New Trust Standard

Budowanie opartych na zaufaniu relacji jutra w dziedzinie technologii

Spis treści

Wprowadzenie.....3

Brak dostępu dla intruzów – zasada braku zaufania.....4

Zarządzanie ryzykiem generowanym przez dostawców.....6

Poszanowanie praw dotyczących danych.....7

Transparentność.....9

Dowody.....11

Podsumowanie.....12

Wprowadzenie

Czy klienci mogą mieć pewność, że ich dane są bezpieczne?

Kiedyś zaufanie sprowadzało się do uścisku dłoni czy danego komuś słowa. Dziś jednak biznesowa rzeczywistość stała się zbyt złożona, by źródłem zaufania mogły być wyłącznie osobiste relacje. Zaufanie klientów zależy obecnie od bezpieczeństwa i transparentności całej organizacji – jej produktów, usług, pracowników, procesów, etyki i wartości, systemów wewnętrznych, dostawców i podwykonawców. Co istotne, na zaufanie klientów wpływa nie tylko strategia bezpieczeństwa firmy, ale również fakt, jak do kwestii bezpieczeństwa podchodzą jej dostawcy i podwykonawcy. Wreszcie, zaufanie klientów nie zależy wyłącznie od poziomu cyberbezpieczeństwa, ale także od działań podejmowanych w razie jego naruszenia, nie tylko od sposobu przechowywania prywatnych danych klientów, ale także od sposobu reakcji na żądanie przekazania tych danych przesłane przez zagraniczne organy ścigania w piątkowe popołudnie.

W dzisiejszej gospodarce cyfrowej konieczne są obiektywne wyznaczniki pozwalające określić poziom zaufania. Wymaga to pełnej transparentności. Informacje przepływające przez internet – trafiające czasem do chmury dostawcy – obejmują dane wrażliwe, takie jak loginy i hasła, rządowe numery identyfikacyjne, informacje finansowe, tajemnice handlowe, biznesplany czy krytyczne dane dotyczące infrastruktury. Jeśli trafią one w niepowołane ręce, może to skutkować naruszeniem prywatności, utratą własności intelektualnej, zakłóceniami w prowadzeniu działalności i osiąganiu dochodów, przerwami w dostawach prądu, a nawet zagrożeniami dla bezpieczeństwa narodowego.

Nadszedł czas na New Trust Standard. Stanowi on kompilację tego, co na przestrzeni lat usłyszeliśmy podczas rozmów z tysiącami klientów na całym świecie. New Trust Standard to wytyczne dotyczące oczekiwań i odpowiedzialności, w ramach których firmy i ich klienci mogą określać nowe zasady rządzące relacjami opartymi na zaufaniu.

Zaufanie nie sprowadza się do jednego działania czy usługi, np. szyfrowania, certyfikacji czy nadzoru nad łańcuchem dostaw. To połączenie wielu czynników, które wraz z upływem czasu w odpowiedzi na ewolucję w zakresie oczekiwań klientów, technologii, cyberataków i międzynarodowego zarządzania danymi niewątpliwie będą się zmieniać. W niniejszym dokumencie prezentujemy kluczowe aspekty New Trust Standard.

Kluczowe elementy New Trust Standard

„Nasi klienci nie tylko bardziej niż kiedykolwiek potrzebują innowacji. Chcą też partnerów, którym mogą ufać.”

Chuck Robbins
Chairman and CEO, Cisco

Brak dostępu dla intruzów – zasada braku zaufania

Weryfikacja każdego połączenia i każdego urządzenia – za każdym razem

Sceptycyzm, ciekawość, drobiazgowość – oto, czego wymaga się od ekspertów ds. bezpieczeństwa, ponieważ zaufanie zaczyna się od zdrowej podejrzliwości. Jak sama nazwa wskazuje, zasada braku zaufania to podejście, w ramach którego należy „nigdy nie ufać, za to zawsze weryfikować”.

