NTT | cisco

INSIGHTS
DRIVEN BY DATA



Sprawdź, a później sprawdź ponownie:

Cyberbezpieczeństwo w świecie zerowego zaufania

Together we do great things
hello.global.ntt



Sprawdź, a później sprawdź jeszcze raz: Cyberbezpieczeństwo w świecie zerowego zaufania

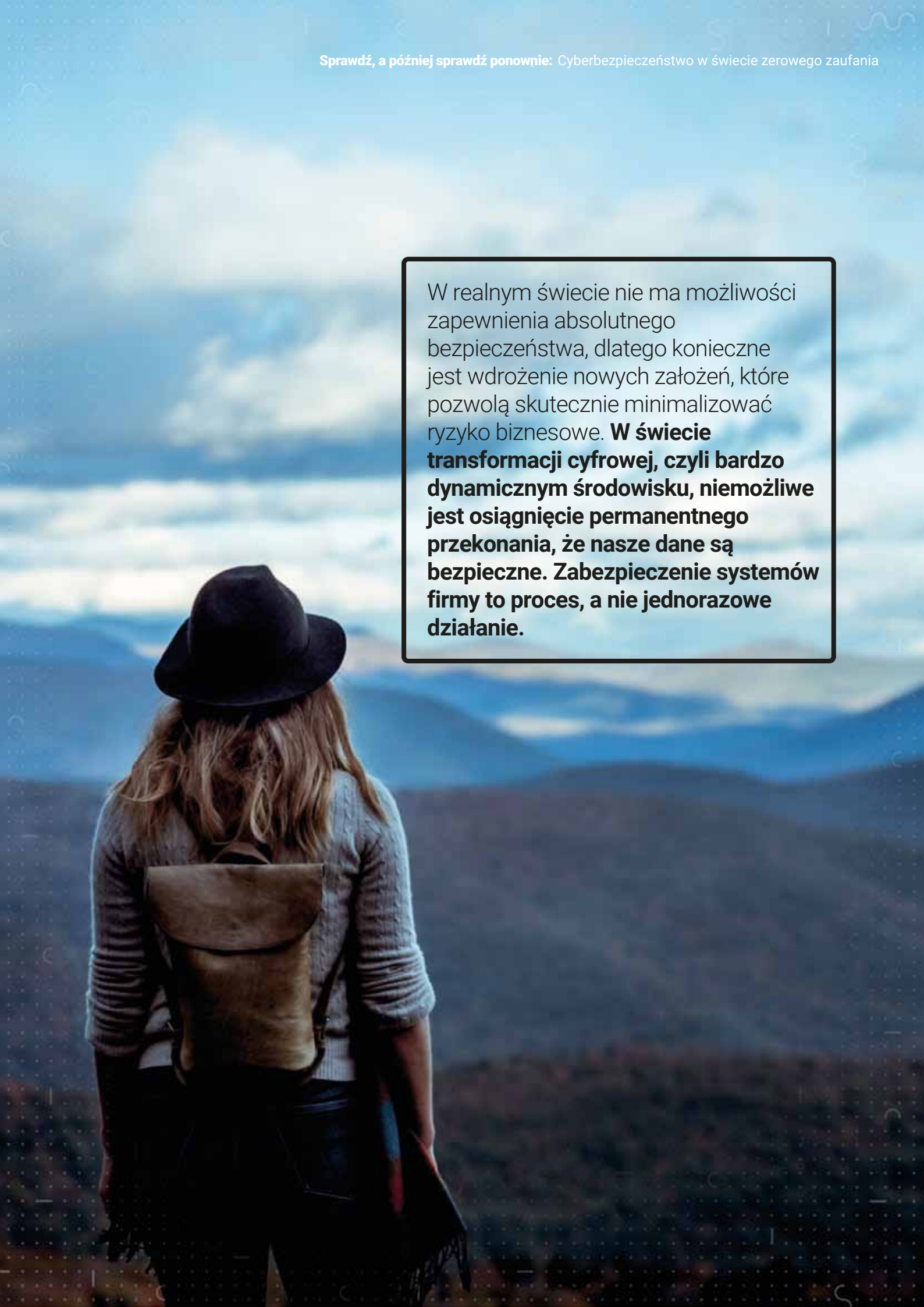
W latach osiemdziesiątych, gdy światu groziła zagłada nuklearna, prezydent Stanów Zjednoczonych, Ronald Reagan, podczas negocjacji ze Związkiem Radzieckim przyjął stosowaną przez Rosjan zasadę „ufaj, ale sprawdzaj". Dzięki jej stosowaniu zarówno Wschód, jak i Zachód przestrzegały warunków traktatów o rozbrojeniu jądrowym, co pomogło doprowadzić do zakończenia zimnej wojny. Jak to się ma do cyberbezpieczeństwa?

