Koncepcje i architektury chmury obliczeniowej

1. Co oznacza „uwierzytelnienie” w procesie?

A. Dowody są uważane za autentyczne.

B. Jest to etap, na którym sędzia jest wyznaczany i znany obu stronom.

C. Świadek jest zatwierdzany jako ekspert, a jego zeznania będą rozpatrywane.

D. Obie strony zaangażowane w proces sądowy są uznawane.

2. Która organizacja zajmuje się prawami do prywatności na szczeblu federalnym w Stanach Zjednoczonych?

A. Federal Communications Commission (FCC)

B. Federal Trade Commission (FTC)

C. Federal Office of the Attorney General

D. Homeland Security

3. GDPR zastąpiło którą dyrektywę o ochronie danych?

A. PIPEDA

B. FRCP

C. Dyrektywa 95/46/WE

D. NIS

4. Kiedy strona jest zwolniona z przedstawiania dowodów w sądzie?

A. Kiedy ich nie ma

B. Kiedy ich odzyskanie jest zbyt kosztowne

C. Nigdy; strona musi zawsze przedstawić

dane, gdy zażąda ich sędzia

D. Gdy nie są one w rozsądny sposób dostępne

5. Jakiego formatu należy użyć, przedstawiając elektronicznie przechowywane informacje (ESI) w sądzie?

A. PDF

B. CSV

C. Format standardowy

D. Format natywny

6. Które z poniższych może prowadzić do problemów z weryfikacją, czy wszelkie znalezione dane są kompletne i dokładne, gdy są przechowywane w środowisku chmurowym?

A. Przejrzystość

B. Korzystanie z nieznanego sprzętu w lokalizacji dostawcy

C. Nie ma problemów z weryfikacją danych przechowywanych w chmurze

D. Brak metadanych w środowiskach chmurowych

7. Które z poniższych jest minimalnym okresem przechowywania danych, które mogą być wymagane w sądzie?

A. 1 rok

B. 5 lat

C. Wszelkie dane, które mogą być uznane za dowód, muszą być przechowywane na zawsze.

D. Nie ma ogólnego minimalnego okresu przechowywania danych.

8. Co jest najważniejszą rzeczą do rozważenia podczas przeglądania audytów i poświadczeń stron trzecich?

A. Firma, która przeprowadziła audyt

B. Usługi, z których korzysta klient

C. Lokalizacja usług

D. Certyfikacja dostawcy usług

9. Co powinien zrobić klient w przypadku umowy niepodlegającej negocjacjom, w której może brakować kontroli?

A. Nie korzystaj z usług dostawcy usług.

B. Zidentyfikuj wszelkie luki i wypełnij je odpowiednimi kontrolami.

C. Wykup ubezpieczenie cybernetyczne, aby zmniejszyć związane z tym ryzyko.

D. Zaakceptuj ryzyko, które akceptuje dostawca.

10. Australijska ustawa o ochronie prywatności wymaga ujawnienia naruszenia w jakim scenariuszu?

A. Kiedy ujawniane są jakiekolwiek dane dotyczące obywatela

B. Kiedy ujawniane są dane osobowe

C. Kiedy ujawnienie mogłoby spowodować poważną szkodę dla danej osoby

D. Australijska ustawa o ochronie prywatności nie odnosi się do wymogów dotyczących powiadamiania o naruszeniu

ODPOWIEDZI

1. A. „Uwierzytelnienie” oznacza, że dowody danych są uważane za autentyczne i dlatego są dopuszczalne w sądzie.

2. B. FTC jest federalną organizacją odpowiedzialną za ochronę konsumentów i prawa do prywatności. Prokurator generalny stanu wykonuje tę samą czynność na szczeblu stanowym.

3. C. GDPR zastąpiło dyrektywę o ochronie danych 95/46/WE. PIPEDA to kanadyjskie prawo o ochronie danych. FRCP to zbiór zasad regulujących prawo cywilne. NIS to ogólnounijne prawo dotyczące cyberbezpieczeństwa.

4. D. Klauzula 26(b)(2)(B) FRCP zezwala na nieprzedstawianie danych jako dowodu, gdy nie są one w rozsądny sposób dostępne. Może to mieć zastosowanie na przykład w przypadku, gdy wymagana jest kopia dysku na poziomie bitowym, gdy dane są przechowywane w środowisku chmurowym.

5. C. Najlepszą odpowiedzią jest to, że dowody są najbardziej przydatne, jeśli są przedstawiane w standardowym formacie. Chociaż zarówno PDF, jak i CSV można uznać za standardowe formaty, żaden z nich nie jest tutaj najlepszą odpowiedzią, ponieważ standardowy format jest dokładniejszy jako odpowiedź. Prezentacja formatu natywnego może być wymagana, jeśli metadane nie są prawidłowo zachowywane jako część rutyny eksportu.

6. A. Problemy z przejrzystością mogą powodować problemy z weryfikacją, czy wszelkie znalezione dane są kompletne i dokładne. Wszelkie problemy muszą zostać zidentyfikowane w ramach należytej staranności środowiska dostawcy.

7. D. Nie ma obowiązkowych okresów przechowywania, które są generycznie stosowane do wszystkich zestawów danych. Różne okresy przechowywania będą stosowane na mocy prawa lub w inny sposób (takich jak standardy, ciągła wartość dla firmy itd.) w zależności od rodzaju danych. Chociaż dane, co do których można zasadnie oczekiwać, że będą służyć jako dowód w sprawie sądowej, powinny być zachowywane przez organizację, nie ma obowiązkowego okresu przechowywania dla tych zestawów danych.

8. B. Usługi wykorzystywane przez klienta są najważniejszą kwestią do rozważenia podczas przeglądania audytów i poświadczeń stron trzecich. Chociaż wszystkie inne opcje są z pewnością ważne, mają one niewielką wartość, jeśli wykorzystywane usługi nie są częścią zakresu przeglądanego audytu.

9. B. Najlepszą odpowiedzią jest zidentyfikowanie potencjalnych luk i wdrożenie kontroli w celu rozwiązania postrzeganego ryzyka. Chociaż reakcja na ryzyko może obejmować unikanie ryzyka poprzez niekorzystanie z usług dostawcy, akceptację ryzyka i łagodzenie szkód finansowych poprzez zakup ubezpieczenia cybernetycznego, najlepszą odpowiedzią jest zidentyfikowanie kontroli, które dostawca jest zobowiązany dostarczyć na mocy umowy, określenie swoich wymagań i zajęcie się lukami poprzez wdrożenie kontroli.

10. C. Australijska ustawa o ochronie prywatności wymaga, aby naruszenie bezpieczeństwa zostało zgłoszone w przypadku ujawnienia danych osobowych, które mogą prowadzić do poważnych szkód.

Zarządzanie i zarządzanie ryzykiem przedsiębiorstwa

1. Chris chce pozyskać nowe rozwiązanie CRM SaaS dla jednostki biznesowej swojej organizacji. Jaki jest pierwszy krok, który Chris powinien podjąć w ramach przeprowadzania oceny ryzyka potencjalnego dostawcy?

A. Określ miesięczne koszty.

B. Zapytaj klientów referencyjnych o ich zadowolenie z produktu.

C. Określ poziom wrażliwości danych, które będą przechowywane w aplikacji.

D. Uzyskaj i przejrzyj dokumentację dostawcy.

2. Pat szuka standardowego zestawu kontroli branżowych, które są specyficzne dla chmury. Z jakich kontroli Pat może wybrać kontrolę, aby utworzyć podstawowy proces oceny ryzyka?

A. ISO 27001

B. NIST RMF

C. COBIT

D. CCM

3. Twój dostawca IaaS zapewnia Cię, że Twoje aplikacje będą zgodne z PCI, jeśli użyjesz jego oferty w chmurze. Co jest nie tak w tym stwierdzeniu?

A. Dostawca nie ma pojęcia, o czym mówi.

B. Dostawca Cię okłamuje.

C. Dostawca nie rozumie modelu współdzielonej odpowiedzialności w chmurze.

D. Wszystkie powyższe stwierdzenia są prawdziwe. 4. Jak często należy przeprowadzać oceny ryzyka u dostawcy usług w chmurze?

A. Po wstępnej ocenie przed wdrożeniem

B. Po wstępnej ocenie i na bieżąco

C. Dostawcy nie pozwalają klientom na przeprowadzanie ocen ryzyka

D. Z usługami w chmurze nie wiążą się żadne ryzyka

5. Który model usług jest najbardziej zgodny z istniejącymi procesami zarządzania i zarządzania ryzykiem?

A. SaaS

B. PaaS

C. IaaS

D. Prywatna chmura zarządzana wewnętrznie

6. Kiedy oceniasz dostawcę, którego z poniższych raportów SOC należy uzyskać od dostawcy podczas oceny kontroli bezpieczeństwa?

A. SOC 1, typ 1

B. SOC 1, typ 2

C. SOC 2, typ 1

D. SOC 3

7. Jaka jest naturalna właściwość multitenancy?

A. Nieelastyczne umowy

B. Hakowanie przez współnajemców

C. Ekonomia skali

D. Wspólna odpowiedzialność

8. Jakie ryzyko musi być złagodzone przez klienta?

A. Jakiekolwiek ryzyko

B. Ryzyko związane z modelem usługi

C. Ryzyko akceptowane przez dostawcę

D. Ryzyko wymienione w macierzy kontroli chmury

9. Jakie jest najważniejsze narzędzie zarządzania w chmurze?

A. Przeglądanie certyfikatów dostawców

B. Szkolenie pracowników w zakresie bezpieczeństwa chmury

C. Współpraca z audytorami z doświadczeniem w chmurze

D. Przeglądy umów

10. Co należy najpierw zrozumieć, rozważając zarządzanie chmurą prywatną?

A. Kto jest właścicielem i zarządza chmurą prywatną

B. Używane oprogramowanie do automatyzacji i koordynacji

C. Uprawnienia osób zarządzających chmurą prywatną

D. Klauzule umowne zawarte z dostawcą chmury prywatnej

ODPOWIEDZI

1. D. Pierwszym krokiem w przeprowadzeniu oceny ryzyka jest poproszenie o dokumentację.

2. D. CCM ma szereg kontroli, które są specyficzne dla chmury. Żadna z pozostałych odpowiedzi nie ma zastosowania.

3. D. Wszystkie stwierdzenia mają zastosowanie.

4. B. Oceny ryzyka należy przeprowadzać przed i w trakcie korzystania z oferty dostawcy.

5. C. IaaS to model usług najbardziej zgodny z tradycyjnym zarządzaniem i zarządzaniem ryzykiem. Prywatna chmura to model wdrożenia, a nie model usługi. Uwaga: Uważaj na podchwytliwe odpowiedzi, takie jak ta, na każdym egzaminie technicznym!

6. C. Najlepsza wymieniona odpowiedź to SOC 2, typ 1. SOC 1 dotyczy kontroli sprawozdawczości finansowej. Raport SOC 3 nie zawiera żadnych wykonanych testów ani ich wyników. Raport SOC 2, typ 2, jest najlepszy do wykorzystania przy ocenie dostawcy z perspektywy bezpieczeństwa, ale ponieważ nie jest wymieniony jako potencjalna odpowiedź, SOC 2, typ 1 jest najlepszą możliwą odpowiedzią. 7.

