CSO

Microsoft Security

SPONSOROWANA ZAWARTOŚĆ

Zabezpieczenia Zero Trust: **Lekcje od pierwszych użytkowników**

CSO Microsoft Security

Spis treści

CSO Microsoft Security

Wprowadzenie

Ostatnie dwa lata zakłóceń wstrząsnęły tradycyjnymi modelami IT i bezpieczeństwa. W rezultacie zabezpieczenia Zero Trust szybko przekształciły się z interesującej koncepcji w podstawę nowoczesnych zabezpieczeń korporacyjnych.

Nowe badanie przeprowadzone przez firmę Foundry wykazało, że 52% organizacji prowadzi pilotaż lub wdrożyło architekturę Zero Trust, a kolejne 15% bada modele Zero Trust. Pierwsi użytkownicy informują o licznych korzyściach z wdrożeń, w tym lepszej ochronie danych klientów, zmniejszeniu złożoności oraz zapewnieniu bezpiecznego, niezawodnego dostępu do zasobów korporacyjnych.

W niniejszym e-booku zostaną omówione wyniki badań Foundry, które podkreślają znaczenie strategii Zero Trust w pomaganiu CISO w ochronie ich organizacji przed wieloma zagrożeniami wynikającymi z licznych wektorów ataków. Zawiera również wskazówki, jak wdrożyć Zero Trust, przygotowane dla osób, które rozpoczynają swoją podróż.

Informacje o ankiecie

W lutym i marcu 2022 roku firma Foundry przeprowadziła ankietę wśród amerykańskich firm, aby zbadać obecny stan przyjęcia Zero Trust. Respondenci musieli pracować na stanowisku menedżera IT lub wyższym w firmie zatrudniającej ponad 500 pracowników i odgrywać rolę w procesie zakupu produktów i usług z zakresu cyberbezpieczeństwa.

Przepytano łącznie 250 respondentów w ankiecie liczącej 23 pytania.

CSO Microsoft Security

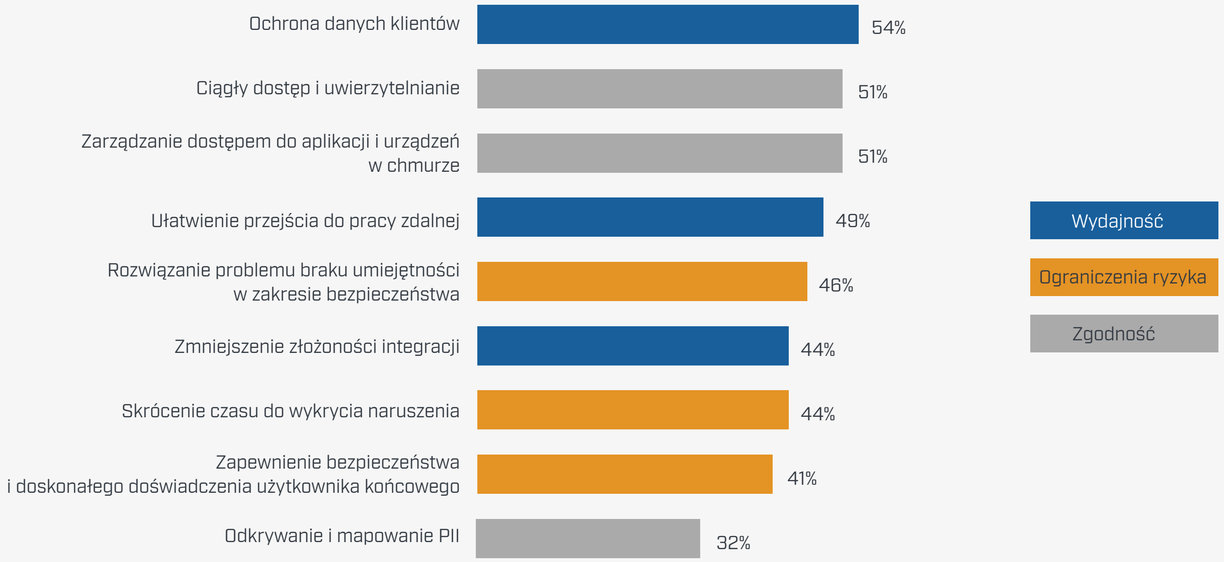
Zero Trust jest tutaj i zapewnia wartość