W dzisiejszych czasach, zasada przyjęta przez Reagana nie ma już zastosowania w świecie polityki ani tym bardziej w świecie bezpieczeństwa sieciowego. Dziś nie ma już tak wyraźnych granic pomiędzy tym, kto lub co znajduje się wewnątrz, a co na zewnątrz sieci przedsiębiorstwa. Obecnie, w dobie transformacji cyfrowej, mamy do dyspozycji rozproszone środowiska pracy i urządzenia użytkowników, usługi internetowe i interfejsy API, automatyzację, Internet Rzeczy, chmury obliczeniowe oraz inne usługi i połączenia – to sprawia, że całkowicie zatarły się granice sieci. Nie można już przyjmować za pewnik, że nasze miejsce pracy, procesy czy pracownicy są bezpieczni – konieczne jest stosowanie zasady zerowego zaufania (zero trust).

W realnym świecie nie ma możliwości zapewnienia absolutnego bezpieczeństwa, dlatego konieczne jest wdrożenie nowych założeń, które pozwolą skutecznie minimalizować ryzyko biznesowe. W świecie transformacji cyfrowej, czyli bardzo dynamicznym środowisku, niemożliwe jest osiągnięcie permanentnego czy statycznego statusu zaufania.

W związku z tym musimy przyjąć podejście „sprawdź, a później sprawdź ponownie” w zakresie bezpieczeństwa sieci, poprzez autoryzowanie dostępu i ochronę miejsc pracy, zadań i pracowników.

Mary K. Pratt, 'What is Zero Trust? A model for more effective security', CSO Australia, 16 January 2018 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html



W realnym świecie nie ma możliwości zapewnienia absolutnego bezpieczeństwa, dlatego konieczne jest wdrożenie nowych założeń, które pozwolą skutecznie minimalizować ryzyko biznesowe. **W świecie transformacji cyfrowej, czyli bardzo dynamicznym środowisku, niemożliwe jest osiągnięcie permanentnego przekonania, że nasze dane są bezpieczne. Zabezpieczenie systemów firmy to proces, a nie jednorazowe działanie.**



Przyspieszona transformacja cyfrowa

Przyspieszona transformacja cyfrowa

Do tej pory większość organizacji mogła pozwolić sobie na luksus działania we własnym tempie przy opracowywaniu i wdrażaniu środków bezpieczeństwa na potrzeby projektów transformacji cyfrowej. Sytuacja zmieniła się jednak wraz z wybuchem pandemii COVID-19. Obecnie procesy cyfryzacji zmieniły perspektywę czasową – są planowane na kilka tygodni, a nie na kilka lat. Świat cyberbezpieczeństwa gwałtownie przyspieszył, a model zero trust dobrze się w tej epoce zmian sprawdza.



