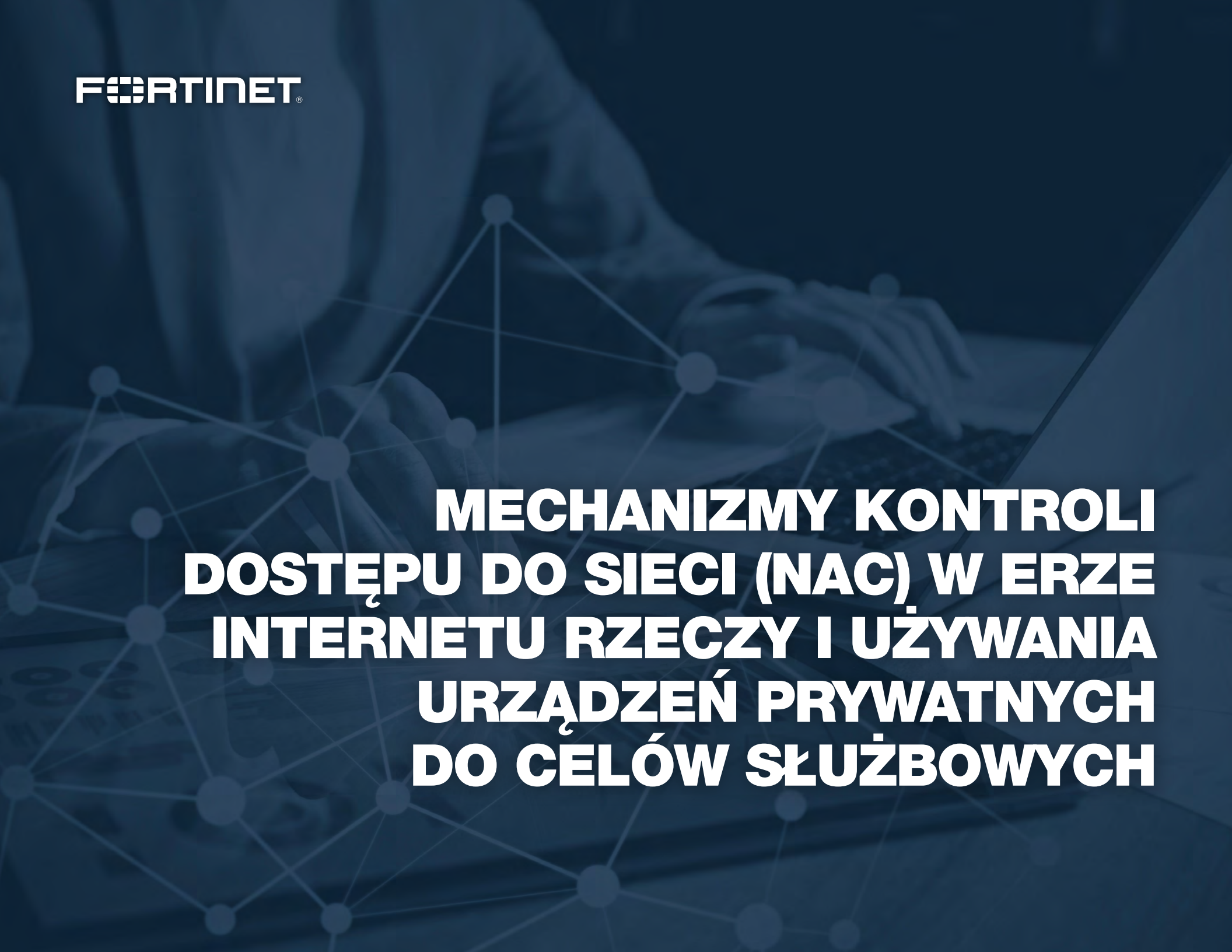


MECHANIZMY KONTROLI DOSTĘPU DO SIECI (NAC) W ERZE INTERNETU RZECZY I UŻYWANIA URZĄDZEŃ PRYWATNYCH DO CELÓW SŁUŻBOWYCH

SPIS TREŚCI

STRESZCZENIE

W miarę upowszechniania się Internetu rzeczy (IoT) i urządzeń przenośnych zwiększa się powierzchnia ataku przedsiębiorstwa, a na granicach jego 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 architekci 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.

WSTĘP — EWOLUCJA 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 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, 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 muszą nadal ewoluować. Aby w pełni zabezpieczyć urządzenia końcowe związane z Internetem rzeczy i zasadami BYOD, przedsiębiorstwa 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 trzeciej generacji muszą być zatem zdolne do koordynowania wszystkich aspektów widoczności urządzeń końcowych, kontroli i automatycznego reagowania na zagrożenia.