Z wyników ankiety, a także ze szczegółowych wywiadów z kierownikami działu IT i bezpieczeństwa jasno wynika, że w większości organizacji priorytetem jest Zero Trust. A ci, którzy wdrożyli różne komponenty Zero Trust, już teraz dostrzegają płynące z nich korzyści.

Większość respondentów, którzy wdrożyli Zero Trust (87%) twierdzi, że architektura jest zgodna z pierwotnych celami wdrożenia, przyjęcia i integracji lub je przekracza.

„[Zero Trust] stało się dla nas standardową procedurą operacyjną. Nie sądzę, żebyśmy kiedykolwiek mieli wrócić do poprzedniego stanu” — mówi dyrektor ds. IT globalnego sprzedawcy detalicznego. (Respondentom zapewniono anonimowość w zamian za swobodne mówienie

Korzyści uzyskane od czasu wdrożenia Zero Trust



12% respondentów twierdzi, że otrzymali *wszystkie* korzyści

Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

o swoich planach w zakresie bezpieczeństwa). Około 44% respondentów stwierdziło również, że podejście Zero Trust zmniejszyło złożoność nieodłącznie związaną z wdrażaniem zintegrowanej architektury bezpieczeństwa. „Ponieważ masz do czynienia z ramami i pracujesz z nimi, to sprawia, że sprawy stają mniej skomplikowane" – twierdzi CISO z firmy call center zatrudniającej 3500 pracowników.

Wiceprezes i CISO w firmie świadczącej usługi finansowe, która zatrudnia 17 000 pracowników mówi, że uwierzytelnianie wieloskładnikowe wdrożone przez jego firmę w ramach Zero Trust jest hitem wśród pracowników. „Właściwie to podniosło poziom zadowolenia wśród pracowników, ponieważ teraz nie muszą siadać do komputera dostarczonego przez firmę i korzystać z klienta VPN; mogą dostać się do zasobów z dowolnego miejsca" – powiedział. CISO zauważa, że koncepcja dostępu z najmniejszymi przywilejami także zapewniła korzyści. „Odnotowaliśmy mniej poważnych w skutkach błędów ze strony administratorów systemu z powodu wdrożenia systemu dostępu do uprawnień", stwierdził. „Otrzymują przywileje dotyczące określonych kwestii i w określonych ramach czasowych, co oznacza, że rzadziej popełniają błędy".

Biorąc pod uwagę rosnące rozpowszechnienie phishingu i innych cyberataków, dyrektor ds. IT w firmie detalicznej podsumował korzyści związane z Zero Trust w następujący sposób: „Gdybyśmy nie mieli tego typu narzędzi, prawdopodobnie mielibyśmy teraz do czynienia z problemami i musielibyśmy płacić komuś w bitcoinie".