Po wprowadzeniu lockdownu część organizacji pracuje zdalnie i w większym niż dotychczas stopniu opiera się na obecności w sieci (np. na portalach i aplikacjach webowych). To z kolei zwiększa zależność systemów, które już wcześniej były celem ataków. Warto spojrzeć na statystyki sprzed pandemii, zebrane jeszcze w znacznie spokojniejszym 2019 roku: według wyników przygotowanego przez firmę NTT raportu „2020 Global Threat Intelligence Report" (GTIR), w jednym z regionów dominowały ataki ukierunkowane na aplikacje (40%) i aplikacje webowe (20%), które łącznie stanowiły prawie 60% wszystkich ataków[1].



Wielu z tych ataków można było uniknąć - były przeprowadzone przy wykorzystaniu kilku starych wersji złośliwego oprogramowania, takich jak WannaCry i Conficker. Te wersje nadal mogą wyrządzać szkody w przypadku niezastosowania łat na znane luki w zabezpieczeniach. Według GTIR, najczęściej atakowaną luką w zabezpieczeniach była technologia OpenSSL (CVE-2017-3731), do której łaty są dostępne od ponad dwóch lat. OpenSSL była drugą najczęściej atakowaną technologią, po atakach na Netis/Netcore oraz inne powiązane routery i urządzenia sieciowe[2].



Dla cyberprzestępców wykrycie tego typu luk jest relatywnie łatwe, ponieważ mogą infiltrować środowiska z ukrycia, wykorzystując słabe zabezpieczenia lub brak stałej weryfikacji i monitorowania bezpieczeństwa. To pozwala im na prowadzenie intensywnej inwigilacji i sondowanie zabezpieczeń bez narażania się na wykrycie. **W świecie „zerowego zaufania" potrzebne jest podejście platformowe i spójny ekosystem dostawców, aby zapewnić możliwość współdzielenia informacji i danych dotyczących bezpieczeństwa w całym środowisku.** W ten sposób można zwiększyć poziom automatyzacji, w tym wykorzystania sztucznej inteligencji i uczenia maszynowego, co pozwoli na codzienne analizowanie i selekcjonowanie alertów na dużą skalę. Szybkość wykrycia zagrożeń jest kluczowym czynnikiem w ich powstrzymywaniu i ograniczaniu szkód w zasobach i systemach korporacyjnych. Widoczność w całym środowisku oraz automatyczna identyfikacja nietypowych zachowań i podejrzanego ruchu sieciowego ma ogromne znaczenie dla szybkiego podejmowania działań. Platformy takie jak Cisco Talos zapewniają organizacjom dostęp do informacji o zagrożeniach w czasie rzeczywistym, bezpośrednio z poziomu rozwiązań bezpieczeństwa Cisco, pomagając im zwiększyć skuteczność i skrócić czas potrzebny na wykrycie zagrożenia.



Większość analityków uważa, że w świecie po pandemii COVID, w celu zapewnienia większej elastyczności, organizacje będą zatrudniać więcej pracowników zdalnych, a także w większym stopniu polegać na usługach w chmurze, automatyzacji i własnej obecności w sieci poprzez portale dla klientów, e-sklepy i aplikacje webowe. Efektem tego będzie większa ekspozycja na ryzyko związane z systemami i aplikacjami, które już teraz są głównym celem cyberprzestępców.
W sytuacji zwiększenia zatrudnienia zdalnych pracowników na stałe, główną linią ataków cyberprzestępców nadal pozostaną zabezpieczenia dotyczące autoryzacji dostępu. „Spośród wszystkich zgłoszonych incydentów, 79% wiązało się z naruszeniem danych uwierzytelniających poprzez phishing, atak brute-force lub inne metody. Oznacza to, że ponad połowa WSZYSTKICH naruszeń, niezależnie od tego, czy zostały spowodowane przez jakiś incydent, błąd ludzki czy błąd systemu, ma swoje źródło w kwestiach związanych z uwierzytelnianiem. Naruszenia danych uwierzytelniających stanowią główną przyczynę większości naruszeń[3].

[1] 2020 Global Threat Intelligence Report', NTT Ltd., May 2020 https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report
[2] Ibid
[3] Ted Kietzman, 'Lessons from Australia's "OAIC's Notifiable Data Breach Statistics Report"', Cisco's Duo Security Blog, 6 February 2020, https://duo.com/blog/lessons-from-australia-s-oaic-s-notifiable-data-breach-statistics-report

© Copyright NTT Ltd.



