enteo CLOUDPOINT

Cloudpoint

Dopytaj swojego dostawcę chmury o...

Cloudpoint

Sprawdź parametry naszego rozwiązania do przechowywania najważniejszych danych Twojej firmy.

Swojego dostawcę chmury dopytaj o:

1. Normy bezpieczeństwa datacenter
2. Technologię informatyczną jaką wykorzystano do budowy chmury
3. Doświadczenie inżynierów w budowie infrastruktury informatycznej centrów danych
4. Mechanizmy bezpieczeństwa zaimplementowane do ochrony infrastruktury chmurowej
5. Podział odpowiedzialności – za które elementy systemu bezpieczeństwa odpowiada dostawca?
6. Zgodność z normą ISO 27001 i dyrektywami w zakresie bezpieczeństwa (NIS2, PCI-DSS)
7. Szybkość i jakość wsparcia

1

Dopytaj swojego dostawcę chmury o...

Normy bezpieczeństwa datacenter, czyli centrum danych, w którym mają być przechowywane cenne dla Twojej firmy dane.

Sprawdź dokładnie, jakiego dostawcę wybrałeś, **jakie datacenter** wykorzystuje i jakie **normy bezpieczeństwa** spełnia.

Dowiedz się, w jakim układzie redundancji jest zbudowana infrastruktura. **Redundancja**, czyli nadmiarowość danych, ma niebagatelne znaczenie, gdy zachodzi awaria i trzeba szybko odzyskać Twoje dane.

Sprawdź także, czy wybrane przez Ciebie datacenter przeszło zewnętrzne **certyfikacje** w zakresie dostępności i posiada potwierdzenie certyfikatami (SaaS, IaaS, PaaS). Takie certyfikacje poprzedzone są bardzo poważnymi testami, symulującymi uszkodzenia przypadkowych elementów infrastruktury i badaniem efektu tych uszkodzeń dla funkcjonowania systemu.

Bezpieczny system mimo zaistniałych problemów powinien działać bez przeszkód.

1

Dopytaj swojego dostawcę chmury o...

Co się stanie jak tego nie będzie?

Ponosisz **ryzyko**. Nie ma pewności, że Twoje dane będą zawsze bezpieczne i dostępne od ręki. W przypadku awarii możesz czekać jakiś **czas** by odzyskać dostęp do danych. Może to generować duże **straty**.

Oto przykłady, gdy coś poszło nie tak:

Awaria klimatyzacji u dostawcy telekomunikacyjnego
https://niebezpiecznik.pl/post/pozar-t-mobile/

Pożar w serwerowni OVH
https://sekurak.pl/ogromny-pozar-w-serwerowni-ovh-jedne-polskie-firmy-podniosly-sie-po-2-godzinach-inne-w-ogole/

Wybuch gazu w serwerowni dostawcy telekomunikacyjnego:
https://niebezpiecznik.pl/post/wybuch-gazu-w-serwerowni-netii/

1

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

Centrum danych, w którym znajduje się nasza infrastruktura są **certyfikowane** przez Uptime Institue zgodnie z normą Tier-III w zakresie dostępności: https://www.gov.pl/web/popcwsparcie/klasyfikacja-tier--centrum-danych-datacenter

Oznacza to, że każdy z elementów wpływających na dostępność i bezpieczeństwo danych jest podwojony, należycie przygotowany i tak zarządzany, aby zagwarantować najwyższy poziom bezpieczeństwa danych.

2

Dopytaj swojego dostawcę chmury o...

Technologię informatyczną jaką wykorzystano do budowy chmury, czyli co działa (lub nie działa), gdy obsługiwane są w chmurze Twoje dane.

Czyż nie interesujemy się zawartością produktów żywnościowych, które spożywamy? Czy budując lub remontując dom nie sprawdzamy dokładnie nie tylko ekipy budowlano-remontowe, ale także sposobów ich działania i technologii, jaka zostanie zastosowana? Czy sposób przechowywania i obsługi danych naszej firmy w chmurze zasługuje na mniejsze zainteresowanie?

