Test: Segura – rozwiązanie klasy PAM s. 46

Tożsamość hybrydowa s. 26

9
2025

Miesięcznik informatyków i menedżerów IT

itprofessional.pl

IT professional

Nr 9 (166) wrzesień 2025

ZABEZPIECZENIA Z CHMURY MICROSOFTU s. 8

Przedstawienie najważniejszych chmurowych rozwiązań bezpieczeństwa w portfolio Microsoftu, które pomagają zachować odpowiedni poziom zabezpieczeń infrastruktury. Omówienie pięciu kluczowych obszarów dojrzałości cyberbezpieczeństwa, a także kontroli tożsamości i dostępu w Entra ID.

Modernizacja oprogramowania legacy za pomocą GenAI s. 62

Refaktoryzacja przestarzałego software'u przy wykorzystaniu sztucznej inteligencji

Kolejne przepisy AI Act wchodzą w życie s. 50

Nowe przepisy aktu o sztucznej inteligencji dotyczące modeli AI ogólnego przeznaczenia

Statyczna i dynamiczna analiza aplikacji s. 71

Proces oceny bezpieczeństwa aplikacji na Androida i iOS-a

Cena 48,00 zł (w tym 8% VAT)
ISSN 2083-9588
9 772083 958004

DOSTĘPNE E-WYDANIE

Dostęp do szeroko rozumianych systemów informatycznych można monitorować na wielu poziomach. Służą do tego również systemy typu Privileged Access Management, w skrócie PAM. I właśnie takim rozwiązaniem zajmiemy się w tym tekście.

KONTROLA DOSTĘPU

Segura – rozwiązanie klasy PAM

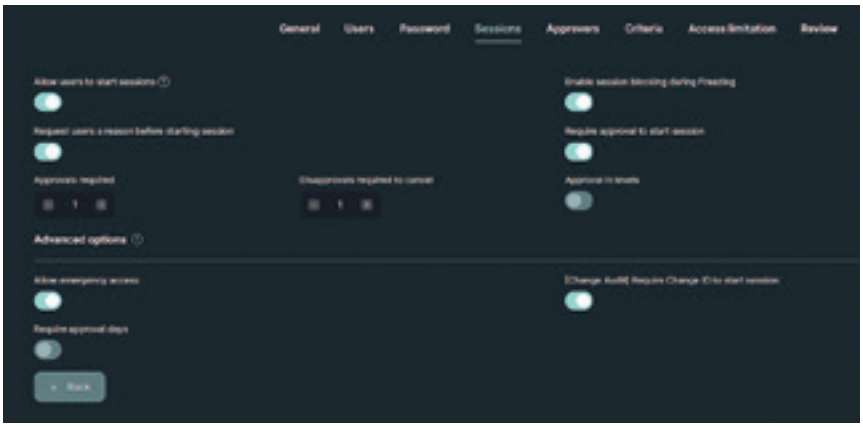
Marcin Jurczyk

Zarządzanie dostępem uprzywilejowanym z definicji dotyczy sprawowania pieczy nad użytkownikami dysponującymi uprawnieniami, pozwalającymi na dość swobodny zakres działania na powierzonych systemach. W praktyce mowa tu zazwyczaj o administratorach działających zarówno wewnątrz organizacji, jak też świadczących usługi zdalnie, często reprezentujących podmiot do tego zakontraktowany. Kontrola dostępu, ale również możliwość weryfikacji działań na zarządzanych zasobach jest możliwa do realizacji na wielu poziomach, w zależności od wymagań zdefiniowanych w polityce bezpieczeństwa oraz restrykcjach narzuconych często przez różnorodne regulacje prawne.

Zgodność ze zróżnicowanymi standardami bezpieczeństwa poza prestiżem i domniemaną gwarancją stosowania najlepszych praktyk jest również wyzwaniem na gruncie dopełnienia określonych obowiązków w zgodzie z restrykcyjnymi wytycznymi. Co więcej, certyfikacja nie jest przyznawana raz na zawsze i wymaga cyklicznego odświeżenia oraz audytowania. W sukurs przychodzą rozwiązania typu PAM, za pośrednictwem których możliwe jest zrealizowanie niektórych wymagań certyfikacyjnych, ale co najważniejsze – podniesienie bezpieczeństwa na płaszczyźnie scentralizowanej kontroli dostępu uprzywilejowanego. Segura to dostawca platformy PAM z kilkunastoletnią historią. Firma z siedzibą w Sao Paolo jeszcze do kwietnia tego roku znana była jako Senhasegura. Rebranding zbiegł się w czasie z premierą najnowszej wersji rozwiązania PAM, które trafiło na testy.