CZĘŚĆ 1: WIDOCZNOŚĆ CAŁEJ SIECI

Nie można chronić tego, czego się nie widzi. Brak widoczności urządzeń końcowych naraża przedsiębiorstwo na niewidoczne ryzyko. W niedawnym badaniu 42% specjalistów ds. IT twierdzi, że mieli u siebie do czynienia z naruszeniem bezpieczeństwa za pośrednictwem urządzeń końcowych, podczas gdy kolejne 20% z nich uważa, że nie byli pewni, czy do takiego naruszenia doszło[1].

Zespoły 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) oraz wszelkich innych urządzeń korzystających z protokołu IP w ramach jednego, zintegrowanego widoku topologii sieci.

[1] Lee Neely, „Endpoint Protection and Response: A SANS Survey", SANS Institute, 12 czerwca 2018 r.

Oferowane przez mechanizmy kontroli dostępu do sieci 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 (headless), które nie mogą obsługiwać wbudowanego zabezpieczenia ze względu na swoje ograniczone funkcje (wiele takich urządzeń wchodzi w skład Internetu rzeczy).

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, 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 punktem końcowym.

63%

przedsiębiorstw nie jest zdolna do monitorowania urządzeń przenośnych po odłączeniu ich od swojej sieci.

„The Cost of Insecure Endpoints", Ponemon Institute, czerwiec 2017 r.

CZĘŚĆ 2: MECHANIZMY KONTROLI OPARTE NA ZASADACH

Po zidentyfikowaniu użytkownika i urządzenia mechanizm rozwiązanie NAC trzeciej generacji musi być zdolne do wdrożenia szczegółowych, opartych na zasadach mechanizmów kontroli dostępu w ramach dynamicznej segmentacji sieci. Segmentacja sieci tworzy głębsze warstwy zabezpieczeń w drodze odizolowania danych wrażliwych i stworzenia barier zapobiegających rozprzestrzenianiu się zagrożeń między maszynami wirtualnymi (wschód-zachód) w przedsiębiorstwie.

W tym celu mechanizmy kontroli dostępu do sieci muszą być 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 urządzeń dostępowych w całej infrastrukturze na potrzeby utworzenia na bieżąco aktualizowanej mapy połączeń i oraz wymuszenia kontroli dostępu do sieci w ramach poszczególnych segmentów.

Mechanizmy kontroli dostępu do sieci powinny 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.

Co tydzień przedsiębiorstwa poświęcają 1156 godzin i wydają

3,4 MLN USD

na ochronę przed atakami na urządzenia końcowe.

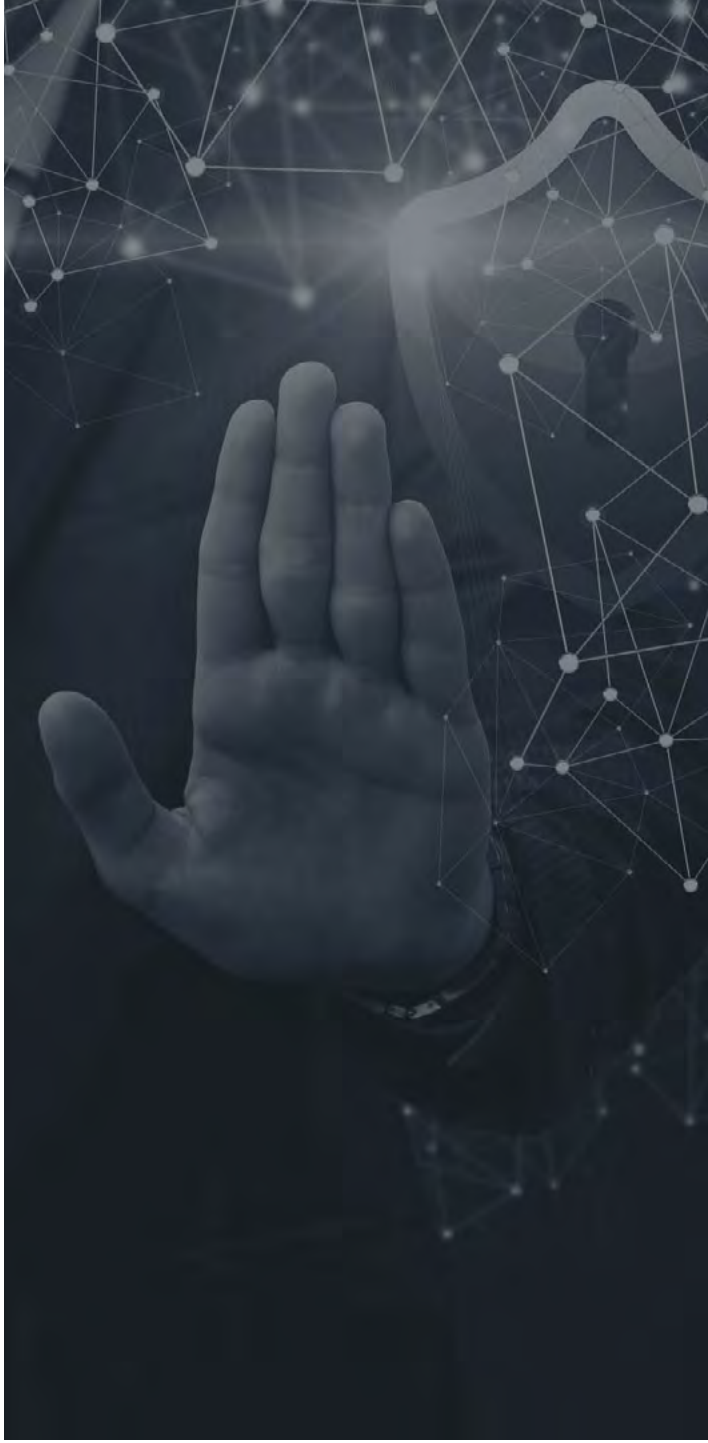
„The Cost of Insecure Endpoints", Ponemon Institute, czerwiec 2017 r.