A. Nieelastyczne umowy są naturalną cechą multitenancy, ponieważ dostawca nie może sobie pozwolić na milion niestandardowych umów ani nimi zarządzać.

8. C. Najlepszą odpowiedzią jest to, że klient musi ograniczyć wszelkie ryzyko zaakceptowane przez dostawcę, z wyjątkiem ryzyka, które klient uzna za nie do przyjęcia. Musi to być oparte na wartości konkretnego systemu i nie może być podejściem ogólnym.

9. D. Przeglądy umów są podstawowym narzędziem związanym z zarządzaniem w chmurze.

10. A. Pierwszą rzeczą, którą należy zrozumieć, mając do czynienia z chmurą prywatną, jest to, kto jest właścicielem i zarządza infrastrukturą chmury. Jeśli infrastruktura jest wewnętrznie posiadana i zarządzana, niewiele się zmienia. Jeśli jest outsourcingowana, zarządzanie zmienia się, aby odzwierciedlić fakt, że kontrolę sprawuje dostawca.

Kwestie prawne, umowy i elektroniczne ujawnianie informacji. Infrastruktura jako usługa

1. Jaki typ dokumentu jest przechowywany w rejestrze STAR dla wpisów poziomu 1?

A. CCM

B. CAIQ

C. Oświadczenia dostawcy o zgodności

D. Pismo upoważniające do działania wydane przez rząd

2. Który model usług ma największą odpowiedzialność po stronie dostawcy?

A. SaaS

B. PaaS

C. IaaS

D. Wszystkie są takie same pod względem przesunięć odpowiedzialności.

3. Który model logiczny obejmuje płaszczyznę zarządzania dostępną dla klientów?

A. Infostruktura

B. Applistructure

C. Metastruktura

D. Infrastruktura

4. Używasz serwera internetowego w środowisku IaaS. Otrzymujesz telefon od klienta, który informuje, że serwer prawdopodobnie został naruszony. Który model logiczny został naruszony?

A. Infostruktura

B. Applistructure

C. Metastruktura

D. Infrastruktura

5. Która z poniższych cech NIE jest istotną cechą chmury według NIST?

A. Elastyczność

B. Multitenancy

C. Pule zasobów

D. Samoobsługa na żądanie

6. W jakim modelu logicznym wdrożyłbyś wirtualną zaporę sieciową?

A. Infostruktura

B. Applistructure

C. Metastruktura

D. Infrastruktura

7. W jaki sposób dostęp jednego konsumenta jest ściśle izolowany od dostępu innych konsumentów w środowisku chmury publicznej?

A. Silne hasła

B. RBAC

C. Zasady po stronie dostawcy

D. Zasady po stronie klienta

8. Orkiestracja umożliwia kontrolerowi żądanie zasobów z puli zasobów. Jak to się robi?

A. System zgłoszeń ustala priorytety klientów na podstawie poziomu wsparcia

B. Poprzez użycie interfejsów API REST

C. Poprzez użycie RPC

D. Poprzez wywołania sieciowe

9. Zostałeś poinstruowany, aby zbudować serwer z ośmioma procesorami i 8 GB pamięci RAM. Jakiego modelu usługi byś użył?

A. SaaS

B. PaaS

C. IaaS

D. Żaden dostawca chmury nie obsługuje maszyny z 8 procesorami

10. Twoja firma korzysta z dostawcy PaaS do hostowania aplikacji opartej na Pythonie 2.7. Pewnego dnia dostawca wysyła Ci wiadomość e-mail, w której informuje, że nie będzie już obsługiwał platformy Python 2.7, a wszystkie aplikacje muszą zostać zaktualizowane do obsługi Pythona 3.6 w ciągu dwóch tygodni. Co powinieneś zrobić jako pierwsze?

A. Przetestuj aplikację w Pythonie 3.6.

B. Powiedz dostawcy, że nie możesz dotrzymać tego terminu.

C. Dostawcy są ograniczeni przez prawo w tym zakresie.

D. Wnieś pozew przeciwko dostawcy za ból i cierpienie.

ODPOWIEDZI

1. B. Dostawcy prześlą kopie wypełnionych odpowiedzi CAIQ. Chociaż ISO i/lub SOC mogą być używane jako część wpisu STAR poziomu 2, wpisy poziomu 1 używają CAIQ, a nie CCM.

2. A. Model usługi SaaS zakłada, że dostawca przyjmuje odpowiedzialność za większość (nie wszystkie) kontrole.

3. C. Płaszczyzna zarządzania jest częścią logicznego modelu metastruktury.

4. B. Serwer WWW jest częścią struktury aplikacji. Kontrole otaczające serwer WWW byłyby implementowane na poziomie metastruktury, ale sam serwer WWW znajduje się na poziomie struktury aplikacji (a dane znajdują się na warstwie infostruktury).

5. C. NIST nie określa wielodostępności jako istotnej cechy. ISO określa jednak wielodostępność jako część istotnych cech puli zasobów.

6. C. Wszystkie kontrole w środowisku wirtualnym są wykonywane na warstwie metastruktury. Jeśli pytanie dotyczy instalacji agenta zapory, nastąpi to na warstwie struktury aplikacji.

7. C. Najemcy są chronieni przez zasady po stronie dostawcy. Rozważmy na przykład podsłuchiwanie sieci. Jeden najemca nigdy nie zobaczy ruchu sieciowego przeznaczonego dla innego najemcy. Zasadniczo jeden najemca nigdy nie powinien wiedzieć, że inny najemca w ogóle istnieje. Chociaż konsumenci również będą mieli własne zasady, dostawca musi zapewnić silną izolację obciążeń i najemców. To sprawia, że C jest najlepszą odpowiedzią.

8. B. Orkiestracja zazwyczaj wykorzystuje wywołania interfejsu API REST. Chociaż orkiestracja jest oczywiście wykonywana w sieci, najlepszą odpowiedzią są wywołania interfejsu API REST. To przykład sztuczek, które autorzy testów lubią stosować u kandydatów.

9. C. To doskonały przykład, dlaczego warto używać IaaS — dostęp do podstawowych obliczeń.

10. A. Gdy platforma jest przestarzała (nie jest już obsługiwana), dostawca zazwyczaj zapewni Ci dostęp do środowiska testowego, w którym możesz przetestować swoją aplikację przy użyciu nowej platformy. Jeśli chodzi o czas podany w pytaniu, to jest on trochę przesadzony, biorąc pod uwagę moje doświadczenia, ale nie ma prawa, które zabraniałoby dostawcy dawania Ci godzin na migrację, nie mówiąc już o tygodniach.

Zarządzanie zgodnością i audytem

1. Jak należy przeprowadzać audyty?

A. Zawsze przez Twoją firmę

B. Zawsze przez dostawcę

C. Zawsze przez niezależnego audytora

D. Zawsze przez federalny organ regulacyjny

2. Czego formą jest audyt przejściowy?

A. Dziedziczenie zgodności

B. Wykazanie przestrzegania przez dostawcę standardów branżowych

C. Ocena fizyczna przeprowadzona w ramach audytu

D. Termin używany w odniesieniu do wszystkich usług objętych zakresem audytu

3. Jak audyty działają w kontekście zgodności?

A. Audyty to techniczne środki oceny systemów.

B. Audyty to procesy i procedury stosowane do oceny systemów.

C. Audyty to kluczowe narzędzie do udowodnienia lub obalenia zgodności.

D. Audyty są wymagane do prawidłowego zarządzania systemami w chmurze.

4. Co jest prawdą w odniesieniu do poświadczenia?

A. Poświadczenie to inne określenie audytu.

B. Poświadczenie to oświadczenie prawne strony trzeciej.

C. Poświadczenie to zeznanie w sądzie.

D. Poświadczenia mogą być wykonywane wyłącznie przez biegłego rewidenta.

5. Jaki jest cel zarządzania audytem?

A. Zarządza częstotliwością audytów

B. Zarządza audytorami i ich świadomością systemów

C. Zarządza zakresem audytów

D. Zapewnia, że dyrektywy audytu są wdrażane prawidłowo

6. Na co należy zwrócić szczególną uwagę podczas przeglądania wcześniej wykonanych raportów z audytu dostarczonych przez dostawcę?

A. Usługi i jurysdykcje w zakresie audytu

B. Firma, która przeprowadziła audyt

C. Data raportu z audytu

D. Wyrażona opinia audytora

7. Co powinien zrobić klient, gdy nie może samodzielnie zebrać dowodów zgodności?

A. Dostosować zakres raportowania, aby odzwierciedlić brak dowodów.

B. Zaakceptować ryzyko nie wykazania zgodności organom regulacyjnym.

C. Dowody nieudostępnione klientowi chmury są usuwane spod nadzoru regulacyjnego.

D. Takie dane powinny być dostarczane klientowi przez dostawcę.

8. Jakie korzyści z ciągłej zgodności ma klient usług w chmurze?

A. Klient otrzymuje aktualizacje w czasie rzeczywistym dotyczące zmian w środowisku dostawcy.

B. Wszelkie zmiany wprowadzane do środowiska dostawcy są dostarczane w ciągu jednego tygodnia.

C. Nie ma żadnych korzyści, ponieważ klienci powinni być zainteresowani jedynie tym, aby dostawca posiadał certyfikat ISO.

D. Zwiększona częstotliwość audytów zmniejsza prawdopodobieństwo nieznanego odchylenia od zasad bezpieczeństwa w środowisku dostawcy.

9. Co powinien zrobić klient, jeśli artefakty zgodności dostawcy są niewystarczające?

A. Złożyć wniosek o wyłączenie zakresu.

B. Tworzyć i zbierać własne artefakty.

C. Nie korzystać z usług dostawcy.

D. Nic nie robić.

10. Co można zrobić, aby uniknąć potencjalnego zamieszania podczas audytu dostawcy usług w chmurze?

A. Współpracować z audytorami posiadającymi certyfikat CCSK.

B. Współpracować z audytorami dostarczanymi przez dostawców.

C. Współpracować z księgowymi.

D. Współpracować z audytorami certyfikowanymi przez Institute of Certified Auditors.

ODPOWIEDZI

1. C. Kluczową koncepcją audytów jest to, że są one przeprowadzane przez niezależnego audytora. Dotyczy to wszystkich audytów. Chociaż możesz chcieć przeprowadzić audyt dostawcy samodzielnie, dostawca może uznać udzielenie Ci dostępu do centrum danych za problem bezpieczeństwa, na przykład.

2. A. Audyty przepustowe są formą dziedziczenia zgodności. Audyt nie mówi o kompletności samego zakresu audytu. Zamiast tego potwierdza, że kontrole wdrożone i zarządzane przez dostawcę są zgodne. Twoja organizacja jest zobowiązana do spełnienia zgodności dla swoich systemów i danych w środowisku dostawcy.

3. C. Najbardziej dokładną, a zatem najlepszą odpowiedzią jest to, że audyty są wykorzystywane do udowodnienia lub obalenia zgodności z zasadami ładu korporacyjnego.

