

Mechanizmy kontroli dostępu do sieci (NAC) w erze Internetu rzeczy i BYOD

Spis treści

Streszczenie	3
Rozwój mechanizmów kontroli dostępu	4
Widoczność całej sieci	5
Stosowanie mechanizmów kontroli opartych na politykach	6
Automatyczne reagowanie na zagrożenia	7
Oczekiwania wobec mechanizmów kontroli dostępu do sieci (NAC) trzeciej generacji	8

Streszczenie

W miarę upowszechniania się Internetu rzeczy (IoT) i urządzeń przenośnych zwiększa się powierzchnia ataku przedsiębiorstwa, a na brzegu sieci pojawiają się nowe luki w zabezpieczeniach. Jednocześnie ataki typu „zero-day” i APT na urządzenia końcowe stają się coraz bardziej złożone i wyrafinowane. W celu ochrony urządzeń i coraz szerszej sieci przez zagrożeniami oraz spełnienia coraz bardziej restrykcyjnych norm w zakresie zgodności z przepisami architektury zabezpieczeń potrzebują zatem coraz lepszych mechanizmów kontroli dostępu. Z tego względu mechanizmy kontroli dostępu do sieci (NAC) muszą być stale rozwijane, aby oferować coraz doskonalsze funkcje zaspokajające zgłaszane potrzeby w zakresie identyfikowania, powstrzymywania i łagodzenia skutków zagrożeń.

Rozwój mechanizmów kontroli dostępu

Szerokie zastosowanie biurowe produktów z zakresu Internetu rzeczy oraz zasad korzystania z urządzeń prywatnych do celów służbowych (BYOD) zapewnia nowe możliwości biznesowe, stwarza również jednak nowe wyzwania. Przede wszystkim nie ma w tym kontekście praktycznie żadnej standaryzacji konfiguracji urządzeń. W każdym przedsiębiorstwie aktywnie używane są potencjalnie setki typów i modeli urządzeń i systemów operacyjnych, a wielu z nich brakuje zabezpieczeń klasy korporacyjnej. Z tego właśnie względu urządzenia końcowe pozostają głównym celem zaawansowanych ataków.

Od samego początku kontrola dostępu urządzeń do sieci była głównym elementem uwzględnianym w kontekście zabezpieczania urządzeń końcowych. Pierwsza generacja mechanizmów kontroli dostępu do sieci (NAC) służyła do uwierzytelniania i autoryzacji urządzeń końcowych (zazwyczaj zarządzanych przez dział IT lokalnych komputerów PC) za pomocą prostej technologii typu „skanuj i blokuj”. Kiedy jednak wzrosło zapotrzebowanie na mechanizmy zarządzania dostępem gości do sieci przedsiębiorstwa, pojawiła się druga generacja mechanizmów kontroli dostępu do sieci

(NAC), która ułatwiała zapewnienie ograniczonego dostępu do Internetu użytkownikom zewnętrznym takim jak goście, wykonawcy i partnerzy biznesowi.

W obliczu zachodzących obecnie dynamicznych zmian w zakresie zarówno infrastruktury sieci, jak i pojawiających się zagrożeń (oraz dodatkowo presji wynikającej z coraz bardziej rygorystycznych regulacji branżowych i przepisów dotyczących ochrony prywatności danych), mechanizmy kontroli dostępu do sieci (NAC) muszą nadal ewoluować. Aby w pełni zabezpieczyć urządzenia końcowe związane z Internetem rzeczy i zasadami BYOD, architekci zabezpieczeń muszą zapewnić sobie widoczność każdego urządzenia w swojej sieci oraz wiedzieć, jakie działania takie urządzenie w danym momencie wykonuje oraz jak łączy się z innymi urządzeniami w ramach tej sieci. Mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji muszą być zatem zdolne do koordynowania wszystkich aspektów widoczności urządzeń końcowych, kontroli i automatycznego reagowania na zagrożenia.