Sprawdź zatem **technologię dostawcy usług chmurowych**, zadając poniższe, istotne pytania:

- Czy jest to technologia **komercyjna czy darmowa**?
- Czy dostawca posiada **aktywne wsparcie producenta** technologii w zakresie jej działania?
- Jakie duże organizacje wykorzystują ich technologie budowy chmury? (SaaS, IaaS, PaaS)
- Czy ewentualna **zmiana dostawcy** chmury gdy zajdzie taka potrzeba jest faktycznie bezproblemowa? Może się zdarzyć, że użycie jakiegoś rozwiązania chmurowego to swoista **pułapka technologiczna**, z której nie ma łatwego i taniego wyjścia w momencie gdy zmienią się założenia Twojego biznesu.

2

Dopytaj swojego dostawcę chmury o...

Co się stanie jak tego nie będzie?

Zwiększasz ryzyko przechowywania swoich danych. Wyobraźmy sobie, że coś przestaje działać w usłudze chmury obliczeniowej, w której trzymane są nasze dane. Przy komercyjnej technologii producent tej technologii pomaga w szybszym rozwiązaniu problemu, przy technologii darmowej nie mamy najczęściej żadnej gwarancji, że taka pomoc zostanie udzielona.

Dla przykładu dla technologii HyperV czy KVM nie ma dostępnego w prosty sposób wsparcia technologicznego, umożliwiającego szybką pomoc w przypadku problemu. Konsekwencją może być przestój w pracy jakiejś usługi chmurowej.

Oto przykład, gdy coś poszło nie tak:

Firma X udostępniająca usługę chmury obliczeniowej opartej o słabo wspieraną technologię musi korzystać z unikalnych trudno dostępnych specjalistów, znających tę technologię.

W momencie, gdy specjalista zaprzestanie współpracy z firmą i wystąpi problem sposobem poszukiwania kompetencji w zakresie używanej technologii jest szukanie informacji w Internecie. ➔

2

Dopytaj swojego dostawcę chmury o...

➔ Efektem dla klienta będzie może być niedostępność części usług w przypadku awarii przez dłuższy czas.

Również bariery wyjścia z chmury opartej o niestandardową technologię są znacznie większe. Brak jest prostej kompatybilności pomiędzy dostawcami chmury czy infrastruktury on-premise.

Jednym z rynkowych przykładów tego typu problemów, który dla dostawcy usług hostingowych zakończył się tragicznie przedstawiony jest pod linkiem:
https://www.purepc.pl/awaria-2be-pl-adweb-to-dramat-i-komedia-hostingowa-w-jednym

2

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

Korzystamy z **platformy chmury obliczeniowej Vmware**. Technologie Vmware są wykorzystywane przed ponad 80% dużych centrów danych na świecie oraz ponad 90% firm Fortune 500.

Infrastruktura zbudowana w oparciu o Vmware jest identyczna u każdego dostawcy wykorzystującego tą technologie na świecie dzięki czemu można prosto i szybko rozszerzać infrastrukturę np. na dwie chmury lub przenosić dane pomiędzy dostawcami.

Vmware zapewnia **wsparcie techniczne** na najwyższym poziomie gwarantując pomoc w rozwiązaniu każdego problemu oraz zapewniając regularne aktualizacje.

Całość infrastruktury jest **wystandaryzowana** i dokładnie opisane co zwiększa bezpieczeństwo i dostępność danych i systemów.

Migracji do naszej chmury z poziomu platformy Vmware można dokonać praktycznie w locie.

3

Dopytaj swojego dostawcę chmury o...

Jakie doświadczenie mają inżynierowie w budowie infrastruktury informatycznej centrów danych, w których przechowywane są Twoje dane?

I znów – teoretycznie nie powinno Cię to interesować. Płacisz za usługę dostępu do chmury obliczeniowej i tam wszystko powinno działać, a jak i kto działa to nie powinno być dla Ciebie istotne.

Jednak – to właśnie od **doświadczenia** i **umiejętności** inżynierów zależy, jak będą obsługiwane, udostępniane oraz zabezpieczane Twoje dane.

To bardzo istotne czy niezwykle skomplikowaną, wielowarstwową infrastrukturę informatyczną przechowującą dane Twojej firmy zaprojektowali i wykonali ludzie, którzy pracowali wcześniej przy projektowaniu centrów danych w odpowiedniej skali dla odpowiednich typów chmury SaaS, IaaS, PaaS.

