Intel IT Center

MAJ 2012

Badanie firm z branży

Co powstrzymuje chmurę?

Badanie firmy Intel na temat wzrostu zaufania specjalistów ds. IT do bezpieczeństwa chmury obliczeniowej

Dlaczego warto zapoznać się z treścią tego dokumentu

Niniejszy raport zawiera najważniejsze wnioski z badania przeprowadzonego metodą ślepej próby wśród 800 specjalistów ds. IT z czterech krajów – Chin, Niemiec, Wielkiej Brytanii i Stanów Zjednoczonych. Celem badania było dostarczenie wiedzy na temat obaw związanych z bezpieczeństwem chmury obliczeniowej oraz metod ich łagodzenia. Niniejszy raport zawiera informacje dostarczone przez specjalistów ds. IT, ułatwiające zrozumienie takich zagadnień jak:

- szczególne problemy specjalistów ds. IT związane z bezpieczeństwem chmury oraz różnice pomiędzy chmurą publiczną a chmurą prywatną w tej dziedzinie – obawy takie jak brak kontroli nad danymi, brak wglądu w integralność infrastruktury oraz problemy ze spełnieniem wymogów prawnych w zakresie zgodności;
- możliwości dostępne dla branży – dostawców sprzętu, oprogramowania i usług przetwarzania w chmurze – mające na celu pokonanie barier związanych z adaptacją oraz zwiększenie zaufania do bezpieczeństwa chmury, m.in. poprzez egzekwowanie zasad bezpieczeństwa pomiędzy chmurami oraz wyznaczanie granic danych;
- podobieństwa i różnice w obrębie problemów napotykanych przez specjalistów ds. IT na terenie Chin, Europy i Stanów Zjednoczonych.

Sponsors of Tomorrow.™ intel

Intel IT Center

Badanie firm z branży

Co powstrzymuje chmurę?

Badanie firmy Intel na temat wzrostu zaufania specjalistów ds. IT do bezpieczeństwa chmury obliczeniowej

MAJ 2012

intel

Sponsors of Tomorrow.™

Spis treści

3 Informacje o raporcie

6 Streszczenie

9 Wzrost obaw związanych z bezpieczeństwem w dobie popularności chmury

12 Szczegółowe obawy specjalistów ds. IT związane z bezpieczeństwem

20 Działania branży umożliwiające zwiększenie zaufania działów IT

26 Ogólny obraz: różnice pomiędzy krajami

27 Podsumowanie

28 Załącznik: metodologia badania i profil respondentów

Informacje o raporcie

Dzięki przetwarzaniu w chmurze organizacje i ich działy IT mogą działać sprawniej, efektywniej i mogą w bardziej opłacalny sposób świadczyć nowe usługi, które umożliwią dalszy rozwój ich działalności.

Dostarczenie chmur spełniających pokładane w nich nadzieje nie jest jednak możliwe bez zwiększenia zaufania specjalistów ds. IT do zabezpieczeń i bezpieczeństwa chmury. Jesteśmy świadomi, że obawy działów IT związane z bezpieczeństwem przetwarzania w chmurze stanowią największe bariery hamujące stopień adaptacji tego typu rozwiązań w przedsiębiorstwach. Zanim jednak branża IT zdoła pokonać istniejące obawy, konieczne jest ich należyte zrozumienie. Jakie problemy powinny zostać rozwiązane w pierwszej kolejności, tak aby zwiększyć zaufanie działów IT do rozwiązań chmurowych?

Firma Intel chciała znaleźć odpowiedź na to pytanie. Niniejszy raport zawiera szczegółowe wyniki przeprowadzonego przez nas badania, którego celem było uzyskanie głębszej wiedzy na takie tematy jak:

- szczególne problemy specjalistów ds. IT związane z bezpieczeństwem chmury oraz różnice pomiędzy chmurą publiczną a chmurą prywatną w tej dziedzinie;
- możliwości dostępne dla branży – dostawców sprzętu, oprogramowania i usług przetwarzania w chmurze – mające na celu pokonanie barier związanych z adaptacją oraz zwiększenie zaufania do bezpieczeństwa chmury;
- podobieństwa i różnice w obrębie problemów napotykanych przez specjalistów ds. IT na terenie Chin, Europy i Stanów Zjednoczonych.

Zgromadzone przez nas dane pozwalają uzyskać wiedzę na temat wspólnych działań, jakie mogą podjąć wszyscy przedstawiciele branży, aby zwiększyć bezpieczeństwo przetwarzania w publicznych i prywatnych chmurach obliczeniowych do poziomu (co najmniej) równego bezpieczeństwu dzisiejszych tradycyjnych architektur informatycznych wykorzystywanych przez przedsiębiorstwa. Co ważne, branża IT przykłada dużą wagę m.in. do zagadnienia ochrony tożsamości, danych i infrastruktury wykorzystywanej w procesie świadczenia usług. Wyniki przeprowadzonego przez nas badania pozwalają sformułować ważne wnioski dotyczące tych kwestii.

Chmura prywatna i publiczna: definicje

Na potrzeby niniejszego raportu zdefiniowaliśmy „chmurę publiczną" jako usługi informatyczne, w tym usługi dostępu do oprogramowania, usługi platform służących do tworzenia oprogramowania lub usługi związane z infrastrukturą, świadczone danej organizacji za pośrednictwem Internetu przez dostawcę usług przetwarzania w chmurze. „Chmurzę prywatną" zdefiniowaliśmy jako centrum przetwarzania danych, często zwirtualizowane, umieszczone za zaporą sieciową organizacji i służące do świadczenia usług IT użytkownikom wewnętrznym. Opisane w niniejszym raporcie zagadnienia związane z bezpieczeństwem chmury obejmują zarówno chmury publiczne, jak i prywatne.

Bezpieczeństwo środowiska informatycznego: infrastruktura tradycyjna a infrastruktura chmury obliczeniowej

W tradycyjnych środowiskach informatycznych infrastruktura umieszczona jest za zaporą sieciową danej organizacji, a zwirtualizowane i niezwirtualizowane serwery są przypisane do jej określonych pionów. Specjaliści ds. IT otrzymują do swojej dyspozycji szeroki arsenał sprawdzonych narzędzi zabezpieczających. Te z kolei zapewniają wysoki poziom kontroli nad środowiskiem zabezpieczeń oraz pozwalają na łatwe spełnienie wymogów regulacyjnych, którymi objęta jest organizacja.

W przypadku infrastruktury chmurowej rzecz ma się zgoła inaczej. Serwery są zazwyczaj zwirtualizowane i współdzielone przez wiele pionów jednej organizacji lub nawet przez wiele organizacji – rzadko są przypisane do poszczególnych, ściśle określonych pionów. Gdy dział IT zapragnie zwiększyć efektywność infrastruktury i połączyć ze sobą kilka centrów przetwarzania danych w chmurze – np. centrum umiejscowione w Singapurze i oparte o chmurę publiczną z chmurą prywatną zlokalizowaną na terenie Wielkiej Brytanii – do swojej dyspozycji otrzymuje wciąż ewoluujące narzędzia, które mają zapewnić bezpieczeństwo tak rozległej infrastruktury. W efekcie dział IT traci widoczność oraz kontrolę nad danymi i obciążeniami roboczymi, co z kolei utrudnia specjalistom ds. IT ustalenie, czy organizacja spełnia określone wymogi w zakresie zgodności, a tym samym ogranicza jej zaufanie do zabezpieczeń środowisk przetwarzania w chmurze.

Nasi respondenci

Do udziału w badaniu zaprosiliśmy 800 specjalistów ds. IT z czterech krajów: po 200 osób z Niemiec, Wielkiej Brytanii, Stanów Zjednoczonych oraz Chin. Osoby te reprezentowały (po równo) firmy o różnej wielkości: od 100 do 499 pracowników, od 500 do 999 pracowników oraz te zatrudniające 1000 i więcej pracowników.

Osoby biorące udział w naszym badaniu były ponadto zaangażowane w procesy strategicznego planowania rozwiązań IT dla swoich organizacji oraz głęboko zaangażowane w inicjatywy mające na celu wdrażanie rozwiązań chmurowych. Większość spośród tych organizacji posiadała już rozwinięte do pewnego stopnia rozwiązania do przetwarzania danych w chmurze oraz oferowała, wdrażania, lub oceniała dostępne technologie chmury obliczeniowej. Szczegółowe informacje na temat specjalistów ds. IT biorących udział w badaniu można znaleźć w Załączniku do niniejszego raportu.

Bezpieczeństwo chmury obliczeniowej – zasoby dla specjalistów ds. IT

Niniejszy raport stanowi jeden z elementów nieprzerwanej inicjatywy firmy Intel mającej na celu poszerzanie wiedzy specjalistów ds. IT na temat zabezpieczeń chmury obliczeniowej oraz mającej ułatwić wdrażanie ich w przedsiębiorstwach. Zachęcamy do zapoznania się z dodatkowymi zasobami:

- Intel® IT Center
  Porady i informacje na temat bezpieczeństwa chmury obliczeniowej, dostarczane przez specjalistów ds. IT firmy Intel, ekspertów ds. produktów firmy Intel, zewnętrznych analityków i osoby decyzyjne z branży IT: intel.com/cloudsecurity

Streszczenie

Obawy specjalistów ds. IT związane z bezpieczeństwem chmury obliczeniowej

Aby stworzyć odpowiednie podłoże dla naszych badań, chcieliśmy poznać ogólny charakter obaw związanych z chmurą obliczeniową, jakie wykazują specjaliści ds. IT. Obawy te są znaczące – zwłaszcza gdy wziąć pod uwagę wzrost liczby potencjalnych zagrożeń i przypadków naruszenia zabezpieczeń – a zagrożenia mogą pochodzić zarówno z samej organizacji, jak i z zewnątrz.

