AUTODESK

Opracowanie dotyczące zabezpieczeń Autodesk® Fusion 360

Październik 2022 r.

Spis treści

1. Wprowadzenie

Autodesk® Fusion 360™ to pierwsze tego typu narzędzie CAD 3D, CAM i CAE. Łączy ono proces rozwoju produktu w ramach pojedynczej platformy chmurowej działającej zarówno na komputerach Mac, jak i PC. Narzędzia Fusion 360 umożliwiają szybkie i łatwe analizowanie pomysłów projektowych dzięki bezpiecznemu i zintegrowanemu zestawowi narzędzi pozwalającemu na przejście od koncepcji do produkcji, który jest dostępny również w przeglądarkach internetowych i na urządzeniach mobilnych.

1.1 Cel i zakres dokumentu

Celem niniejszego dokumentu jest wyjaśnienie sposobu działania firmy Autodesk, procesu tworzenia oprogramowania i środków bezpieczeństwa wdrożonych w środowisku. W niniejszym dokumencie Autodesk Fusion 360 odnosi się zarówno do oprogramowania klienckiego Fusion 360, jak i do oprogramowania Fusion 360 dostępnego przez przeglądarkę.

Podstawą ram zabezpieczeń firmy Autodesk są standardy branżowe chroniące poufność, integralność i dostępność informacji o klientach.

Fusion 360 zaprojektowano z myślą o wysokiej dostępności i skalowalności w celu zapewnienia naszym klientom szybkiej i niezawodnej usługę chmurowej. Usługi hostingu w chmurze są świadczone na rzecz firmy Autodesk przez Amazon Web Services (AWS), lidera w dziedzinie infrastruktury chmurowej. Firma Autodesk opiera się na modelu współodpowiedzialności dostawcy hostingu AWS obejmującym infrastrukturę składającą się ze sprzętu, oprogramowania, sieci i obiektów, w których działają usługi chmurowe AWS. (Więcej informacji: https://aws.amazon.com/compliance/shared-responsibility-model/).

2. Zabezpieczenia firmy Autodesk

Ramy zabezpieczeń firmy Autodesk opierają się na standardach branżowych w celu zapewnienia spójnych praktyk w zakresie zabezpieczeń, które umożliwiają nam bezpieczne tworzenie, bezpieczne działanie i zachowanie bezpieczeństwa.

- **Bezpieczne tworzenie** — Wbudowanie zabezpieczeń w nasze produkty już na etapie ich tworzenia jest kluczowym elementem ochrony inwestycji naszych klientów w produkty

i usługi firmy Autodesk. Integrujemy zabezpieczenia na wszystkich etapach tworzenia oprogramowania.

- **Bezpieczne działanie** — Zabezpieczenia są wbudowane bezpośrednio w naszą infrastrukturę. Nasze całościowe podejście obejmuje wdrożenie narzędzi do ochrony punktów końcowych, znormalizowane wymagania dotyczące wdrażania poprawek i ograniczania funkcjonalności, kontrolę tożsamości i kontroli dostępu oraz ofensywne działania w zakresie bezpieczeństwa.

- **Zachowanie bezpieczeństwa** — Zabezpieczenia w firmie Autodesk koncentrują się na trzech podstawowych celach, którymi są ochrona poufności, integralności i dostępności (CIA, confidentiality, integrity and availability) informacji:

    - Poufność: informacje są dostępne tylko dla osób upoważnionych.
    - Integralność: informacje są kompletne i dokładne.
    - Dostępność: dane są dostępne dla klientów.

Dyrektor ds. bezpieczeństwa (CSO, Chief Security Officer) odpowiada za opracowanie i wdrożenie strategii i programu bezpieczeństwa oraz zarządzanie nim, jak również dba o stosowanie zasad i standardów bezpieczeństwa we wszystkich produktach i środowiskach firmy Autodesk. CSO i zespół ds. bezpieczeństwa są wspierani przez kierownictwo i zarząd firmy Autodesk.

3. Zespół techniczny Fusion 360

Zespół techniczny Fusion 360 jest odpowiedzialny za projektowanie, wdrażanie i testowanie oprogramowania klienckiego i aplikacji usług chmurowych Fusion 360.