Zasada ta nakazuje, by przy wyborze firmy upewnić się, jakie stosuje praktyki i polityki w zakresie zabezpieczeń. New Trust Standard zakłada prawo do zadawania pytań i oczekiwania jasnych odpowiedzi. Jeśli nasza firma ma do czynienia z wrażliwymi danymi, zasada braku zaufania zawsze oznacza kwestionowanie naszych założeń. Czy klienci są tymi, za kogo się podają? Czy ich urządzenia są bezpieczne? Czy aplikacja A ma ważny powód, by komunikować się z aplikacją B?

Obowiązujące przez kilkadziesiąt lat podejście do kontroli dostępu i wirtualnej sieci prywatnej (VPN) zdezaktualizowało się. Zakładało ono, że każde urządzenie łączące się z sieci korporacyjnej jest godne zaufania. Dodatkowo, po tym jak użytkownik i urządzenie pomyślnie przeszli weryfikację, mieli możliwość łączenia się z wieloma aplikacjami bez potrzeby ponownego uwierzytelnienia. Dziś żadne z tych założeń nie ma już racji bytu. Używany w celach zawodowych prywatny laptop czy tablet mógł zostać zainfekowany w domu. Urządzenie, które o godzinie 8:00 jest bezpieczne, o 8:03 może już takie nie być, bo uległo atakowi typu phishing. Ze względu na to, że przechowywanie i przetwarzanie danych ma dziś miejsca na obrzeżach sieci, nie istnieje już centralny „warowny zamek", który można otoczyć fosą. Co więcej, poza autoryzowaniem połączeń urządzeń użytkowników z serwerami zespoły IT muszą sprawdzać też, czy dozwolone są połączenia pomiędzy aplikacjami, urządzeniami i czujnikami. Nie ma na przykład żadnego powodu, by coś, co wygląda jak kamera monitoringu, łączyło się z bazą danych klienta.

Nowoczesne podejście do kontroli dostępu to architektura braku zaufania. Traktuje ona wszystkie zasoby tak, jakby były zewnętrzne. Weryfikuje zaufanie do nich przed każdą próbą uzyskania dostępu. I zezwala

na niego wyłącznie temu zasobowi, który jest wymagany – nawet jeśli żądanie pochodzi z biura dyrektora wykonawczego, a zabezpieczenia urządzenia zostały sprawdzone 30 sekund wcześniej przy okazji łączenia z inną aplikacją.

Zasady braku zaufania

- Wrażenia klienta powinny być najwyższym priorytetem. Uwierzytelnienie nie może stanowić obciążenia. Użytkownicy potrzebują wygodnego dostępu do aplikacji zarówno na miejscu, jak i w chmurze, by móc wykonywać swoją pracę.
- Należy stale weryfikować, czy użytkownicy, urządzenia i aplikacje są godne zaufania.
- Za pomocą maszynowego uczenia się należy identyfikować próby logowania odbiegające od typowego zachowania użytkownika. Ponieważ zdarzają się też fałszywe alarmy, warto pamiętać o ryzyku blokowania pełnoprawnych prób dostępu.
- Siłę zabezpieczeń aplikacji należy dostosować do stopnia wrażliwości danych. Wymaga to odpowiedniej klasyfikacji danych, a także świadomości, jak wygląda normalny ruch w danej aplikacji, co pozwoli wyłapać wszelkie odstępstwa.
- Należy zabezpieczyć połączenia pomiędzy poszczególnymi komponentami aplikacji, takimi jak jej logika i baza danych.
- Hakerom, którzy uzyskali dostęp do jednego serwera, warto utrudnić przejście na inne. Sprawdzi się tu np. segmentacja sieci, rozbudowane uwierzytelnianie i szyfrowanie, a także oznaczanie zaufanych urządzeń.

„ Już dziś większość dostawców chmury sprawdza zabezpieczenia urządzeń, zanim umożliwi im dostęp. Nowy Standard Zaufania zakłada natychmiastową identyfikację podejrzanych, nie wróżących nic dobrego prób dostępu i automatyzację tego, jak na nie reagujemy.”

Den Jones
Senior Director, Enterprise Security, Cisco

„ Architektura braku zaufania to niezwykła inwestycja w lepsze rozumienie ryzyka i zarządzanie nim poprzez różnorodne kontrole, a także w ciągłe udoskonalanie zabezpieczeń za sprawą maszynowego uczenia się.”