Najważniejsze wnioski:

- **Przedsiębiorstwa doświadczają większej liczby przypadków naruszenia zabezpieczeń w porównaniu z tradycyjną architekturą informatyczną.** 28% badanych doświadczyło przypadku naruszenia bezpieczeństwa związanego z korzystaniem z publicznej chmury obliczeniowej.

  Niezależnie od liczby tego typu zdarzeń 65% specjalistów ds. IT, którzy mieli do czynienia z przypadkami naruszenia bezpieczeństwa chmury publicznej, przyznało, że liczba ta była większa w porównaniu z tradycyjną infrastrukturą informatyczną. Więcej szczegółów na stronie 10.

- **Specjaliści ds. IT przyznają, że blisko 1/3 przypadków naruszenia bezpieczeństwa w ich przedsiębiorstwach pochodziła ze źródeł wewnętrznych.** Niezależnie od typu środowiska (tradycyjnego/chmurowego) według specjalistów ds. IT 1/3 spośród wszystkich przypadków naruszenia zabezpieczeń pochodziła z samej organizacji. Mimo iż wiele z podobnych zagrożeń było najprawdopodobniej wynikiem niezamierzonego działania (pracownicy padali bowiem ofiarami wirusów i innych złośliwych programów, sami nie planując uzyskania dostępu do zasobów firmy), zagrożenia pochodzenia wewnętrznego stanowią znaczące źródło obaw specjalistów ds. IT. Więcej szczegółów na stronie 11.

Szczegółowe obawy specjalistów ds. IT związane z bezpieczeństwem chmury obliczeniowej

Aby zgłębić obawy specjalistów ds. IT, zapytaliśmy ich o problemy związane z chmurami prywatnymi i publicznymi oraz zachowaniem zgodności z wymogami prawnymi. Zbadaliśmy również obawy związane z lukami w zabezpieczeniach hiperwizorów.

Najważniejsze wnioski:

- **Największą obawą specjalistów ds. IT związaną z prywatną chmurą obliczeniową jest brak kontroli.** Trzy największe obawy specjalistów ds. IT związane z chmurą prywatną dotyczą kontroli – a raczej braku kontroli, jakiego doświadczają w środowiskach chmury prywatnej. Największą obawę specjalistów stanowi brak kontroli pozwalającej na skuteczne zapewnianie dostępu do danych i usług wyłącznie upoważnionym użytkownikom.

  Drugą największą obawą jest brak wglądu w wydzielane zasoby. W przypadku wydzielania zasobów (ich wirtualizacji bądź współdzielenia pomiędzy różnymi pionami przedsiębiorstwa lub klientami korzystającymi z tych samych serwerów) specjaliści ds. IT stają przed trudnym wyzwaniem osiągnięcia takiego samego poziomu kontroli jak w przypadku tradycyjnych środowisk informatycznych. Trzecia największa obawa wiąże się z koniecznością zapewnienia należytej ochrony za pomocą zapory sieciowej. Więcej szczegółów na stronie 12.

- **W przypadku chmury publicznej specjaliści ds. IT obawiają się o brak możliwości pomiaru skuteczności zabezpieczeń oraz brak kontroli.** Specjaliści odczuwają brak dostępnych metod pomiaru skuteczności usług zabezpieczających oferowanych przez dostawców chmury publicznej – ten element znalazł się na pierwszym miejscu listy obaw związanych z publiczną chmurą obliczeniową. Z tym problemem wiąże się również kolejny – ogólny brak kontroli nad danymi przechowywanymi w centrach przetwarzania danych opartych o publiczną chmurę obliczeniową. Więcej szczegółów na stronie 14.

- **Obawy wynikające ze zgodności z przepisami skutecznie powstrzymują specjalistów od przenoszenia określonych typów obciążenia roboczego do chmury.** Od przedsiębiorstw na całym świecie wymaga się przestrzegania wymogów rządowych regulujących procesy przepływu i przechowywania określonych typów informacji – zazwyczaj informacji medycznych, finansowych i innego typu informacji poufnych – na terenie danego kraju lub poza jego granicami.

  78% spośród naszych respondentów przyznało, że musi przestrzegać takich przepisów. Dla 57% z nich obawy związane między innymi z bezpieczeństwem stanowią barierę uniemożliwiającą przeniesienie określonych typów danych oraz obciążenia roboczego do chmury. Szczegółowe obawy związane ze zgodnością w środowisku chmury obliczeniowej, na jakie zwrócili uwagę specjaliści ds. IT, obejmują wymogi w dziedzinie audytu i raportowania, odpowiedzialność prawną (w tym brak pewności, czy odpowiedzialność ta leży po stronie organizacji czy dostawcy usług) oraz ogólne obawy związane z brakiem możliwości spełnienia szczegółowych wymogów przez daną organizację.

  Spośród 43% ankietowanych organizacji, które przenosiły objęte regulacjami dane i obciążenia robocze do chmury, znacząca większość nie wykorzystuje w tym procesie żadnych zautomatyzowanych metod śledzenia stanu zgodności z wymogami regulacyjnymi. Taki stan rzeczy może skutkować poważnymi trudnościami oraz może sprawić, że organizacje te zostaną pociągnięte do odpowiedzialności z tytułu braku zgodności z obowiązującymi regulacjami. Więcej szczegółów na stronach 17–18.

- **Zarówno w przypadku chmur publicznych, jak i prywatnych często wyrażaną obawę stanowią luki w zabezpieczeniach hiperwizorów.** Hiperwizory – krytyczne elementy zwirtualizowanej infrastruktury chmurowej – stanowią warstwę programową zlokalizowaną pomiędzy sprzętem a maszynami wirtualnymi, umożliwiającą współdzielenie pojedynczej platformy sprzętowej przez wiele maszyn. 87% specjalistów ds. IT wyraziło swoje obawy związane z lukami w zabezpieczeniach hiperwizorów, które mogą pozwolić hakerom na uzyskanie dostępu do danych lub wprowadzenie złośliwego oprogramowania do środowiska informatycznego. Więcej szczegółów na stronie 16.

Możliwości dostępne dla branży

Nasze badanie pozwala określić konkretne kroki, jakie mogą podjąć dostawcy sprzętu, oprogramowania i usług przetwarzania w chmurze oraz inni przedstawiciele ekosystemu technologicznego, aby złagodzić obawy związane z bezpieczeństwem chmury. Podjęcie tych kroków pozwoli zwiększyć zaufanie specjalistów ds. IT do procesu przenoszenia danych i usług biznesowych do środowiska chmury – zarówno prywatnej, jak i publicznej.

Najważniejsze wnioski:

- **W przypadku chmury publicznej specjaliści ds. IT zidentyfikowali cztery elementy zdolne zwiększyć ich zaufanie.** Dostawcy usług przetwarzania w chmurach publicznych, podobnie jak inni przedstawiciele ekosystemu technologicznego, powinni zwiększyć zaufanie specjalistów do chmury poprzez udostępnienie możliwości:
  - ustanawiania i egzekwowania zasad bezpieczeństwa pomiędzy chmurami, dzięki którym działy IT byłyby w stanie zapewnić spójność zasad pomiędzy środowiskami chmury prywatnej i publicznej oraz otrzymałyby możliwość zarządzania nimi;
  - wyznaczania granic danych, dzięki którym działy IT otrzymałyby większą kontrolę nad procesem przydzielania określonych typów obciążenia roboczego do miejsc ich wykonywania;
  - zapewnienia, że infrastruktury publiczne cechuje należyta integralność oraz są one wolne od potencjalnego złośliwego oprogramowania;
  - porównywania jakości usług zabezpieczeń oferowanych przez poszczególnych dostawców chmur publicznych.

Więcej szczegółów na stronie 21.

- **Co również jest niezwykle ważne w przypadku chmury publicznej, 98% specjalistów ds. IT pragnie otrzymać do swojej dyspozycji metody pomiaru stanu zabezpieczeń oferowanych przez dostawców usług przetwarzania w chmurze.** Znakomita większość specjalistów ds. IT wyraża swoje zainteresowanie usługą, która pozwoliłaby im obserwować w czasie rzeczywistym środki kontroli wdrażane przed dostawców usług oraz status bezpieczeństwa udostępnianych przez nich środowisk. 76% specjalistów wyraża „bardzo wysokie zainteresowanie" tego typu usługą, a 96% potwierdza, że posiadanie takiej możliwości zwiększyłoby ich zaufanie do chmury publicznej. Więcej szczegółów na stronie 22.

- **W przypadku chmury prywatnej specjaliści ds. IT zidentyfikowali trzy elementy zdolne zwiększyć ich zaufanie.** Dostawcy sprzętu i oprogramowania umożliwiającego świadczenie usług przetwarzania w chmurze prywatnej mogą zwiększyć zaufanie specjalistów, udostępniając możliwość:
  - wyznaczania granic danych, dzięki którym (jak wspomnieliśmy wcześniej) działy IT otrzymałyby większą kontrolę nad procesem przydzielania określonych typów obciążenia roboczego do miejsc ich wykonywania;
  - poświadczania integralności infrastruktury chmury prywatnej, co z kolei pozwoliłoby im określić, czy oferowana infrastruktura jest na przykład wolna od złośliwego oprogramowania;
  - zapewnienia, że pakiety sieciowe nie są naruszane, tj. ruch sieciowy nie został zmieniony, zakłócony ani naruszony przez złośliwe oprogramowanie lub oprogramowanie innego typu.