> ARCHITEKTURA

Budowa rozwiązania PAM Segura opiera się na architekturze logicznej podzielonej na warstwy, odpowiedzialne za realizację różnych funkcji. Moduły PAM to warstwa realizująca najwięcej kluczowych funkcji całego rozwiązania, jak zarządzanie sesjami, realizacja web i transparent proxy dla wspieranych protokołów połączeniowych (http, HTTPS, TELNET, SSH, RDP, VLC, X.11, RDP RemoteApp), kontrola dostępu, bezpieczne przechowywanie poświadczeń, ale także panele kontroli, raporty czy analiza behawioralna dla użytkowników PAM. Warstwa aplikacyjna realizuje obsługę użytkowników i aplikacji, funkcje bezpieczeństwa, uwierzytelniania czy integracji za pośrednictwem API. Działanie warstwy aplikacyjnej opiera się na frameworku Orbini autorstwa grupy technologicznej MT4. Kolejne warstwy architektury zdefiniowane przez producenta dotyczą sposobu wdrożenia i komponentów fizycznych rozwiązania,



Kontrola dostępu pozwala na szczegółową definicję warunków uzyskania dostępu.

jak wirtualne urządzenie, ale także jego odpowiednik fizyczny, który również znajduje się w ofercie.

W praktyce Segura opiera się właśnie na virtual appliance dostarczanym w różnych formatach, jak OVA, VMDK, RAW, VHD i QCOW2, który można uruchomić zarówno w środowisku tradycyjnym, jak również w chmurze publicznej AWS, GCP lub Azure, dla których oferowane jest oficjalne wsparcie. Maszyna wirtualna – działająca pod kontrolą systemu operacyjnego Linux – może zostać wdrożona zarówno w scenariuszu standalone, jak również w opcji HA lub DR, z uwzględnieniem replikacji pomiędzy środowiskiem on-premises i chmurą publiczną. Replikacja na poziomie plików realizowana jest z wykorzystaniem Rsync. Z kolei w przypadku bazy danych jest to klaster Galera dla MariaDB. Producent dopuszcza także replikacje pomiędzy wirtualnym urządzeniem i jego fizycznym odpowiednikiem PAM Crypto Appliance.

Nadążając za trendami, Segura umożliwia także wdrożenie swojego rozwiązania w modelu SaaS, dzięki czemu rozważania na temat scenariusza wdrożeniowego, sizingu i doboru innych komponentów przestają być zasadne – wszelkie wysiłki można przekierować na właściwą konfigurację.

> MOŻLIWOŚCI

Głównym zadaniem rozwiązania PAM jest kontrola dostępu i działań użytkowników z uprzywilejowanym dostępem. W przypadku Segury jest to jedynie niewielki wycinek funkcjonalności, którą oferuje platforma, zamknięty w ramach modułu PAM Core. W dużym uproszczeniu mamy do czynienia z rozwiązaniem, które pozwala na zdalny dostęp do zróżnicowanych systemów bez ujawniania rzeczywistych poświadczeń użytkownikom końcowym. Co więcej, poświadczenia te są przechowywane w sposób bezpieczny, a hasła mogą być automatycznie zmieniane przy wykorzystaniu zdefiniowanego harmonogramu, włącznie z automatyczną modyfikacją po każdym użyciu.