Projektowanie, kodowanie, testowanie i obsługa Fusion 360 są oparte na procesie tworzenia oprogramowania zgodnym z metodologią Agile. Podczas sprintów projektowych architekci opracowują i sprawdzają szczegółowe dokumenty projektowe, aby ocenić funkcjonalność i skalowalność projektu. Podczas sprintów wdrażania inżynierowie i architekci oprogramowania przeprowadzają wzajemną weryfikację kodu w celu wykrycia odstępstw od praktyk tworzenia aplikacji Fusion 360. Cały kod powstały podczas procesu jest objęty jednostkowym testowaniem

funkcjonalnym, a żadna historyjka użytkownika nie jest uznawana za ukończoną, dopóki personel ds. zapewniania jakości nie zweryfikuje kryteriów akceptacji i definicji ukończenia. Z cyklem programistycznym zintegrowane jest również testowanie wydajności Fusion 360. Zespół Fusion 360 przeprowadza testy obciążenia podczas sprintów programistycznych, aby zidentyfikować zmiany, które negatywnie wpływają na wydajność, na jak najwcześniejszym etapie procesu.

3.1 Szkolenie pracowników

Wszyscy pracownicy firmy Autodesk muszą potwierdzić znaczenie bezpieczeństwa informacji w ramach wdrażania nowo zatrudnionych. Pracownicy są zobowiązani do przeczytania, zrozumienia i odbycia szkolenia na temat Kodeksu postępowania firmy. Kodeks wymaga od każdego pracownika prowadzenia działalności w sposób zgodny z prawem, etyczny, uczciwy i z poszanowaniem siebie nawzajem oraz użytkowników, partnerów i konkurentów firmy.

Pracownicy firmy Autodesk są zobowiązani do przestrzegania wytycznych firmy dotyczących poufności, etyki biznesowej, właściwego użytkowania i standardów zawodowych. Nowi pracownicy muszą podpisać umowę dotyczącą zachowania poufności. W ramach wdrażania nowych pracowników podkreślane jest znaczenie poufności i prywatności danych klientów.

Aby stosować najlepsze praktyki w zakresie bezpieczeństwa, firma Autodesk wprowadziła roczny program certyfikacji zabezpieczeń oprogramowania (SSCP, Software Security Certification Program) dla wszystkich osób z działu technicznego i infrastruktury chmurowej.

4. Zabezpieczenia produktu Fusion 360

Autodesk Fusion 360 ma wbudowane funkcje zabezpieczeń, obejmujące zarówno komunikację z usługami chmurowymi, jak i zabezpieczenia na poziomie produktu oraz funkcje współpracy, które użytkownicy mogą kontrolować.

4.1 Bezpieczeństwo komunikacji

Wszystkie połączenia między Autodesk Fusion 360 a usługami chmurowymi wymagają bezpiecznych połączeń HTTPS.

4.2 Szyfrowanie i szyfry

Komunikacja między Fusion 360 a usługami backendu i w obrębie usług backendu odbywa się za pośrednictwem szyfrowanego kanału.

4.3 Uwierzytelnianie

Aby uzyskać dostęp do Autodesk Fusion 360, wymagane są poświadczenia składające się z identyfikatora Autodesk ID, identyfikatora użytkownika i hasła. Poświadczenia są zabezpieczone podczas transmisji sieciowej i przechowywane tylko jako skrót posolony (salted hash).

Fusion 360 umożliwia użytkownikom końcowym korzystanie z uwierzytelniania wieloskładnikowego podczas logowania. Użytkownicy, którzy zdecydują się na włączenie tej funkcji, mogą używać autoryzowanego bezpiecznego urządzenia osobistego (np. telefonu komórkowego) w celu otrzymywania kodu do użycia w połączeniu z ich hasłem.

4.4 Bezpieczeństwo danych

Wszystkie projekty Fusion 360 są zapisywane w chmurze na szyfrowanym urządzeniu pamięci masowej. Rozwiązanie pamięci masowej używa do szyfrowania danych algorytmu Advanced Encryption Standard z kluczem 256-bitowym (AES-256).

Projekty buforowane lokalnie bazują na uprawnieniach użytkownika systemu operacyjnego w zakresie kontroli dostępu.

4.5 Przechowywanie wersji projektu

W przypadku każdego projektu w Autodesk Fusion 360 jest przechowywana historia wersji. Przechowywanie wersji chroni integralność danych, umożliwiając użytkownikom cofnięcie się do wcześniejszych wersji i zapewniając podlegającą audytowi listę zawierającą informacje o każdej modyfikacji pliku.