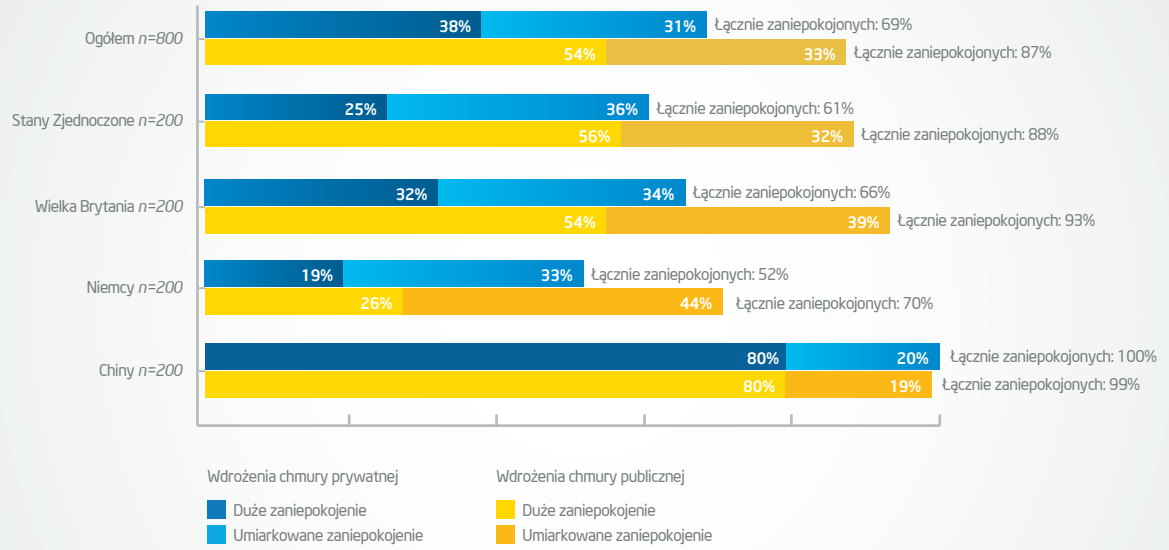
  Więcej szczegółów na stronie 23.
- **Specjaliści ds. IT chcą móc mierzyć stopień przestrzegania przepisów.** 98% z nich wyraziło swoje zainteresowanie wprowadzeniem usługi, która zwiększyłaby ich zdolność kontrolowania stanu zgodności z wymogami regulacyjnymi, przy czym 65% wyraziło „bardzo wysokie zainteresowanie" tego typu usługą. Więcej szczegółów na stronie 24.
- **Konieczne jest udostępnienie specjalistom ds. IT możliwości uzyskiwania dostępu do danych przechowywanych na urządzeniach klienckich lub ich dezaktywowania w przypadku utraty bądź kradzieży takich urządzeń.** Wraz z adaptacją języka programowania HTML5 dane przechowywane lokalnie na urządzeniach użytkowników pozwolą im na kontynuowanie pracy również po odłączeniu urządzeń od usługi przetwarzania w chmurze. W przypadku utraty lub kradzieży urządzeń fakt ten stwarza jednak bardzo poważne problemy związane z bezpieczeństwem. Możliwość uzyskania dostępu do danych przechowywanych na takich urządzeniach (lub ich dezaktywowania) jest ważna niemal dla wszystkich specjalistów (99%), przy czym 73% uważa ją za „bardzo ważną". Więcej szczegółów na stronie 25.

Wzrost obaw związanych z bezpieczeństwem w dobie popularności chmury

Wprowadzenie chmur obliczeniowych spowodowało powstanie licznych zagrożeń, z jakimi muszą dziś mierzyć się specjaliści ds. IT. Niektóre z tych problemów są zupełnie nowe, podczas gdy inne znane były już administratorom tradycyjnych infrastruktur, jednak teraz przeniosły się do środowiska chmury, w którym wiele pionów lub organizacji może współdzielić te same zwirtualizowane serwery.

W pierwszej kolejności chcieliśmy zrozumieć ogólne obawy specjalistów ds. IT związane z chmurą obliczeniową oraz różnice pomiędzy chmurą publiczną a chmurą prywatną w tej dziedzinie. Mimo iż obawy te są znaczące dla obu typów rozwiązań, co do zasady są one większe w przypadku chmury publicznej.

Obawy związane z bezpieczeństwem wdrożeń publicznych i prywatnych chmur obliczeniowych



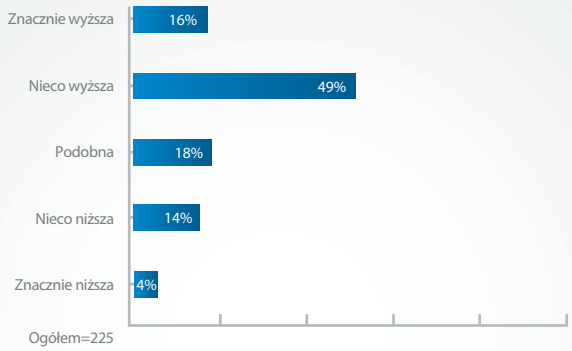
P: *Proszę wskazać państwa ogólny poziom obaw związanych z ochroną danych i bezpieczeństwem w przypadku chmury publicznej.*

P: *Proszę wskazać państwa ogólny poziom obaw związanych z ochroną danych i bezpieczeństwem w przypadku chmury prywatnej.*

Większa liczba napotkanych przypadków naruszenia bezpieczeństwa w chmurach publicznych

Nasze badanie wykazało, że obawy związane z bezpieczeństwem chmury obliczeniowej są uzasadnione. 28% ankietowanych specjalistów ds. IT doświadczyło przypadków naruszenia bezpieczeństwa związanych z chmurą publiczną. Niezależnie od liczby tego typu zdarzeń zdaniem 65% z nich liczba ta była większa w porównaniu z tradycyjną infrastrukturą informatyczną.

Liczba przypadków naruszenia bezpieczeństwa: chmura publiczna a tradycyjna infrastruktura informatyczna



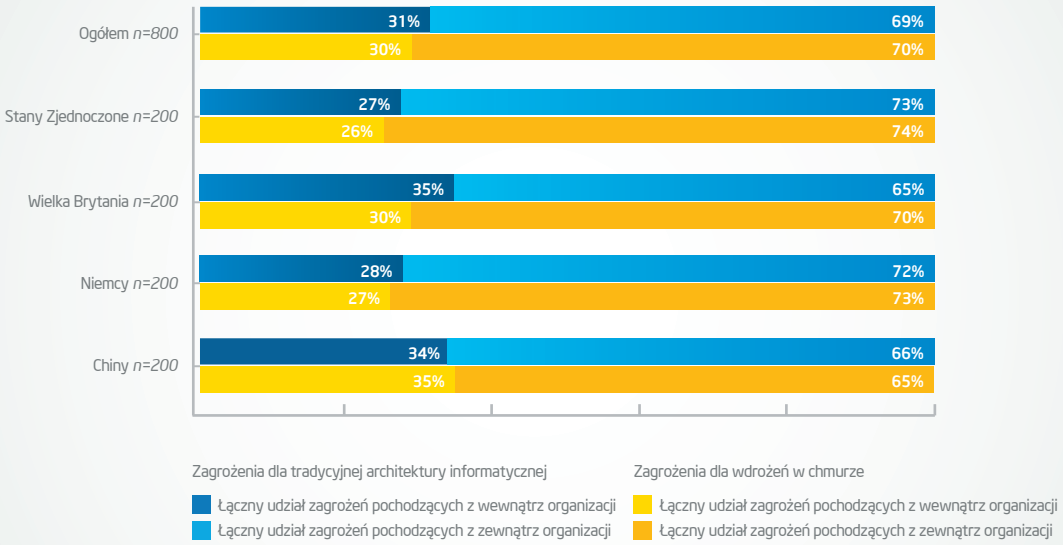
P: *Jak, w porównaniu z posiadanym przez państwa tradycyjnym środowiskiem informatycznym przedsiębiorstwa, oceniają państwo liczbę przypadków naruszenia bezpieczeństwa w chmurze publicznej? (Ankietowani = użytkownicy chmur publicznych i hybrydowych, którzy doświadczyli przypadków naruszenia bezpieczeństwa w chmurze publicznej).*

Skąd pochodzą zagrożenia – z wewnątrz czy z zewnątrz organizacji?

Aby lepiej zrozumieć charakter stwierdzonych przypadków naruszenia bezpieczeństwa, spytaliśmy specjalistów ds. IT, jaki procent zagrożeń dla bezpieczeństwa ich środowiska IT pochodził z wewnątrz, a jaki z zewnątrz organizacji. Spytaliśmy również, czy stosunek ten był różny dla tradycyjnej architektury informatycznej i chmury obliczeniowej (publicznej lub prywatnej). Otrzymaliśmy dwa najważniejsze wnioski:

- Zdaniem specjalistów blisko 1/3 zagrożeń pochodziła z wewnątrz ich przedsiębiorstw.
- Wartość ta była praktycznie taka sama dla architektury tradycyjnej i chmury obliczeniowej.

Z wewnątrz czy z zewnątrz?
Zagrożenia dla tradycyjnej architektury informatycznej i chmury obliczeniowej



P: *Jaki procent wszystkich zagrożeń dla bezpieczeństwa tradycyjnego środowiska informatycznego przedsiębiorstwa pochodził państwa zdaniem z wewnątrz, a jaki z zewnątrz organizacji?*

P: *Jaki procent wszystkich zagrożeń dla bezpieczeństwa chmury obliczeniowej przedsiębiorstwa pochodził państwa zdaniem z wewnątrz, a jaki z zewnątrz organizacji?*

Zrozumienie powagi obaw wyrażanych przez specjalistów oraz charakteru zagrożeń, jakim muszą stawiać czoła, umożliwiło nam przygotowanie pytań odnoszących się do konkretnych problemów z bezpieczeństwem, napotykanych w środowiskach chmury publicznej i prywatnej.