Brad Arkin
SVP, Chief Security and Trust Officer, Cisco

Zarządzanie ryzykiem generowanym przez dostawców

Wiara, że dostawca stworzył zaufany łańcuch dostaw

Kupując samochód, ufamy, że producent podjął odpowiednie działania w celu zweryfikowania jakości dostarczanych przez dostawców części takich jak hamulce czy pasy bezpieczeństwa. Podobnie rzecz ma się z klientami – oczekują, że dostawcy usług są świadomi wszystkich składowych swoich produktów oraz że podejmują właściwe kroki służące wyłapaniu wszelkich słabych punktów i uniemożliwienie manipulowanie danymi, szpiegostwa, awarii czy fałszerstwa.

To duże wymagania. W przypadku działań takich jak przetwarzanie płatności, uwierzytelnianie czy zarządzanie danymi i ich przechowywanie, dostawcy usług w chmurze zwykle korzystają z oprogramowania innych firm. Nawet ich własny kod zawiera zazwyczaj komponenty typu open-source stworzone przez ludzi z całego świata, a wiele z nich obejmuje liczne elementy zagnieżdżone.

Zakres „uzasadnionych" działań w kontekście kontroli dostawców, wciąż ewoluuje. Do zmian zmuszają nas nowe rodzaje zagrożeń, nowe branżowe praktyki, a także nowe osiągnięcia w dziedzinie cyberbezpieczeństwa.

Rekomendowane praktyki dotyczące łańcuch dostaw

Ochrona przed modyfikacją. Warto uruchomić program, który zagwarantuje, że firmowane przez nas rozwiązania są autentyczne, działają zgodnie z życzeniami klientów, a także że nie są kontrolowane przez niezidentyfikowane osoby, oraz że osoby takie nie mają do nich dostępu.

Wymaganie, by dostawcy spełniali właściwe standardy. Należy razem z zewnętrznymi dostawcami oceniać, monitorować i usprawniać ich praktyki w zakresie bezpieczeństwa. Dobrym punktem wyjścia są tu branżowe standardy: NIST 800-53 w zakresie kontroli bezpieczeństwa i prywatności, ISO/IEC 27001 w zakresie zarządzania bezpieczeństwem informacji, ISO 27018 w zakresie ochrony danych umożliwiających identyfikację w chmurach publicznych oraz ISO 27701 w zakresie zarządzania informacjami o prywatności.

Ustanowienie łańcucha zaufania. To, co najważniejsze, to wymaganie od dostawców oprogramowania i sprzętu dokumentacji określającej pochodzenie ich produktów. Niczym paszport, dokumenty te informują dokładnie o tym, jaką drogę przeszedł dany produkt – od etapu projektowania i tworzenia przez produkcję aż po dostawę. Dostawcy oprogramowania dokumentują, gdzie dane fragmenty kodu zostały stworzone, kto się pod nimi podpisał, jakich komponentów użyto do zarządzania tożsamością, gdzie kod został skompilowany itp. Zaś dostawcy sprzętu zapisują szczegóły takie jak numer seryjny każdej płytki obwodu drukowanego, a także informację, który pracownik ją pakował.

Zaufanie jako element umowy. Należy wymagać od dostawców przestrzegania tych samych standardów bezpieczeństwa i prywatności, które sami staramy się spełniać. Powinniśmy ustanowić procedury testowania i raportowania w zakresie słabych punktów. W umowie warto zawrzeć zapisy o ochronie danych klientów także po zakończeniu współpracy z dostawcą – w takiej sytuacji może on być np. zobowiązany do zwrócenia bądź zniszczenia takich danych.

Testowanie integracji przy pomocy produktów własnych i innych sprzedawców. W ten sposób zyskamy pewność, że dana integracja nie zaowocuje nowymi słabymi punktami.

Regularne przeprowadzanie audytów, w tym testów pod kątem słabych punktów. Wraz z dostawcą opracujmy plan identyfikacji słabości i zapobiegania im. Uwzględnijmy go w umowie.