Co się stanie jak tego nie będzie?

Podnosi się ryzyko przechowywania Twoich danych. Jeśli inżynier nie ma doświadczenia w projektowaniu i budowaniu odpowiedniej infrastruktury może ona działać jak źle zaprojektowany dom.

Brak systemowego, holistycznego podejścia skutkować może tym, że np. 80% infrastruktury będzie dobrze zaprojektowane ale pozostałe 20% będzie miało luki i to niezauważalne dla projektanta, który po prostu pominie pewne elementy systemu. Po jakimś czasie może to skutkować np. udanymi atakami hakerskimi na taki system.

Oto przykład, gdy coś poszło nie tak:

Nie tak dawno mieliśmy prawdziwą plagę zhakowanych szpitali, w których przerwano pracę.
https://www.termedia.pl/mz/Po-co-szpitalom-to-cale-cyberbezpieczenstwo-,50470.html

Znamienny cytat:

„Wbrew pozorom najlepszym z rozwiązań wcale nie jest zakup kolejnych urządzeń firewall czy licencji dla systemów opartych na rozwiązaniach co najmniej klasy Endpoint Detection and Response w architekturze ➔

3

Dopytaj swojego dostawcę chmury o...

➔ serwera. **To, co w zakresie cyberbezpieczeństwa jest kluczowe, to kadry.** To zapewnienie, że architektura IT będzie możliwie odporna na zagrożenia, a sprzęt i oprogramowanie będzie dobierane pod kątem skuteczności oraz skonfigurowane tak, by efektywnie realizowało swoje cele. Nowe architektury bezpieczeństwa wręcz tworzone są z założeniem, że przestępcom uda się zdobyć przyczółek w chronionej sieci – to tzw. model *zero trust*."

O atakach na szpitale w kontekście ich systemowego nieprzygotowania można przeczytać także tutaj: https://crn.pl/aktualnosci/ataki-na-szpitale-w-polsce--a-te-sa-zadowolone-z-bezpieczenstwa/

3

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

Inżynierowie tworzących chmurę Enteo Cloudpoint są certyfikowani z następujących technologii IT:

- Vmware,
- Cisco,
- Dell,
- Fortinet,
- Acronis,
- Veeam
- Microsoft Azure
- Amazon AWS

Są to specjaliści z doświadczeniem w realizacji projektów z zakresu przygotowania i wykonania infrastruktury IT oraz cyberbezpieczeństwa dla największych firm w Polsce i na świecie.

Nasi projektaci prowadzą szkolenia dla dużych firm z zakresu projektowania i zabezpieczania centrów danych. Architektury, które tworzymy są zawsze dogłębnie przemyślane i dopracowane, a wykonane systemu udowodniły swoją skuteczności u klientów nieprzerwanym działaniem od wielu lat.

Wśród naszych projektów można spotkać systemy obsługujące 5 000, 10 000 a nawet 300 000 jednoczesnych użytkowników.

4

Dopytaj swojego dostawcę chmury o...

Jakie mechanizmy bezpieczeństwa są zaimplementowane do ochrony infrastruktury chmurowej, tam gdzie przechowywane są Twoje dane?

W powszechnej opinii utrwaliło się przekonanie, że skoro jest chmura obliczeniowa, to i jest od razu w pełni zabezpieczona przed WSZYSTKIMI zagrożeniami.

Nic bardziej mylnego. Dostępne na rynku rozwiązania chmurowe w modelach SaaS, IaaS, IaaS **należy zabezpieczyć dla każdego ich elementu osobno**. W każdym z tych modeli miejscu jest inny poziom odpowiedzialności i styku między chmurą z rzeczywistością zewnętrzną.

4

Dopytaj swojego dostawcę chmury o...

Co się stanie jak tego nie będzie?

Brak jasnej komunikacji w jaki sposób zabezpieczona jest infrastruktura w konkretnym modelu przetwarzania, może wprowadzać klientów w błąd. Pominięcie któregoś z elementów zabezpieczeń prowadzi do utraty dostępu do systemów lub danych. Nieświadomość możliwości zaistnienia problemów skutuje niedoszacowaniem ryzyka.