Szczegółowe obawy specjalistów ds. IT związane z bezpieczeństwem

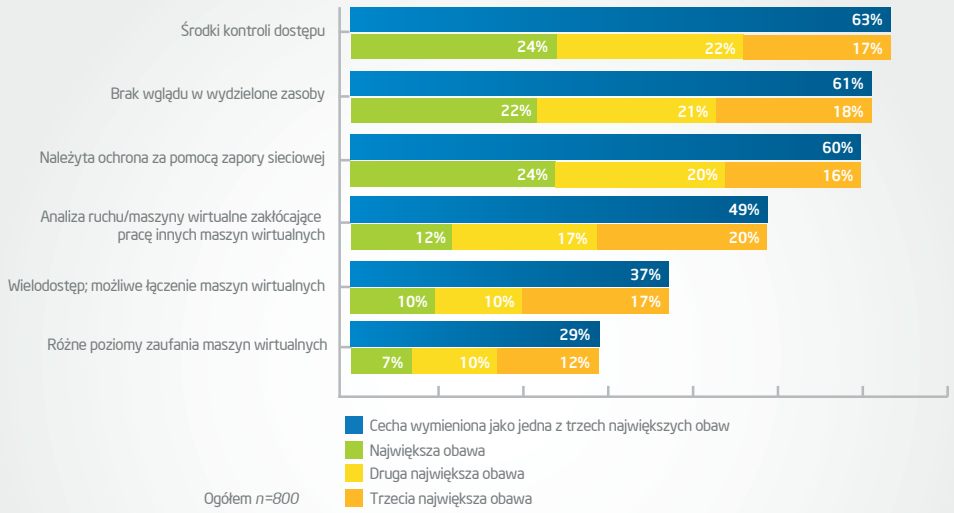
Celem naszych badań było szczegółowe zidentyfikowanie obaw specjalistów ds. IT dotyczących bezpieczeństwa środowisk chmury publicznej i prywatnej. Mimo iż w branży IT otwarcie mówi się o poważnych obawach związanych z bezpieczeństwem chmury publicznej i prywatnej, specjalistów biorących udział w badaniu w większym stopniu niepokoiło bezpieczeństwo chmury publicznej.

Chmura prywatna: liczy się poziom kontroli

Poprosiliśmy specjalistów ds. IT o wskazanie trzech największych obaw związanych z bezpieczeństwem prywatnej chmury obliczeniowej. Najczęściej wymienianym elementem była możliwość kontrolowania środowiska chmury prywatnej – a raczej brak takiej możliwości. Pierwsze miejsce na liście zajęła dostępność środków kontroli, pozwalających zapewnić, że dane i usługi firmowe będą dostępne wyłącznie dla upoważnionych użytkowników.

Drugim największym problemem był brak widoczności wydzielonych zasobów (a co za tym idzie brak kontroli nad nimi). Trzecią największą obawę stanowiła należyta ochrona za pomocą zapory sieciowej.

Największe obawy związane z bezpieczeństwem: chmura prywatna



P: *Które trzy spośród wymienionych obaw związanych z bezpieczeństwem chmury prywatnej uważają państwo za największe?*

Wskazane obawy były stosunkowo podobne we wszystkich czterech krajach objętych badaniem: Stanach Zjednoczonych, Wielkiej Brytanii, Niemczech i Chinach.

Największe obawy związane z bezpieczeństwem w poszczególnych krajach: chmura prywatna

Przetwarzanie w chmurze prywatnej Obawy związane z bezpieczeństwem	Stany Zjednoczone (n=200)		Wielka Brytania (n=200)		Niemcy (n=200)		Chiny (n=200)	
	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy
Należyta ochrona za pomocą zapory sieciowej	**26%**	**60%**	24%	**60%**	22%	**56%**	**24%**	**64%**
Środki kontroli dostępu	25%	**66%**	**28%**	**64%**	20%	**62%**	23%	58%
Wydzielone zasoby/brak widoczności	24%	**66%**	18%	**56%**	**24%**	**59%**	22%	**62%**
Analiza ruchu w przypadku zakłócania pracy maszyn wirtualnych przez inne maszyny	10%	42%	10%	47%	14%	48%	16%	**62%**
Wielodostęp; możliwe łączenie maszyn wirtualnych	10%	37%	12%	40%	12%	45%	8%	30%
Różne poziomy zaufania maszyn wirtualnych	4%	29%	9%	34%	8%	30%	6%	22%

P: *Które trzy spośród wymienionych obaw związanych z bezpieczeństwem chmury prywatnej uważają państwo za największe?*

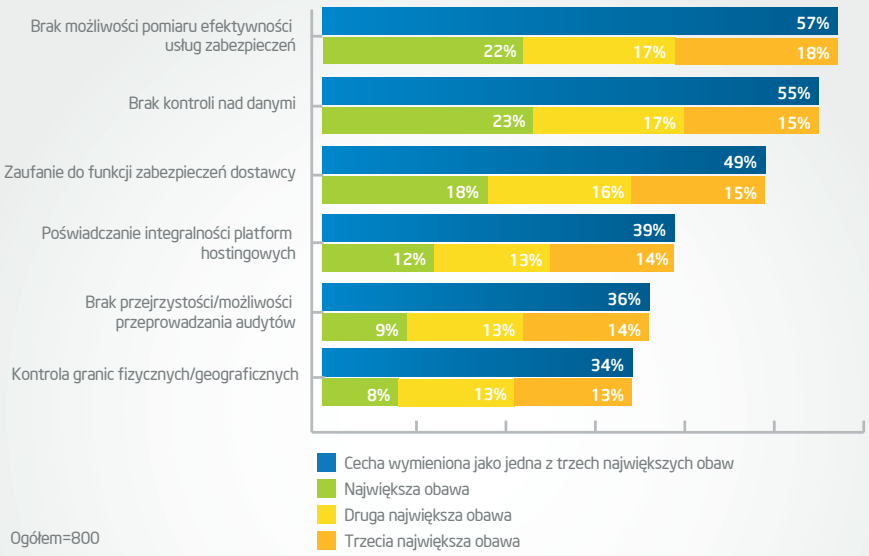
Chmura publiczna: większy nacisk na możliwość pomiaru jakości usług zabezpieczeń

Obawy związane z bezpieczeństwem informatycznym są większe w przypadku chmury publicznej. Tutaj bowiem zadanie kontrolowania zabezpieczeń powierzane jest w większym stopniu dostawcom zewnętrznym, udostępniającym zazwyczaj infrastrukturę centrum przetwarzania danych wielu swoim klientom.

Podobnie jak w przypadku chmury prywatnej w środowisku chmury publicznej specjaliści ds. IT dostrzegają problem braku kontroli. W jeszcze większym stopniu obawiają się natomiast braku środków, które pozwoliłyby na dokonywanie pomiaru jakości usług zabezpieczeń oferowanych przez dostawców chmury publicznej. To z kolei obniża zaufanie specjalistów do ogólnej zdolności dostawców do zapewnienia należytych zabezpieczeń.

Obawy są podobne we wszystkich krajach objętych badaniem – z wyjątkiem Niemiec, gdzie największą obawę stanowi brak środków kontroli granic fizycznych i geograficznych.

Największe obawy związane z bezpieczeństwem: chmura publiczna



Ogółem=800

P: *Które trzy spośród wymienionych obaw związanych z bezpieczeństwem chmury publicznej uważają państwo za największe?*

Największe obawy związane z bezpieczeństwem w poszczególnych krajach: chmura publiczna

Przetwarzanie w chmurze publicznej Obawy związane z bezpieczeństwem	Stany Zjednoczone (n=200)		Wielka Brytania (n=200)		Niemcy (n=200)		Chiny (n=200)	
	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy	Największa obawa	3 największe obawy
Brak kontroli nad danymi	22%	**52%**	24%	**56%**	**24%**	**60%**	20%	**51%**
Brak środków pomiaru jakości usług zabezpieczających	**28%**	**67%**	**24%**	**58%**	10%	38%	**23%**	**61%**
Zaufanie do funkcji zabezpieczeń dostawcy	22%	**55%**	14%	**50%**	18%	**50%**	16%	42%
Poświadczanie integralności platform hostingowych	10%	42%	12%	41%	9%	28%	19%	**45%**
Brak przejrzystości/możliwości przeprowadzania audytów	7%	33%	8%	36%	12%	36%	10%	41%
Kontrola granic fizycznych/ geograficznych	6%	25%	8%	30%	14%	**48%**	6%	34%
Brak ładu prawnego i ochrony cywilnoprawnej	6%	26%	8%	30%	13%	40%	6%	26%

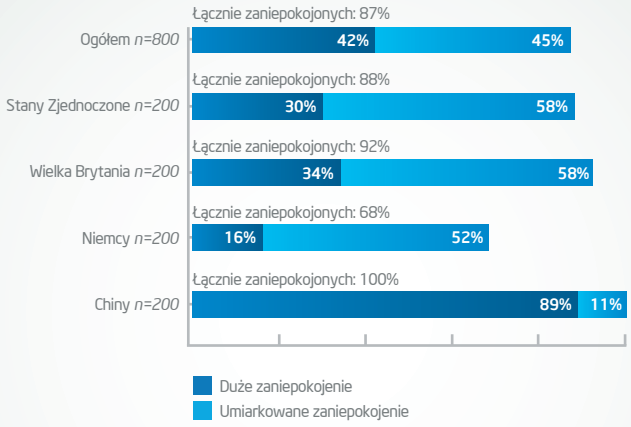
P: *Które trzy spośród wymienionych obaw związanych z bezpieczeństwem chmury publicznej uważają państwo za największe?*

Bezpieczeństwo hiperwizorów – częste obawy wśród specjalistów z całego świata

Hiperwizory – krytyczne elementy zwirtualizowanej infrastruktury chmurowej – stanowią warstwę programową zlokalizowaną pomiędzy sprzętem a maszynami wirtualnymi, umożliwiającą współdzielenie pojedynczej platformy sprzętowej przez wiele maszyn. Nie jest więc zaskoczeniem, że luki w zabezpieczeniach hiperwizorów stanowią ważne źródło obaw specjalistów ds. IT. Jeśli hiperwizor będzie podatny na ataki, wówczas integralność całego środowiska chmury publicznej lub prywatnej zostanie postawiona pod znakiem zapytania. Mimo iż specjaliści ds. IT w coraz większym stopniu wykorzystują techniki wirtualizacji i korzystają z hiperwizorów dla zwiększenia efektywności posiadanej infrastruktury IT, nasze badanie pokazuje, że wciąż mają oni obawy związane z potencjalnymi lukami w zabezpieczeniach wykorzystywanych lub ocenianych hiperwizorów.