4. B. Atesty to oświadczenia prawne strony trzeciej. Są one wykorzystywane jako kluczowe narzędzie, gdy klienci oceniają i współpracują z dostawcami usług w chmurze, ponieważ klienci często nie mają prawa przeprowadzać własnych ocen. Poświadczenia różnią się od audytów tym, że audyty są zazwyczaj przeprowadzane w celu zbierania danych i informacji, podczas gdy poświadczenie sprawdza ważność tych danych i informacji w ramach uzgodnionej procedury (takiej jak SOC). Poświadczenia mogą być przeprowadzane przez biegłych rewidentów (CPA), ale ta odpowiedź nie odpowiada właściwie na pytanie.

5. D. Zarządzanie audytem zapewnia, że dyrektywy audytu są wdrażane prawidłowo. Wszystkie inne możliwe odpowiedzi stanowią część tej aktywności, ale najlepszą odpowiedzią jest to, że wszystkie te dyrektywy są wdrażane prawidłowo.

6. A. Chociaż nie wszystkie odpowiedzi są koniecznie nieprawidłowe, najlepsze praktyki CSA zalecają zwrócenie szczególnej uwagi na usługi i jurysdykcje, które są częścią zakresu audytu, więc jest to najlepsza odpowiedź.

7. D. Dostawcy powinni dostarczać klientom dowody zgodności i artefakty, gdy klienci nie mogą ich sami wygenerować. Wszystkie inne odpowiedzi są po prostu błędne.

8. D. Zwiększona częstotliwość audytu zmniejsza prawdopodobieństwo nieznanego odchylenia od postawy bezpieczeństwa w środowisku dostawcy. Ciągły nie oznacza czasu rzeczywistego i nie oznacza żadnego ustalonego harmonogramu. Oznacza to, że wszelkie zmiany lub ustalenia są odkrywane pomiędzy cyklami certyfikacji, zwykle poprzez wykorzystanie automatyzacji.

9. B. Jeśli artefakty zgodności dostawcy są niewystarczające, klienci powinni zebrać własne. Nie ma czegoś takiego jak żądanie wykluczenia zakresu.

10. A. Wybierając audytorów, zawsze chcesz współpracować z audytorami, którzy mają wiedzę na temat chmury obliczeniowej. Certyfikacja CCSK potwierdza zrozumienie usług w chmurze przez audytora.

Zarządzanie informacją

1. Cykl życia bezpieczeństwa danych uwzględnia który z poniższych elementów?

A. Lokalizacja

B. Jak skonfigurować kontrole bezpieczeństwa

C. Kto może uzyskać dostęp do danych

D. Modele usług

2. Który z poniższych elementów można wykorzystać do ustalenia, czy informacje powinny być przechowywane w chmurze?

A. Polityka prywatności

B. Klasyfikacja informacji

C. Cykl życia bezpieczeństwa danych

D. Zasady akceptowalnego użycia

3. Które z poniższych elementów są uważane za część cyklu życia bezpieczeństwa danych?

A. Lokalizacja danych

B. Lokalizacja urządzenia dostępowego

C. Lokalizacja centrum danych

D. A i B

4. Jaki jest cel zarządzania informacjami (wybierz najlepszą odpowiedź)?

A. Zapewnienie dostępu odpowiedniego personelu do wymaganych danych.

B. Zapewnienie przechowywania danych w zatwierdzonych lokalizacjach.

C. Formalne zarządzanie danymi w całym przedsiębiorstwie.

D. Tworzenie i zarządzanie zasadami bezpieczeństwa informacji.

5. Które z poniższych elementów jest uważane za narzędzie do wdrażania zarządzania danymi?

A. Zasady bezpieczeństwa

B. Kontrole bezpieczeństwa

C. Klasyfikacja informacji

D. Wszystkie powyższe

6. Jakie jest narzędzie prawne zapewniające wdrożenie i przestrzeganie odpowiednich wymogów zarządzania przez dostawcę chmury?

A. Kontrole bezpieczeństwa

B. Kontrole umowne

C. Silne zarządzanie zmianami

D. Uprawnienia

7. Co można wykorzystać do określenia, co aktorzy mogą robić, a czego nie?

A. Uprawnienia

B. Klasyfikacja informacji

C. Zarządzanie informacjami

D. Kontrole umowne

8. Przejście do chmury stwarza okazję do ponownego zbadania czego?

A. Jak zarządzasz informacjami i znajdujesz sposoby na poprawę sytuacji

B. Istniejące zasady bezpieczeństwa

C. Istniejące kontrole bezpieczeństwa

D. Istniejące możliwości klasyfikacji informacji

9. Rozszerzenie zarządzania informacjami o usługi w chmurze wymaga:

A. Kontroli bezpieczeństwa

B. Kontroli umownych

C. Zarówno kontroli umownych, jak i kontroli bezpieczeństwa

D. Dostawca dostarczający pisemną umowę z podmiotem współpracującym

10. Co określa autoryzacja?

A. Strona prawnie odpowiedzialna za bezpieczeństwo danych użytkownika końcowego

B. Czy dane mogą być przechowywane w środowisku chmury

C. Dozwoleni dostawcy usług w chmurze na podstawie klasyfikacji danych

D. Kto ma prawo dostępu do określonych informacji i/lub danych

ODPOWIEDZI

1. A. Cykl życia bezpieczeństwa danych różni się od cyklu życia zarządzania informacjami, ponieważ uwzględnia lokalizację. W rezultacie wiele lokalizacji może prowadzić do zarządzania wieloma cyklami życia bezpieczeństwa danych. Chociaż cykl życia bezpieczeństwa danych zajmuje się kontrolami bezpieczeństwa na każdym etapie, nie dyktuje, w jaki sposób mają być tworzone ani kto powinien mieć dostęp do jakich danych. Uprawnienia służą do określania, kto powinien mieć dostęp do konkretnych danych. Cykl życia bezpieczeństwa danych w ogóle nie dotyczy modeli usług.

2. B. Najlepszą odpowiedzią jest klasyfikacja informacji. Polityka dopuszczalnego użytku może określać, jaki poziom klasyfikacji danych może być przechowywany, ale opiera się to na posiadaniu klasyfikacji na początek. Cykl życia bezpieczeństwa danych może służyć do określania, jakie kontrole należy stosować w oparciu o etap cyklu życia, więc C nie jest najlepszą odpowiedzią na to konkretne pytanie. Podobnie jak w przypadku zasad akceptowalnego użycia, polityka prywatności może określać sposób przetwarzania danych, a zatem mogą obowiązywać ograniczenia dotyczące przechowywania danych osobowych w chmurze — ale, powtórzę, klasyfikacja informacji jest najlepszą odpowiedzią na to pytanie.

3. D. Przepraszam za podchwytliwe pytanie. Cykl życia bezpieczeństwa danych uwzględnia lokalizację danych i urządzenia dostępowego. Czy to oznacza, że w rezultacie dorozumiana jest lokalizacja centrum danych? Może tak, może nie. Można by argumentować, że lokalizacja centrum danych określałaby jurysdykcję, a zatem dyktowałaby, jakie kontrole należy zastosować, ale nie ma z kim dyskutować, gdy zdajesz egzamin.

4. C. Najlepszą odpowiedzią jest to, że zarządzanie informacjami istnieje w celu formalnego zarządzania danymi w całym przedsiębiorstwie. Pozostałe odpowiedzi są prawdziwymi stwierdzeniami, ale zarządzanie informacjami dotyczy czegoś więcej niż tylko tych pojedynczych stwierdzeń. Dlatego najlepszą odpowiedzią jest C.

5. B. Kontrole bezpieczeństwa są uważane za narzędzie do wdrażania zarządzania danymi. Same zasady nie robią nic, aby wdrożyć zarządzanie danymi. Tak, są one absolutnie potrzebne, ale są to stwierdzenia (kontrole dyrektywne), a nie rzeczywiste kontrole zapobiegawcze, które mają powstrzymać kogoś przed zrobieniem czegoś. Klasyfikacja jest również wymagana do silnego zarządzania, ale znowu, sama klasyfikacja nie powstrzyma aktora przed wykonywaniem funkcji.

6. B. Jedynym narzędziem prawnym zapewniającym wdrożenie i przestrzeganie odpowiednich wymogów zarządzania przez dostawcę chmury są kontrole umowne. Żadna z pozostałych opcji nie jest narzędziem prawnym.

7. A. Uprawnienia określają, co aktorzy mogą robić, a czego nie. Kontrole umowne są narzędziem prawnym, a zarządzanie informacjami jest znacznie szersze niż określanie, co aktorzy mogą, a czego nie mogą robić, więc B i C nie są najlepszymi odpowiedziami. Klasyfikacja danych może pomóc w wyborze kontroli, ale znowu nie jest to najlepsza odpowiedź.

8. A. Przejście do chmury daje możliwość przyjrzenia się sposobowi zarządzania informacjami i znalezienia sposobów na poprawę sytuacji. Może to obejmować również wszystkie inne odpowiedzi, ale ponieważ pierwsza odpowiedź obejmuje wszystkie inne opcje, jest to najlepsza odpowiedź.

9. C. Najlepszą odpowiedzią jest to, że zarówno kontrola bezpieczeństwa, jak i kontrola umowna są wymagane, aby rozszerzyć zarządzanie informacjami na chmurę. Umowa z podmiotem współpracującym ma zastosowanie wyłącznie do danych regulowanych przez HIPAA i byłaby objęta kontrolą umowną.

10. D. Upoważnienia określają, kto ma dostęp do określonych informacji i/lub danych i są częścią zarządzania informacjami. Klient zawsze ponosi odpowiedzialność prawną w przypadku naruszenia danych użytkownika końcowego. Chociaż chcemy, aby zarządzanie informacjami pomagało w wyborze odpowiednich dostawców chmury i określało klasyfikacje danych, nie są to upoważnienia.