4.6 Bezpieczeństwo współpracy na poziomie centrum i grupy

Projekty zapewniają prostą podstawę do przyznawania lub ograniczania dostępu do projektów Autodesk Fusion 360 dla grupy współpracowników. Zaproszenia do projektów są zatwierdzane przez właściciela lub moderatora projektu, co gwarantuje ścisłą kontrolę członków przyznających dostęp nowym użytkownikom.

Firmy mogą zdecydować się na korzystanie z centrów Team Hub, które pozwalają im na kontrolowanie własności i dostępu do wszystkich projektów tworzonych przez członków. Ustawienia prywatności projektu, takie jak otwarte, zamknięte i poufne projekty, umożliwiają kontrolę współpracy. Dzięki centrom Team Hub członkowie mogą ograniczyć dostęp do współpracowników, którzy zostali zaproszeni do projektu. Centra Team Hub umożliwiają również administratorom klienta dezaktywowanie kont byłych pracowników i przenoszenie własności projektu na innych członków zespołu.

4.7 Udostępnianie publiczne

Udostępnianie publiczne umożliwia użytkownikom współpracę z partnerami zewnętrznymi, którzy nie mają identyfikatora Autodesk ID ani uprawnienia do korzystania z Fusion 360. Użytkownicy Fusion 360 mogą utworzyć łącze, które zapewnia dostęp do projektu w trybie tylko do odczytu. Użytkownicy mają również możliwość włączenia funkcji pobierania/eksportowania. W dowolnej chwili użytkownik może wycofać udostępnianie publiczne za pośrednictwem danego łącza.

5. Infrastruktura chmurowa

Zespół ds. infrastruktury chmurowej odpowiada za definiowanie i stosowanie procedur zarządzania wydawaniem aplikacji, modernizację sprzętu i aktualizację systemu operacyjnego, monitorowanie kondycji systemu i inne czynności wymagane do obsługi Autodesk Fusion 360.

5.1 Wysoka dostępność

Autodesk Fusion 360 zaprojektowano tak, aby zapewnić wysoki poziom dostępności poprzez zastosowanie nadmiarowych systemów w infrastrukturze pomocniczej i rozłożenie obciążenia na skalowalną flotę instancji.

5.2 Replikacja i nadmiarowość danych

Replikacja danych klienta jest wykonywana między strefami dostępności (AZ, Availability Zone) Amazon Web Services (AWS). Replikacja ogranicza możliwość utraty danych lub opóźnienia we wznowieniu usługi, jeśli wymagane jest przełączenie awaryjne do zapasowego centrum danych.

5.3 Nadmiarowość systemu zasilania

Centra danych AWS są wyposażone w nadmiarowe systemy zasilania, dzięki czemu mogą działać 24 godziny na dobę, siedem dni w tygodniu. Zasilacze UPS automatycznie zastępują podstawowe systemy elektryczne w przypadku awarii. Generatory w każdym centrum danych zapewniają długoterminowe zasilanie awaryjne w przypadku awarii.

5.4 Nadmiarowość połączeń internetowych

Do utrzymania łączności internetowej z każdym z centrów danych jest wykorzystywany nadmiarowy system składający się z wielu dostawców.

Oprogramowanie klienckie Autodesk Fusion 360 działa również w trybie offline, co umożliwia użytkownikom dostęp do lokalnych kopii projektu i pracę z nimi, gdy nie mają połączenia z Internetem.

5.5 Fizyczne bezpieczeństwo infrastruktury

Aplikacja Autodesk Fusion 360 działa w bezpiecznych centrach danych AWS, które są chronione przed nieuprawnionym dostępem fizycznym i zagrożeniami środowiskowymi za pomocą szerokiej gamy środków kontroli bezpieczeństwa. Poniżej podsumowano niektóre środki kontroli fizycznej i środowiskowej. Pełny przegląd procesów zabezpieczeń AWS jest dostępny tutaj.

