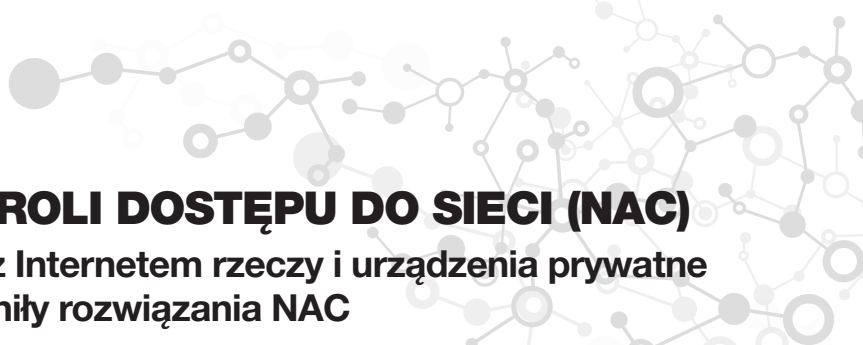
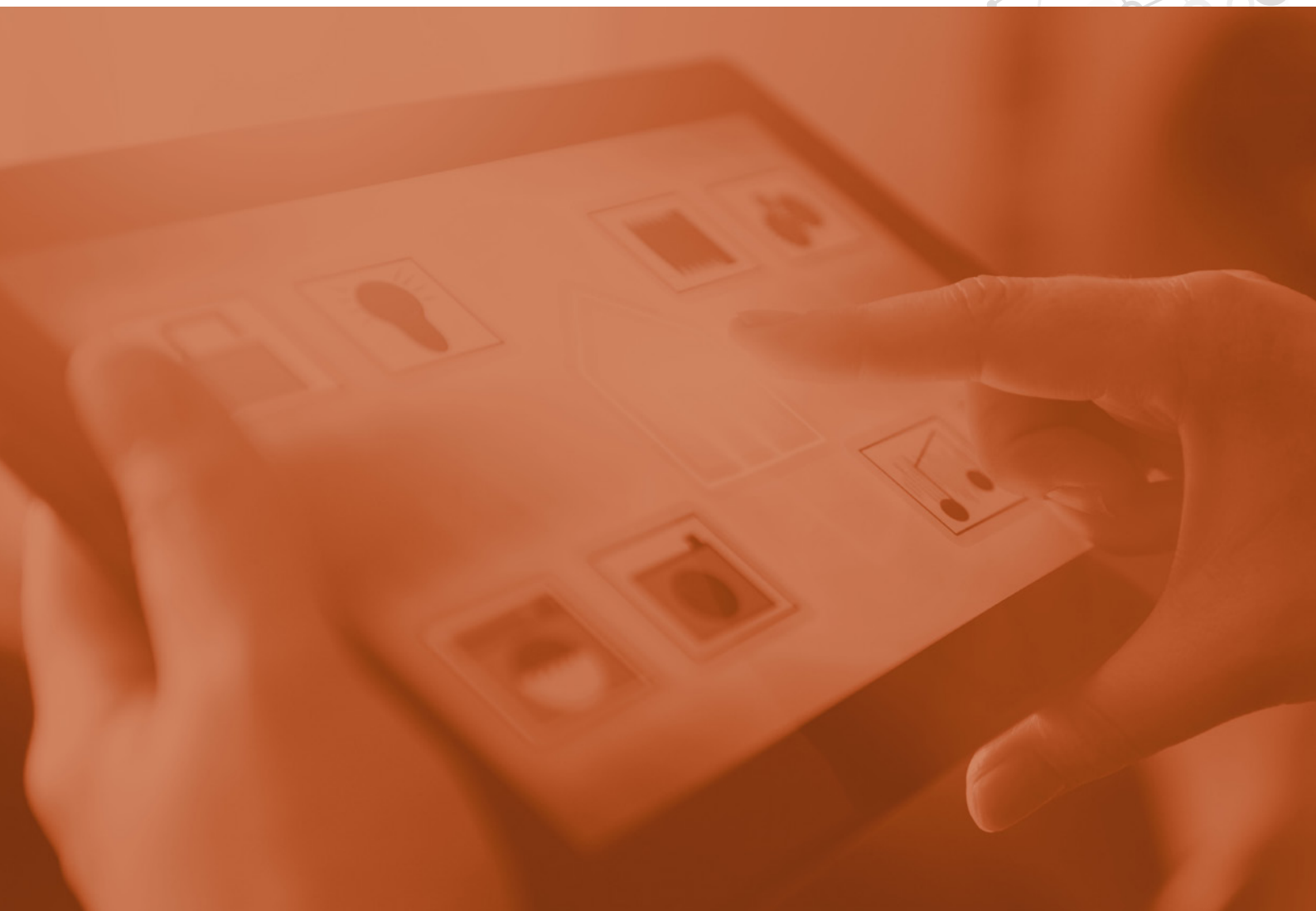