Płaszczyzna zarządzania i ciągłość działania

1. Jaki poziom uprawnień powinien zostać przypisany do konta użytkownika z dostępem do metastruktury?

A. Tylko do odczytu

B. Dostęp administracyjny

C. Najmniejsze uprawnienia wymagane do wykonania zadania

D. Dostęp administracyjny tylko do systemu, którego używa użytkownik

2. W jaki sposób konto główne powinno być używane w środowisku chmurowym?

A. Powinno być traktowane jak każde inne konto uprzywilejowane.

B. Hasło do konta powinno być udostępniane tylko za pośrednictwem zaszyfrowanej poczty e-mail.

C. Powinno być używane tylko do kończenia instancji.

D. Powinno mieć przypisane uwierzytelnianie wieloskładnikowe i być zamknięte w sejfie.

3. Jakie warstwy stosu logicznego powinny być uważane za część BCP/DR?

A. Infostruktura

B. Metastruktura

C. Infrastruktura

D. Wszystkie warstwy modelu logicznego

4. W jaki sposób BCP/DR powinno być projektowane w chmurze?

A. Architekt na wypadek awarii.

B. Architekt korzystający z usług jednego dostawcy chmury.

C. Architekt korzystający z usług wielu dostawców chmury.

D. Architekt wykorzystujący replikację w czasie rzeczywistym dla wszystkich danych.

5. Co oznacza „zablokowanie”?

A. Zablokowanie ma zastosowanie, gdy nie masz możliwości eksportowania danych na mocy umowy.

B. Eksportowanie danych poza dostawcę wymagałoby znacznego wysiłku.

C. Wyeksportowane dane mogą być używane tylko z usługami pierwotnego dostawcy.

D. Wszystkie powyższe odpowiedzi są poprawne.

6. Które z poniższych musi być częścią planowania ciągłości działania przez klienta?

A. Określenie sposobu zagwarantowania dostępności w regionie DR poprzez omówienie planów DR z dostawcą

B. Określenie sposobu, w jaki dostawca IaaS naprawi wszelkie problemy z dostępnością w Twojej aplikacji

C. Korzystanie z umów w celu zapewnienia, że DR nie spowoduje użycia innej jurysdykcji do przechowywania i przetwarzania danych

D. Wdrażanie inżynierii chaosu

7. Czym jest infrastruktura jako kod (IaC)?

A. IaC wykorzystuje szablony do budowania infrastruktury sieci wirtualnej.

B. IaC wykorzystuje szablony do budowania całej infrastruktury wirtualnej, od sieci po systemy.

C. IaC to system zgłoszeń, za pośrednictwem którego od dostawcy żądane są dodatkowe wystąpienia.

D. IaC to system zgłoszeń, za pośrednictwem którego od dostawcy żądane są zwiększenia limitów.

8. Jaki jest cykl wydawania nowych funkcji?

A. Funkcjonalność API jest udostępniana jako pierwsza, po niej CLI, a następnie konsola internetowa.

B. Funkcjonalność CLI jest udostępniana jako pierwsza, po niej API, a następnie konsola internetowa.

C. Funkcjonalność konsoli internetowej i API jest udostępniana jako pierwsza, a następnie CLI.

D. Metoda używana do udostępniania nowych możliwości jest określana przez dostawcę.

9. Alicja chce zaktualizować, ale nie zastąpić, plik za pośrednictwem interfejsu API REST. Jakiej metody powinna użyć Alicja?

A. GET

B. POST

C. PUT

D. PATCH

10. Która z poniższych opcji wprowadza największą złożoność przy rozważaniu podejścia wielochmurowego do BCP/DR?

A. Infrastruktura aplikacji

B. Metastruktura

C. Infrastruktura

D. Infostruktura

ODPOWIEDZI

1. C. Zawsze należy używać najmniejszych uprawnień. Żadna z pozostałych odpowiedzi nie ma zastosowania.

2. D. Konto główne powinno mieć przypisane urządzenie sprzętowe MFA, a dane uwierzytelniające wraz z urządzeniem MFA powinny być zamknięte w sejfie, aby można było z nich korzystać wyłącznie w nagłych wypadkach.

3. D. Wszystkie warstwy modelu logicznego powinny być brane pod uwagę w przypadku BCP/DR.

4. A. Zawsze należy projektować na wypadek awarii w przypadku BCP/DR.

5. D. Blokada występuje, gdy nie można łatwo zmienić dostawców i wyeksportować danych. Można to rozwiązać tylko poprzez solidne procesy należytej staranności w celu przyjęcia dostawców usług w chmurze.

6. A. Należy skonsultować się z dostawcą, aby określić gwarantowaną dostępność w regionie. Nie wszystkie regiony mają taką samą ilość pojemności i mogą być przepełnione w przypadku awarii w innym regionie. Dostawca IaaS nie zajmie się problemami z Twoimi własnymi aplikacjami. Chociaż przepisy dotyczące rezydencji danych mogą mieć kluczowe znaczenie dla niektórych firm z określonych branż, nie wszystkie firmy będą musiały zmierzyć się z tym problemem, więc C nie jest najlepszą odpowiedzią. Inżynieria chaosu może nie być dla każdego.

7. B. Najlepszą odpowiedzią jest to, że IaC używa szablonów do budowania całej wirtualnej infrastruktury, od sieci po systemy. Używając IaC, możesz nie tylko zbudować całą infrastrukturę, w tym instancje serwerów na podstawie skonfigurowanych obrazów, ale niektórzy dostawcy IaaS idą tak daleko, że obsługują konfigurację serwerów w czasie rozruchu. To nie jest system biletowy.

8. D. Połączenie i funkcjonalność udostępniane klientom są zawsze zależne od dostawcy. Mogą one udostępniać nowe funkcjonalności na wiele różnych sposobów.

9. D. Alicja powinna użyć metody PATCH do aktualizacji, ale nie zastępowania pliku. Metoda PUT tworzy nowy plik. POST jest podobny do PATCH, ale POST zaktualizuje i usunie plik.

10. B. Metastruktura wprowadza najwięcej złożoności, gdy rozważa się podejście wielochmurowe do BCP/DR.

Bezpieczeństwo infrastruktury

1. Co powinno być głównym zmartwieniem przy rozważaniu agentów bezpieczeństwa dla instancji w chmurze?

A. Dostawca zdobył nagrody.

B. Dostawca używa wykrywania opartego na heurystyce, a nie na wykrywaniu opartym na sygnaturach.

C. Dostawca wybrany dla instancji serwera w chmurze to ten sam dostawca, którego używasz dla instancji wewnętrznych.

D. Agent dostawcy nie używa adresów IP do identyfikacji systemów.

2. Które z poniższych stwierdzeń jest/są dokładne na temat różnic między SDN i VLAN?

A. SDN izoluje ruch, co może pomóc w mikrosegmentacji. Sieci VLAN segmentują węzły sieciowe na domeny rozgłoszeniowe.

B. Sieci VLAN mają około 65 000 identyfikatorów, podczas gdy SDN ma ich ponad 16 milionów.

C. SDN oddziela płaszczyznę sterowania od urządzenia sprzętowego i umożliwia aplikacjom komunikację z płaszczyzną sterowania.

D. Wszystkie powyższe stwierdzenia są dokładne.

3. W przypadku korzystania z niezmiennych serwerów, w jaki sposób należy przyznać dostęp administracyjny do struktury aplikacji, aby wprowadzać zmiany w uruchomionych instancjach?

A. Dostęp administracyjny powinien być ograniczony do zespołu operacyjnego. Jest to zgodne ze standardowym podejściem do bezpieczeństwa opartym na podziale obowiązków.

B. Dostęp administracyjny powinien być ograniczony do zespołu programistów. Jest to zgodne z nowym podejściem do tworzenia oprogramowania, w którym programiści są właścicielami tworzonych przez siebie aplikacji.

C. Dostęp administracyjny powinien być ograniczony dla wszystkich. Wszelkie zmiany wprowadzane na poziomie struktury aplikacji powinny być wprowadzane do obrazu, a nowa instancja powinna być tworzona przy użyciu tego obrazu.

D. Dostęp administracyjny do struktury aplikacji jest ograniczony do dostawcy w niezmiennym środowisku.

4. Który z poniższych jest głównym celem mikrosegmentacji?

A. Jest to szczegółowe podejście do grupowania maszyn, aby ułatwić administrowanie nimi.

B. Jest to szczegółowe podejście do grupowania maszyn, które ogranicza promień zasięgu.

C. Mikrosegmentacja może wykorzystywać tradycyjną technologię VLAN do grupowania maszyn.

D. Mikrosegmentacja implementuje sieć o zerowym zaufaniu.

5. Które z poniższych stwierdzeń jest dokładne przy omawianiu różnic między kontenerem a maszyną wirtualną?

A. Kontener zawiera aplikację i wymagane zależności (takie jak biblioteki). Maszyna wirtualna zawiera system operacyjny, aplikację i wszelkie zależności.

B. Maszynę wirtualną można przenosić do i od dowolnego dostawcy usług w chmurze, podczas gdy kontener jest powiązany z konkretnym dostawcą.

C. Kontenery usuwają zależność od konkretnego jądra. Maszyny wirtualne mogą działać na dowolnej platformie.

D. Wszystkie powyższe stwierdzenia są dokładne.

6. Jaka jest główna cecha chmury, która ma największy wpływ na bezpieczeństwo obciążeń?

A. Sieci zdefiniowane programowo

B. Elastyczna natura

C. Wielodostępność

D. Model współdzielonej odpowiedzialności

7. Wybierz dwa atrybuty, które urządzenie wirtualne powinno mieć w środowisku chmury.

A. Automatyczne skalowanie

B. Szczegółowe uprawnienia dla administratorów

C. Przełączanie awaryjne

D. Możliwość powiązania z możliwościami orkiestracji dostawcy

8. Wendy chce dodać instancję do swojej implementacji w chmurze. Gdy próbuje dodać instancję, zostaje odrzucona. Sprawdza swoje uprawnienia i nigdzie nie jest napisane, że odmówiono jej uprawnienia do dodania instancji. Co może być nie tak?

A. Wendy próbuje uruchomić serwer Windows, ale ma uprawnienia do tworzenia tylko instancji Linux.

B. Wendy nie ma dostępu root do serwera Linux, który próbuje uruchomić.

C. Wynika to z domyślnej natury chmury, która odmawia dostępu. Jeśli Wendy nie ma wyraźnego uprawnienia do dodania instancji, jest ona automatycznie domyślnie odrzucana.

D. Wendy jest członkiem grupy, której odmówiono dostępu do dodawania instancji.

9. W jaki sposób zarządzanie jest scentralizowane w SDN?

A. Usuwając płaszczyznę sterowania z podstawowego urządzenia sieciowego i umieszczając ją w kontrolerze SDN

B. Używając północnych interfejsów API, które umożliwiają oprogramowaniu wykonywanie działań na warstwie sterowania

C. Używając południowych interfejsów API, które umożliwiają oprogramowaniu wykonywanie działań na warstwie sterowania

D. SDN to zdecentralizowany model

10. Co należy zrobić przed rozpoczęciem oceny podatności (VA) jednej z uruchomionych instancji?

A. Wybierz produkt VA, który działa w środowisku chmurowym.

B. Określ, czy dostawca pozwala klientom na wykonanie VA i czy wymagane jest wcześniejsze powiadomienie.

C. Otwórz wszystkie zapory SDN, aby umożliwić wykonanie VA.

D. Ustal godzinę i datę, w których uzyskasz dostęp do centrum danych dostawcy, aby móc uruchomić VA na fizycznym serwerze, na którym działa Twoja instancja.

ODPOWIEDZI

1. D. Najlepszą odpowiedzią jest to, że agent nie używa adresowania IP jako mechanizmu identyfikacji. Instancje serwerów w chmurze mogą być ulotne, zwłaszcza gdy używane są niezmienne instancje. Wszystkie pozostałe odpowiedzi są opcjonalne i nie są priorytetami dla agentów bezpieczeństwa chmury.

2. D. Wszystkie odpowiedzi są poprawne.

3. C. Dostęp administracyjny do serwerów w niezmiennym środowisku powinien być ograniczony dla wszystkich. Wszelkie wymagane zmiany powinny zostać wprowadzone do obrazu, a następnie obraz ten jest używany do zbudowania nowej instancji. Wszystkie pozostałe odpowiedzi są niepoprawne.