5.6 Kontrola dostępu do obiektów

Centra danych AWS są strzeżone 24 godziny na dobę, 7 dni w tygodniu przez profesjonalnych pracowników ochrony. Teren każdego centrum danych, a także pomieszczenia, w których znajduje się sprzęt komputerowy i pomocniczy, są objęte monitoringiem wideo. Dane z monitoringu wideo są zapisywane na nośnikach cyfrowych, które umożliwiają przeglądanie ostatnich aktywności na żądanie. W wejściach do centrów danych znajdują się śluzy osobowe, które ograniczają dostęp do jednej osoby w danym momencie. Wszyscy odwiedzający i wykonawcy muszą okazać dowód tożsamości, aby zostać wpuszczeni na teren obiektu, i są przez cały czas eskortowani przez upoważniony personel. Dostęp do centrum danych jest możliwy wyłącznie dla pracowników mających uzasadnioną potrzebę biznesową, a wszystkie wizyty są rejestrowane elektronicznie.

5.7 Ochrona przeciwpożarowa

W każdym centrum danych w celu ochrony pomieszczeń zawierających sprzęt obliczeniowy i systemy pomocnicze są zainstalowane systemy przeciwpożarowe, takie jak czujniki dymu i wodne instalacje tryskaczowe. Czujniki wykrywania ognia są zamontowane na suficie i pod podłogą podniesioną.

5.8 Klimatyzacja

Klimatyzacja w centrum danych chroni serwery, routery i inne urządzenia narażone na awarię w przypadku naruszenia rygorystycznych zakresów środowiskowych. Monitorowanie zarówno przez systemy, jak i personel ma na celu zapobieganie wystąpieniu niebezpiecznych warunków, takich jak przegrzanie. Systemy sterowania automatycznie wprowadzają regulacje, które utrzymują temperaturę i inne parametry środowiskowe w dopuszczalnych przedziałach.

6. Zarządzanie incydentami związanymi z eksploatacją

Firma Autodesk stosuje zasady zarządzania incydentami, które określają najlepsze praktyki w zakresie rozwiązywania incydentów. Zasady zarządzania incydentami firmy Autodesk kładą nacisk na rejestrowanie kroków naprawczych i wykorzystanie analizy głównych przyczyn w celu opracowania bazy wiedzy na temat możliwych do zastosowania procedur. Celem polityki zarządzania incydentami firmy Autodesk jest nie tylko szybkie i skuteczne zamykanie incydentów, ale również zbieranie i rozpowszechnianie informacji o incydentach, aby procesy były stale ulepszane, a przyszłe reakcje były oparte na zgromadzonej wiedzy.

7. Zarządzanie poprawkami

Zespół ds. infrastruktury chmurowej stosuje zasadami zarządzania poprawkami, które pomagają zapewnić skuteczne wdrażanie poprawek. Tam, gdzie to możliwe, wprowadzono automatyzację w celu sprawdzania dostępności nowych poprawek i przygotowywania list wdrożeń, które mogą być zatwierdzane przez autoryzowany personel działu infrastruktury chmurowej. Zasady wdrażania poprawek definiują również kryteria określania wpływu poprawki na stabilność systemów. Jeśli poprawka zostanie zidentyfikowana jako mająca potencjalnie duży wpływ, przed jej wdrożeniem przeprowadzane jest testowanie regresji. System zarządzania zmianami śledzi wdrażanie poprawek w systemach produkcyjnych.

8. Zarządzanie zmianami

Zespół ds. infrastruktury chmurowej stosuje zasady zarządzania zmianami, które obejmują następujące elementy:

- **Formularz wniosku o zmianę (RFC, Request For Change).** Formularz RFC musi zostać przesłany w przypadku wszystkich zmian. Formularz zawiera nazwę inicjatora zmiany, priorytet zmiany, uzasadnienie biznesowe zmiany oraz żądaną datę wdrożenia zmiany.

- **Plany wycofania.** Zespół ds. infrastruktury chmurowej tworzy przed wdrożeniem szczegółowe plany wycofania, aby stan systemu mógł zostać przywrócony, jeśli zmiana spowoduje zakłócenie usługi. Plany wycofania zawierają wykonywalne instrukcje zdefiniowane w skryptach, które przywracają stan systemu przy minimalnej liczbie czynności wykonywanych ręcznie.

- **Zdefiniowane okna konserwacji.** Zespół ds. infrastruktury chmurowej określa okna konserwacji planowanej, awaryjnej i wydłużonej. Zespół planuje planowaną konserwację poza godzinami szczytu.

- **Plan testów.** Zespół ds. infrastruktury chmurowej definiuje zestaw testów sprawdzających dostępność funkcji po wdrożeniu zmiany.