ROZWÓJ SYSTEMÓW KONTROLI DOSTĘPU DO SIECI (NAC)

W jaki sposób urządzenia związane z Internetem rzeczy i urządzenia prywatne używane do celów służbowych zmieniły rozwiązania NAC



STRESZCZENIE

Upowszechnianie się zasad dotyczących korzystania z urządzeń prywatnych do celów służbowych (BYOD) oraz Internetu rzeczy (IoT) zmieniło ukształtowanie sieci oraz sposób ochrony tych urządzeń. W kontekście ochrony urządzeń końcowych strategię zabezpieczenia sieci, takie jak mechanizmy kontroli dostępu do sieci (NAC) poprzedniej generacji, są już przestarzałe, nie mogą bowiem zapewnić kompleksowej widoczności, kontroli i zdolności do automatycznego reagowania na zagrożenia niezbędnych do zabezpieczenia przeprowadzanych w przedsiębiorstwie wdrożeń urządzeń związanych z Internetem rzeczy i urządzeń prywatnych używanych do celów służbowych. Taka luka w zabezpieczeniach nie tylko naraża na ryzyko użytkowników, dane i operacje biznesowe w przedsiębiorstwie, ale również naraża przedsiębiorstwo na potencjalne grzywny i innego rodzaju odszkodowania o charakterze karnym.



Analitycy IDC szacują, że w ramach transformacji cyfrowej wydatki dotyczące

**Internetu rzeczy
na całym świecie
osiągną w 2018 r.
772,5 mld USD**

i przekroczą poziom

1 biliona USD
do 2021 r.¹.



OD PRZENOŚNYCH URZĄDZEŃ KOŃCOWYCH DO URZĄDZEŃ ZWIĄZANYCH Z INTERNETEM RZECZY

Przedsiębiorstwa nadal mają problemy z zabezpieczeniem przenośnych urządzeń końcowych. Goście, wykonawcy, usługodawcy i inne osoby z zewnątrz często wymagają dostępu do sieci. O ile w tym przypadku pomocne bywają zapory i technologie z zakresu zarządzania dostępem do danych i aplikacji przedsiębiorstwa na urządzeniach przenośnych (EMM), nie mają one jednak (a) zdolności do zapewnienia wystarczającej widoczności urządzeń i statusu użytkownika w celu określenia, czy tacy użytkownicy / takie urządzenia mogą uzyskać zgodę na dostęp do sieci ani (b) odpowiednio szczegółowych mechanizmów kontroli, aby nałożyć odpowiednie ograniczenia dostępu.

Tymczasem cyberprzestępcy również często atakują urządzenia związane z Internetem rzeczy, ponieważ stanowią one najsłabsze ogniwa sieci. Na przykład w przypadku wielu takich urządzeń nie da się zainstalować poprawek lub nie mają one żadnych lub prawie żadnych wbudowanych zabezpieczeń.

O ile przepisy branżowe dotyczące urządzeń związanych z Internetem rzeczy są dopiero tworzone, zabezpieczenie tych urządzeń jest ważnym elementem rozważań związanych z zapewnieniem zgodności z istniejącymi standardami i wymogami. Większość przedsiębiorstw musi przestrzegać przepisów wymagających wdrożenia ścisłych zasad kontroli



Liczba osób korzystających z urządzeń prywatnych do celów służbowych również rośnie i przekroczyła **1,76 mld, co stanowi około **59,4%** łącznej populacji pracowników na świecie².**

dostępu do sieci i ochrony danych takich jak przepisy RODO, ustawy HIPAA (Health Insurance Portability and Accountability Act) i ustawy SOX (Sarbanes-Oxley), przepisy Komisji Papierów Wartościowych i Giełd (SEC) oraz norm Payment Card Industry Data Security Standard (PCI DSS). Aby zapewnić taką zgodność, przedsiębiorstwa muszą zabezpieczyć wszystkie urządzenia końcowe, ponieważ w przeciwnym razie mogą zostać ukarane grzywną liczoną w milionach dolarów za naruszenie.