CSO Microsoft Security

Czynniki wpływające na wdrażanie Zero Trust

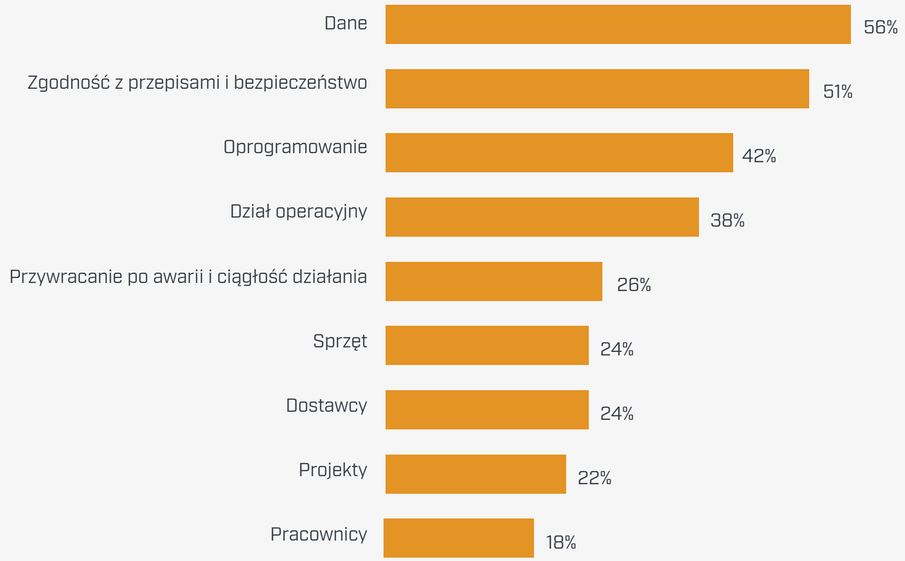
Zbieg wydarzeń zachęca firmy do co najmniej rozważenia architektury Zero Trust. Na szczycie listy znajduje się potrzeba zarządzania ryzykiem dla wielu zasobów w odniesieniu do licznych zagrożeń. Respondenci w ankiecie wiązali incydenty związane z bezpieczeństwem i występujące przez wiele lat z wieloma przyczynami, na czele z lukami w za-bez-pie-cze-niach ze strony osób lub organizacji zewnętrznych. Inne przyczyny obejmują:

- Nieoczekiwane ryzyko biznesowe
- Nieprawidłową konfigurację usług lub systemów
- Złośliwe, celowe ataki z wewnątrz
- Niezłośliwe błędy użytkownika, w tym ofiary phishingu
- Kradzieże tożsamości
- Niezaktualizowane oprogramowanie
- Kradzieże poświadczeń

Incydenty niosą ze sobą różnorodne zagrożenia, oparte na danych.

W przypadku wielu organizacji nagłe przejście do pracy zdalnej wynikające z pandemii przyspieszyło plany przyjęcia Zero Trust, ponieważ tradycyjne modele bezpieczeństwa oparte na krawędzi stały się przestarzałe. Wiele organizacji już zmierzało w tym kierunku, przenosząc coraz więcej aplikacji i infrastruktury IT do chmury, ale pandemia wywołała dodatkowy wstrząs.

Najważniejsze kategorie zagrożeń w zakresie cyberbezpieczeństwa



Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

CSO Microsoft Security

Na przykład CISO z firmy zajmującej się technologiami medycznymi z 1700 pracownikami twierdzi, że chmura i pandemia były czynnikami napędzającymi przyjęcie Zero Trust, które teraz zapewnia bezpieczną podstawę dla dowolnego modelu miejsca pracy, który ma nadejść..

„Czynnikami biznesowymi był fakt, że jesteśmy firmą opartą na chmurze i musieliśmy być w stanie zabezpieczyć nasze środowisko", mówi. „W czasie pandemii musieliśmy też zapewnić zdolną zdalną siłę roboczą. Podejście [Zero Trust] pozwoliło nam radykalnie ograniczyć nasz ślad na rynku nieruchomości i prawdopodobnie pozostaniemy zdalną firmą wirtualną w co najmniej 60%".

CSO Microsoft Security

Nie brak zagrożeń

Potrzeby w zakresie zgodności zapewniły również impuls do stworzenia bardziej niezawodnych modeli zabezpieczeń. „Regulatorzy obserwują nas i oczekują, że będziemy w dalszym ciągu ulepszać nasze ramy bezpieczeństwa”, twierdzi starszy wiceprezes ds. globalnego bezpieczeństwa informacji w firmie świadczącej usługi finansowe z 290 000 pracowników.

Niektóre organizacje aktywnie podjęły kroki w kierunku Zero Trust, aby uniknąć głośnego naruszenia, które sprawi, że znajdą się w centrum uwagi z niewłaściwych powodów. „Chodziło o bycie aktywnym, aby nie występować w wiadomościach”, mówi CIO z wyższej instytucji zatrudniającej 3500 pracowników. „W innych lokalnych instytucjach mniej więcej naszej wielkości, które przez długi czas były nieczynne, wydarzył się prawdziwy horror”.