4. B. Najlepszą odpowiedzią jest to, że celem wdrożenia mikrosegmentacji jest ograniczenie promienia rażenia, jeśli atakujący naruszy zasób. Korzystając z mikrosegmentacji, możesz zastosować bardzo szczegółowe podejście do grupowania maszyn (takich jak pięć serwerów WWW w strefie DMZ, ale nie każdy system w strefie DMZ może się komunikować). Ta odpowiedź wykracza poza odpowiedź D, że mikrosegmentacja tworzy sieć „zerotrust", więc B jest lepszą i bardziej stosowną odpowiedzią.

5. A. Kontener zawiera aplikację i wymagane zależności (takie jak biblioteki). Maszyna wirtualna zawiera system operacyjny, aplikację i wszelkie zależności.

6. C. Najlepsza odpowiedź jest taka, że wielodostępność ma największy wpływ na głośne zabezpieczenia i z tego powodu dostawcy chmury muszą upewnić się, że mają bardzo ścisłą kontrolę nad możliwościami izolacji w środowisku. Chociaż inne odpowiedzi mają swoje zalety, żadna z nich nie jest najlepszą odpowiedzią.

7. A, C. Automatyczne skalowanie i przełączanie awaryjne to dwa najważniejsze atrybuty, jakie powinno mieć urządzenie wirtualne w środowisku chmury. Każde urządzenie może stać się pojedynczym punktem awarii i/lub wąskim gardłem wydajności, a te aspekty muszą być uwzględnione przez urządzenia wirtualne w środowisku chmury. Granularne uprawnienia są dobrą rzeczą, ale nie są specyficzne dla chmury. Na koniec, powiązanie z orkiestracją dostawcy byłoby świetne, ale to nie jest jedna z dwóch najlepszych odpowiedzi. Możesz myśleć, że elastyczność wiąże się z orkiestracją i masz rację. Jednak stopień integracji nie jest wymieniony. Jako przykład orkiestracji, czy urządzenie wirtualne ma możliwość zmiany zestawu reguł zapory na podstawie działań użytkownika w chmurze lub wywołania określonego interfejsu API? To jest typ orkiestracji, który byłby idealny, ale wymaga od dostawcy bardzo ścisłej integracji z określonym dostawcą. Ten typ orkiestracji jest zwykle natywny dla usług dostawcy (na przykład grupa zabezpieczeń może zostać automatycznie zmieniona na podstawie określonego działania).

8. C. Dostawca chmury powinien przyjąć podejście „odmów domyślnie" do bezpieczeństwa. Dlatego jest najbardziej prawdopodobne, że Wendy nie ma wyraźnego pozwolenia na uruchomienie instancji.

Chociaż możliwe jest, że Wendy jest również członkiem grupy, której wyraźnie odmówiono dostępu do uruchomienia instancji, lepszą odpowiedzią jest C. Uprawnienia metastruktury są całkowicie różne od uprawnień systemu operacyjnego, więc A i B są niepoprawnymi odpowiedziami.

9. A. SDN jest scentralizowane poprzez wyjęcie „mózgów" z podstawowego urządzenia sieciowego i umieszczenie tej funkcjonalności w kontrolerze SDN. Odpowiedź B jest prawdziwym stwierdzeniem, że północne interfejsy API pozwalają aplikacjom (lub oprogramowaniu, jeśli wolisz) na wprowadzanie zmian, ale nie odpowiada na postawione pytanie. Przypuszczam, że można argumentować, że C jest również prawdziwym stwierdzeniem, ale ponownie, nie odpowiada na postawione pytanie.

10. B. Należy ustalić, czy dostawca pozwala klientom na przeprowadzenie VA ich systemów. Jeśli tego nie robią i nie sprawdziłeś, możesz zostać zablokowany, ponieważ dostawca nie będzie znał źródła skanowania, które może pochodzić od złego aktora. Agent zainstalowany w strukturze aplikacji serwera będzie działał niezależnie od tego, czy serwer jest wirtualny w chmurze, czy fizycznym serwerem w centrum danych. Otwarcie wszystkich zapór sieciowych w celu wykonania VA, odpowiedź C, byłoby bardzo niefortunną decyzją, ponieważ może to otworzyć cały ruch na świecie, jeśli zostanie wykonane nieprawidłowo (na przykład dowolny adres IP w Internecie może mieć dostęp do dowolnego portu na instancji). Wreszcie, jest bardzo mało prawdopodobne, że uzyskasz dostęp do centrum danych dostawcy, a co dopiero otrzymasz pozwolenie na uruchomienie VA na dowolnym sprzęcie należącym do dostawcy i zarządzanym przez niego.

Wirtualizacja i kontenery

1. Dlaczego dostawca musi szyfrować dyski twarde na poziomie fizycznym?

A. Zapobiega to naruszeniu danych w wyniku kradzieży.

B. Zapobiega dostępowi do danych przez innych za pośrednictwem warstwy wirtualnej.

C. Zapobiega naruszeniu danych po wymianie dysku.

D. Odpowiedzi A i C są poprawne.

2. W jaki sposób kontenery zapewniają izolację?

A. Zapewniają izolację warstwy aplikacji.

B. Zapewniają izolację na wszystkich warstwach, tak jak robi to maszyna wirtualna.

C. Zapewniają izolację repozytorium.

D. Wszystkie powyższe odpowiedzi są poprawne.

3. Który z poniższych elementów jest najważniejszym priorytetem bezpieczeństwa dla dostawcy usług w chmurze?

A. Wdrażanie zapór SDN dla klientów

B. Izolowanie dostępu dzierżawców do puli zasobów

C. Zabezpieczanie obwodu sieciowego

D. Oferowanie klientom możliwości monitorowania sieci

4. Które z poniższych elementów są przykładami wirtualizacji obliczeniowej?

A. Kontenery

B. Sieci nakładkowe w chmurze

C. Szablony oprogramowania

D. A i C

5. Nathan próbuje rozwiązać problem z narzędziem do przechwytywania pakietów na działającej instancji. Zauważa nazwy użytkowników FTP w postaci zwykłego tekstu i hasła w przechwyconym ruchu sieciowym przeznaczonym dla komputera innego dzierżawcy. Co powinien zrobić Nathan?

A. To normalne zachowanie w chmurze. Powinien skontaktować się z innym dzierżawcą i poinformować go, że używanie poświadczeń w postaci zwykłego tekstu w chmurze to zły pomysł.

B. Nathan powinien skontaktować się z innym dzierżawcą i przesłać swoje ustalenia w celu uzyskania nagrody za błędy.

C. Nie jest to możliwe, ponieważ FTP jest zabronione w środowisku chmury.

D. Powinien skontaktować się z dostawcą i poinformować go, że anuluje korzystanie z jego usług w chmurze, ponieważ dostawca nie odizolował sieci.

6. Jakie są zalety sieci wirtualnej w porównaniu z sieciami fizycznymi?

A. Można podzielić stosy aplikacji na oddzielne, odizolowane sieci wirtualne, co zwiększa bezpieczeństwo.

B. Całą wirtualną siecią można zarządzać z jednej płaszczyzny zarządzania.

C. Filtrowanie sieci w sieci fizycznej jest łatwiejsze.

D. Wszystkie powyższe stwierdzenia są prawdziwe.

7. Jak tworzony jest zbiór pamięci masowej?

A. Dostawca używa bezpośredniego zbioru pamięci masowej z wieloma dyskami twardymi podłączonymi do serwera.

B. Dostawca używa sieci obszaru pamięci masowej.

C. Dostawca używa NAS.

D. Dostawca tworzy zbiór pamięci masowej w dowolny sposób.

8. Dostawca chce mieć pewność, że dane klienta nie zostaną utracone w przypadku awarii dysku. Co powinien zrobić dostawca?

A. Użyć sieci SAN i skopiować dane na wiele dysków w kontrolerze pamięci masowej.

B. Replikować dane do zagranicznej strony trzeciej.

C. Utworzyć wiele kopii danych i przechowywać je w wielu lokalizacjach pamięci masowej.

D. Przechowywać dane klienta przy użyciu dysków SSD.

9. Dlaczego pamięć ulotna stanowi problem bezpieczeństwa dla dostawców?

A. Nie stanowi. Ochrona pamięci ulotnej jest odpowiedzialnością klienta.

B. Pamięć ulotna może zawierać niezaszyfrowane informacje.

C. Pamięć ulotna może zawierać poświadczenia.

D. B i C są poprawne.

10. Które z poniższych komponentów w środowisku kontenerowym wymagają kontroli dostępu i silnego uwierzytelniania?

A. Środowisko wykonawcze kontenera

B. System orkiestracji i planowania

C. Repozytorium obrazów

D. Wszystkie powyższe

1. D. Odpowiedzi A i C są poprawne. Dostawcy szyfrują dyski twarde, aby nie można było odczytać danych, jeśli dysk zostanie skradziony lub wymieniony. Szyfrowanie na poziomie fizycznym nie chroni danych żądanych za pośrednictwem warstwy wirtualnej.

2. A. Kontenery zapewniają izolację tylko na poziomie aplikacji. Jest to odmienne od maszyny wirtualnej, która może zapewnić izolację dla wszystkich warstw. Repozytoria wymagają wdrożenia odpowiednich kontroli w celu ograniczenia nieautoryzowanego dostępu do kodu i plików konfiguracyjnych przechowywanych w nich.

3. B. Najważniejszym priorytetem dostawców jest zapewnienie, że wdrożą silne możliwości izolacji. Wszystkie pozostałe odpowiedzi są możliwymi priorytetami, ale odpowiedź B jest najlepsza.

4. A. Z przedstawionej listy tylko kontenery można uznać za wirtualizację obliczeniową. Szablony oprogramowania służą do szybkiego budowania całego środowiska. Chociaż można użyć tych szablonów w infrastrukturze jako kod (IaC) do budowania lub wdrażania kontenerów i maszyn wirtualnych, nie jest to uważane za wirtualizację obliczeniową. Sieć nakładkowa w chmurze umożliwia sieci wirtualnej obejmowanie wielu sieci fizycznych.

5. D. Nathan widzi ruch sieciowy przeznaczony dla innych maszyn, więc nastąpiła awaria izolacji sieciowej, a to powinno być najwyższym priorytetem bezpieczeństwa dostawcy. Gdybym był Nathanem, zmieniłbym dostawcę chmury tak szybko, jak to możliwe. Wszystkie pozostałe odpowiedzi nie mają zastosowania (chociaż zapisanie wielu zrzutów ekranu do katalogu FTP innego dzierżawcy, aby poinformować go o narażeniu, byłoby dość zabawne).

6. A. Jedyną prawidłową odpowiedzią jest to, że sieci wirtualne można podzielić na sekcje, co może zwiększyć bezpieczeństwo; jest to kosztowne, jeśli nie niemożliwe, w sieci fizycznej. SDN może oferować jedną płaszczyznę zarządzania dla fizycznych urządzeń sieciowych, a „łatwość" filtrowania jest dość subiektywna. Filtrowanie w sieci wirtualnej jest inne, ale może być trudniejsze lub nie.