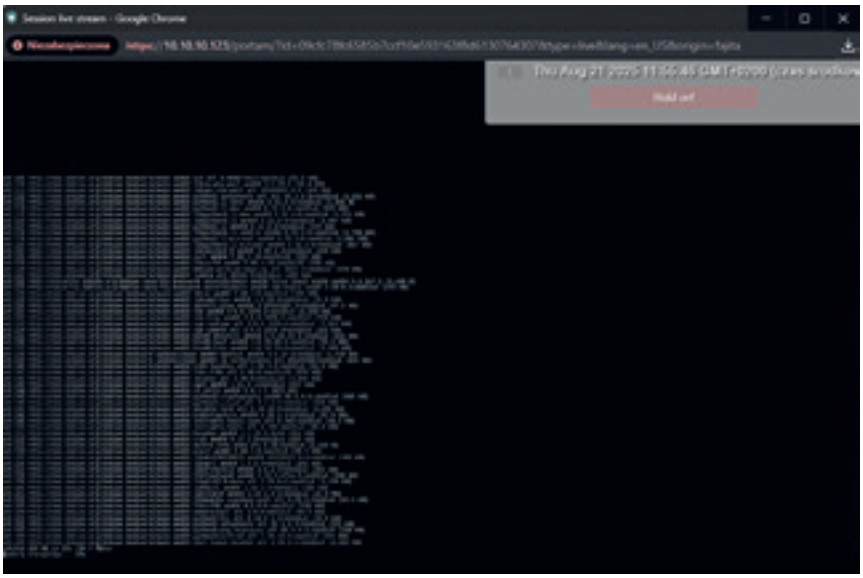
Rozwiązanie może zostać wdrożone w trybie wysokiej dostępności.

W praktyce oznacza to, że użytkownik w żadnym momencie nie dysponuje rzeczywistym hasłem do żadnego systemu, do którego przydzielono mu dostęp. Jedyne poświadczenia, które musi znać, to dostęp do PAM-a, a ten może być chroniony na innych poziomach. Oczywiście wspierane jest także wieloskładnikowe uwierzytelnianie TOTP i to zarówno na poziomie dostępu do Segury, jak też do systemu docelowego. Za pośrednictwem grup dostępu administrator Segury może zdefiniować, kto ma dostęp do określonych urządzeń i usług dostępnych za pośrednictwem PAM-a. Sam dostęp może być również reglamentowany ze względu na ramy czasowe, dzięki czemu łatwo zdefiniować czas życia dla określonych grup użytkowników, eliminując potrzebę ręcznego odcinania dostępu, ale także można zdefiniować okna czasowe, w których logowanie do systemów będzie w ogóle możliwe. Sam proces wnioskowania oraz akceptacji dostępu może zostać zdefiniowany poprzez kilka poziomów kontroli na różnych szczeblach. Dzięki temu można uprościć sam proces wydawania akcesów lub wręcz przenieść go w całości do Segury. Mechanizm przyznawania dostępu, zarządzanie poświadczeniami i bezpieczne przechowywanie haseł to podstawowe funkcje wymagane przed rzeczywistym wpuszczeniem użytkowników do naszej infrastruktury. Od momentu zalogowania kontrola odbywa się na innym poziomie, począwszy od zwykłego logowania aktywności, na nagrywaniu sesji kończąc. Administratorzy Segury mogą dostosować konfigurację do wymagań funkcjonalnych, decydując o poziomie zbierania ewidencji. Jakość nagrań wideo można skonfigurować, uwzględniając zasoby dyskowe i retencję przechowywania danych. Oczywiście nic nie stoi na

Rozbudowane możliwości pozwalają plasować Segurę PAM jako kompletne rozwiązanie IAM dla środowisk lokalnych, hybrydowych oraz chmury publicznej, z uwzględnieniem kontroli również na poziomie stacji roboczych.

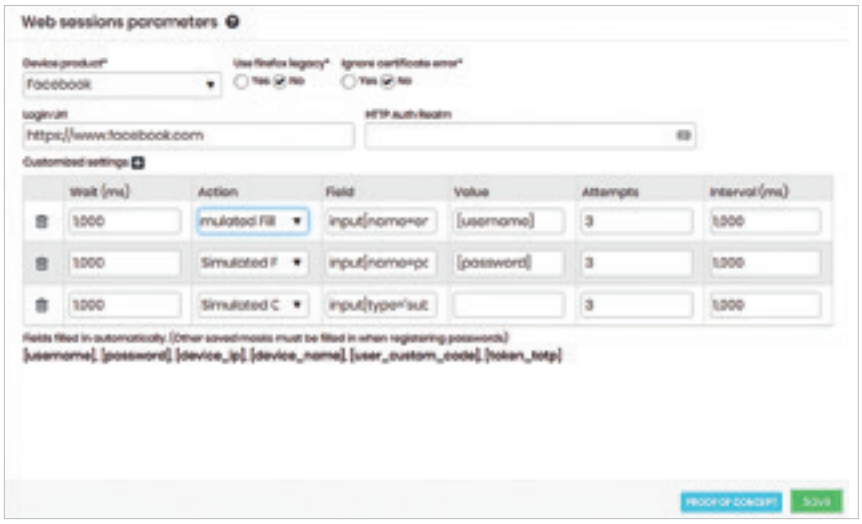
przeszkodzie, aby śledzić sesję na żywo. W takim wariancie możliwe są szybka reakcja i natychmiastowe wstrzymanie dostępu w razie wykrycia niepożądanych aktywności.