Inni mieli już poważne incydenty związane z cyberbezpieczeństwem, co skłoniło ich do szybkiego zrewidowania swojej strategii bezpieczeństwa. Po tym, jak firma ubezpieczeniowa z 6000 pracownikami przeszła atak ransomware, który doprowadził do zamknięcia sieci korporacyjnej na dwa tygodnie, chęć przyjęcia Zero Trust wyszła bezpośrednio od dyrektora generalnego. „Przyspieszyliśmy wdrożenie” – mówi wiceprezes ds. rozwoju IT firmy. „Na początku była to zdecydowanie najlepsza praktyka, która po ataku ransomware bardzo przyspieszyła”.

Katalizator oparty na chmurze

Wiceprezes i CISO w dużej firmie świadczącej usługi finansowe twierdzi, że jego zespół kilka lat temu dostrzegł potrzebę nowej architektury bezpieczeństwa, ponieważ zaczęto wdrażać coraz więcej zasobów opartych na chmurze, a użytkownicy stali się bardziej mobilni.

„Zdaliśmy sobie sprawę, że tradycyjna architektura bezpieczeństwa zamku i fosy, na której polegaliśmy w przeszłości, nie uchroni nas przed atakami w przyszłości”, mówi.

Ta rzeczywistość stała się całkowicie oczywista na początku 2020 roku, kiedy to firma odkryła, że jakiś czas temu napastnik przeszedł przez jej granicę i poruszał się w środowisku bez wykrycia. „Potrzebowaliśmy nowej architektury, w której moglibyśmy chronić i uwierzytelniać korzystanie z tych zasobów, gdziekolwiek się znajdują, a Zero Trust to architektura zaprojektowana do tego celu”.

CSO Microsoft Security

Przeszkody w przyjęciu Zero Trust

W przypadku wielu organizacji podejście Zero Trust oznacza fundamentalną zmianę w strukturze bezpieczeństwa, procesie i sposobie myślenia, co wyjaśnia niektóre z barier, które trzeba pokonać przed jego przyjęciem.

„Istniało tak wiele różnych silosów, w które zaczęliśmy uderzać w organizacji”, zauważył CISO z call center, wyjaśniając, że każdy zespół zajmujący się serwerami, sieciami i bazami danych ma swój własny kontyngent serwerów internetowych i narzędzi. „To nas zablokowało, ponieważ każdy miał inny pomysł na to, gdzie można pójść i jak to zrobić”.

Co przeszkadza w przyjęciu podejścia Zero Trust?

Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

CSO Microsoft Security

Według Anthony'ego Mocny'ego, starszego kierownika ds. marketingu produktów w firmie Microsoft, odkrywanie takich problemów może być w rzeczywistości pozytywnym efektem ubocznym Zero Trust. „Architektura Zero Trust ma na celu przełamanie silosów zespołów ds. bezpieczeństwa, które znajdują się w filarach technologicznych i pomaga zespołom w spójnej współpracy” – mówi. „Może to też oznaczać zmianę kulturową, jeśli chodzi o sposób, w jaki zespoły współpracują”.