7. D. To całkowicie zależy od dostawcy, w jaki sposób zbuduje pulę pamięci masowej. Może użyć dowolnej z innych technologii wymienionych w odpowiedziach lub może użyć czegoś zupełnie innego i zastrzeżonego.

8. C. Aby zapewnić większą odporność, dostawca powinien wykonać wiele kopii danych klienta i przechowywać je w wielu lokalizacjach pamięci masowej. Odpowiedź A wygląda dobrze, ale nie jest

najlepsza, ponieważ SAN nie jest wymagany, a co ważniejsze, zapisywanie danych na wielu dyskach w tym samym kontrolerze nie ochroni przed pojedynczym punktem awarii w kontrolerze (lub uszkodzeniem danych przez kontroler). Na koniec, nie omówiliśmy różnicy między „zwykłymi" dyskami magnetycznymi a dyskami półprzewodnikowymi, ale dyski SSD mogą ulec awarii tak jak dyski magnetyczne, więc odpowiedź D również nie jest najlepszą odpowiedzią.

9. D. Prawidłowa odpowiedź brzmi, że pamięć ulotna może zawierać poufne informacje, takie jak dane uwierzytelniające i dane, które muszą być niezaszyfrowane, aby mogły zostać przetworzone. Zarówno dostawca, jak i klient odgrywają rolę w zapewnianiu bezpieczeństwa związanego z pamięcią ulotną. Dostawca musi zapewnić, że pamięć ulotna jednego dzierżawcy nigdy nie będzie widoczna dla innego dzierżawcy (jeszcze lepszym sposobem by o tym pomyśleć jest to, że jedno obciążenie nie powinno mieć dostępu do innego obciążenia). Klient musi się upewnić, że pamięć ulotna zostanie wyczyszczona z systemu przed utworzeniem obrazu. Można to osiągnąć, ponownie uruchamiając instancję przed utworzeniem obrazu.

10. D. Tak, tym razem wszystko powyższe jest właściwym wyborem. Ale czekaj! Jest tu dobra historia, którą dołączam dla tych z was, którzy nadal ze mną są. W lutym 2018 r. Tesla (firma samochodowa) została naruszona. Na szczęście dla Tesli atakujący chcieli wykorzystać zasoby chmury Tesli tylko do wydobywania bitcoinów. W jaki sposób Tesla została naruszona? Czy był to atak typu zero-day? Czy to byli zaawansowani agenci sponsorowani przez państwo? Nie! Jej oprogramowanie do koordynacji kontenerów (w tym przypadku Kubernetes) było dostępne z Internetu i nie wymagało hasła, aby uzyskać do niego dostęp! Dało to atakującym nie tylko możliwość uruchomienia własnych kontenerów, za które zapłacili Tesla, ale w systemie Kubernetes znajdował się obszar tajny, w którym przechowywane były klucze Amazon S3. Klucze te służyły do uzyskiwania dostępu do niepublicznych informacji z Tesli. Ponownie, bezpieczeństwo kontenerów obejmuje znacznie więcej niż tylko bezpieczeństwo aplikacji w kontenerze.

Reagowanie na incydenty

1. Który obszar reagowania na incydenty jest najbardziej dotknięty automatyzacją działań?

A. Przygotowanie

B. Wykrywanie

C. Ograniczanie, likwidacja i odzyskiwanie

D. Po incydencie

2. Co należy zrobić w pierwszej kolejności po zbadaniu potencjalnego incydentu?

A. Należy pobrać dane uwierzytelniające konta głównego i użyć ich do przeprowadzenia dochodzenia w metastrukturze, aby upewnić się, że atakujący nie znajduje się już w płaszczyźnie zarządzania.

B. Należy wylogować się z każdego konta i zresetować jego hasła.

C. Należy zakończyć działanie każdego serwera.

D. Należy wykonać migawki każdej instancji za pomocą interfejsów API.

3. W jaki sposób można szybko poddać kwarantannie instancję serwera w środowisku IaaS?

A. Wykonać migawkę.

B. Zalogować się do instancji serwera i wyłączyć wszystkie konta użytkowników.

C. „Wstrzymać” instancję, jeśli dostawca zezwala na takie działanie.

D. Zmienić zestaw reguł wirtualnej zapory sieciowej, aby zezwolić na dostęp tylko ze stacji roboczej śledczego.

4. Które z poniższych jest kwestią dotyczącą danych dziennika dostarczonych przez dostawcę?

A. Spełni wymagania prawne dotyczące łańcucha dostaw.

B. Jest w formacie, który może być używany przez klientów.

C. Jest dostarczany w odpowiednim czasie w celu wsparcia dochodzenia.

D. A i B są poprawne.

5. Jak często należy testować plany reagowania na incydenty?

A. Rocznie

B. Miesięcznie

C. Kwartalnie

D. W ramach należytej staranności przed użyciem systemu w produkcji

6. Do której fazy zalicza się proaktywne skanowanie i monitorowanie sieci, oceny podatności i przeprowadzanie ocen ryzyka?

A. Przygotowanie

B. Wykrywanie

C. Ograniczanie, eliminacja i odzyskiwanie

D. Po incydencie

7. Jakie są najważniejsze aspekty reagowania na incydenty w środowisku chmury?

A. Uzyskiwanie wirtualnych narzędzi do badania serwerów wirtualnych

B. Szkolenie personelu reagującego na incydenty

C. Ustalanie umów o poziomie usług i ustalanie ról i obowiązków

D. Wszystkie powyższe

8. Jaki jest cel „mapy stosu aplikacji”? A. Aby zrozumieć różne systemy używane jako część aplikacji

B. Aby zrozumieć, gdzie będą przechowywane dane

C. Aby zrozumieć języki programowania używane w aplikacji

D. Aby zrozumieć różne zależności związane z aplikacją

9. Czym jest zestaw do skoku w chmurze?

A. Posiadanie zaktualizowanego CV gotowego na wypadek RGE (zdarzenia generującego wznowienie)

B. Zestaw z wymaganymi kablami, złączami i dyskami twardymi gotowy do przeprowadzenia dochodzenia na serwerze fizycznym

C. Zbiór narzędzi potrzebnych do przeprowadzania dochodzeń w zdalnej lokalizacji

D. Procedury, których należy przestrzegać podczas przekazywania dochodzenia dostawcy

10. Czym może różnić się rejestrowanie w PaaS od rejestrowania w IaaS?

A. Dzienniki PaaS muszą być dostarczane przez dostawcę na żądanie.

B. Prawdopodobnie będzie potrzebne niestandardowe rejestrowanie na poziomie aplikacji.

C. Formaty dzienników PaaS będą w formacie JSON i będą wymagały specjalnych narzędzi do odczytu.

D. Wszystkie powyższe są poprawne.

ODPOWIEDZI

1. C. Prawidłowa odpowiedź to powstrzymanie, wyeliminowanie i odzyskanie. Chociaż narzędzia dostarczane przez dostawcę chmury mogą również znacznie zwiększyć wykrywanie, narzędzia dostępne w środowisku chmury mają największy wpływ na działania związane z powstrzymaniem, wyeliminowaniem i odzyskaniem.

2. A. Badanie należy przeprowadzić przy użyciu konta głównego, aby zapewnić pełną widoczność wszystkich działań mających miejsce na płaszczyźnie zarządzania. Można wykonać migawki badanych serwerów, ale należy to zrobić dopiero po potwierdzeniu, że atakujący nie znajduje się już na płaszczyźnie zarządzania. Wylogowanie wszystkich może mieć ograniczone korzyści, ale ponownie potwierdzenie, że atakujący nie ma już dostępu do płaszczyzny zarządzania, jest pierwszym krokiem w reagowaniu na incydenty metastruktury. Zakończenie wszystkich instancji serwera nie jest wcale odpowiednią odpowiedzią.

3. D. Najlepszą odpowiedzią jest zmiana zestawu reguł wirtualnej zapory, aby zezwolić na dostęp tylko ze stacji roboczej badacza. Kroki w pozostałych odpowiedziach można wykonać po tym, jak atakujący nie będzie już mógł uzyskać dostępu do instancji serwera. 4. D. Prawidłowe odpowiedzi to A i B. Terminowy dostęp do danych dostarczonych przez dostawcę nie jest wymieniony w wytycznych.

5. A. Plany IR powinny być testowane co roku. Pamiętaj jednak, że wytyczne CSA wyraźnie stanowią, że testy powinny być przeprowadzane corocznie lub gdy wprowadzane są znaczące zmiany. Pamiętaj o obu, gdy będziesz zdawać egzamin.

6. A. Proaktywne skanowanie i monitorowanie sieci, oceny podatności i przeprowadzanie ocen ryzyka znajdują się w fazie przygotowawczej w wytycznych CSA.

7. C. Tak, wszystkie wpisy są ważne, ale pytanie wyraźnie określa, który jest (są) najważniejszy. Wytyczne CSA stanowią, że „umowy SLA i ustalanie oczekiwań dotyczących tego, co robi klient, a co robi dostawca, są najważniejszymi aspektami reagowania na incydenty w przypadku zasobów w chmurze”. Musisz to zrobić, zanim będziesz mógł pracować nad narzędziami i szkoleniem osób.

8. B. Najlepszą odpowiedzią jest to, że można wdrożyć mapę stosu aplikacji, aby zrozumieć, gdzie będą przechowywane dane. Oprócz wiedzy o tym, gdzie mogą znajdować się Twoje dane, pomoże to rozwiązać różnice geograficzne w monitorowaniu i przechwytywaniu danych.

9. C. Zestaw Cloud Jump to zbiór narzędzi wymaganych do przeprowadzania dochodzeń w zdalnych lokalizacjach (takich jak usługi w chmurze). To zestaw „wirtualnych narzędzi do wirtualnego świata", jeśli wolisz. Oczywiście, jeśli masz incydent w środowisku chmury i dopiero wtedy zdajesz sobie sprawę, że brakuje Ci wirtualnych narzędzi i wiedzy na ich temat, jest to najprawdopodobniej wydarzenie generujące CV. Jeśli dostawca przejmie dochodzenie po swojej stronie, prawdopodobnie będzie używał własnych narzędzi dochodzeniowych.

10. B. PaaS (i architektury aplikacji bezserwerowych) prawdopodobnie będą wymagały niestandardowego rejestrowania na poziomie aplikacji, ponieważ prawdopodobnie będą występować luki w tym, co oferuje dostawca, a co jest wymagane do obsługi reagowania na incydenty. Dostawcy PaaS mogą mieć bardziej szczegółowe dzienniki, ale będziesz musiał określić, kiedy dostawca może je udostępnić. Na koniec, chociaż format danych ma znaczenie, JSON jest łatwy do odczytania i nie wymaga specjalnych narzędzi.

Bezpieczeństwo aplikacji

1. Jakie szkolenia powinni odbyć członkowie zespołu ds. bezpieczeństwa przed opracowaniem aplikacji w chmurze?

A. Szkolenie w chmurze niezależne od dostawcy

B. Szkolenie specyficzne dla dostawcy

C. Szkolenie z narzędzi programistycznych

D. A i B

2. Tristan został właśnie zatrudniony na stanowisku dyrektora ds. informatyki w firmie. Jego pierwszym pożądanym działaniem jest wdrożenie DevOps. Na którym z poniższych elementów Tristan powinien się skupić w pierwszej kolejności w ramach DevOps?