Zajrzyjmy przy okazji do pryncypiów potentata rynku IT w kontekście budowania rozwiązań chmury obliczeniowej: *„By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud."*
https://www.ibm.com/topics/cloud-security

Oto przykład, gdy coś poszło nie tak:

Firma implementuje chmurę w modelu IaaS, ulegając obiegowym opiniom, że chmura jest „od razu" bezpieczna. IaaS zapewnia odpowiedni poziom zabezpieczenia w zakresie dostępności, ale wymaga właściwego przygotowania całego ekosystemu zabezpieczeń dla wytworzonych systemów i aplikacji. Pominięcie tego kroku doprowadza firmę do sytuacji, w której staje się ofiarą ataku hackerskiego i traci część swoich danych.

4

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

- Jasno **komunikujemy** różnice między typami usług, chmurowych.
- **Analizujemy** potrzeby i możliwości Klienta i **doradzamy** właściwy model.
- Świadczymy **eksperckie wsparcie** w odpowiednim przygotowaniu infrastruktury w szczególności w zachowaniu najwyższych standardów bezpieczeństwa.

Nasze usługi:

IaaS – przygotowana w oparciu o **sprawdzoną technologię VMware**. Wszystkie wykorzystywane urządzania to sprzęt nowy, renomowanych producentów z aktywnym wsparciem technicznym.

Każdy element infrastruktury jest **podwojony** i **przetestowany** pod kątem odporności całości chmury IaaS na awarię.

Każdy klient jest **odseparowany** od innych i dostaje w standardzie **dedykowany firewall** oraz możliwość implementacji **mikrosegemntacji**. ➔

4

Dopytaj swojego dostawcę chmury o...

➔ **Paas** – zdejmuje z Klienta konieczność troszczenia się o bieżące trzymanie systemów operacyjnych i platform programowych (np. Bazy danych).

Przygotujemy środowisko dokładnie dopasowane do potrzeb i zabezpieczamy je stosując standardy oczekiwane np. firmach finansowych. Następnie **bierzemy pełna odpowiedzialność za jego bieżące utrzymanie**.

SaaS – przygotowana przez nas zamknięta usługa desktopa/terminala, bazy danych czy sytemu Enova365Web w chmurze. Zbudowana w oparciu o elastyczną i gwarantującą pełną wysoką dostępność **platformę K8S** oraz rozproszony system przechowywania danych.

Usługa jest w standardzie poddana **kopii zapasowej**, zabezpieczona przed atakami **systemem antywirusowym** oraz system **Web Application Firewall** i **VPN**.

5

Dopytaj swojego dostawcę chmury o...

Jaki jest podział odpowiedzialności, za które elementy systemu bezpieczeństwa odpowiada dostawca?

W ramach, konkretnego modelu zakres odpowiedzialności dostawcy i klienta powinien być jasno sprecyzowany i przekazany Klientowi tak aby Klient był w pełni świadomy podziału i wynikających z niego konsekwencji.

Co się stanie jak tego nie będzie?

W przypadku nieprecyzyjnego podziału odpowiedzialności, często dochodzi do krzyżowania się uprawnień. Podmioty zaangażowane w IT nie są wówczas do końca świadome za jaki zakres odpowiadają.

W razie problemów z działaniem usług, podmioty zaangażowane nie będąc w pełni świadome zakresu obowiązków mogą przerzucać się odpowiedzialnością, co wydłuża czas rozwiązania problemu.

Analogicznie konieczność angażowanie wielu podmiotów w zarządzanie pojedynczym elementem wymusza konieczność koordynacji niepowiązanych ze sobą firm i ludzi. Rodzi to dodatkowe ryzyko.

5

Dopytaj swojego dostawcę chmury o...

Oto przykład, gdy coś poszło nie tak:

Jedna z firm świadcząca usługi chmury obliczeniowej (nazwijmy go na nasze potrzeby **firmą X**) udostępnia klientom usługi systemów operacyjnych przetwarzanych na utrzymywanej przez siebie infrastrukturze.