Poszanowanie praw dotyczących danych

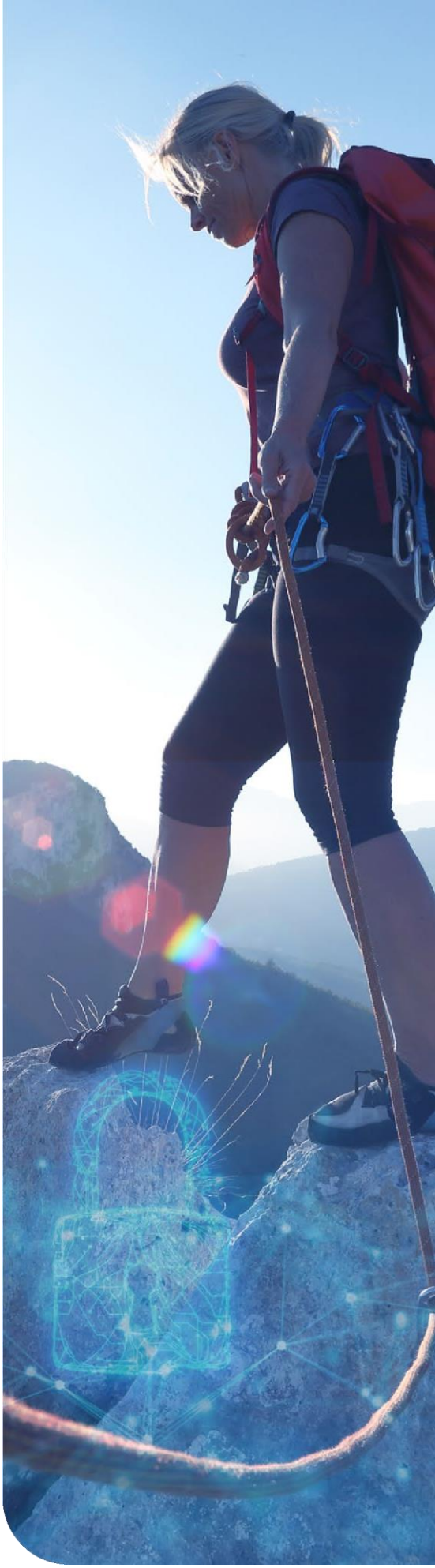
Świadomość ewoluujących oczekiwań klientów i rządowych regulacji

Klienci oczekują, że dostawcy zapewnią ich danym ochronę i bezpieczeństwo – to fundamentalny aspekt zaufania w cyfrowym świecie. Ponadto chcą być informowani o tym, jak ich dane są pozyskiwane, wykorzystywane i zarządzane, pragną też mieć nad swoimi danymi kontrolę. Oczekiwanie widoczności i kontroli dotyczy każdego typu relacji – od indywidualnego użytkownika mediów społecznościowych przez szpital przechowujący dane medyczne po korporację korzystającą z opartych na chmurze usług współpracy. Klienci coraz częściej będą podejmować decyzje o tym, jakiego dostawcę wybrać, kierując się prywatnością i transparentnością.

Oczekiwania klientów

Aby móc zaufać dostawcy, klient pragnie zwykle zapewnień, że:

- nasze treści faktycznie są nasze,
- podlegają tym samym przepisom prawnym co my,
- są dostępne tylko dla osób przez nas autoryzowanych.



Klienci polegają na rządowych regulacjach mających na celu ochronę prywatności i zasadniczo je akceptują. Międzynarodowe ustalenia w zakresie zarządzania danymi[1] to wszystkie globalne przepisy, regulacje i normy dotyczące ochrony danych, ich prywatności, udostępniania i wykorzystywania. Według New Trust Standard dostawcy usług powinni zachować transparentność, jeśli chodzi o swoje podejście do suwerenności danych, czyli koncepcji, według której podlegają one prawom kraju, w którym zostały pozyskane. Przepisy dotyczące prywatności wprowadzono w ponad 130 krajach pragnących ustanowić standardy dbania o dane osobowe pobrane na ich terytorium. Są to m.in. europejskie Ogólne zarządzenie o

ochronie danych (RODO), indyjski Personal Data Protection Bill oraz tajska Personal Data Protection Act.