Do 2025 r. Internet rzeczy ma na całym świecie obejmować 41,6 mld urządzeń generujących 79,4 zettabajtów (ZB) danych¹.

Widoczność całej sieci

W przypadku mechanizmów kontroli dostępu do sieci (NAC) stwierdzenie, że „nie da się ochronić tego, czego się nie widzi” jest odpowiednie. Brak widoczności urządzeń końcowych naraża sieci na niewidoczne ryzyko. Większość (83%) przedsiębiorstw twierdzi, że jest narażona na ryzyko wynikające z zastosowania urządzeń przenośnych, a dwie trzecie z nich (67%) uważa, że bardziej obawia się o bezpieczeństwo zasobów na urządzeniach przenośnych niż na innych urządzeniach².

Specjaliści ds. bezpieczeństwa muszą być w stanie śledzić cały sprzęt składający się na infrastrukturę sieci w wielu różnych lokalizacjach, w tym na brzegach sieci. Budowa skutecznego systemu ochrony rozpoczyna się od zapewnienia pełnej widoczności urządzeń wewnętrznych (komputerów PC, smartfonów, laptopów, serwerów, urządzeń Internetu rzeczy, urządzeń medycznych, terminali POS, kontrolerów HVAC, czytników kart i kamer IP) oraz wszelkich innych urządzeń korzystających z protokołu IP w ramach jednego, zintegrowanego widoku topologii sieci.

Oferowane przez mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji funkcje oceny ryzyka muszą być zdolne do identyfikacji typu urządzenia i konfiguracji oprogramowania, w tym do sprawdzenia, czy mechanizmy ochrony przed wirusami i złośliwym

oprogramowaniem są zaktualizowane. Ocena podatności urządzeń końcowych na zagrożenia musi również obejmować urządzenia nieposiadające monitorów (ang. headless), które nie mogą obsługiwać wbudowanego zabezpieczenia ze względu na swoje ograniczone funkcje (wiele takich urządzeń wchodzi w skład Internetu rzeczy). Niewinne urządzenia podłączone do Internetu rzeczy (m.in. lodówki, konsole do gier lub inteligentne głośniki) oraz typowe elementy sieciowe (m.in. przełączniki, punkty dostępowe i routery bezprzewodowe) dodawane do sieci przedsiębiorstwa bez wiedzy działu IT stanowią zagrożenie, które może bezpośrednio doprowadzić do naruszenia bezpieczeństwa sieci³.

Przedsiębiorstwa muszą również być zdolne do automatycznego wykrywania i kategoryzowania wszystkich potencjalnych użytkowników związanych z ich urządzeniami przed przyznaniem im dostępu do sieci (powinny zatem na przykład wykrywać, jakie urządzenia zostały zarejestrowane w sieci, a nawet lokalizację i godzinę nadejścia żądania połączenia). Ponadto mechanizmy kontroli dostępu do sieci (NAC), w ramach swoich funkcji zapewnienia widoczności i oceny ryzyka, powinny być zdolne do stałego skanowania sieci w poszukiwaniu odbiegających od normy zachowań użytkowników lub oznak naruszenia bezpieczeństwa po uzyskaniu połączenia z urządzeniem końcowym.

Stosowanie mechanizmów kontroli opartych na politykach

Po zidentyfikowaniu użytkownika i urządzenia mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji musi być zdolne do wdrożenia szczegółowej, opartej na politykach mikrosegmentacji sieci i ograniczenia dostępu do poszczególnych segmentów tylko do niezbędnych użytkowników. Płaska i otwarta sieć wewnętrzna daje cyberprzestępcom i złośliwemu oprogramowaniu nieograniczony dostęp do danych wrażliwych i własności intelektualnej. Segmentacja sieci powinna na podstawie wstępnie zdefiniowanych zasad kontroli dostępu dynamicznie określać zakres i czas dostępu użytkowników i urządzeń w ramach sieci oraz zasoby, do których mogą mieć dostęp.

Mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji powinno również obsługiwać segmentację opartą na celach biznesowych, przesyłając najważniejsze informacje o danym urządzeniu przenośnym (na przykład grupy użytkowników i informacje otagowane), aby ułatwić egzekwowanie zasad zapory sieciowej. Dostęp może być wówczas ograniczony w celu zapewnienia, że użytkownicy i urządzenia mogą korzystać tylko z tych aplikacji i plików, które są odpowiednie dla określonych potrzeb biznesowych.

W tym celu skuteczne mechanizmy kontroli dostępu do sieci muszą być również zdolne do integracji z innymi najlepszymi w swojej klasie rozwiązaniami w zakresie bezpieczeństwa, w tym z rozwiązaniami innych producentów. Jest to kluczowa cecha pozwalająca na ochronę nowoczesnych sieci korzystających z rozwiązań różnych producentów. Mechanizmy kontroli dostępu do sieci muszą być również zdolne do korzystania z istniejących przełączników, ruterów i punktów dostępowych w całej infrastrukturze na potrzeby utworzenia na bieżąco aktualizowanej mapy połączeń i oraz wymuszenia kontroli dostępu do sieci w ramach poszczególnych segmentów.

Naruszenia spowodowane usterkami systemu (3,24 mln USD) i nieumyślnymi błędami osób mających dostęp do informacji poufnych (3,5 mln USD) są nadal kosztowne dla przedsiębiorstw. Wielu z tych naruszeń można jednak uniknąć dzięki wdrożeniu odpowiednich zasad dostępu do sieci i mechanizmów kontroli⁴.

Automatyczne reagowanie na zagrożenia

Wyniki najnowszych badań wskazują, że średni czas identyfikacji przypadku naruszenia bezpieczeństwa to ponad dziewięć miesięcy (279 dni), co oznacza koszty szkód w wysokości niemal 4 mln USD na zdarzenie⁵.

Dzięki integracji rozwiązania w zakresie bezpieczeństwa mogą wysyłać i odbierać w czasie rzeczywistym informacje o zagrożeniach w celu podejmowania skoordynowanych działań obronnych w ramach całego przedsiębiorstwa. Ten rodzaj automatyzacji jest swoistym „świętym Graalem” sieciowej architektury zabezpieczeń. Mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji powinny oferować poziom orkiestracji, który agreguje wszystkie dane dotyczące bezpieczeństwa w celu automatycznego kategoryzowania zagrożeń zgodnie z określonymi priorytetami, a następnie uruchamia skoordynowane działania mające na celu łagodzenie skutków zagrożeń.

Jeśli urządzenie lub użytkownik narusza ustalone zasady korzystania z sieci, powinno to natychmiast

zainicjować jednolitą reakcję obronną w ramach całej architektury zabezpieczeń. Reakcja ta może obejmować automatyczne kończenie połączeń, uruchomienie ograniczeń dostępu do sieci, kwarantannę lub szereg działań związanych z powiadamianiem centrum zarządzania bezpieczeństwem (SOC).

Tego rodzaju zautomatyzowane reakcje na zagrożenia mogą skrócić czas potrzebny na podjęcie działań obronnych z dni do sekund, aby odpowiednio chronić informacje wrażliwe i adresy IP, a jednocześnie zapewnić zgodność z coraz bardziej rygorystycznymi regulacjami, normami i przepisami prawa ochrony prywatności danych.

Głównym celem dobrze zaprojektowanego mechanizmu kontroli dostępu do sieci (NAC) jest zautomatyzowanie procesu ograniczania dostępu do sieci oraz zapewnienie uwzględniających kontekst wytycznych dotyczących działań naprawczych⁶.