- **Wykonywanie testów.** Po zakończeniu wdrażania zespoły ds. infrastruktury chmurowej i zapewniania jakości Autodesk Fusion 360 przeprowadzają testy sprawdzające, czy funkcje zidentyfikowane jako zagrożone pozostają dostępne.

9. Zarządzanie potencjałem wykonawczym

Dostęp klientów do usług chmurowych jest zapewniany na żądanie za pośrednictwem modelu samoobsługowego, dlatego wzorce ruchu są bardzo zmienne i mogą występować nagłe wzrosty obciążenia. W przypadku wystąpienia takiego wzrostu dostępność usługi może ulec pogorszeniu, jeśli pula zasobów obliczeniowych zasilających usługę zostanie wyczerpana. Aby zapewnić wysoki poziom dostępności, zespół ds. infrastruktury chmurowej stosuje zasady zarządzania potencjałem wykonawczym. Te praktyki obejmują:

- **Częste rejestrowanie użycia zasobów.** Dane dotyczące użycia zasobów Autodesk Fusion 360 są często zbierane w wielu różnych komponentach infrastruktury, w tym w wystąpieniach wirtualnych, woluminach magazynu wirtualnego i urządzeniach sieci wirtualnej. Statystyki użycia są przechowywane w repozytorium zarządzania potencjałem wykonawczym.

- **Planowanie potencjału wykonawczego.** Zespół ds. infrastruktury chmurowej wykorzystuje zarządzanie potencjałem wykonawczym do generowania szczegółowego planu potencjału wykonawczego, który dokumentuje bieżące poziomy użycia i modeluje przyszłe poziomy na podstawie analizy statystycznej oraz wpływu nadchodzących udoskonaleń funkcji biznesowych. Plan potencjału wykonawczego jest aktualizowany zgodnie z potrzebami lub w przypadku wykrycia istotnych zmian we wzorcach użycia.

- **Alokacja zasobów.** Zasoby obliczeniowe są przydzielane w miarę zgłaszania zapotrzebowania przez klientów. Wstępnie zainicjowane zasoby obliczeniowe są zawsze dostępne. W przypadku gwałtownego wzrostu aktywności tworzone są nowe zasoby. Przykładowo dostępność zasobów przeglądarki Autodesk Fusion jest zazwyczaj osiągana w ciągu mniej niż 10 minut.

- **Monitorowanie aktywności.** Pulpity i alerty aktywności są zdefiniowane w usługach backendu, umożliwiając inżynierom obserwowanie aktywności systemu oraz przeprowadzanie badań i analiz po wystąpieniu incydentu.

10. Alerty i monitorowanie

Aby zapewnić jak najkrótszy średni czas naprawy, firma Autodesk używa zautomatyzowanych systemów do monitorowania Fusion 360, weryfikując stan kondycji usługi. Każdy pojedynczy komponent, od bazy danych po usługi, jest monitorowany indywidualnie.

W przypadku zdarzenia, które ma wpływ na usługę, generowane są alerty, a zespół ds. infrastruktury chmurowej jest powiadamiany w procesie eskalacji.

Kondycja usługi opisuje również wzajemne relacje między usługami firmy Autodesk. Usługa, taka jak Autodesk Fusion 360, jest bardzo wrażliwa na działanie usługi kontroli dostępu ACM

(Access Control). Każda usługa musi być odporna na awarie usługi zależnej i powinna zostać bezpiecznie wyłączona, gdy nie będzie mogła dłużej działać bez utraty danych przez klienta.

Informacje o stanie usługi Fusion 360 są publicznie dostępne w witrynie Health Dashboard Service firmy Autodesk: https://health.autodesk.com.

11. Brak przestojów podczas wdrożeń

W trakcie wprowadzania poprawek w środowisku produkcyjnym w przypadku przeglądarki Autodesk Fusion i innych usług Fusion 360 jest stosowane podejście wdrożenia w modelu Blue-Green. Dzięki temu klienci nie napotykają przestojów w funkcjonowaniu usługi.

12. Kontrole operacyjne w przypadku Autodesk Fusion 360

Autodesk Fusion 360 zapewnia ochronę poufnych danych klientów przed nieautoryzowanym dostępem.