Choć przepisy te różnią się pod względem konkretnych ustaleń, przyświecają im te same idee i obawy. Jedną z nich jest przekonanie – słuszne bądź nie – że dane są bezpieczniejsze w państwie podmiotu, którego dotyczą, gdzie chronione są przez krajowe przepisy prawne. Kolejną jest obawa, że organy ścigania, zagraniczne czy też krajowe, mogą zmusić dostawcę usług do przekazania danych klientów bez ich wiedzy lub zaangażowania. Firmy korzystające z usług w chmurze muszą być świadome tych zagrożeń i zestawić je z oferowanymi przez chmurę korzyściami – szybką implementacją, skalowalnością i ciągłą innowacją.

Metody ograniczenia ujawniania danych klientów

Kontrola techniczna. Powinniśmy do minimum ograniczyć ilość danych, które pozyskujemy i przechowywać je tylko przez czas określony potrzebą biznesową bądź wymogiem prawnym. W celu ochrony treści klientów używajmy rozbudowanego szyfrowania i kontroli dostępu.

Kontrola prawna. Jeśli rząd domaga się dostępu do danych klientów, najpierw powinniśmy spróbować przekierować osobę zgłaszającą żądanie bezpośrednio do klienta lub właściciela danych. Powołujmy się na dostępne procesy prawne, by kwestionować żądania, które bezprawnie naruszają prywatność lub inne prawa klientów.

Strategiczny wybór lokalizacji centrów danych. Bierzmy pod uwagę, jak umiejscowienie centrów danych w różnych częściach świata wpłynie na klientów. Jeśli właściwie ją wykorzystamy, kontrola zarządzania danymi poprawi ogólne wrażenia z użytkowania, na przykład zapewniając klientom pewien stopień decyzyjności w odniesieniu do ich treści i tego, jak zarządzają danymi. W miarę możliwości powinniśmy rozważyć umożliwienie klientom wyboru regionu, w którym ich dane będą przechowywane, by w ten sposób spełnić ich wymagania w zakresie suwerenności, prywatności lub latencji.

Przyszłość danych: cyfrowa suwerenność

Ta sama technologia, która umożliwia napędzany internetem, wszechstronnie połączony świat, skomplikowała sytuację w zakresie suwerenności danych. Kraje reagują na cyfryzację swoich gospodarek i generowaną przez to ogromną ilość danych, przyjmując koncepcję suwerenności, by zagwarantować sobie najwyższy autorytet, jeśli chodzi o dane, a tym samym – kontrolę nad nimi i ich ochronę. „Moje dane, moje przepisy" to nowa norma. Na całym świecie nowe ustalenia podkreślają narodowe bariery utrudniające przepływ danych, dostęp do nich, ich wykorzystanie i przechowywanie.

Choć zasady te stosowane są w dobrej wierze, grożą ugraniczeniem gospodarczych korzyści oferowanych przez nowoczesne technologie. Dlatego musi pojawić się nowe, przyszłościowe podejście do danych – podejście, które umocni zarówno prawa ich właścicieli, jak i narodową suwerenność, jednak zrobi to w oparciu nie tylko o przepisy prawne, ale również o technologię. Zaawansowane szyfrowanie, obliczanie poufne, zaciemnianie kodu i inne nowo powstające technologie i metody zwiększające prywatność oferują możliwość stworzenia modelu cyfrowej suwerenności w ramach bezpiecznego, otwartego i tętniącego życiem internetu.

[1] „Data Governance Principles for the Global Digital Economy", Center for Strategic & International Studies

Transparentność

Ujawniajmy wszystkie informacje potrzebne klientom, by mogli podejmować świadome, przemyślane decyzje

Transparentność to coś więcej niż tylko przestrzeganie regulacji dotyczących ujawniania informacji. To szczerość i otwartość na temat tego, jak prowadzimy działalność biznesową, jak obchodzimy się z treściami klientów i co robimy z informacjami objętymi zasadami prywatności. W szczególności transparentność dotyczy:

Transparentność ma miejsce wtedy, gdy istotne fakty dotyczące przedsiębiorstwa są udostępniane klientom w sposób szybki i efektywny.