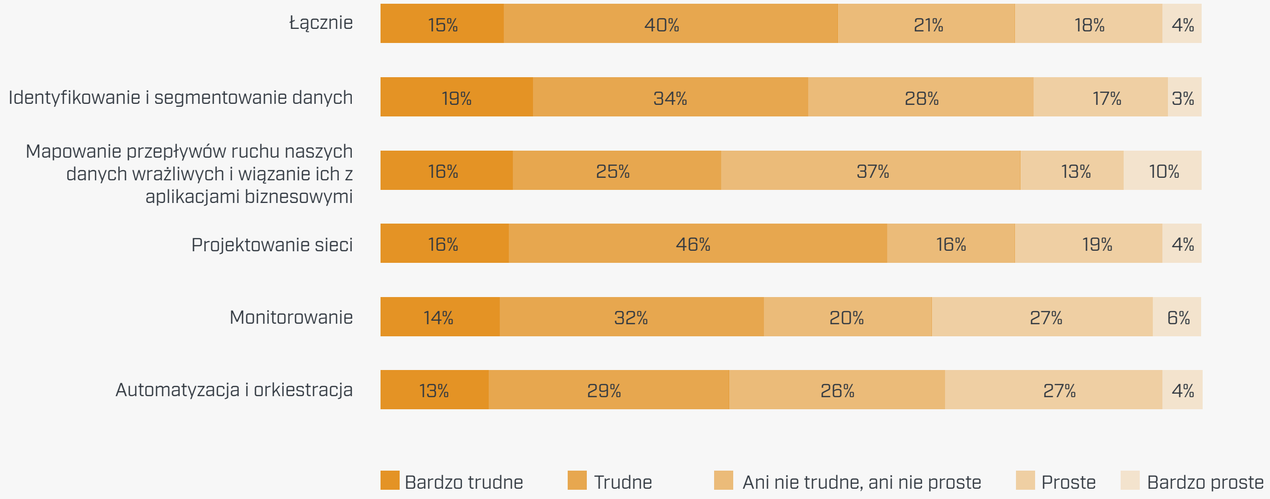
Dla wiceprezesa ds. usług finansowych/CISO starsze aplikacje były przeszkodą do pokonania na drodze prowadzącej do Zero Trust. „Trzeba wyposażyć się w nowoczesną technologię uwierzytelniania”, mówi. „W zależności od tego, ile mają lat, może to nie być łatwe”.

CSO Microsoft Security

Wyzwania związane z wdrażaniem

Gdy firmy wejdą na drogę w kierunku Zero Trust, mogą pojawić się też różne wyzwania związane z wdrożeniem. Ponad połowa respondentów (56%) przyznała, że wdrożenie Zero Trust było trudne lub bardzo trudne. Przykładowo:

Jak trudne jest wdrożenie Zero Trust?



Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 168

CSO Microsoft Security

W szczegółowych wywiadach często wymieniano wyzwania związane z segmentacją i mikrosegmentacją.

„Segmentujesz swoją sieć do pojedynczego hosta” – opowiada wiceprezes ds. usług finansowych/CISO. „To tak, jakby ustawić małą zaporę sieciową między każdym hostem w sieci wewnętrznej, dzięki czemu można zobaczyć cały ruch i kontrolować go aż do pojedynczej maszyny. Zapewnia to ogromne korzyści w zakresie bezpieczeństwa, ale jest bardzo trudne do wdrożenia, ponieważ teraz musisz zarządzać dziesiątkami tysięcy zapór ogniowych”.

Mapowanie przepływów ruchu może być kolejnym procesem, który zajmie wiele miesięcy. Jako mówi CTO z firmy wydawniczej i medialnej zatrudniającej 5000 pracowników, po wskazaniu strategicznych danych, aplikacji i usług sieciowych, które trzeba chronić, „mapowaliśmy przepływy transakcji w sieci i staraliśmy się zrozumieć je jako grupy informacji”, mówi.

„[Następnie] segmentowaliśmy części tych informacji i sposób, w jaki faktycznie przechodzą one przez sieć, nawet do pojedynczych pakietów informacji”. W tym momencie firma zastosowała zasady Zero Trust do każdego rodzaju przepływu ruchu. „Opracowaliśmy również nowe możliwości monitorowania i konserwacji naszej sieci”.

Pomimo wyzwań wielu respondentów uważa, że w końcu Zero Trust upraszcza codzienne operacje. W przypadku tradycyjnych technologii „wprowadzenie zmian zajmuje kilka dni; musisz je rozpowszechniać we wszystkich komponentach sprzętowych i programowych, i wykorzystujemy w tym celu wiele zasobów” – powiedział wiceprezes ds. usług finansowych i globalnego bezpieczeństwa informacji. „Kiedy analizujemy podejście Zero Trust, naprawdę w perspektywie długoterminowej minimalizuje ono złożoność architektoniczną i zmniejsza liczbę pracowników, których potrzebujemy do wykonywania tych samych zadań”.