Klient dostaje dostęp do wstępnie skonfigurowanego systemu operacyjnego. Nie ma jednak dostępu do infrastruktury, na której jest on przetwarzany. Nie tworzy sieci i maszyn wirtualnych, nie ma możliwości ich rekonfiguracji czy restartu, a także nie ma możliwości konfiguracji zabezpieczeń sieciowych (brak portalu do zarządzania). Każda modyfikacja musi być zgłaszana i wykonywana przez dostawcę. ➔

5

Dopytaj swojego dostawcę chmury o...

➔ Taka infrastruktura nie spełnia definicji usługi IaaS (czyli infrastruktury jako usługi). Klient nie może samodzielnie zarządzać infrastrukturą, zdany jest na dostawcę i jego kompetencje, których nie może zweryfikować. Ewentualne problemy wymuszają pracę Klienta, dostawcy, wsparcia technicznego aplikacji itd.

Usługa ta bardziej wypełnia definicję PaaS. W tym wypadku dostawca powinien wziąć na siebie ciężar i odpowiedzialność monitorowania, zabezpieczania, konfigurowania i aktualizowania systemów. Tymczasem oddaje pusty system opublikowany w Internecie po SSH lub RDP i **nie bierze za niego żadnej odpowiedzialności**. Jednocześnie sam ma do systemów **zbyt wysoki poziom dostępu** uzyskany podczas wstępnej konfiguracji.

Analogicznie sytuacja wygląda w ramach chmury obliczeniowej innego dostawcy (nazwijmy go **dostawcą Y**). Nie jest to ani IaaS, ani PaaS, lecz pomieszanie modeli i brak jasnego określenia, kto jest odpowiedzialny za który element usługi.

W razie problemów w działaniu systemu operacyjnego diagnoza wymaga zarówno dostępu do konfiguracji maszyny wirtualnej, jak i do samego OS-u. **Kto więc w takim modelu jest odpowiedzialny za który** ➔

5

Dopytaj swojego dostawcę chmury o...

➔ **element?** Dostawca tworzy i konfiguruje systemy, ale nimi nie zarządza. Klient zarządza, ale nie ma dostępu do konfiguracji (np. zabezpieczeń sieciowych).

Inny przykład to dostawca oprogramowania w chmurze (**firma Z**), który tworzy w Azure infrastrukturę pod swoje oprogramowanie, konfiguruje i udostępnia ją Klientom, ale nie udziela dostępu do portalu Azure, gdzie znajduje się ta infrastruktura.

Usługę sprzedaje nazywając ją IaaS. Kto więc odpowiada za rekonfiguracje maszyn, kto za problemy wydajnościowe? Proste zgłoszenie techniczne w firmie Z potrafi **trwać tygodniami**, a firma prawie zawsze **unika odpowiedzialności** za problemy.

5

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

W naszej ofercie zarówno dla **IaaS**, **PaaS** jak i **SaaS** wszystko jest klarowne i czytelne.

W **IaaS** nasi specjaliści przygotowali zabezpieczoną na najwyższym poziomie, w pełni wysokodostępną umieszczoną w certyfikowanym centrum danych infrastrukturę serwerową, sieciową i przechowywania danych. Bazując na topowej technologii Vmware udostępniają jej zasoby do dowolnej konfiguracji przez Klienta za pomocą **prostego portalu Cloud Director**.

Klient sam tworzy sieci, firewalle, maszyny wirtualne, określa ich parametry i zasoby oraz instaluje w nich odpowiednie systemu operacyjne. My dbamy o dostępność serwerów fizycznych, sieci, danych a Klient dba o resztę, korzystając z najwyższej jakości infrastruktury i wydajnego oprogramowania.

W **PaaS** bazując na przygotowanej dla IaaS infrastrukturze nasi specjaliści projektują i wykonują dla Klientów dedykowane środowisko wraz z przygotowaniem całości konfiguracji sieci, poprzez maszyny aż do konfiguracji systemów operacyjnych i ich elementów jak np. bazy danych. Całość przygotowujmy zgodnie z najlepszymi

5

Dopytaj swojego dostawcę chmury o...

dostępnymi praktykami rynkowymi i stosując standardy i mechanizmy bezpieczeństwa wykorzystywane w największych firmach w tym z branży finansowej.