- tego, jakie dane pozyskujemy, a także jak je wykorzystujemy i chronimy,
- tego, jak szanujemy prawa tych, których dane dotyczą,
- kluczowych zapisów naszych polityk dot. ujawniania naruszeń i zagrożeń dla bezpieczeństwa,
- tego, jak reagujemy na rządowe prośby o przekazanie danych, oraz

• naszych planów w zakresie ciągłości biznesowej.

Zasadniczo transparentna firma ma pewność, że postępuje z danymi fair, etycznie i odpowiedzialnie. Podejmuje odpowiednie działania, by chronić dane klientów i szanować ich prywatność. Dodatkowo jest gotowa upubliczniać polityki, procesy i technologie, jakich używa w celu zabezpieczenia danych. Niedawne nagłówki sprawiły, że firmy stały się bardziej świadome ponoszonych strat, zarówno w wymiarze finansowym jak i wizerunkowym, powstałych w wyniku niewystarczających zabezpieczeń.

Sposoby na zwiększenie transparentności

Ułatwianie klientom uzyskiwania pożądanych informacji. Pytajmy klientów o to, co chcieliby wiedzieć, a następnie zapewnijmy im te informacje, nie każąc im ich szukać. Używajmy przy tym prostego, przejrzystego języka.

Upublicznianie wszystkich krytycznych słabych punktów. Zasada ta dotyczy luk wykrytych zarówno wewnętrznie, jak i przez strony trzecie. Pomagajmy klientom zrozumieć ryzyko i nim zarządzać.

Jednoczesne powiadamianie wszystkich istotnie dotkniętych naruszeniem. Prawo do informacji mają w równiej mierze wszyscy dotknięci naruszeniem klienci, niezależnie od tego, jak małą czy dużą są organizacją lub w jakiej działają branży.

Stawanie po stronie klientów, gdy rządy domagają się przekazania danych. Pokażmy, że przestrzegamy prawa i staramy się chronić informacje klientów przed bezprawnymi żądaniami przekazania. Kiedy przepisy na to zezwalają, powiadamiajmy klienta o żądaniu. Gdy to tylko możliwe, żądanie powinno zostać przekazane bezpośrednio klientowi, a nie dostawcy usług IT. Na prośbę klienta pomóżmy mu zapisać lub wydobyć treści, których dotyczy żądanie.

> *„Kiedy pojawiają się zagrożenia, ważne, by klienci wiedzieli, jak na nie zareagujemy. Wymaga to opracowania szczegółowego procesu zarządzania pozyskiwaniem informacji i składaniem na ich temat raportów.”*
>
> **Anthony Grieco**
> VP, Chief Information Security Officer, Cisco

> *„Transparentność zaczyna się tam, gdzie kultura. To oczekiwanie, że pracownicy będą odpowiedzialni za to, jak wchodzą w interakcję z klientami i ogólnie ze światem.”*
>
> **Noelle Warburton**
> Director, Security and Trust Strategic Communications, Cisco

Dowody

Zgodność z przepisami potwierdzona niezależną, zewnętrzną weryfikacją

Pozostałe filary New Trust Standard to kluczowe zobowiązania – do przestrzegania zasad transparentności, do opartego na braku zaufania podejścia do dostępu do sieci, do suwerenności danych oraz do zaufanego łańcucha dostaw. Certyfikaty stanowią dowód, że organizacja faktycznie się z tych zobowiązań wywiązuje. Najczęściej spotykane poświadczenia w zakresie bezpieczeństwa produktów to m.in. międzynarodowy standard ISO/IEC 27001, północnoamerykański System and Organization Controls (SOC 2), obowiązujący w amerykańskim sektorze publicznym FedRAMP, jak również niemiecki Cloud Computing Compliance Controls Catalog (C5).