CSO Microsoft Security

Najlepsze praktyki wdrażania Zero Trust

Coraz więcej firm wdraża architekturę Zero Trust, opracowuje plany działania i najlepsze praktyki, którymi inni mogą się kierować. Poniżej kilka innych zagadnień, które należy wziąć pod uwagę przy planowaniu wdrożenia.

Nie bierz na siebie za dużo na początku

Wyznaczanie strategii Zero Trust może zniechęcać, jeśli spojrzysz na nią tylko w szerokim kontekście konieczności zmiany zasad i zabezpieczeń w sieciach, danych, aplikacjach, tożsamościach, punktach końcowych i infrastrukturze. „Na początku po prostu patrzyliśmy na ogromną górę, na którą trzeba się wspiąć, i zastanawialiśmy się, czy naprawdę zamierzamy to zrobić” – mówi CIO wyższego szczebla. „Trzeba to robić krok po kroku”.

CIO ze swoim zespołem ostatecznie przyjęli podejście „podążaj za pieniędzmi”, nadając priorytet segmentacji aplikacji finansowych i płacowych w oddzielnej sieci.

Według Mocny'ego określenie najbardziej strategicznych zasobów w celu ochrony to rozsądne podejście. „Miej na uwadze powód, dla którego wdrażasz Zero Trust” – twierdzi.

W razie wątpliwości zacznij od wielu czynników

Przy ustalaniu priorytetów stosu zabezpieczeń wielu CISO i dostawców zabezpieczeń zaleca początkowo koncentrację na uwierzytelnianiu i innych zabezpieczeniach opartych na tożsamości. „Jeśli nie myślisz o konkretnym starcie, uwierzytelnianie wieloskładnikowe to dobre miejsce, aby zacząć”, mówi Mocny. Microsoft szacuje, że uwierzytelnianie wieloskładnikowe może zapobiegać ponad 90% ataków opartych na tożsamości.

Wiceprezes ds. usług finansowych/CISO zgadza się. „Uwierzytelnianie jest podstawowym elementem wdrażania architektury Zero Trust. Żaden z pozostałych komponentów nie działa, jeśli nie można zweryfikować tożsamości użytkownika końcowego, więc od tego zaczęliśmy”.

Następnie wiceprezes ds. usług finansowych/CISO zajął się komponentem sieciowym, który zapewnił natychmiastowe korzyści we wsparciu zdalnych pracowników. Zespół zostawił mikrosegmentację na później, ponieważ nie jest ona łatwo widoczna w obrębie całej firmy. „Kiedy z tym skończysz, zyskasz większe bezpieczeństwo, ale nikt nie zna różnicy” – mówi.