Następnie takie środowisko zabezpieczamy przed atakami: przygotowujemy schemat kopii zapasowych i Disaster Recovery. Ustalamy z Klientem najefektywniejszy i bezpieczny sposób dostępu, koordynujemy projekty z dostawcami aplikacji udostępniamy do przygotowania środowiska aplikacyjnego.

Klient skupia się na swoich aplikacjach. My dbamy o całe środowisko, pozostawiając mu przetwarzane na nim systemy merytoryczne jak np. EPR czy WMS.

W **SaaS** przygotowaliśmy na najwyższym poziomie zamkniętą usługę w której oferujemy: terminal, bazy danych i/lub system Enova365Web – dostępne od ręki, w prostym modelu rozliczeniowym.

Dla klientów nieposiadających złożonego środowiska IT prosta usługa SaaS to najwyższa elastyczność i wygoda. My dbamy o każdy aspekt usługi łącznie realizacją aktualizacji baz danych, systemu Enova365Web czy terminala. Klient skupia się na pracy w ramach aplikacji i dostosowaniu terminala (zainstalowanego na nim oprogramowania) do swoich potrzeb.

6

Dopytaj swojego dostawcę chmury o...

Czy Twoje dane są przetwarzane zgodnie z normą ISO 27001 i dyrektywami w zakresie bezpieczeństwa (NIS2, PCI-DSS)?

Czy wykorzystując usługę chmurową, macie pewność, że zewnętrzny audytor uzna ją za zgodną z normą ISO 27001 lub innymi dyrektywami w zakresie bezpieczeństwa np. NIS2, PCI--DSS etc. (SaaS, PaaS)?

6

Dopytaj swojego dostawcę chmury o...

Co się stanie jak tego nie będzie?

Wszyscy Klienci chcą aby ich IT było zgodne z wymogami RODO. Niektórzy zaś, aby wykorzystywane przez nich IT było zgodne wymogami norm ISO 27001, rekomendacją D, dyrektywą NIS2 czy PCI DSS. Może to być związanie np. z wymuszaniem pewnych norma przez naszego dostawcę. Nie posiadając ich możemy nie być zdolni do posiadania klientów z jakiejś, czasem bardzo zyskownej, części rynku.

Oto przykład, gdy coś może pójść nie tak:

Brak odpowiedniego przygotowania w ramach każdej warstwy od centrum danych, serwery i sieci aż do zabezpieczenia dostępu i użytkowników powoduje, że razie wycieku danych narażamy się na karę od UOD czy utratę reputacji przed Klientami lub nawet odpowiedzialność cywilną za poniesione straty.

Niespełnienie norm wymaganych przez naszych Klientów może np. doprowadzić do zaprzestania współpracy z nami np. kancelaria prawna współpracuje z bankiem i bez spełnienia wymogów bezpieczeństwa współpraca nie może być kontynuowana.

6

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

W ramach usługi **PaaS** i **SaaS** gwarantujemy, że infrastruktura spełnia najwyższe standardy bezpieczeństwa. Służymy również naszą ekspercką wiedzą i doświadczeniem pomagając projektować rozwiązania spełniające nawet najbardziej wyśrubowane wymagania.

W ramach usługi **PaaS**, bazując na naszym doświadczeniu w cyberbezpieczeństwie przy największych projektach w Polsce, projektujemy kompleksowy system bezpieczeństwa i dbamy o jego utrzymanie zgodnie z najwyższymi standardami.

7

Dopytaj swojego dostawcę chmury o...

Jaka jest szybkość i jakość wsparcia dla Twoich danych?