Tego typu obawy wyrazili niemal wszyscy respondenci, jednak ich poziom różnił się w zależności od kraju. Specjalistów amerykańskich i brytyjskich cechował podobny poziom zaniepokojenia. W przypadku Niemiec był on jednak znacznie niższy, a w Chinach zdecydowanie najwyższy.

Poziom zaniepokojenia związanego z lukami w zabezpieczeniach hiperwizorów



P: *W jak dużym stopniu są państwo zaniepokojeni lukami w zabezpieczeniach hiperwizorów pracujących w środowiskach chmury prywatnej i/lub publicznej?*

Chmura publiczna i prywatna: zgodność z wymogami regulacyjnymi

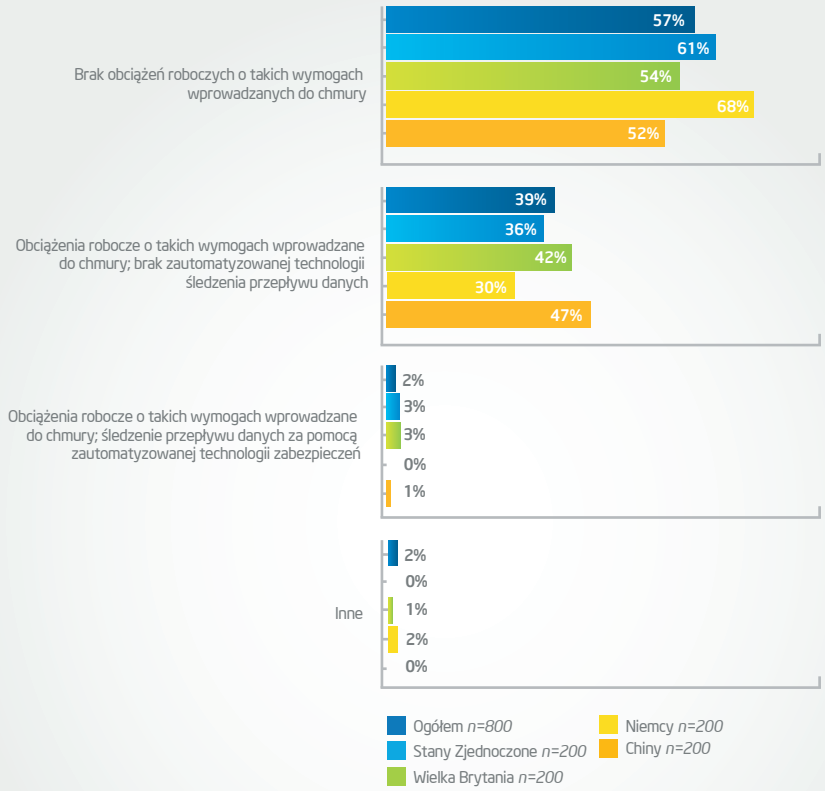
Biorąc pod uwagę, jak dużym problemem dla firm jest zgodność z obowiązującymi wymogami – zwłaszcza w silnie regulowanych sektorach, takich jak sektor bankowy, finansowy i opieki zdrowotnej – zadaliśmy specjalistom ds. IT szereg różnych pytań na temat wpływu zgodności z wymogami na planowane wdrożenia rozwiązań chmurowych. Z ich odpowiedzi jasno wynikało, że problem ten w znaczącym stopniu wpływa na proces przenoszenia określonych typów danych i obciążenia roboczego do chmury.

78% specjalistów przyznało, że w swojej pracy musi liczyć się z wymogami regulującymi procesy przepływu i przechowywania określonych typów informacji (zazwyczaj informacji poufnych – np. danych medycznych lub finansowych) poza granicami państw. Większość (57%) spośród specjalistów wskazujących na istnienie takich ograniczeń powstrzymuje się od przenoszenia objętych regulacjami danych i obciążeń roboczych do chmury prywatnej bądź publicznej. 40% specjalistów, którzy decydują się na przenoszenie danych i obciążeń objętych regulacjami, stosuje metody ręcznego śledzenia zgodności z przepisami – nie dysponują oni żadnymi zautomatyzowanymi metodami śledzenia procesów przepływu i przechowywania danych poza granicami państw. Taki stan rzeczy może skutkować poważnymi trudnościami oraz może sprawić, że organizacje te zostaną pociągnięte do odpowiedzialności z tytułu braku zgodności z obowiązującymi regulacjami. Tylko 2% specjalistów objętych regulacjami przyznaje, że dysponuje zautomatyzowanymi technologiami zabezpieczeń, która pozwalają im śledzić proces utrzymywania zgodności.

Zgodność z wymogami regulacyjnymi

P: *Istnieje ogromna liczba wymogów regulujących procesy przepływu i przechowywania danych poza granicami państw. Czy od państwa firmy wymaga się przestrzegania takich wymogów?*

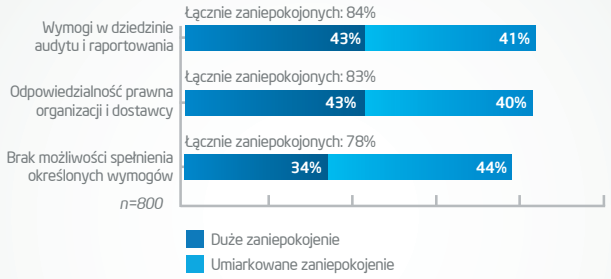
Przenoszenie objętych regulacjami danych i obciążeń roboczych do chmury



P: *W jaki sposób zapewniają państwo zgodność regulowanego obciążenia roboczego z przepisami w dzisiejszym środowisku chmury publicznej lub prywatnej? (Ankietowani = specjaliści ds. IT, którzy muszą przestrzegać wymogów regulujących procesy przepływu i przechowywania danych poza granicami państw).*

Aby lepiej zrozumieć specyfikę problemów związanych z wymogami regulacyjnymi, zadaliśmy specjalistom dodatkowe pytania na temat ich największych obaw związanych z chmurą publiczną. Nasi respondenci wskazali na szeroko rozpowszechnione obawy związane z wymogami w dziedzinie audytu i raportowania, rozumieniem wymogów prawnych stawianych wobec organizacji i dostawców usług przetwarzania w chmurze oraz brakiem możliwości spełnienia niektórych wymogów w środowisku chmurowym. Poziom zaniepokojenia był w tym przypadku najwyższy w Chinach, średni w Stanach Zjednoczonych i Wielkiej Brytanii oraz najniższy w Niemczech.

Obawy związane z zachowaniem zgodności w przypadku chmury publicznej



P: *Proszę ocenić stopień państwa zaniepokojenia związanego z zachowaniem zgodności w przypadku korzystania z chmury publicznej.*

Obawy związane z zachowaniem zgodności w przypadku chmury publicznej: największe obawy w poszczególnych krajach

Procent respondentów wykazujących „duże zaniepokojenie”	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
Wymogi w dziedzinie audytów i raportowania	42%	38%	22%	69%
Odpowiedzialność prawna organizacji i dostawcy	39%	39%	25%	68%
Brak możliwości spełnienia określonych wymogów	34%	28%	16%	58%

P: *Proszę ocenić stopień państwa zaniepokojenia związanego z zachowaniem zgodności w przypadku korzystania z chmury publicznej.*

Działania branży umożliwiające zwiększenie zaufania działów IT

Mimo iż głównym celem naszego badania było zidentyfikowanie szczegółowych obaw specjalistów ds. IT związanych z bezpieczeństwem chmury publicznej i prywatnej, chcieliśmy ponadto sprawdzić dostępne działania, jakie mogą podjąć przedstawiciele branży, aby rozwiązać istniejące problemy i zdobyć zaufanie specjalistów do chmur publicznych i prywatnych.