Nowe poważne luki w zabezpieczeniach

Nowe poważne luki w zabezpieczeniach

Transformacja cyfrowa przyspiesza, jednocześnie zwiększa się obszar potencjalnych cyberataków, rośnie ekspozycja organizacji na zagrożenia, konieczne staje się wzmacnianie środków bezpieczeństwa. Wiele firm decyduje się na przenoszenie usług i aplikacji do chmury. To oznacza, że zmieni się także podejście cyberprzestępców – również skoncentrują się na cloudzie i wykorzystywaniu luk w zabezpieczeniach.

Ataki phishingowe zawsze opierały się na wykorzystaniu słabości czynnika ludzkiego. Tego typu ryzyko zwiększyło się, wraz z nagłym wzrostem liczby pracowników zdalnych, którzy uzyskują dostęp do usług i danych korporacyjnych za pośrednictwem swoich domowych łączy. Cyberprzestępcy niezmiennie żerują na ludzkich obawach, wątpliwościach i niepewności oraz na aktualnie występujących problemach. Teraz jest to przede wszystkim pandemia.

Od połowy stycznia 2020 roku strony internetowe podszywające się pod oficjalne źródła informacji o COVID-19 - ale hostujące zestawy exploitów lub złośliwe oprogramowanie - powstawały w niezwykłym tempie, czasami przekraczającym 2000 nowych serwisów dziennie. Miały miejsce również ataki polegające na spoofingu lub przekierowywaniu DNS, a także na przechwytywaniu ustawień DNS routerów, zabezpieczonych słabymi lub domyślnymi hasłami administratora.

Przeprowadzano też udane ataki typu ransomware i cryptojacking, które były inicjowane z urządzenia użytkownika za pomocą złośliwego oprogramowania, nieumyślnie pobranego z załącznika wiadomości e-mail lub poprzez łącze internetowe.

Ogromnym wyzwaniem dla organizacji jest dbanie o świadomość i czujność swoich pracowników w odniesieniu do tego typu ataków oraz zapewnienie lepszego zarządzania urządzeniami punktów końcowych i infrastrukturą bezpieczeństwa. Celem jest zapobieżenie uzyskaniu przez złośliwe oprogramowanie dostępu do systemów korporacyjnych. W przeprowadzonym przez Cisco badaniu „2020 CISO Benchmark Study" ponad połowa (52%) respondentów stwierdziła, że obecnie ochrona urządzeń mobilnych przed atakami jest bardzo albo ekstremalnie trudna. Jest to większe wyzwanie niż zapanowanie nad zachowaniami użytkowników, które były na pierwszym miejscu w poprzedniej edycji raportu .

W sytuacji braku wczesnego wykrywania i widoczności, gdy hakerowi uda się uzyskać dostęp, jest traktowany jak zaufany użytkownik – to kolejny ważny problem. W ten sposób sprawni hakerzy mają znacznie więcej czasu na długoterminowe planowanie i stosowanie nowych sposobów na naruszenie bezpieczeństwa środowiska. Prowadzi to do drugiej i trzeciej fali ataków, które mogą wyrządzić bardzo poważne szkody w organizacji.

W tak dynamicznym środowisku ciągła weryfikacja bezpieczeństwa jest niezwykle istotna.

Przeprowadzano też udane ataki typu ransomware i cryptojacking, które były **inicjowane z urządzenia użytkownika za pomocą złośliwego oprogramowania, nieumyślnie pobranego z załącznika wiadomości e-mail lub poprzez łącze internetowe.**

Cisco 2020 CISO Benchmark Report', Cisco, February 2020 https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

[4] Cisco 2020 CISO Benchmark Report', Cisco, February 2020 https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

© Copyright NTT Ltd.