CZĘŚĆ 3 — AUTOMATYCZNE REAGOWANIE NA ZAGROŻENIA

Wyniki najnowszych badań wskazują, że średni czas identyfikacji naruszenia bezpieczeństwa pozostaje długi (197 dni), podobnie jak średni czas potrzebny na jego powstrzymanie (69 dni)[2]. 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. Rozwiązania 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, kwarantanny lub szereg działań związanych z powiadamianiem.

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.



[2] Larry Ponemon, „Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT", SecurityIntelligence, 11 lipca 2018 r.

AUTOMATYZACJA ROZWIĄZAŃ W ZAKRESIE WYKRYWANIA ZAGROŻEŃ I REAGOWANIA NA NIE W PUNKTACH KOŃCOWYCH TO PRIORYTET DLA SPECJALISTÓW DS. CYBERBEZPIECZEŃSTWA, KTÓRZY CHCĄ UZYSKAĆ SKUTECZNĄ KONTROLĘ NAD TYMI URZĄDZENIAMI. **TYLKO 45% Z TYCH SPECJALISTÓW WSKAZAŁO, ŻE OBSŁUGIWANE PRZEZ NICH PROCESY SĄ W PEŁNI ZAUTOMATYZOWANE.**

Lee Neely, „Endpoint Protection and Response: A SANS Survey", SANS Institute, 12 czerwca 2018 r.

PODSUMOWANIE — JAKIEGO ROZWIĄZANIA SZUKAĆ

W obliczu zmieniającej się infrastruktury sieci, zaawansowanych ataków na urządzenia końcowe i coraz bardziej restrykcyjnych przepisów przedsiębiorstwa 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 rozwiązanie NAC powinno spełniać następujące kryteria:

- ☐ **Widoczność.** Rozwiązanie NAC powinno „widzieć" i móc ocenić wszystkie rodzaje urządzeń końcowych (w tym urządzenia końcowe w ramach Internetu rzeczy) przed podłączeniem ich do sieci. Ponadto powinno 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 być zdolne do zautomatyzowania egzekwowania zasad bezpieczeństwa i działania mechanizmów kontroli, a także do współdzielenia informacji o zagrożeniach.

- ☐ **Integracja.** Rozwiązanie NAC powinno 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 punktu końcowego rozwiązanie NAC powinno 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.** Rozwiązanie NAC trzeciej generacji powinno udostępniać skalowalną architekturę, która w przystępnej cenie będzie obsługiwać wiele lokalizacji w całym przedsiębiorstwie i nieograniczoną liczbę urządzeń. Ponadto musi oferować elastyczne możliwości wdrażania z opcją fizyczną, wirtualną i w chmurze.

FORTINET

www.fortinet.com

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

POLSKA
ul. Złota 59
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapur 038988
Tel: +65-6395-7899
Faks: +65-6295-0015

CENTRALA — AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

275502-0-0-PL 16 maja, 2019 1:59 PM

ebook-nac-in-the-era-of-iot-and-byod