Chmura publiczna: środki kontroli, gwarancje i techniki pomiaru

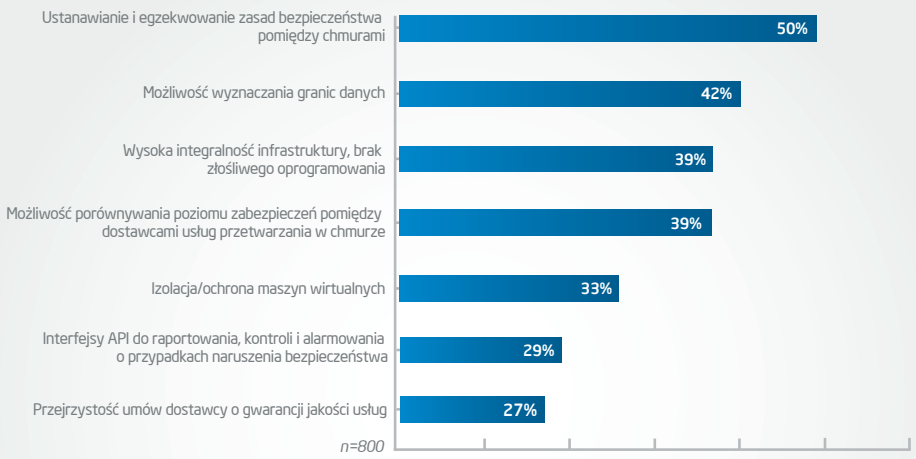
Poprosiliśmy specjalistów ds. IT o dokonanie oceny znaczenia siedmiu działań, jakie mogą podjąć przedstawiciele branży, aby zwiększyć ich zaufanie do chmury obliczeniowej. Według nich najważniejszym działaniem byłoby rozwiązanie problemu ustanawiania i egzekwowania zasad bezpieczeństwa pomiędzy chmurami. Dzięki temu działy IT byłyby w stanie zapewnić spójność zasad pomiędzy środowiskami chmury prywatnej i publicznej oraz otrzymałyby możliwość zarządzania nimi.

Specjaliści ds. IT chcą także, aby przedstawiciele branży:

- zapewnili możliwość wyznaczania granic danych, która pozwoliłaby na kontrolowanie miejsc uruchamiania poszczególnych typów obciążenia roboczego;
- udostępnili środki ułatwiające sprawdzanie, czy infrastrukturę dostawcy cechuje wysoka integralność oraz brak złośliwego oprogramowania;
- zapewnili możliwość porównywania poziomu zabezpieczeń pomiędzy wieloma dostawcami usług przetwarzania w chmurze.

To pytanie pozwoliło nam jednak odkryć pewne interesujące różnice pomiędzy poszczególnymi krajami. Specjaliści z Chin wykazali znacznie większe (w porównaniu z pozostałymi krajami) zainteresowanie rozwiązaniem problemu izolacji i ochrony maszyn wirtualnych – co nie jest zaskoczeniem, gdy weźmiemy pod uwagę poziom ich zaniepokojenia lukami w zabezpieczeniach hiperwizorów (omówionego na stronie 16 niniejszego raportu). Dla specjalistów ze Stanów Zjednoczonych znacznie ważniejsze (niż w przypadku innych krajów) było jednak uzyskanie możliwości porównywania poziomu zabezpieczeń pomiędzy wieloma dostawcami usług przetwarzania w chmurze.

Czynniki budujące zaufanie do chmury publicznej



P: *Rozwiązanie których z powyższych problemów najbardziej zwiększyłoby państwa zaufanie do chmury publicznej? Prosimy o wybranie maksymalnie trzech odpowiedzi.*

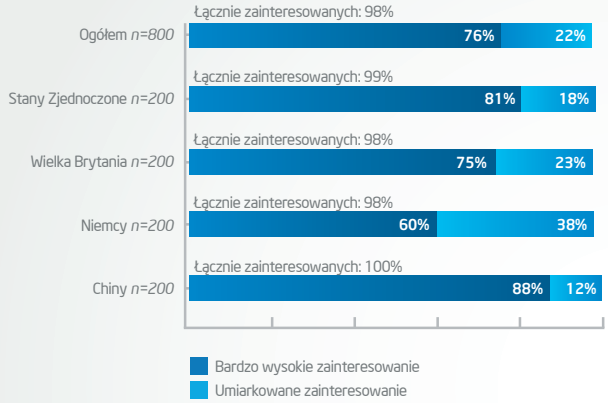
Czynniki budujące zaufanie do chmury publicznej w poszczególnych krajach

	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
Ustanawianie i egzekwowanie zasad bezpieczeństwa pomiędzy chmurami	42%	**50%**	**53%**	**56%**
Możliwość wyznaczania granic danych	42%	36%	**47%**	42%
Wysoka integralność infrastruktury, brak złośliwego oprogramowania	**43%**	36%	33%	43%
Możliwość porównywania poziomu zabezpieczeń pomiędzy dostawcami usług przetwarzania w chmurze	**50%**	**38%**	36%	32%
Izolacja/ochrona maszyn wirtualnych	26%	26%	32%	**49%**
Interfejsy API do raportowania, kontroli i alarmowania o przypadkach naruszenia bezpieczeństwa	26%	28%	28%	36%
Przejrzystość umów dostawcy o gwarancji jakości usług	24%	30%	24%	31%

P: *Rozwiązanie których z powyższych problemów najbardziej zwiększyłoby państwa zaufanie do chmury publicznej? Prosimy o wybranie maksymalnie trzech odpowiedzi.*

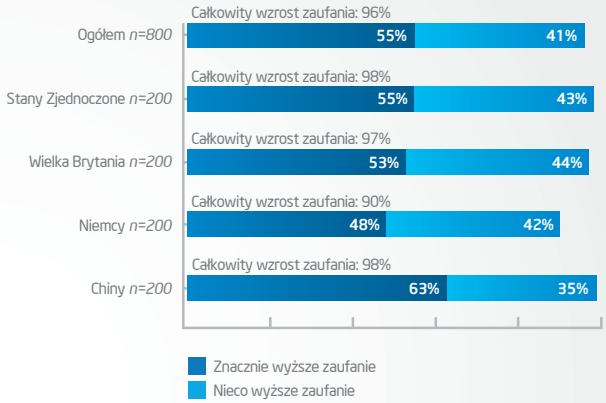
Spytaliśmy ponadto specjalistów ds. IT, czy możliwość pomiaru jakości usług zabezpieczeń oferowanych przed dostawców zwiększyłaby poziom ich zaufania. Jak wskazaliśmy wcześniej, brak tego typu możliwości stanowił największą obawę specjalistów ds. IT związaną z korzystaniem z publicznej chmury obliczeniowej. Nie jest zatem niespodzianką, że 98% specjalistów wyraziło swoje zainteresowanie usługą pozwalającą na pomiar w czasie rzeczywistym stanu zabezpieczeń dostawców, a 96% specjalistów przyznało, że udostępnienie stosownego narzędzia zwiększyłoby ich zaufanie do chmury publicznej i jej bezpieczeństwa.

Zainteresowanie usługą pomiaru jakości zabezpieczeń dostawców usług



P: *Jak duże byłoby państwa zainteresowanie usługą pozwalającą na pomiar (w czasie rzeczywistym) stanu zabezpieczeń infrastruktury oferowanej przez dostawców?*

Wpływ dostępności usługi pomiaru zabezpieczeń na zaufanie specjalistów do chmury obliczeniowej



P: *Jak bardzo wprowadzenie usługi pomiaru zabezpieczeń w czasie rzeczywistym wpłynęłoby na państwa zaufanie do publicznej chmury obliczeniowej?*

Chmura prywatna: trzy czynniki budujące zaufanie

Jak wspomnieliśmy wcześniej w niniejszym raporcie, wszystkie największe obawy specjalistów ds. IT związane z chmurą prywatną dotyczyły poczucia braku kontroli. Spytaliśmy specjalistów, co najbardziej zwiększyłoby ich zaufanie do chmury prywatnej – najczęściej wymieniane działania dotyczyły zwiększenia kontroli.

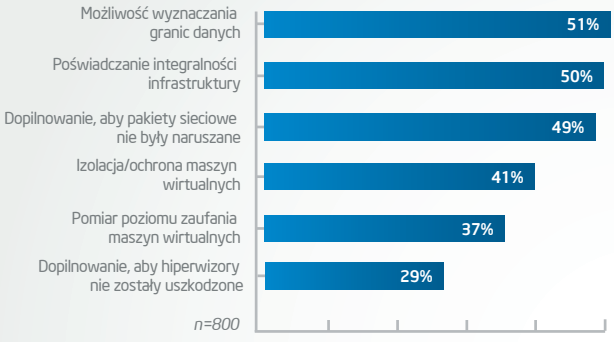
Zdaniem większości respondentów możliwość wyznaczania granic danych podniosłaby ich zaufanie do chmury prywatnej w największym stopniu. Wyznaczanie granic danych pozwoliłoby specjalistom uzyskać większą kontrolę nad procesem przydzielania określonych typów obciążenia roboczego do miejsc ich wykonywania, co z kolei ułatwiłoby im spełnienie obowiązujących wymogów regulacyjnych.

Nieznacznie mniejszym zainteresowaniem cieszyły się przy tym zagadnienia związane z zaufaniem:

- specjaliści ds. IT pragną otrzymać możliwość weryfikowania integralności posiadanej infrastruktury chmury prywatnej, tak aby zapewnić, że obciążenia robocze są uruchamiane na godnej zaufania infrastrukturze, oraz aby możliwe było dostarczenie dowodu niezbędnego do spełnienia wymogów w zakresie zgodności;
- specjaliści chcieliby również móc zagwarantować nienaruszalność pakietów sieciowych.

To pytanie pozwala również odkryć pewne ciekawe różnice pomiędzy poszczególnymi krajami objętymi badaniem. W tym przypadku znów na pierwszy plan wysuwają się obawy Chin związane z lukami w zabezpieczeniach hiperwizorów, podczas gdy zaufanie specjalistów z pozostałych krajów w największym stopniu zwiększyłoby rozwiązanie problemów na tle izolacji i ochrony maszyn wirtualnych. Zdecydowanie najważniejszym zagadnieniem dla specjalistów niemieckich jest możliwość zapewnienia integralności pakietów sieciowych.