Przyjęcie zasady zerowego zaufania

Przyjęcie zasady zerowego zaufania

Za czasów Ronalda Reagana, w epoce zimnej wojny, jednym z największych osiągnięć USA w dziedzinie bezpieczeństwa było rozmieszczenie satelitów szpiegowskich, co zwiększyło zdolność Stanów Zjednoczonych do gromadzenia informacji wywiadowczych, utrzymywania widoczności i analizowania działań innych graczy geopolitycznych. Analogicznie jest w przypadku organizacji. Kluczowym zadaniem jest zapewnienie kompleksowej widoczności w czasie rzeczywistym oraz zdolności do analizy kontekstu zdarzeń i dzielenia się informacjami w całym korporacyjnym środowisku teleinformatycznym, aby jak najlepiej radzić sobie z zaawansowanymi, uporczywymi zagrożeniami występującymi obecnie oraz tymi, które pojawią się po zakończeniu pandemii COVID-19.

Dobra wiadomość jest taka, że w kwestii działań w sferze bezpieczeństwa zmierzamy we właściwym kierunku. W badaniu Cisco „2020 CISO Benchmark Study" respondenci zostali zapytani o inwestycje ich organizacji w środki służące do identyfikacji, ochrony i wykrywania zagrożeń w celu zapobiegania przyszłym incydentom. W latach 2019-2020 wydatki na identyfikację wzrosły z 21% do 27%, natomiast wydatki na ochronę i wykrywanie zagrożeń pozostały na stałym poziomie, odpowiednio 25% i 18%. Trend ten pokazuje, że organizacje przeznaczają więcej środków na zapobieganie zagrożeniom, niż na reaktywne podejście do cyberbezpieczeństwa.

Widoczność stanowi ważny element w budowaniu odporności firmy na zagrożenia. Cybreodporność to zdolność organizacji do zachowania ciągłości w dostarczaniu produktów i usług pomimo zdarzeń, które mają wpływ na jej normalne funkcjonowanie. Bezpieczeństwo nigdy nie jest absolutne i firmy muszą być przygotowane na nieoczekiwane zdarzenia, umieć zapobiegać, reagować i skutecznie przywracać działanie bez zakłóceń lub obniżenia standardów.

Oprócz większej widoczności oraz zautomatyzowanej analizy zagrożeń, istotne jest wdrożenie infrastruktury, aplikacji i operacji, które są z założenia bezpieczne. Przyjmując zasadę zerowego zaufania można zidentyfikować i zweryfikować każdą osobę, urządzenie i aplikację, próbującą uzyskać dostęp do infrastruktury.

Podejście Cisco i NTT do kwestii bezpieczeństwa obejmuje pracowników, procesy i miejsce pracy. Oferta zawiera szereg kluczowych technologii, dzięki czemu możliwe jest zaspokojenie potrzeb nowoczesnego przedsiębiorstwa zarówno pod względem bezpieczeństwa, jak i zgodności z przepisami. Koncentruje się na trzech kluczowych elementach:

- egzekwowaniu kontroli opartej na określonych zasadach
- większej widoczności całego środowiska
- prowadzeniu szczegółowych dzienników i raportów ułatwiających wykrywanie i reagowanie na zagrożenia.

Zasada zerowego zaufania zapewni wdrożenie warstwowej ochrony, ciągłe uwierzytelnianie użytkowników, zarządzanie i kontrolę urządzeń, widoczność aplikacji oraz, poprzez segmentację, ograniczanie miejsc, w których procesy mogą być uruchamiane w sieci.

Zasada zerowego zaufania obejmuje trzy kluczowe filary stałej weryfikacji dostępu:

- Identyfikacja i autoryzacja użytkownika następującprzy użyciu uwierzytelniania wieloskładnikowego (MFA).
- Używane urządzenie lub punkt końcowy są znane i zgodne z polityką i standardami bezpieczeństwa.
- Użytkownik (i wszelkie aplikacje lub procesy, które uruchamia) ma dostęp jedynie do wyznaczonych obszarów w obrębie firmowego środowiska.