CSO Microsoft Security

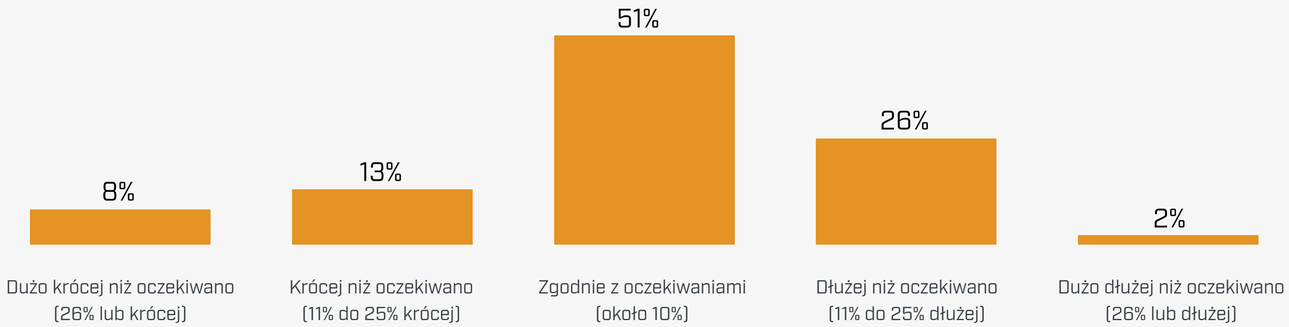
Podchodź realistycznie do terminów

To ważne, aby CISO ustalali realistyczne oczekiwania dotyczące wdrożeń Zero Trust. „Wdrożenie architektury Zero Trust to program, a nie projekt”, twierdzi wiceprezes ds. usług finansowych/CISO. „To była ogromna zmiana. Właściwe wykonanie obejmuje wiele projektów i prawdopodobnie potrwa latami; szybka i łatwa implementacja architektury Zero Trust nie istnieje”.

Jego kolega zajmujący się sprawami finansowymi, starszy wiceprezes zgadza się. „Nie sądzę, że kiedykolwiek skończymy, ponieważ zawsze pojawia się nowa technologia, zawsze pojawia się nowe złośliwe oprogramowanie, zawsze pojawiają się nowe zagrożenia” – mówi.

Większość respondentów (72%) twierdzi, że ich terminy wdrożenia były zgodne z planem lub przebiegały lepiej niż planowano, ale pozostali twierdzą, że wdrożenie trwało dłużej niż oczekiwano.

Czy Zero Trust zapewnia realizację Twoich celów na osi czasu?



Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 168

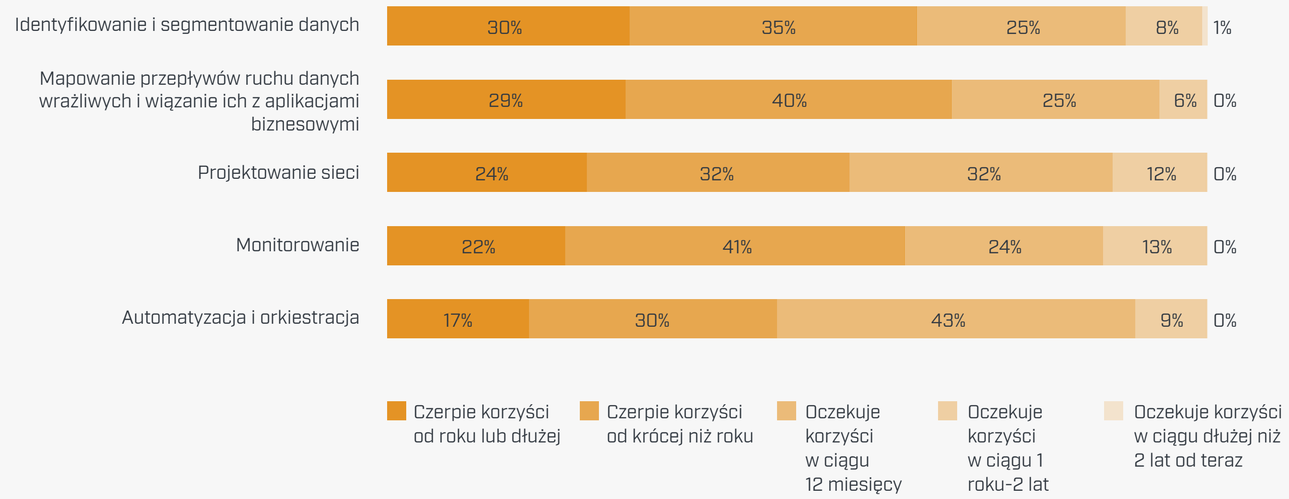
CSO Microsoft Security

Mierz na bieżąco

Podczas gdy wdrożenie Zero Trust trwa, CISO mogą i powinni opracowywać najważniejsze etapy na drodze w celu mierzenia postępów. To dobry znak, że około dwie trzecie ankietowanych twierdzi, że czerpie korzyści z większości aspektów swoich projektów w ciągu roku, a co około co najmniej jeden kwartał spodziewa się, że to nastąpi w ciągu 12 miesięcy, w ramach najważniejszych działań, w tym identyfikacji i segmentacji danych, mapowania ruchu przepływów i projektowanie sieci.