Czynniki budujące zaufanie do chmury prywatnej



P: *Rozwiązanie których z powyższych problemów najbardziej zwiększyłoby państwa zaufanie do chmury prywatnej? Prosimy o wybranie maksymalnie trzech odpowiedzi.*

Czynniki budujące zaufanie do chmury prywatnej w poszczególnych krajach

	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
Możliwość wyznaczania granic danych	**56%**	**52%**	46%	52%
Poświadczanie integralności infrastruktury	54%	50%	42%	52%
Dopilnowanie, aby pakiety sieciowe nie były naruszane	40%	48%	**58%**	52%
Izolacja/ochrona maszyn wirtualnych	40%	31%	36%	**57%**
Pomiar poziomu zaufania maszyn wirtualnych	42%	43%	30%	34%
Dopilnowanie, aby hiperwizory nie zostały uszkodzone	28%	25%	26%	38%

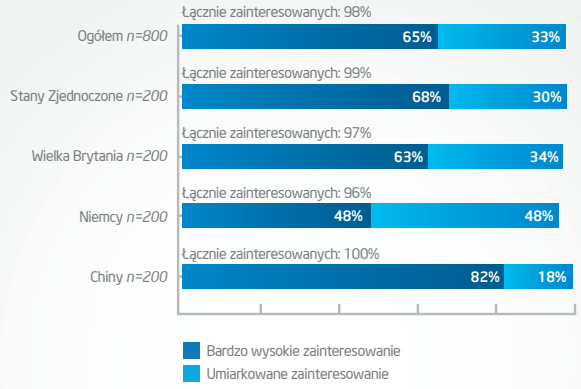
P: *Rozwiązanie których z powyższych problemów najbardziej zwiększyłoby państwa zaufanie do chmury prywatnej? Prosimy o wybranie maksymalnie trzech odpowiedzi.*

Pomiar zgodności z wymogami regulacyjnymi

Jak wskazaliśmy wcześniej w treści niniejszego raportu, 57% specjalistów ds. IT, którzy zgłaszali konieczność spełniania wymogów regulacyjnych, decyduje się nie przenosić określonych typów danych i obciążenia roboczego do chmury publicznej lub prywatnej. Ci, którzy zdecydują się przenieść poufne dane do chmury, w znakomitej większości przypadków robią to bez pomocy zautomatyzowanych technologii śledzenia procesów przepływu lub przechowywania takich danych.

Fakt ten prawdopodobnie wyjaśnia 98-procentowe zainteresowanie specjalistów ds. IT usługą, która pozwoliłaby im sporządzać za pomocą jednego systemu raporty na potrzeby wielu standardów zgodności. Zainteresowanie tego typu usługą jest wysokie we wszystkich krajach objętych badaniem, przy czym największe wykazują specjaliści z Chin – 96% z nich podkreśla konieczność spełniania wymogów regulacyjnych dotyczących przepływu i przechowywania danych.

Zainteresowanie usługą raportowania na potrzeby zachowania zgodności z wymogami regulacyjnymi



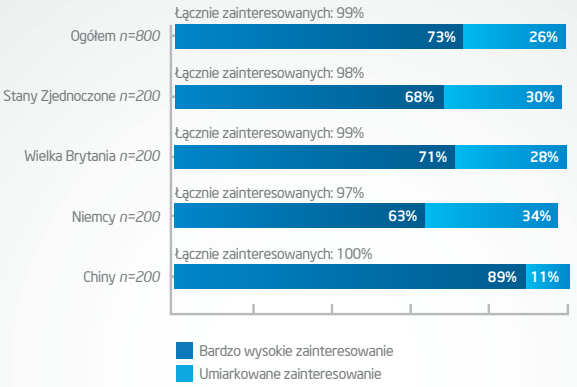
P: *Jak duże byłoby państwa zainteresowanie usługą umożliwiającą sporządzanie za pomocą jednego systemu raportów związanych z wieloma standardami zgodności?*

Niemal jednogłośna potrzeba dezaktywacji zagubionych lub skradzionych urządzeń

Wraz z adaptacją języka programowania HTML5 dane przechowywane lokalnie na urządzeniach użytkowników pozwolą im na kontynuowanie pracy również po odłączeniu urządzeń od usługi przetwarzania w chmurze. Mimo iż zabieg ten wiąże się z potencjalnym wzrostem produktywności przedsiębiorstw, sam fakt lokalnego przechowywania środowiska pracy budzi poważne obawy specjalistów ds. IT związane z możliwością utraty lub kradzieży urządzeń.

W związku z powyższym bardzo ważna dla specjalistów jest możliwość zdalnego reagowania w przypadku takiej utraty lub kradzieży. Nasi respondenci niemal jednogłośnie wyrazili zainteresowanie możliwością dezaktywowania danych przechowywanych na utraconych urządzeniach, zanim te trafią w ręce hakerów. Oznacza to, że działy IT przedsiębiorstw otrzymałyby na przykład możliwość zdalnego zablokowania dostępu do urządzenia pozostawionego w taksówce (lub dezaktywowania przechowywanych na nim danych), zanim trafi ono w niepowołane ręce.

Chęć kontroli środowisk przechowywanych lokalnie oraz możliwość dezaktywowania utraconych/skradzionych urządzeń



P: *Jak ważna byłaby dla państwa organizacji możliwość dezaktywowania urządzeń lub blokowania dostępu do danych w przypadku utraty bądź kradzieży urządzeń w związku z rozpowszechnieniem lokalnie przechowywanych środowisk HTML5?*

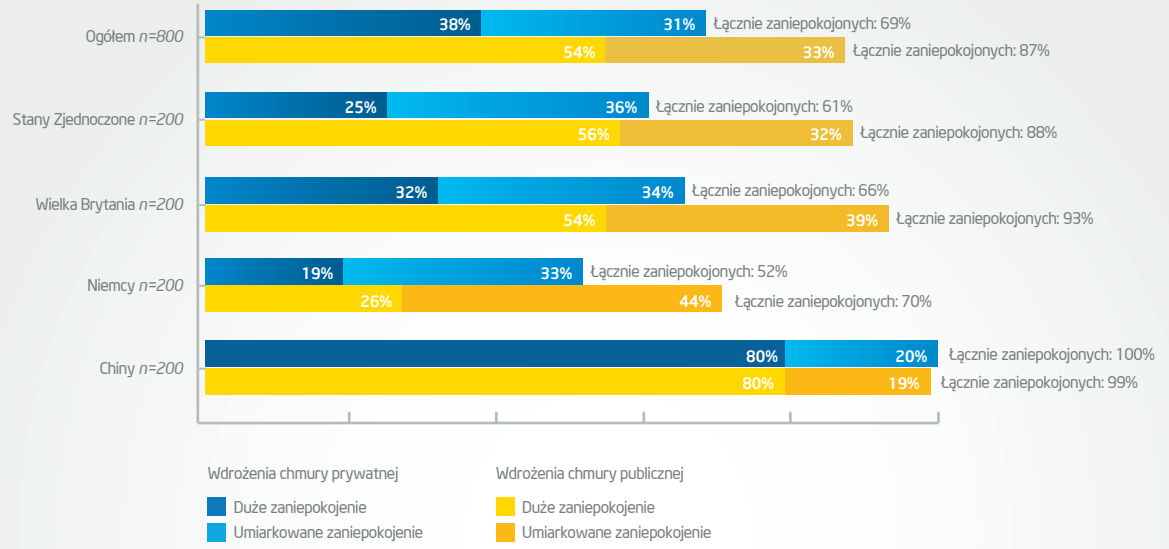
Ogólny obraz: różnice pomiędzy krajami

Jednym z celów naszego badania było zidentyfikowanie różnic pomiędzy obawami specjalistów ds. IT w czterech krajach objętych badaniem: Stanach Zjednoczonych, Wielkiej Brytanii, Niemczech oraz Chinach.

Według uzyskanych przez nas informacji same obawy nie różniły się zbytnio pomiędzy krajami. Różnił się natomiast stopień zaniepokojenia poszczególnymi problemami. Co do zasady specjaliści ze wszystkich czterech krajów wskazali te same obszary zagrożeń oraz te same działania, jakie można podjąć, aby zwiększyć ich zaufanie do chmury. Ogólny poziom zaniepokojenia związanego z bezpieczeństwem chmury jest jednak większy w przypadku specjalistów chińskich niż w przypadku specjalistów amerykańskich i brytyjskich. Z drugiej strony, ogólny poziom zaniepokojenia w przypadku specjalistów niemieckich jest niższy od wyżej wymienionych.

Poniżej zamieściliśmy rozkład odpowiedzi specjalistów na temat ogólnego poziomu ich zaniepokojenia związanego z przetwarzaniem w chmurze publicznej i prywatnej.

Poziom zaniepokojenia bezpieczeństwem chmury obliczeniowej w poszczególnych krajach



P: *Proszę wskazać państwa ogólny poziom zaniepokojenia związanego z ochroną danych i bezpieczeństwem w przypadku chmury prywatnej i publicznej.*

Najważniejsze przyczyny odnotowanych różnic mogą wynikać z rozbieżności w obrębie kultury biznesowej, środowiska zabezpieczeń oraz ram regulacyjnych poszczególnych krajów. Pełne zrozumienie tych różnic prawdopodobnie wymagałoby przeprowadzenia odrębnego badania.

Podsumowanie

Celem badania było uzyskanie głębszej wiedzy na temat szczegółowych przyczyn, dla których specjaliści ds. IT darzą prywatną i publiczną chmurę obliczeniową mniejszym zaufaniem niż posiadane przez swoje organizacje tradycyjne infrastruktury informatyczne. Za pomocą tego badania chcieliśmy ponadto zidentyfikować wspólne działania, jakie mogą podjąć przedstawiciele branży IT, aby złagodzić istniejące obawy i zwiększyć zaufanie specjalistów do chmury obliczeniowej.