- **Fizyczne ograniczenia dostępu do centrów danych.** Fizyczne ograniczenia dostępu do centrów danych zapobiegają dostępowi osób nieupoważnionych do sprzętu i systemów pomocniczych wykorzystywanych przez Autodesk Fusion 360.
- **Kontrole przeszłości.** W przypadku pracowników z fizycznym dostępem do zasobów obliczeniowych i systemów pomocniczych wykorzystywanych przez Autodesk Fusion 360 wymagane są kontrole przeszłości.
- **Replikacja danych.** Replikacja danych polega na kopiowaniu danych klientów do nadmiarowych centrów danych, dzięki czemu można zachować ciągłość działalności biznesowej w przypadku awarii jednego z obiektów.
- **Technologie nadmiarowe**. Technologie nadmiarowe, takie jak moduły równoważenia obciążenia i klastrowane bazy danych, ograniczają liczbę pojedynczych punktów awarii.

13. Zabezpieczenia firmy Autodesk

Zespół ds. zabezpieczeń firmy Autodesk to dedykowana grupa specjalistów ds. bezpieczeństwa informacji, którzy koncentrują się na identyfikowaniu i stosowaniu praktyk bezpieczeństwa w środowisku chmurowym firmy Autodesk. Do obowiązków zespołu ds. zabezpieczeń firmy Autodesk należy:

- Przegląd stanu bezpieczeństwa projektu i wdrożenia infrastruktury chmurowej firmy Autodesk.
- Definiowanie i zapewnianie wdrażania zasad zabezpieczeń, w tym zarządzania tożsamością i dostępem, zarządzania hasłami i zarządzania lukami w zabezpieczeniach.
- Zapewnienie zgodności z ustanowionymi procedurami zabezpieczeń poprzez przeprowadzanie wewnętrznych przeglądów i audytów.
- Identyfikowanie i wdrażanie technologii chroniących informacje o klientach.
- Angażowanie zewnętrznych ekspertów ds. zabezpieczeń w celu przeprowadzania ocen bezpieczeństwa informacji.
- Monitorowanie usług chmurowych pod kątem możliwych problemów z bezpieczeństwem i reagowanie na incydenty w razie potrzeby.
- Przeprowadzanie corocznych przeglądów polityki bezpieczeństwa firmy Autodesk.

13.1 Skanowanie w poszukiwaniu luk w zabezpieczeniach i testowanie penetracyjne

Usługi Fusion 360 są poddawane corocznym testom penetracyjnym i regularnemu skanowaniu pod kątem zagrożeń i luk w zabezpieczeniach. Jest również przeprowadzana analiza statyczna aplikacji i skanowanie bibliotek innych firm. Skanowanie zabezpieczeń i testy penetracyjne obejmują szeroki zakres luk w zabezpieczeniach zdefiniowanych przez organizację Open Web Application Security Project (OWASP) i na liście SANS top 25.

13.2 Bezpieczeństwo sieci

Bezpieczeństwo sieci jest zapewniane przy użyciu kombinacji kontroli fizycznych i logicznych, w tym szyfrowania, zapór i procedur utwardzania systemów. Ponadto AWS zapewnia środki

kontroli bezpieczeństwa sieci, które chronią ich fizyczne centra danych. Więcej informacji można znaleźć na stronie Best Practices for Security, Identity, & Compliance (Najlepsze praktyki w zakresie bezpieczeństwa, tożsamości i zgodności z przepisami).

13.3 Szyfrowanie

Cały ruch sieciowy jest szyfrowany podczas transmisji przez Internet do granic środowiska chmurowego firmy Autodesk. W trakcie magazynowania szyfrowane są dane poufne, takie jak poświadczenia, informacje o sesji aplikacji, tokeny dostępu i profile użytkowników.

13.4 Ochrona prywatności

Firma Autodesk zapewnia transparentność odnośnie do sposobu zbierania i wykorzystywania danych osobowych klientów. Więcej informacji zawiera Oświadczenie o ochronie prywatności firmy Autodesk.

14. Zasoby

Poniższe zasoby zawierają ogólne informacje dotyczące firmy Autodesk i innych tematów, o których mowa w głównej części tego dokumentu.

- **Autodesk** — aby wyświetlić informacje na temat firmy Autodesk, odwiedź witrynę https://www.autodesk.pl.
- **Autodesk Trust Center** — aby wyświetlić informacje na temat Autodesk Trust Center, odwiedź witrynę http://trust.autodesk.com.
- **Autodesk Fusion 360** — aby uzyskać informacje na temat Fusion 360, odwiedź witrynę http://fusion360.autodesk.com/.