Oczekiwania wobec mechanizmów kontroli dostępu do sieci (NAC) trzeciej generacji

W obliczu zmieniającej się infrastruktury sieci, zaawansowanych ataków na urządzenia końcowe i coraz bardziej restrykcyjnych przepisów architektury zabezpieczeń potrzebują mechanizmów kontroli dostępu do sieci (NAC) trzeciej generacji, aby lepiej zabezpieczać urządzenia przenośne i produkty wchodzące w skład Internetu rzeczy. W związku z powyższym mechanizmy te powinny spełniać następujące kryteria:

- ☐ **Widoczność.** Mechanizmy kontroli dostępu do sieci (NAC) powinny „widzieć” i móc ocenić wszystkie rodzaje urządzeń końcowych (w tym urządzenia końcowe w ramach Internetu rzeczy) przed podłączeniem ich do sieci. Ponadto powinny być w razie potrzeby zdolne do dokonania kategoryzacji użytkownika urządzenia. Ocena ryzyka związanego z urządzeniem i użytkownikiem powinna być kontynuowana również po podłączeniu do sieci.
- ☐ **Ocena luk w zabezpieczeniach urządzeń końcowych.** Rozwiązanie NAC powinno być również zdolne do określenia krytycznych luk w zabezpieczeniach danego urządzenia takich jak nieaktualne wersje oprogramowania lub odinstalowane poprawki.
- ☐ **Szczegółowe zasady kontroli dostępu.** Po zidentyfikowaniu urządzenia i użytkownika rozwiązanie NAC powinno obsłużyć segmentację opartą na celach biznesowych, aby automatycznie stosować zasady zabezpieczeń oparte na informacjach o zdefiniowanych użytkownikach/urządzeniach.
- ☐ **Integracja.** Mechanizmy kontroli dostępu do sieci (NAC) powinny być zdolne do bezproblemowej integracji z innymi rozwiązaniami w ramach szerzej rozumianej architektury zabezpieczeń, w tym z produktami innych producentów, aby móc aktywnie współdzielić istotne informacje o potencjalnych zagrożeniach oraz egzekwować zasady kontroli dostępu w całym szeroko rozumianym przedsiębiorstwie.
- ☐ **Reagowanie na zagrożenia w czasie rzeczywistym.** W przypadku potencjalnego naruszenia bezpieczeństwa urządzenia końcowego mechanizmy kontroli dostępu do sieci (NAC) powinny ułatwić zautomatyzowaną reakcję na zagrożenia w czasie rzeczywistym, aby uniemożliwić podejrzanemu urządzeniu dokonanie poważnych uszkodzeń lub infekcji.
- ☐ **Automatyzacja procesów.** Rozwiązanie NAC powinno pozwalać na samodzielne przydzielanie zasobów przez użytkownika, automatyczne wdrażanie urządzenia do pracy oraz wysyłanie użytkownikowi odpowiednich zaleceń, ilekroć okaże się, że dane urządzenie nie spełnia minimalnych standardów bezpieczeństwa.
- ☐ **Skalowalność i elastyczność.** Mechanizmy kontroli dostępu do sieci (NAC) trzeciej generacji powinny udostępniać skalowalną architekturę, która w przystępnej cenie będzie obsługiwać wiele lokalizacji w całym przedsiębiorstwie i nieograniczoną liczbę urządzeń. Ponadto muszą oferować elastyczne możliwości wdrażania z opcją fizyczną, wirtualną i w chmurze.

¹ „[The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast](#)”, IDC, 18 czerwca 2019 r.

² „[Mobile Security Index 2019](#)”, Verizon, marzec 2019 r.

³ „[In the Rush to Join the Smart Home Crowd, Buyers Should Beware](#)”, The New York Times, 22 stycznia 2019 r.

⁴ „[2019 Cost of a Data Breach Report](#)”, Ponemon Institute and IBM Security, lipiec 2019 r.

⁵ Ibid.

⁶ Kirk Anderson, „[NAC: Usability and Security for Users](#)”, Security Boulevard, 3 października 2019 r.



www.fortinet.com

Copyright © 2020 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojnie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działał zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).