„Zero Trust to droga ze względu na ciągłą ocenę, której potrzebujesz, aby bronić się przed zmieniającym się charakterem ataków” – mówi Mocny. „Zawsze szukaj ulepszeń”.

Harmonogram czerpania korzyści z Zero Trust



Źródło: Zero Trust Adoption Survey, March 2022, Foundry. Base: 103

Skup się na ludziach, nie tylko na technologii

Model bezpieczeństwa Zero Trust ze względu na swój szeroki zasięg ma wpływ na każdego pracownika, w tym na zespoły IT i bezpieczeństwa, których zadaniem jest jego wdrożenie. Dlatego, podobnie jak w przypadku każdego dużego projektu technologicznego, jest ważne, aby upewnić się, że wdrożenia są zsynchronizowane z nowymi procesami i praktykami zarządzania zmianami, aby zapewnić płynne i pomyślne wdrożenie.

„Oprócz zmiany technologicznej następuje także zmiana kulturowa", mówi Mocny. „Jeśli masz wiele zespołów zajmujących się bezpieczeństwem, w tym architektów sieci lub ekspertów ds. tożsamości, musisz też zmienić sposób, w jaki zespoły współpracują. Aby zapewnić spójność wszystkich technologii, trzeba rozbić silosy".

Eliminowanie silosów polega na ścisłym zaangażowaniu zespołów ze wszystkich dziedzin w projekty pilotażowe i weryfikację koncepcji (POC). Dyrektor systemów IT w firmie telekomunikacyjnej z około 2000 pracownikami nauczył się tej lekcji po zmierzeniu się z kilkoma pojedynczymi punktami awarii podczas wdrażania, w tym usługami, które nie mogły się uwierzytelnić i nagle stały się „niezaufane", co sprawiło, że były niedostępne, a także niektóre systemy.

„Wdrożenie jednej usługi może wywołać efekt domina i zaszkodzić innym", mówi. Idąc dalej, „jesteśmy znacznie ostrożniejsi, przeznaczamy więcej czasu na POC, weryfikację i przeglądy architektury z ekspertami w danej dziedzinie przed wdrożeniem".

ROI Zero Trust

Zlecone w 2021 roku **badanie Forrester Consulting Total Economic Impact™** wylicza oszczędności i korzyści biznesowe wynikające z rozwiązań Microsoft Zero Trust. Na podstawie pięciu przedsiębiorstw, z którymi firma Forrester przeprowadziła wywiady, złożona organizacja zrealizowała trzyletni zwrot z inwestycji w wysokości 92% dzięki wdrożeniu architektury Zero Trust z Microsoft.

Ta złożona organizacja zaoszczędziła również średnio 20 dolarów na pracownika miesięcznie, eliminując potrzebę narzędzi bezpieczeństwa, które stały się zbędne w ramach Zero Trust, w tym rozwiązań do zarządzania punktami końcowymi, rozwiązań antywirusowych i chroniących przed złośliwym oprogramowaniem.

CSO Microsoft Security

Gdzie znajdujesz się na drodze do Zero Trust?

Jak wynika z ankiety, korzyści wynikające z modelu bezpieczeństwa Zero Trust wyraźnie przewyższają niektóre z wyzwań związanych z wdrożeniem, przed którymi stoją CISO i ich zespoły ds. bezpieczeństwa. Sprostanie tym wyzwaniom dzięki dobrze przemyślanemu planowi może pomóc Twojej organizacji w szybkim ulepszeniu zabezpieczeń, zmniejszeniu ryzyka i dostarczaniu wartości w całej firmie.

Aby ocenić stan zabezpieczeń Zero Trust w organizacji, wykonaj **ocenę dojrzałości Zero Trust Microsoft**.