comarch zastrzega sobie prawo do wprowadzenia zmian w zakresie systemów operacyjnych i dostępnych aplikacji, zwłaszcza wykonując aktualizacje, które mają na celu łatanie luk bezpieczeństwa. Klient/Partner jest odpowiednio wcześniej informowany o wykonywanych aktualizacjach;
- Naruszenie bezpieczeństwa oraz dane wrażliwe:
- Klient/Partner zobowiązuje się zgłaszać firmie Comarch, wykorzystując oficjalną drogę komunikacji, wszelakie naruszenia bezpieczeństwa w swojej organizacji. Dotyczy to również podejrzeń o wystąpieniu incydentu bezpieczeństwa.
- W przypadku wykrycia złośliwego oprogramowania, nielegalnego oprogramowania do którego Klient/Partner nie posiada licencji lub pochodzącego z nieznanych źródeł (tzw. oprogramowanie pirackie) lub stwierdzenia innych naruszeń bezpieczeństwa Klient/Partner zobowiązany jest do natychmiastowego (w ciągu 12h) usunięcia tego oprogramowania/powstałych naruszeń. W przeciwnym przypadku firma Comarch zastrzega sobie prawo do zablokowania dostępu do usługi, a następnie wypowiedzenia umowy. W przypadku, gdy oprogramowanie może spowodować wystąpienie zakłóceń, firma Comarch zastrzega sobie prawo do jego modyfikacji lub usunięcia. Klient zobowiązany jest usunąć podatność (wg kategorii z pkt 1.4. regulaminu) zgodnie z poniższym harmonogramem:
  - podatność krytyczna w ciągu 3 dni kalendarzowych;
  - podatność wysoka w ciągu 14 dni kalendarzowych;
  - podatność średnia w ciągu 30 dni kalendarzowych;
  - podatność niska w ciągu 90 dni kalendarzowych.

  W przeciwnym przypadku firma Comarch zastrzega sobie prawo do zablokowania dostępu do usługi, a następnie wypowiedzenia umowy;
- Zaleca się:
  - aby Klient/Partner stworzył pisemną procedurę postępowania w przypadku wystąpienia naruszenia bezpieczeństwa, np. wycieku danych, zaszyfrowania zasobów, usługi itp.;
  - aby procedura zawierała informację o osobach odpowiedzianych;
  - aby Klient/Partner stworzył oraz stosował wewnętrzną politykę bezpieczeństwa.

- W przypadku konieczności przekazania danych wrażliwych opisanych w punkcie 1.3 Klient/Partner zobowiązuje się do zabezpieczenia tych danych przed dostępem osób nieupoważnionych i do zachowania szczególnych zasad bezpieczeństwa.
- Zalecenia do bezpiecznego przekazania danych wrażliwych:
    - przekazanie danych powinno odbywać się z użyciem szyfrowanej komunikacji email;
    - plik z danymi wrażliwymi powinien być zaszyfrowany, zabezpieczony hasłem;
    - drugim kanałem komunikacji (np. w formie SMS) powinno zostać przesłane hasło, bez żadnych dodatkowych informacji, opisów, np. do czego jest dane hasło, dlaczego jest przekazywane itp.;
    - dane wrażliwe nie mogą być przesłane tekstem jawnym, nieszyfrowanym;
    - przesłane dane powinny zostać usunięte najszybciej jak to możliwe za pomocą kasowania nieodwracalnego;
    - lista adresatów powinna zostać ograniczona do osób uprawnionych.

W przypadku wystąpienia naruszenia bezpieczeństwa, spowodowanego nieprzestrzeganiem regulaminu lub jawnym zaniedbaniem ze strony Klienta/Partnera, odpowiedzialność ponosi Klient/Partner.

5 Monitoring bezpieczeństwa

W celu zapewnienia bezpieczeństwa systemów teleinformatycznych, Klient/Partner zobowiązany jest do stałego monitoringu swojej infrastruktury. W tym celu należy:

- kontrolować stacje robocze, pod kątem wykorzystywanego oprogramowania;
- monitorować próby dostępu (zarówno autoryzowane, jak i nieautoryzowane) do systemów IT;
- analizować ruch sieciowy pod względem szkodliwej komunikacji.

6 Edukacja w zakresie zasad bezpieczeństwa

Klient/Partner zobowiązany jest do cyklicznej edukacji pracowników w zakresie bezpieczeństwa. Zalecane szkolenia to:

- szkolenie podnoszące świadomość istnienia problemów bezpieczeństwa IT dla wszystkich pracowników organizacji Klienta/Partnera;
- szkolenie dot. phishingu dla wszystkich pracowników organizacji Klienta/Partnera;
- szczegółowe szkolenie poruszające różne aspekty bezpieczeństwa dla administratorów systemów IT w organizacji Klienta/Partnera.

7 Odpowiedzialność pracowników za dane poufne

Każdy pracownik organizacji Klienta/Partnera zobowiązany jest do ochrony swoich danych dostępowych do systemów teleinformatycznych. Dane te obejmują:

- hasła dostępowe;
- klucze dostępowe (zarówno softwareowe, jak i sprzętowe);
- inne mechanizmy umożliwiające dostęp do systemów IT.