Wyniki jednego z badań wskazują, że 63% przedsiębiorstw nie jest zdolnych do monitorowania urządzeń przenośnych wylogowanych z sieci przedsiębiorstwa, a **53% przedsiębiorstw ujawniło, że liczba urządzeń końcowych zainfekowanych złośliwym oprogramowaniem wzrosła w ciągu ostatnich 12 miesięcy³.**

W kontekście licznych usług wirtualnych/chmurowych, przełączników, routerów i oddziałów podłączonych do sieci i wymieniających się danymi na całym świecie zadanie identyfikacji i zabezpieczenia urządzeń końcowych może wydawać się przytłaczające. O ile indywidualne zabezpieczenia mogą objąć część potencjalnych ścieżek ataku, brakuje im zasadniczo zintegrowanych i kompleksowych funkcji rejestrowania zdarzeń oraz informacji analitycznych, które potrzebne są zespołom ds. reagowania na incydenty i zapewnienia zgodności do zapobiegania naruszeniom oraz wykrywania i usuwania skutków naruszeń.

W tym przypadku problemem są przestarzałe mechanizmy kontroli dostępu, które niedostatecznie zabezpieczają sieci przed atakami (na przykład infekcjami pochodzącymi z zaatakowanych złośliwym oprogramowaniem urządzeń lub zagrożeniami wynikającymi z nieuprawnionego dostępu uzyskanego za pomocą skradzionych danych uwierzytelniających). Pierwsza generacja produktów NAC (produktów służących kontroli dostępu do sieci) służyła do

uwierzytelniania i autoryzacji urządzeń końcowych (zazwyczaj zarządzanych zewnętrznie komputerów PC) za pomocą prostej technologii typu „skanuj i blokuj”. Druga generacja produktów NAC miała zaspokoić rosnący popyt na mechanizmy zarządzania dostępem gości do sieci przedsiębiorstwa i ułatwiała zapewnienie ograniczonego dostępu do Internetu użytkownikom zewnętrznym takim jak goście, wykonawcy i partnerzy biznesowi.

Zmiany w infrastrukturze sieci (transformacja cyfrowa) i charakterze złożonych, ukierunkowanych ataków ujawniły obecnie kilka nowych luk w zabezpieczeniach sieci, które muszą zostać wyeliminowane.

1. Brak widoczności i informacji o zagrożeniach. Nie da się chronić czegoś, czego nie widać. Obecny brak kompleksowej i scentralizowanej widoczności urządzeń (zarówno urządzeń prywatnych używanych do celów służbowych, jak i produktów związanych z Internetem rzeczy) naraża przedsiębiorstwa na poważne zagrożenia. Osoby zajmujące się zabezpieczeniami muszą widzieć wszystkie elementy infrastruktury sieci w różnych lokalizacjach, w tym na najbardziej narażonych brzegach sieci. Zważywszy na fakt, że zabezpieczenia urządzeń końcowych i zabezpieczenia sieci zazwyczaj działają odrębnie od siebie, nie mogą wówczas wymieniać się ze sobą w czasie rzeczywistym istotnymi informacjami. Jeśli zaatakowane zostanie jedno urządzenie, pozostałe podłączone do sieci urządzenia (wraz z resztą architektury zabezpieczeń sieci) powinny bezzwłocznie otrzymać informację o tym zagrożeniu, aby podjąć przed takim zagrożeniem skoordynowane działania obronne w ramach całego przedsiębiorstwa (nie jest to jednak możliwe w przypadku wielu tradycyjnych podejść do zabezpieczeń).

2. Brak możliwości automatycznego reagowania na zagrożenie. W obliczu pojawiających się każdego dnia tysięcy alertów bezpieczeństwa dział IT nie jest zdolny do

PIERWSZA I DRUGA GENERACJA ROZWIĄZAŃ NAC

PIERWSZA GENERACJA ROZWIĄZAŃ NAC: PRZEŁĄCZNIKI WŁ./WYŁ.