Innymi słowy „sprawdzaj i jeszcze raz sprawdzaj"!

© Copyright NTT Ltd.

Szefowie firm, zdając sobie sprawę, że istniejące do tej pory zasady bezpieczeństwa już nie są wystarczające, poszukują lepszych rozwiązań - i przekonują się, że model Zero Trust może przynieść najlepsze rezultaty.

Chase Cunningham, główny analityk firmy Forrester

Zasada zerowego zaufania to pragmatyczne i przyszłościowe założenie, które może pomóc w zapewnieniu skutecznego bezpieczeństwa całej architekturze przedsiębiorstwa obejmującej pracowników, procesy i miejsca pracy. Wdrożenie zasady zerowego zaufania eliminuje wiele wątpliwości związanych z ochroną infrastruktury przedsiębiorstwa przed wszystkimi potencjalnymi zagrożeniami, łącznie z tymi, które niesie ze sobą korzystanie z urządzeń mobilnych.

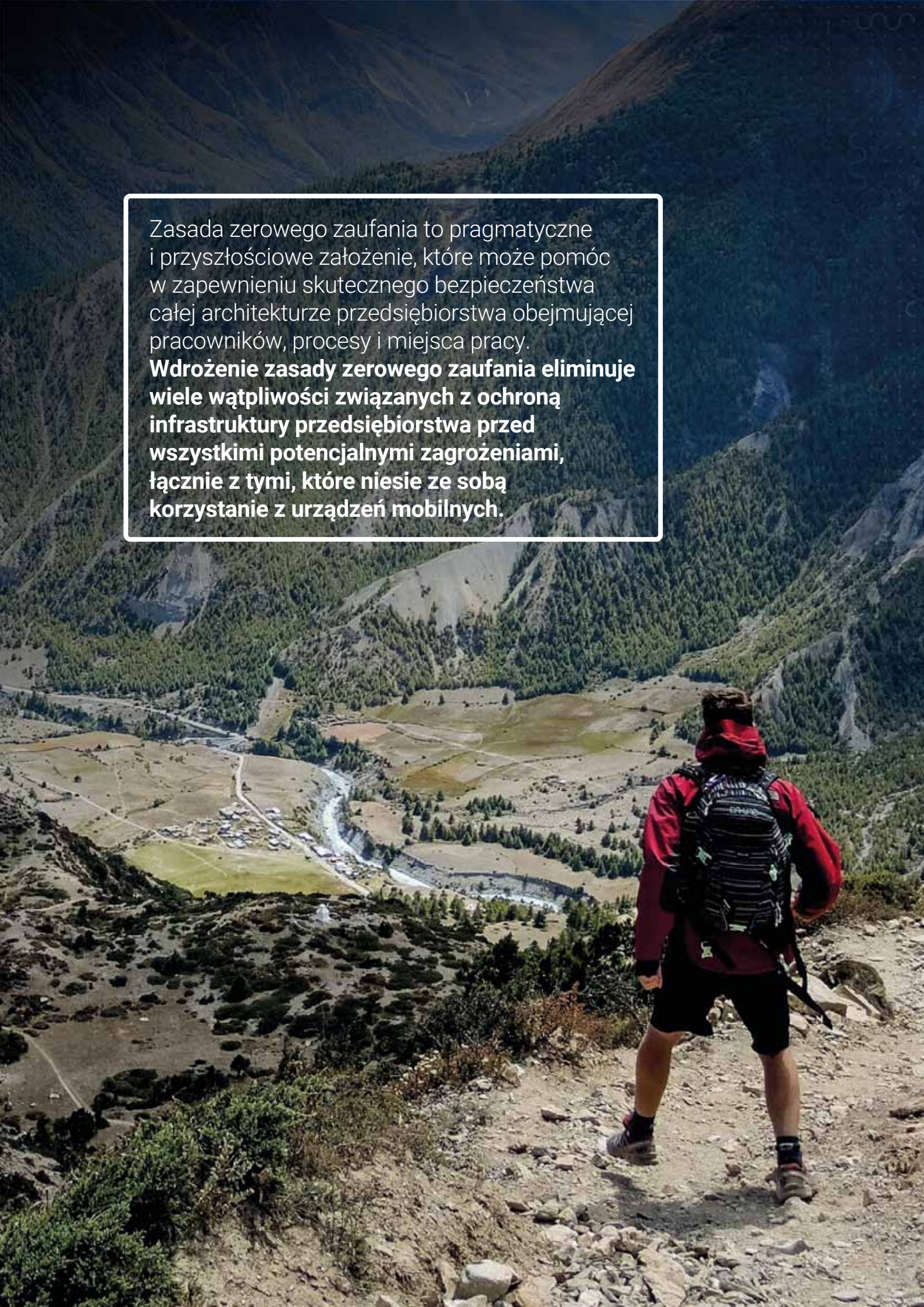
Przyjmując zasadę zerowego zaufania ważne jest, aby świadomie z założenia traktować kwestie bezpieczeństwa jako kluczowy i decydujący czynnik przy projektowaniu kompleksowych rozwiązań biznesowych. Dzięki temu powstanie rozwiązanie odporne na zagrożenia cybernetyczne, a przedsiębiorstwa będą mogły w przyszłości lepiej radzić sobie z niespotykanymi wcześniej i nieoczekiwanymi zdarzeniami, na przykład takimi, jak obecna sytuacja wynikająca z wybuchu pandemii COVID-19.