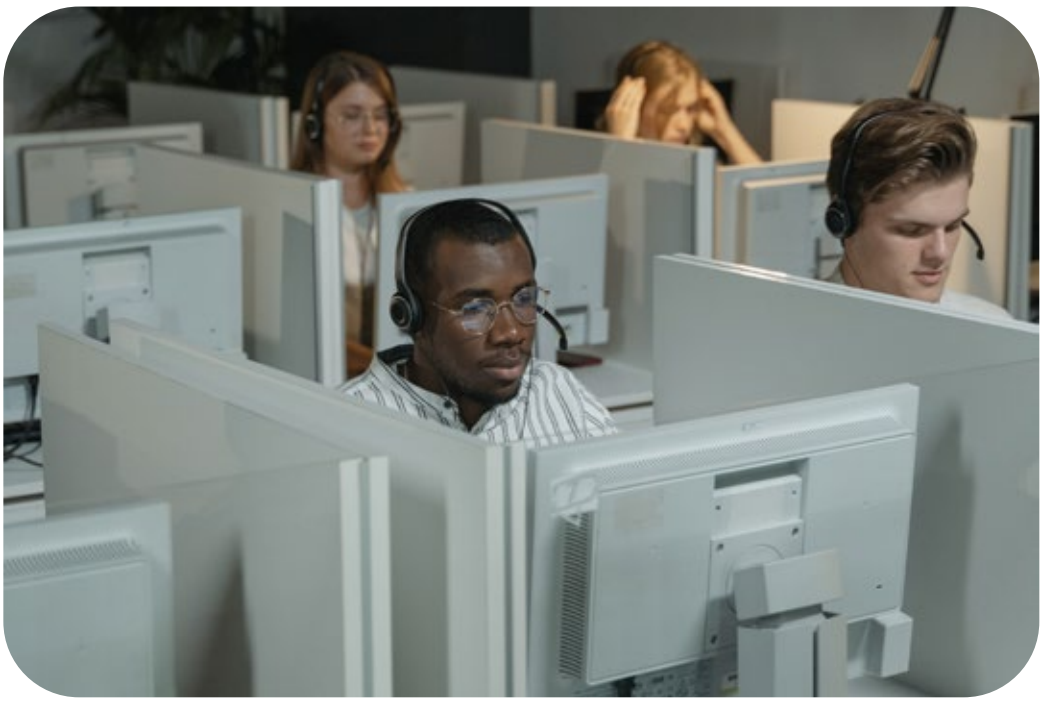
— Jak szybko możesz uzyskać wparcie techniczne kompetentnego pracownika?
— Czy wsparcie świadczone jest w języku polskim, czy wymagany jest długotrwały kontakt z infolinia?
— Czy inżynierowie wsparcia posiadają wiedzę i doświadczenia?
— Czy dostawca świadczy wsparcie w zakresie projektowania infrastruktury?
— Czy ma doświadczenie w dużych projektach także tych związanych z cyberbezpieczeństwem?

7

Dopytaj swojego dostawcę chmury o...

Co się stanie jak tego nie będzie?

Niski poziom wsparcia, utrudniony do niego dostęp, pierwsza linia wsparcia realizowana przez niskowykwalifikowany personel, brak doświadczenia dostawcy. Wszystko to powoduje, że w razie rozbudowy, zmiany, awarii czas obsługi będzie się wydłużać angażując czas i środki Klienta.



7

Dopytaj swojego dostawcę chmury o...

Oto przykład, gdy coś może pójść nie tak:

Wsparcie techniczne w Azure, Google realizowane jest w języku angielskim m.in. przez inżynierów z Indii, Pakistanu, Egiptu itp. Czas oczekiwania jest długi, a pierwsza realna pomoc wymaga przejścia skomplikowanej i często niepotrzebnej procedury.

W polskich dużych podmiotach telekomunikacyjnych świadczących usługi chmurowe zgłoszenia obsługiwane są przez infolinie. Kontakt z kompetentnym inżynierem jest niemożliwy lub bardzo utrudniony, a zgłoszenia ciągną się tygodniami.

U mniejszych dostawców często brak jest kompetentnych inżynierów czy architektów mających doświadczenie w skomplikowanych projektach. Bardzo mało jest dostawców mających realne doświadczenie w cybersecurity.

Każdy problem obsługiwany przez opisany powyżej support **zwiększa koszty** działania firmy, **marnuje czas** i obniża efektywność.

7

Dopytaj swojego dostawcę chmury o...

Jak działa to u nas:

- Posiadamy doświadczenie w budowie infrastruktury i cyberbezpieczeństwie dla największych firm w Polsce.
- Nasi inżynierowie to wyłącznie doświadczeni specjaliści z najwyższym poziomem wiedzy technicznej.
- Ścieżka wsparcia jest krótka i szybka. Bardzo szybko otrzymuje się kontakt do inżyniera z kompetencjami.