Dostawcy produktów i usług IT ubiegający się o certyfikacje poddają się audytowi przeprowadzanemu przez akredytowany niezależny podmiot zewnętrzny, często będący firmą zajmującą się księgowością (w Stanach Zjednoczonych akredytację takim audytorom przyznaje np. ANSI-ASQ National Accreditation Board (ANAB)). Poświadczenia z zakresu prywatności stanowią dla klientów, organów regulacyjnych i innych interesariuszy dowód, że sprzedawca przestrzega uznawanych na arenie międzynarodowej zasad prywatności oraz że w odniesieniu do informacji umożliwiających identyfikację szanuje główne prawa tych, których dane te dotyczą. Uznawane certyfikaty to m.in. europejskie Wiążące reguły korporacyjne (BCR), Transgraniczne zasady prywatności APEC (CBPR) i amerykański Privacy Shield (nieuznawany w przypadku przesyłu danych do i z UE, ale nadal obowiązujący w USA). Poświadczenia te są przyznawane i weryfikowane przez organy regulacyjne zajmujące się kwestiami prywatności lub przez zatwierdzonych przez takie organy, niezależnych agentów ds. odpowiedzialności.

Rosnące znaczenie certyfikatów w świecie zdominowanym przez chmury

Kiedy kupujemy sprzęt bądź oprogramowanie, które chcemy użyć w naszym centrum danych, informacje dotyczące firm i klientów nigdy nie opuszczają naszego budynku, a nam wystarczy ufność, że wybrane produkty spełnią swoje zadanie. Jednak kiedy decydujemy się korzystać z usług w chmurze, dane nie znajdują się już na terenie naszej firmy – przechowywane są na serwerach dostawcy i przesyłane w ramach jego sieci.
Teraz musimy więc ufać, że dostawca usług w odpowiedzialny sposób obchodzi się z danymi klientów, szybko usuwa błędy i wdraża aktualizacje, spełnia wymogi dotyczące suwerenności danych, zaradza słabym punktom, stosuje się do SLA w zakresie dostępności, a także szanuje prawa podmiotów danych do prywatności. Nieustanna ewolucja usług w chmurze to także ewolucja kontroli bezpieczeństwa. Coroczna certyfikacja zapewnia stały sposób oceny profilu bezpieczeństwa sprzedawcy i ułatwia klientom podejmowanie świadomych decyzji.

Podsumowanie

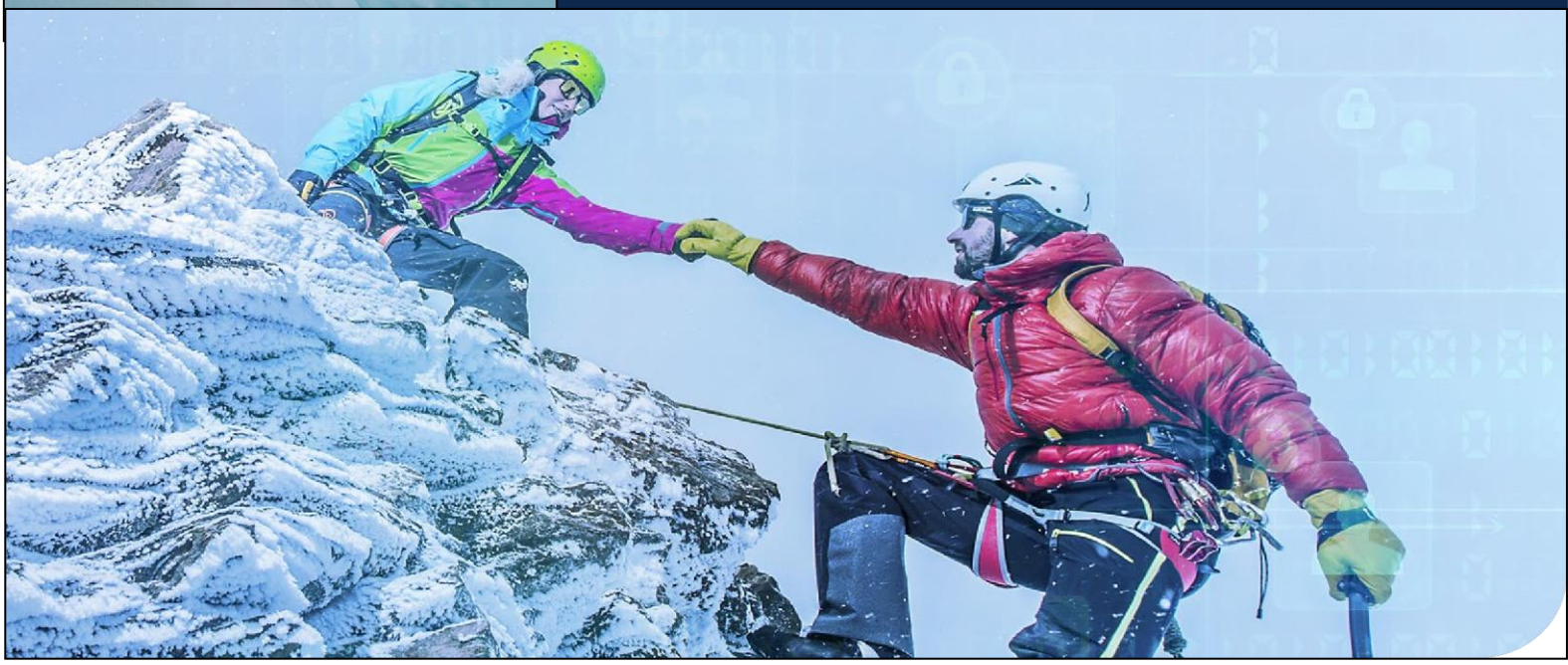
Według New Trust Standard nie jest ono już kwestią intuicji ani aspiracją bez pokrycia wymienioną na korporacyjnej stronie internetowej. Dziś klienci – świadomi ryzyka, z jakim wiąże się sytuacja, w której wrażliwe dane trafiają w niepowołane ręce – stawiają poprzeczkę wyżej. Oczekują namacalnych dowodów, że firmy, z którymi współpracują, działają z pełnym zaangażowaniem i posiadają technologię oraz procesy, które pozwolą im chronić dane. To, jak skutecznie firmy wywiążą się z tego wyzwania, wpłynie nie tylko na ich dochody, ale także na ciągłość krytycznej infrastruktury, na której polega całe społeczeństwo.