Właściwie wdrożona polityka bezpieczeństwa łączy w sobie bezpieczeństwo informacji, ciągłość działania i odporność organizacyjną. Należy uwzględniać najlepsze praktyki bezpieczeństwa przy tworzeniu wytycznych, procedur, infrastruktury i aplikacji, a także zagwarantować odpowiednią widoczność i kontrolę nad tymi komponentami, zarówno w przypadku ich normalnego funkcjonowania, jak i w sytuacji wystąpienia niepożądanego działania. Tylko dzięki takiemu podejściu, opartemu na zasadzie zerowego zaufania, organizacje mogą faktycznie zminimalizować ryzyko biznesowe.

Zaufanie jest naturalną potrzebą człowieka i odgrywa fundamentalną rolę w sposobie interakcji i komunikacji. Zbudowanie wzajemnego zaufania umożliwiło upadek Muru Berlińskiego i zakończenie zimnej wojny. W dzisiejszym świecie nadal konieczne jest tworzenie zaufanego środowiska, ale przyspieszone tempo transformacji cyfrowej sprawia, że jest to coraz trudniejsze. Aby ochronić zmienne i dynamiczne środowisko, w którym działają dziś przedsiębiorstwa, potrzebujemy ciągłej weryfikacji: nigdy nie zapominajmy więc o zasadzie „sprawdzaj i jeszcze raz sprawdzaj"!

Przyjmując zasadę zerowego zaufania ważne jest, aby świadomie z założenia traktować kwestie bezpieczeństwa jako **kluczowy i decydujący czynnik przy projektowaniu kompleksowych rozwiązań biznesowych.**

Mary K. Pratt, 'What is Zero Trust? A model for more effective security', CSO Australia, 16 January 2018 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html



Zasada zerowego zaufania to pragmatyczne i przyszłościowe założenie, które może pomóc w zapewnieniu skutecznego bezpieczeństwa całej architekturze przedsiębiorstwa obejmującej pracowników, procesy i miejsca pracy. **Wdrożenie zasady zerowego zaufania eliminuje wiele wątpliwości związanych z ochroną infrastruktury przedsiębiorstwa przed wszystkimi potencjalnymi zagrożeniami, łącznie z tymi, które niesie ze sobą korzystanie z urządzeń mobilnych.**



Współpracujemy w celu zapewnienia klientom spójnych doświadczeń