- Zasady dostępu mające zastosowanie do każdego użytkownika
- Sztuczne, jednakowe mechanizmy kontroli dostępu



DRUGA GENERACJA ROZWIĄZAŃ NAC: WIDOCZNOŚĆ I ELASTYCZNOŚĆ

- Rozszerzona widoczność na potrzeby świadomego podejmowania decyzji o zasadach dostępu
- Zasady dotyczące dostępu gości i urządzeń niespełniających wymogów

TRZECIA GENERACJA ROZWIĄZAŃ NAC: PLATFORMA ZAPEWNIAJĄCA BEZPIECZNE KORZYSTANIE Z URZĄDZEŃ ZWIĄZANYCH Z INTERNETEM RZECZY I URZĄDZEŃ PRYWATNYCH UŻYWANYCH DO CELÓW SŁUŻBOWYCH

- Dobra widoczność sieci internetowych i urządzeń osobistych
- Szczegółowe profile użytkowników — kto, co, gdzie i kiedy



ręcznych interwencji w odniesieniu do każdego z nich. Gdy zapora, system wykrywania włamań (IDS), system ochrony przed włamaniami (IPS) lub podobne narzędzie zidentyfikuje naruszenie bezpieczeństwa w odniesieniu do konkretnego adresu IP, architektura zabezpieczeń powinna szybko i efektywnie automatycznie ograniczyć skutki takiego naruszenia, zmniejszając tym samym ekspozycję przedsiębiorstwa na zagrożenia.

3. Brak zautomatyzowanych procesów. Wiele przestarzałych procesów (dotyczących na przykład przydzielania zasobów) wymaga ręcznej interwencji pracownika działu IT. W efekcie przekłada się to na (a) spowolnienie procesu wdrażania nowych pracowników, (b) większą możliwość pojawiania się błędów ludzkich zwiększających ekspozycję przedsiębiorstwa na ryzyko, (c) większe obciążenie pracą działu IT oraz (d) obniżenie ogólnej efektywności działania systemu zabezpieczeń.

O ile wspomniane procesy mogą zapewniać kontrolę nad tradycyjnie zarządzanymi urządzeniami, niedający się zatrzymać marsz w kierunku Internetu rzeczy i korzystania z urządzeń prywatnych do celów służbowych niesie ze sobą wyjątkowe wyzwania. Najtrudniejszym z nich jest brak jakiegokolwiek standardowej konfiguracji dla urządzeń reprezentujących oba te zjawiska. Istnieją bowiem setki permutacji dotyczących typu, marki, systemu operacyjnego i statusu bezpieczeństwa takich urządzeń, przy czym w szczególności urządzenia te nie mają zabezpieczeń wymaganych przez przedsiębiorstwa. Z biegiem czasu wspomniany problem staje się coraz bardziej złożony w miarę dołączanych do Internetu rzeczy w zawrotnym tempie nowych elementów takich jak roboty, monitory, czujniki temperatury, pompy insulinowe, czujniki HVAC, zautomatyzowane systemy kontroli dostępu itp.

Według szacunków specjalistów na świecie jest obecnie **9 mld urządzeń związanych z Internetem rzeczy**, a liczba ta najprawdopodobniej wzrośnie do **55 mld w 2025 r.**⁴

ZABEZPIECZENIA MUSZĄ BYĆ ROZWIJANE, ABY KONTROLOWAĆ EKSPOZYCJĘ NA RYZYKO ZWIĄZANE Z UZYSKIWANIEM DOSTĘPU DO SIECI

Wraz z upowszechnianiem się stosowania urządzeń prywatnych do celów służbowych i korzystania z urządzeń związanych z Internetem rzeczy wymagania dotyczące bezpieczeństwa urządzeń końcowych zaczęły przewyższać możliwości mechanizmów kontroli dostępu poprzedniej generacji. W obliczu coraz częstszych i coraz bardziej zaawansowanych ukierunkowanych ataków typu „zero-day” i APT potrzeba eliminacji luk w zabezpieczeniach z dnia na dzień staje się coraz bardziej nagląca. Architekci zabezpieczeń muszą na nowo projektować mechanizmy kontroli dostępu, aby odpowiednio chronić urządzeń końcowe, użytkowników i ogólnie rozumiane przedsiębiorstwo przed potencjalnie katastrofalnymi skutkami naruszeń bezpieczeństwa, których źródłem były wspomniane urządzenia.

¹ „IDC Forecasts Worldwide Spending on the Internet of Things to Reach \$772 Billion in 2018”, IDC, 7 grudnia 2017 r.

² Nick Elia, „Mobile Worker Report Announcement”, VDC Research, 11 sierpnia 2017 r.

³ „The Cost of Insecure Endpoints”, Ponemon Institute, czerwiec 2017 r.

⁴ Peter Newman, „IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers”, Business Insider, 27 lipca 2018 r.