A. Wybór odpowiedniego serwera ciągłej integracji

B. Wybór projektu proof-of-concept, który będzie pierwszym zastosowaniem DevOps

C. Zrozumienie istniejącej kultury korporacyjnej i uzyskanie akceptacji kierownictwa

D. Wybór odpowiedniej usługi w chmurze dla DevOps

3. Jakie jest pierwsze działanie, które należy podjąć, planując ocenę podatności?

A. Określ zakres oceny podatności.

B. Określ platformę, która zostanie przetestowana.

C. Określ, czy dostawca musi zostać powiadomiony przed oceną.

D. Określ, czy ocena będzie wykonywana jako osoba z zewnątrz, czy na instancji serwera używanej przez działającą aplikację.

4. Lepsze oddzielenie płaszczyzny zarządzania można uzyskać, wykonując którą z poniższych czynności?

A. Uruchom wszystkie aplikacje w PaaS.

B. Uruchom aplikacje na ich własnym koncie w chmurze.

C. Wykorzystaj DevOps.

D. Użyj niezmiennych obciążeń.

5. W jaki sposób można zwiększyć bezpieczeństwo w niezmiennym środowisku?

A. Wyłączając zdalne logowanie

B. Wdrażając zabezpieczenia sterowane zdarzeniami

C. Wykorzystując przetwarzanie bezserwerowe, jeśli jest oferowane przez dostawcę

D. Zwiększając częstotliwość ocen podatności

6. Które z poniższych stwierdzeń CI/CD jest fałszywe?

A. Testy bezpieczeństwa można zautomatyzować.

B. System CI/CD może automatycznie generować dzienniki audytu.

C. System CI/CD zastępuje bieżące procesy zarządzania zmianami.

D. CI/CD wykorzystuje serwer ciągłej integracji.

7. W jaki sposób testy penetracyjne zmieniają się w wyniku chmury?

A. Tester penetracyjny musi rozumieć różne usługi dostawcy, które mogą być częścią aplikacji.

B. W większości przypadków wystąpienia serwera używane do uruchamiania aplikacji będą miały dostosowane jądra, których nikt poza dostawcą nie będzie w stanie zrozumieć.

C. Ze względu na charakter sieci wirtualnych testy penetracyjne musi wykonywać dostawca chmury.

D. Testy penetracyjne nie są możliwe w przypadku kontenerów, więc wiele wyników testów penetracyjnych będzie niejednoznacznych.

8. W której fazie SSDLC klienci powinni przeprowadzić modelowanie zagrożeń?

A. Projekt

B. Rozwój

C. Wdrożenie

D. Operacje

9. W której fazie SSDLC klienci powinni najpierw przeprowadzić testy penetracyjne?

A. Projekt

B. Rozwój

C. Wdrożenie

D. Operacje

10. Czym jest bezpieczeństwo oparte na zdarzeniach?

A. Kiedy dostawca zamknie usługę dla klientów w przypadku wykrycia ataku

B. Automatyzacja odpowiedzi w przypadku powiadomienia, zgodnie z ustaleniami dostawcy

C. Automatyzacja odpowiedzi w przypadku powiadomienia, zgodnie z ustaleniami klienta

D. Automatyczne powiadomienie administratora systemu o wykonywanej akcji

ODPOWIEDZI

1. D. Członkowie zespołu ds. bezpieczeństwa powinni odbyć zarówno szkolenie niezależne od dostawcy (takie jak CCSK), jak i szkolenie specyficzne dla dostawcy (są one również zalecane dla programistów i personelu operacyjnego). Narzędzia, które są specyficzne dla wdrożeń, nie są wymienione jako wymagane dla członków zespołu ds. bezpieczeństwa, tylko dla personelu operacyjnego i programistycznego.

2. C. Pamiętaj, że DevOps to kultura, a nie narzędzie ani technologia (chociaż usługa ciągłej integracji jest kluczowym elementem procesu CI/CD, który będzie wykorzystywany przez DevOps). Zrozumienie istniejącej kultury korporacyjnej i uzyskanie poparcia kierownictwa powinno być pierwszym krokiem Tristana we wdrażaniu DevOps na jego nowym stanowisku. DevOps nie jest technologią chmury.

3. C. Zawsze należy ustalić, czy dostawca musi zostać poinformowany o jakiejkolwiek ocenie z wyprzedzeniem. Jeśli dostawca wymaga wcześniejszego powiadomienia jako części warunków korzystania z usługi, niepoinformowanie go o ocenie może zostać uznane za naruszenie umowy. Odpowiedzi A i B to standardowe procedury w ramach oceny i muszą zostać wykonane niezależnie od chmury. Odpowiedź D jest interesująca, ponieważ nie masz gwarancji, że będziesz mieć nawet instancję serwera, do której możesz się zalogować w ramach oceny. Aplikacja może zostać zbudowana przy użyciu PaaS, bezserwerowej lub innej technologii zarządzanej przez dostawcę.

4. B. Uruchamianie aplikacji na ich własnych kontach w chmurze może prowadzić do ściślejszego podziału płaszczyzny zarządzania. Żadna z pozostałych odpowiedzi nie ma zastosowania do tego pytania.

5. A. Podczas korzystania z niezmiennych obciążeń bezpieczeństwo można zwiększyć, usuwając możliwość zdalnego logowania. Wszelkie zmiany muszą być wprowadzane centralnie w niezmiennych środowiskach. Monitorowanie integralności plików można również wdrożyć w celu zwiększenia bezpieczeństwa, ponieważ każda zmiana wprowadzona w niezmiennej instancji jest prawdopodobnym dowodem incydentu bezpieczeństwa.

6. C. Fałszywe stwierdzenie jest takie, że system CI/CD zastępuje bieżące procesy zarządzania zmianami. W rzeczywistości system CI/CD może zintegrować się z bieżącym systemem zarządzania zmianami. Wszystkie pozostałe stwierdzenia są prawdziwe.

7. A. Istnieje duże prawdopodobieństwo, że aplikacje będą korzystać z różnych usług dostawcy chmury. Sposób komunikacji między tymi usługami ma kluczowe znaczenie dla testera penetracyjnego, dlatego testy te powinni wykonywać wyłącznie testerzy z doświadczeniem na konkretnej platformie.

8. A. Modelowanie zagrożeń powinno być wykonywane w ramach fazy projektowania aplikacji, zanim w fazie rozwoju zostanie napisana choćby jedna linijka kodu.

9. C. Testy penetracyjne powinny być początkowo wykonywane w ramach fazy wdrażania SSDLC. Musisz mieć rzeczywistą aplikację, na której można wykonać testy penetracyjne, a testy te powinny być wykonywane przed uruchomieniem aplikacji w środowisku produkcyjnym. Oczywiście okresowe

testy penetracyjne są dobrą rzeczą w fazie operacyjnej, ale pojawia się pytanie, kiedy należy je wykonać po raz pierwszy.

10. C. Bezpieczeństwo oparte na zdarzeniach to implementacja zautomatyzowanych odpowiedzi na powiadomienia. Jest ono tworzone przez klienta, który często wykorzystuje jakąś formę monitorowania API. Jeśli używany jest API, spowoduje to uruchomienie przepływu pracy, który może obejmować zarówno wysłanie wiadomości do administratora systemu, jak i uruchomienie skryptu w celu automatycznego zajęcia się wystąpieniem (takiego jak cofnięcie zmiany, zmiana zestawów reguł wirtualnej zapory itd.).

Bezpieczeństwo danych i szyfrowanie

1. Co powinni oferować dostawcy SaaS, aby wymusić izolację wielodostępności?

A. Klucze zarządzane przez dostawcę

B. Szyfrowanie oparte na AES-256

C. Klucze dla każdego klienta

D. Moduł bezpieczeństwa sprzętowego zarządzany przez klienta

2. Jeśli Twoja organizacja musi się upewnić, że dane przechowywane w środowisku chmurowym nie będą dostępne bez zezwolenia przez nikogo, w tym dostawcę, co możesz zrobić?

A. Użyj lokalnego modułu HSM i zaimportuj wygenerowane klucze do systemu szyfrowania dostawcy jako klucz zarządzany przez klienta.

B. Użyj klucza szyfrowania opartego na zastrzeżonym algorytmie.

C. Nie przechowuj danych w środowisku chmurowym.

D. Użyj kluczy zarządzanych przez klienta, aby umożliwić szyfrowanie, mając jednocześnie pełną kontrolę nad samym kluczem.

3. Które z poniższych kontroli można wykorzystać do przekształcania danych w oparciu o osobę uzyskującą do nich dostęp?

A. Zarządzanie prawami przedsiębiorstwa

B. Dynamiczne maskowanie danych

C. Generowanie danych testowych

D. Zapobieganie utracie danych

4. Dlaczego dostawca SaaS wymagałby, aby klienci korzystali z szyfrowania dostarczanego przez dostawcę?

A. Dane zaszyfrowane przez klienta przed wysłaniem do aplikacji dostawcy mogą przerwać działanie.

B. Klucze zarządzane przez klienta nie istnieją w SaaS.

C. SaaS nie może używać szyfrowania, ponieważ przerywa ono działanie.

D. Wszystkie implementacje SaaS wymagają, aby wszyscy dzierżawcy używali tego samego klucza szyfrowania.

5. Który z poniższych typów pamięci masowej jest prezentowany jako system plików i jest zwykle dostępny za pośrednictwem interfejsów API lub interfejsu front-end?

A. Pamięć masowa obiektów

B. Pamięć masowa woluminów

C. Pamięć masowa bazy danych

D. Pamięć masowa aplikacji/platformy

6. Który z poniższych elementów należy uznać za podstawową kontrolę bezpieczeństwa?

A. Szyfrowanie

B. Rejestrowanie

C. Ograniczenia dotyczące rezydencji danych

D. Kontrola dostępu

7. Który z poniższych modeli wdrażania umożliwia klientowi pełną kontrolę nad zarządzaniem kluczami szyfrowania po wdrożeniu w środowisku chmurowym dostawcy?

A. Zarządzanie kluczami oparte na HSM/urządzeniu

B. Zarządzanie kluczami wirtualnego urządzenia/oprogramowania

C. Zarządzanie kluczami zarządzane przez dostawcę

D. Zarządzanie kluczami zarządzane przez klienta

8. Które z poniższych kontroli bezpieczeństwa są wymienione przez branżę kart płatniczych jako forma ochrony danych kart kredytowych?

A. Tokenizacja

B. Klucze zarządzane przez dostawcę

C. Dynamiczne maskowanie danych

D. Zarządzanie prawami przedsiębiorstwa

9. Które z poniższych jest głównym czynnikiem różnicującym filtrowanie adresów URL i CASB?

A. DLP

B. DRM

C. ERM

D. Możliwość blokowania dostępu na podstawie białych list i czarnych list

10. Które z poniższych NIE jest głównym składnikiem przy rozważaniu kontroli bezpieczeństwa danych w środowiskach chmurowych?