Żaden z przedstawicieli ekosystemu – dostawca sprzętu, oprogramowania czy też usług przetwarzana w chmurze – nie może samodzielnie rozwiązać problemów związanych z bezpieczeństwem chmury. Wyniki badania pokazują, że specjaliści ds. IT mają duże obawy związane z możliwościami kontroli i pomiaru – pragną otrzymać większą kontrolę dostępu i kontrolę nad danymi oraz lepsze metody pomiaru integralności, zgodności i jakości usług oferowanych przez dostawców zewnętrznych. Rozwiązanie tych problemów będzie wymagało wspólnego wysiłku całej branży IT.

Naszym zdaniem badanie to wskazuje na konieczność nawiązania szeroko zakrojonej współpracy całej branży, która umożliwi opracowanie ujednoliconych ram i standardów. Aby w pełni wykorzystać potencjał chmury obliczeniowej, musimy podjąć wspólne, kompleksowe działania na rzecz rozwiązania zidentyfikowanych problemów. Koszt braku takiej współpracy będzie wysoki: przedsiębiorstwa nie będą w stanie powierzyć swoich najważniejszych danych i obciążeń roboczych środowiskom chmurowym, a model przetwarzania w chmurze straci swój potencjał.

Opracowanie branżowych standardów zabezpieczeń oraz wspólnych ram umożliwiających specjalistom ds. IT kontrolowanie środowisk chmury i dokonywanie pomiaru ich parametrów pozwoli sprawić, że model przetwarzania w chmurze stanie się wiodącym trendem, a nie wyjątkiem. Firma Intel uważa, że wspólne działania branży na rzecz poprawy zabezpieczeń i opracowania standardów zapewnią chmurom obliczeniowym taki sam (lub nawet wyższy) poziom bezpieczeństwa jak w przypadku dzisiejszych tradycyjnych architektur informatycznych.

Załącznik: metodologia badania i profil respondentów

Badanie przeprowadzono metodą ślepej próby, a odpowiedzi zgromadzono za pośrednictwem kwestionariusza internetowego. 800 respondentów (po 200 ze Stanów Zjednoczonych, Wielkiej Brytanii, Niemiec i Chin) udzieliło odpowiedzi w okresie od 26 stycznia do 14 lutego 2012 r. Liczebność próby wynosząca 800 osób pozwoliła osiągnąć maksymalną wariację w próbie na poziomie ±3,3% przy 95-procentowym poziomie ufności. Liczebność próby wynosząca 200 osób pozwoliła osiągnąć maksymalną wariację w próbie na poziomie ±6,9% przy 95-procentowym poziomie ufności.

Respondenci musieli spełniać następujące kryteria:

- pracownicy przedsiębiorstw zatrudniających co najmniej 100 osób;
- osoby decyzyjne odpowiedzialne za infrastrukturę informatyczną;
- osoby zaangażowane w procesy podejmowania decyzji oraz strategicznego planowania wdrożeń środowisk przetwarzania w chmurze w swoich przedsiębiorstwach;
- osoby, które wdrożyły, wdrażają lub planują wdrożenie środowisk przetwarzania w chmurze.

Fakt korzystania lub niekorzystania z produktów firmy Intel nie był brany pod uwagę. W celu zapewnienia reprezentatywności próby wprowadzono ograniczenia dotyczące wielkości przedsiębiorstw oraz branż, w których prowadzą one działalność gospodarczą.

Obowiązki służbowe respondentów	Razem (n=800)	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
Wybór dostawców kluczowych składników technologii przetwarzania w chmurze	94%	94%	91%	94%	98%
Udział w procesie planowania strategicznych rozwiązań technologicznych	93%	97%	94%	89%	94%
Współpraca z członkami kadry kierowniczej najwyższego szczebla mająca na celu określenie kierunku rozwoju strategii informatycznej przedsiębiorstwa	93%	97%	94%	88%	94%
Planowanie, wdrażanie i utrzymywanie technologii przetwarzania w chmurze	92%	95%	94%	87%	94%
Kierowanie zespołem specjalistów ds. IT wspierającym inicjatywy biznesowe	87%	87%	86%	81%	93%
Praktyczne wdrażanie rozwiązań	76%	76%	79%	83%	68%

Wielkość firmy	Razem (n=800)	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
100–499 pracowników	35%	27%	27%	42%	46%
500–999 pracowników	31%	33%	20%	38%	35%
min. 1000 pracowników	33%	40%	53%	21%	20%
Mediana	*735*	*849*	*1057*	*612*	*565*

Lokalizacje na świecie	Razem (n=800)	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
1 lokalizacja	13%	12%	8%	23%	12%
2–4 lokalizacje	29%	27%	19%	33%	37%
5–9 lokalizacji	28%	24%	35%	21%	33%
10–14 lokalizacji	14%	18%	17%	11%	11%
15–19 lokalizacji	14%	18%	19%	12%	8%
Brak pewności	1%	1%	3%	2%	--

Branża	Razem (n=800)	Stany Zjednoczone (n=200)	Wielka Brytania (n=200)	Niemcy (n=200)	Chiny (n=200)
Produkcja	17,5%	15,0%	15,0%	15,0%	25,0%
Usługi finansowe	14,1%	15,0%	8,0%	17,0%	16,5%
Usługi specjalistyczne	11,8%	16,5%	15,0%	10,0%	5,5%
Działalność usługowa (lub inna) związana z komputerami	8,5%	10,0%	10,0%	8,5%	5,5%
Sprzedaż detaliczna	7,5%	8,5%	8,0%	5,0%	8,5%
Opieka zdrowotna	7,1%	9,0%	4,0%	10,0%	5,5%
Budownictwo	6,1%	2,5%	9,5%	5,0%	7,5%
Transport i logistyka	5,9%	5,5%	6,0%	7,0%	5,0%
Oświata	4,9%	5,0%	6,0%	5,0%	3,5%
Telekomunikacja	4,3%	1,5%	2,5%	5,5%	7,5%
Sprzedaż hurtowa i dystrybucja	3,4%	4,5%	2,0%	4,5%	2,5%
Przedsiębiorstwa użyteczności publicznej	2,4%	3,0%	2,5%	1,5%	2,5%
Administracja państwowa	2,1%	1,5%	5,0%	1,0%	1,0%
Rozrywka i multimedia	1,3%	0,5%	3,0%	1,0%	0,5%
Rolnictwo, leśnictwo i rybołówstwo	1,0%	0,5%	1,5%	0,5%	1,5%
Usługi hostingowe	0,4%	--	--	1,0%	0,5%
Organizacje non-profit	0,3%	0,5%	0,5%	--	--

Więcej od Intel® IT Center

Badanie przeprowadzone wśród innych firm z branży: co powstrzymuje chmurę? Badanie firmy Intel na temat zwiększania zaufania specjalistów ds. IT do bezpieczeństwa chmury obliczeniowej zostało przeprowadzone przez Intel® IT Center – program przeznaczony dla specjalistów ds. IT, prowadzony przez firmę Intel. Zadaniem Intel IT Center jest dostarczanie przystępnych, pełnych i obiektywnych informacji mających na celu ułatwienie specjalistom ds. IT terminowej realizacji strategicznych projektów związanych m.in. z wirtualizacją, projektowaniem centrów przetwarzania danych oraz wdrażaniem inteligentnych klientów i rozwiązań zabezpieczających dla chmury obliczeniowej. Odwiedź Intel IT Center, aby uzyskać:

- Przewodniki po planowaniu, badania przeprowadzone wśród innych firm z branży oraz dyskusje dostawców ułatwiające wdrażanie projektów kluczowych dla działalności firmy
- Praktyczne studia przypadku prezentujące sposób rozwiązywania problemów przez inne firmy z branży
- Informacje na temat sposobu wdrażania rozwiązań chmurowych, wirtualizacji, zabezpieczeń i innych strategicznych inicjatyw przez dział IT firmy Intel
- Informacje o wydarzeniach umożliwiających poznanie opinii ekspertów ds. produktów Intel oraz specjalistów firmy Intel ds. IT

Więcej informacji można znaleźć na stronie intel.com/ITCenter.

Podziel się z innymi

Niniejszy raport ma wyłącznie charakter informacyjny. NINIEJSZY DOKUMENT JEST DOSTARCZANY W STANIE TAKIM, W JAKIM JEST, BEZ JAKICHKOLWIEK GWARANCJI, W TYM JAKICHKOLWIEK GWARANCJI PRZYDATNOŚCI HANDLOWEJ, NIENARUSZANIA PRAW ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU, A TAKŻE BEZ JAKICHKOLWIEK GWARANCJI WYNIKAJĄCYCH W INNY SPOSÓB Z JAKIEJKOLWIEK PROPOZYCJI, SPECYFIKACJI LUB PRÓBKI. Firma Intel wyłącza wszelką odpowiedzialność, w tym odpowiedzialność z tytułu naruszenia jakichkolwiek praw własności, związaną z procesem wykorzystywania informacji zawartych w niniejszym dokumencie. Na podstawie niniejszego dokumentu nie są udzielane w sposób jawny ani dorozumiany, przez wykluczenie odmowy ani w jakikolwiek inny sposób, żadne licencje dotyczące jakichkolwiek praw własności intelektualnej.

Copyright © 2012 Intel Corporation. Wszelkie prawa zastrzeżone. Intel, logo Intel, Intel Kształtujemy przyszłość i logo Intel Kształtujemy przyszłość są znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i w innych krajach.

0512/JM/ME/PDF-USA 327311-001PL

Sponsors of Tomorrow.™