Dużo większe możliwości kontroli są dostępne dla sesji tekstowych. Segura domyślnie pełni rolę pośrednika pomiędzy użytkownikiem a systemem docelowym, dzięki czemu można zdefiniować polecenia, których wykonanie w sesji zdalnej wywoła alarm. W ostateczności administrator ma także opcję całkowitego zablokowania dostępu w przypadku wykrycia polecenia z czarnej listy. Audyt w trybie rzeczywistym na tym poziomie to silny mechanizm podnoszący bezpieczeństwo. Zapisywanie transkrypcji z każdej sesji tekstowej to także bardzo przydatne narzędzie w kontekście audytów formalnych oraz analizy zdarzeń post factum i RCA. Wśród innych ciekawych funkcji Segury warto zwrócić uwagę na możliwość dzielenia poświadczeń. Mechanizm ten sprawdzi się w organizacjach zarządzających systemami krytycznymi, do których dostęp możliwy jest tylko w momencie, gdy wszyscy zdefiniowani użytkownicy wprowadzą swoje prawidłowe hasła. W scenariuszu tym dostęp indywidualny jest bez żadnego znaczenia i ewentualna kompromitacja jednostki nie ma wpływu na bezpieczeństwo całego systemu. Dostęp dla użytkowników można także ograniczyć do pojedynczej aplikacji w ramach sesji zdalnej, bez konieczności eksponowania pełnego dostępu do maszyny hosta. Podstawowym klientem dla kontrolowanych połączeń jest zakładka przeglądarki, choć Segura wspiera także używanie klientów standalone, jak chociażby putty.



Dostępny jest podgląd sesji użytkowników na żywo, z możliwością ręcznego wstrzymania dostępu.

Wspomniane możliwości to w zasadzie funkcjonalność tylko jednego, choć podstawowego modułu dla całej Segury – PAM Core. Poza tym istnieje kilka funkcji dodatkowych, które wykraczają poza ramy testu, choć z pewnością warto o nich wspomnieć. Pierwszy z nich to Domum Remote Access – rozwiązanie pozwalające na zdalny dostęp do PAM i systemów chronionych bez konieczności zastosowania VPN-a. Działanie wykorzystuje usługę chmurową producenta, będącą pośrednikiem lub mediatorem pomiędzy użytkownikami zdalnymi a infrastrukturą chronioną przez PAM Segura. Kolejny moduł to MySafe, czyli korporacyjny menedżer haseł z funkcją autouzupełniania, generowania haseł, a przede wszystkim bezpiecznego przechowywania poświadczeń. Segura oferuje także moduł Endpoint Privilege Manager (EPM) dla systemów Windows, MacOS oraz Linux, pozwalający kontrolować działania za pomocą podniesionego poziomu uprawnień na końcówkach klienckich, jak chociażby instalacja oprogramowania. Wśród modułów dodatkowych znajdziemy też DevOps Secret Manager, Cloud Entitlement Manager, Cloud IAM czy menedżera certyfikatów. Co najważniejsze, zarządzanie każdym z nich odbywa



Segura PAM umożliwia symulowanie użytkownika w aplikacjach webowych.

się z poziomu tego samego interfejsu, co dla PAM Core, oferując uproszczone zarządzanie, ustandaryzowane raportowanie i kontrolę.

> ZARZĄDZANIE

Podstawowym interfejsem zarządzania Segurą jest webGUI, choć pewne czynności wstępne tuż po instalacji wymagają również dostępu do CLI. Nasze testy wyjątkowo objęły dwie wersje systemu, wspomnianą już najnowszą odsłonę v4, a także poprzednią generację oznaczoną jako v3.33. Celem „ćwiczenia" nie był test porównawczy, ale szybka weryfikacja zmian, które producent określa jako nowe otwarcie, idące w parze ze wspomnianym wcześniej rebrandingiem. Najnowsza wersja jest relatywnie świeża, a samo przejście na nią dla klientów korzystających z wersji trzeciej może wymagać przyzwyczajenia. Poza szatą graficzną zmieniło się całkiem sporo, choć sam interfejs to zapewne niewielki, choć istotny procent wszystkich modyfikacji.