W Cisco New Trust Standard zmienił sposób, w jaki prowadzimy działalność. Wsłuchujemy się w oczekiwania naszych klientów, zapewniamy odpowiednie technologie, procesy, polityki i pracowników, by je realizować, i niezmiennie pracujemy na rzecz wytyczenia drogi ku cyfrowej przyszłości opartej na zaufaniu.

„Certyfikaty dotyczące prywatności mają ogromne znaczenie. 90% badanych organizacji potwierdza, że poświadczenia prywatności wydawane przez ISO, APEC i UE stanowią istotne czynniki przy wyborze sprzedawców i podejmowaniu decyzji zakupowych."

Harvey Jang
VP, Chief Privacy Officer, Cisco

Źródło: Przeprowadzone przez Cisco badanie „2021 Data Privacy Benchmark Study"



A oto kilka ze zrealizowanych przez nas działań. Stworzyliśmy architekturę zgodną z zasadą braku zaufania. W umowach z dostawcami zawieramy zapisy zapewniające, że przestrzegają oni tych samych co my standardów dotyczących bezpieczeństwa i prywatności. Publikujemy Zasadnicze podejście do rządowych próśb o przekazanie danych i postępujemy zgodnie z nim. Dla produktów i usług przetwarzających dane osobowe publikujemy Arkusze danych dot. prywatności zawierające maksymalnie szczegółowe odpowiedzi na często zadawane pytania, by umożliwić klientom podjęcie decyzji, jak najlepiej i

najbezpieczniej korzystać z danego produktu. Zdobywamy też certyfikaty w zakresie bezpieczeństwa i prywatności, by klienci nie musieli ufać naszym produktom „na słowo”.

Zainicjowany przez klientów New Trust Standard stanowi pozytywne osiągnięcie dla naszego coraz bardziej cyfrowego świata. Wyraźne określenie, czego klienci oczekują od firm, z którymi współpracują, przekształca zaufanie z uczucia w obiektywny wskaźnik.

Więcej informacji o wadze, jaką Cisco przywiązuje do zaufania, znaleźć można na stronie trust.cisco.com