Najbardziej rzucającą się w oczy zmianą jest odejście od otwierania kolejnych okien przeglądarki w trakcie wykonywania podstawowych czynności konfiguracyjnych, typu dodanie poświadczeń. W najnowszej wersji odświeżana jest po prostu główna część ekranu, w której wyświetlany jest formularz pozwalający na wprowadzenie wszystkich danych. To modyfikacja o tyle istotna, że podczas kilkudniowych testów często zdarzało się zostawiać pootwierane dodatkowe okna przeglądarki w ferworze modyfikacji i eksperymentów. Część elementów menu zmieniła również swoje umiejscowienie, a sposób konfiguracji wybranych mechanizmów zmienił się na tyle, iż trzeba było podeprzeć się oficjalną dokumentacją, jak chociażby w przypadku integracji z Active Directory. Nie zabrakło też zmian czysto kosmetycznych, jak chociażby zmiana trybów wyświetlania jasny/ciemny. Od strony CLI łatwo sprawdzić, co kryje się „pod maską" naszego wirtualnego urządzenia, i tutaj na pierwszy rzut oka przynajmniej podstawy pozostały bez zmian. W dalszym ciągu mamy do czynienia z systemem operacyjnym bazującym na Debianie, na którym odpalone są kontenery Dockera – realizują one choćby funkcje proxy dla baz danych. WebGUI pozostaje czytelne w obu testowanych wersjach, choć – pomimo epizodycznego obcowania z każdą z nich – starszy interfejs ma swoje mocne strony. Elementem, którego nie przetestowano, są mechanizmy wysokiej dostępności. Szczególnie replikacja pomiędzy geograficznie rozproszonymi lokalizacjami i potencjalny troubleshooting mogą być interesujące z perspektywy administratora. Decydując się na sprawdzenie obu wersji oprogramowania, mieliśmy również szansę na przetestowanie aktualizacji do wersji 4.0. Sam update przebiegł bezproblemowo, choć należy zaznaczyć, że instancja testowa nie była obciążana złożoną konfiguracją.

Nasze redakcyjne testy odbyły się bez udziału wsparcia technicznego dostawcy, choć warto wspomnieć, iż producent deklaruje niezobowiązujące i darmowe wsparcie inżyniera, a także prezentację produktu podczas testów Proof of Concept. Co więcej, polski dystrybutor to również centrum kompetencyjne Segura obsługujące klientów z naszego regionu geograficznego. IT

Autor pracuje jako architekt IT w firmie Kyndryl. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

Segura oferuje znacznie więcej, niż początkowo spodziewaliśmy się po rozwiązaniu PAM. Oczywiście mowa tu także o modułach rozszerzających funkcjonalność, doskonale adresujących potrzeby współczesnych środowisk IT. Analizując rozbudowaną ofertę funkcjonalną, można wręcz odnieść wrażenie, że cała otoczka wokół funkcjonalności podstawowej PAM plasuje Segurę jako kompletne rozwiązanie IAM dla środowisk lokalnych, hybrydowych oraz chmury publicznej, z uwzględnieniem kontroli również na poziomie stacji roboczych. Niepodważalnym atutem rozwiązania jest też relatywnie szybki czas wdrożenia, dzięki architekturze opartej na wirtualnym urządzeniu, gotowym do zaimplementowania niemalże w dowolnym środowisku. Pierwsze efekty wdrożenia w postaci bezpiecznego dostępu do systemów za pośrednictwem Segury można uzyskać w mniej niż godzinę, choć to dopiero początek drogi. Wykorzystanie wszystkich dostępnych mechanizmów bezpiecznej kontroli dostępu z wykorzystaniem samego modułu PAM Core będzie wymagało nieco więcej pracy, ale efekty są tego warte. Dołożenie kolejnych funkcji to tylko kolejne warstwy podnoszące bezpieczeństwo na wielu płaszczyznach.

Werdykt

Segura PAM

Zalety

- ⊕ szybkie wdrożenia
- ⊕ intuicyjny interfejs
- ⊕ rozbudowane funkcje kontroli dostępu
- ⊕ szczegółowy audyt aktywności
- ⊕ rozbudowana funkcjonalność oparta na modułach dodatkowych
- ⊕ integracja poprzez API

Wady

- ⊖ nielogicznie umiejscowienie niektórych opcji w menu

Ocena **9**/10