A. Kontrolowanie danych, których wysyłanie do chmury jest dozwolone

B. Ochrona i zarządzanie bezpieczeństwem danych w chmurze

c. Przeprowadzanie oceny ryzyka potencjalnych dostawców chmury

D. Wymuszanie zarządzania cyklem życia informacji

ODPOWIEDZI

1. C. Dostawcom SaaS zaleca się wdrażanie kluczy per-customer, kiedy tylko jest to możliwe, aby zapewnić lepsze egzekwowanie izolacji multitenancy.

2. C. Jedyną opcją jest niekorzystanie z chmury. Jeśli dane są szyfrowane lokalnie, a następnie kopiowane do chmury, uniemożliwi to również dostawcy odszyfrowanie danych, jeśli zostanie do tego zmuszony przez organy prawne. Zasadniczo nie zaleca się tworzenia własnych algorytmów szyfrowania, a prawdopodobnie i tak nie będą one działać w środowisku dostawcy.

3. B. Tylko dynamiczne maskowanie danych przekształci dane w locie za pomocą urządzenia, takiego jak serwer proxy, którego można użyć do ograniczenia prezentacji rzeczywistych danych na podstawie użytkownika uzyskującego do nich dostęp. Generowanie danych testowych wymaga, aby dane były eksportowane i przekształcane dla każdego użytkownika uzyskującego dostęp do skopiowanej bazy danych. Żadna z pozostałych odpowiedzi nie ma zastosowania.

4. A. Jeśli klient szyfruje dane przed wysłaniem ich do dostawcy SaaS, może to mieć wpływ na funkcjonalność. Dostawcy SaaS powinni oferować klucze zarządzane przez klienta w celu zwiększenia izolacji multitenancy.

5. A. Obiektowe przechowywanie jest prezentowane jak system plików i jest zwykle dostępne za pośrednictwem interfejsów API lub interfejsu front-end. Pozostałe odpowiedzi są niepoprawne.

6. D. Kontrola dostępu jest zawsze Twoją najważniejszą kontrolą bezpieczeństwa.

7. B. Jedyną opcją dla systemu zarządzania kluczami szyfrowania w środowisku chmury jest wdrożenie maszyny wirtualnej lub oprogramowania uruchomionego na maszynie wirtualnej, którą zarządza klient.

8. A. Tokenizacja to kontrola, którą branża kart płatniczych wymienia jako opcję ochrony danych kart kredytowych.

9. A. Główną różnicą między filtrowaniem adresów URL a CASB jest to, że w przeciwieństwie do tradycyjnego umieszczania nazw domen na białej lub czarnej liście, CASB może używać DLP podczas wykonywania inspekcji połączeń SaaS.

10. C. Chociaż ocena ryzyka dostawców chmury ma kluczowe znaczenie, ta czynność nie jest kontrolą bezpieczeństwa danych.

Zarządzanie tożsamością, uprawnieniami i dostępem

1. Który z poniższych jest przykładem atrybutu, którego można użyć z ABAC?

A. Jeśli użytkownik zalogował się za pomocą MFA

B. Dane biometryczne

C. Status uwierzytelnienia biometrycznego

D. A i C

2. Dlaczego zawsze należy brać pod uwagę uwierzytelnianie wieloczynnikowe?

A. Jest to najlepsza praktyka zgodnie z wytycznymi CSA.

B. Do usług w chmurze może uzyskać dostęp każdy, kto korzysta z przeglądarki internetowej.

C. Usługi w chmurze mają podstawową cechę szerokiego dostępu do sieci.

D. MFA nie jest zalecane, ponieważ użytkownicy, którzy zgubią swoje telefony, będą musieli ręcznie zresetować swoje konta.

3. Który z poniższych jest najlepszym protokołem federacyjnym do wdrożenia i obsługi?

A. SAML

B. OAuth

C. OpenID

D. Nie ma najlepszego protokołu. Przed wyborem protokołu należy określić przypadki użycia i ograniczenia.

4. Jakie jest wiarygodne źródło tożsamości?

A. System, z którego propagowane są tożsamości

B. System HR

C. System usług katalogowych

D. System IAM dostawcy chmury

5. Podczas tworzenia tożsamości federacyjnej z dostawcą IaaS, która strona jest stroną polegającą, a która dostawcą tożsamości?

A. Organizacja jest stroną polegającą, a dostawca IaaS jest dostawcą tożsamości.

B. Organizacja jest dostawcą tożsamości, a dostawca IaaS jest stroną polegającą.

C. Organizacja jest zarówno dostawcą tożsamości, jak i stroną polegającą, ponieważ jest zależna od dostawcy chmury w zakresie wdrażania federacji.

D. Dostawca chmury jest zarówno dostawcą tożsamości, jak i stroną polegającą w modelu federacyjnym.

6. Który standard wykorzystuje koncepcje punktów decyzyjnych polityki (PDP) i punktów egzekwowania polityki (PEP)?

A. SAML

B. OAuth

C. XACML

D. SCIM

7. Jaka jest różnica między tożsamością a personą?

A. Twoja tożsamość to Twoja nazwa użytkownika; twoja persona to grupa, której jesteś członkiem.

B. Twoja tożsamość to twoja nazwa użytkownika; twoja persona to twoja tożsamość i wszystkie inne atrybuty powiązane z tobą w określonej sytuacji.

C. Twoja tożsamość jest używana do autoryzacji; twoja persona jest używana do uwierzytelnienia ciebie.

D. Twoja tożsamość jest używana do uwierzytelnienia ciebie; twoja persona jest używana do autoryzacji ciebie.

8. Czym jest rola?

A. Rola jest częścią federacji. To sposób, w jaki członkostwo twojej grupy w twojej firmie otrzymuje uprawnienia u twojego dostawcy IaaS.

B. Rola to praca, którą wykonujesz w pracy.

C. Rola to tymczasowe poświadczenie, które jest dziedziczone przez system w środowisku chmury.

D. Wszystkie powyższe odpowiedzi są poprawne.

9. Który z poniższych czynników jest czynnikiem w uwierzytelnianiu wieloskładnikowym?

A. Tajny uścisk dłoni

B. Kolor twoich oczu

C. Jednorazowe hasło

D. Wszystkie powyższe

10. Który z poniższych protokołów jest oparty na XML i obsługuje zarówno uwierzytelnianie, jak i autoryzację?

A. SAML

B. OAuth

C. OpenID

D. SCIM

ODPOWIEDZI

1. D. Wszystko o użytkowniku i jego połączeniu można wykorzystać jako atrybut do określenia kontroli dostępu. Jednak w modelu biometrycznym rzeczywiste dane biometryczne są przechowywane w samym urządzeniu. Fakt, że wykorzystano dane biometryczne, jest atrybutem, który można wykorzystać.

2. C. Usługi w chmurze mają zasadniczą cechę szerokiego dostępu do sieci. Jest to podobne do faktu, że można uzyskać do niego dostęp za pomocą dowolnej przeglądarki (B), ale C jest lepszą odpowiedzią, ponieważ nie każdy dostęp do usługi w chmurze zawsze będzie wymagał przeglądarki internetowej. Oczywiście wdrożenie MFA jest najlepszą praktyką CSA, ale samo to nie jest powodem, dla którego powinno zostać wdrożone. Podczas gdy utrata telefonu komórkowego z urządzeniem MFA z tokenem programowym prawdopodobnie będzie wymagała ręcznego wysiłku w celu zresetowania ustawień MFA, nie jest to uzasadniony powód, aby unikać korzystania z MFA, szczególnie w przypadku kont uprzywilejowanych.

3. D. Nie ma protokołu „magicznej kuli" dla federacji. Zawsze należy rozważyć swoje wymagania w oparciu o przypadki użycia i ograniczenia.

4. A. Autorytatywnym źródłem tożsamości może być dowolny system. Jest to system, w którym konta użytkowników są tworzone, a następnie propagowane do innych. W niektórych środowiskach może to być serwer katalogowy, a w innych system HR. Nigdy nie chcesz, aby usługa w chmurze, z którą tworzysz łącze federacyjne, była autorytatywnym źródłem lub dostawcą tożsamości.

5. B. Organizacja jest dostawcą tożsamości, a dostawca IaaS jest stroną polegającą. Zawsze chcesz zachować rolę dostawcy tożsamości podczas ustanawiania federacji.

6. C. XACML wykorzystuje koncepcje decyzji polityki i punktów egzekwowania polityki. XACML jest używany do bardziej szczegółowych decyzji dotyczących kontroli dostępu i może współpracować z SAML lub OAuth. Implementacje XACML są rzadkie.

7. B. Twoja tożsamość to Twoja nazwa użytkownika, a Twoja persona to Twoja tożsamość i wszystkie inne atrybuty w określonej sytuacji.

8. D. Wszystkie odpowiedzi są poprawne. Dlatego CSA Guidance mówi, że „rola to mylący i nadużywany termin używany na wiele sposobów".

9. D. Czynniki to coś, co wiesz (tajny uścisk dłoni), coś, co masz (jednorazowe hasło) i coś, czym jesteś (kolor oczu). Czy mają one sens z technicznego punktu widzenia? Prawdopodobnie nie, ale spełniają kryteria trzech czynników tak czy inaczej.

10. A. SAML jest oparty na XML i obsługuje zarówno uwierzytelnianie, jak i autoryzację. OAuth zajmuje się tylko „AuthOrization" (sztuczka pamięci), a OpenID zajmuje się tylko uwierzytelnianiem. SCIM jest językiem provisioningu.

Bezpieczeństwo jako usługa

1. Które z poniższych rozwiązań SecaaS można wykorzystać do inspekcji ruchu HTTP i zatrzymania ataków DDoS?

A. BC/DR

B. WAF

C. CASB

D. Filtrowanie sieci

2. Które z poniższych rozwiązań SecaaS można wykorzystać do egzekwowania zasad przy użyciu systemów innej osoby?

A. WAF

B. Filtrowanie sieci

C. Bezpieczeństwo poczty e-mail

D. Wszystkie powyższe

3. Zwracasz się do dostawcy SecaaS z prośbą o eksport danych dziennika filtrowania sieci. Informuje on, że możesz uzyskać dostęp do danych tylko za pomocą jego narzędzi. Jaki jest w tym problem?

A. Może to być scenariusz blokady.

B. Musisz mieć możliwość eksportowania danych w formacie CSV do celów analitycznych.

C. Danych nie można wczytać do SIEM.

D. Wszystkie powyższe są poprawne.

4. Jakie kryteria musi spełniać SecaaS?

A. Musi mieć produkt lub usługę bezpieczeństwa dostarczoną jako usługa w chmurze

B. Musi mieć raport SOC 2 i/lub certyfikat ISO/IEC 27001

C. Musi spełniać podstawowe cechy przetwarzania w chmurze

D. A i C

5. Co NIE jest wymienione jako korzyść SecaaS?

A. Izolacja klientów

B. Oszczędności kosztów

C. Elastyczność wdrażania

D. Udostępnianie informacji

6. Które z poniższych najlepiej definiuje IDS/IPS SecaaS?

A. Lokalni agenci są instalowani na stacjach roboczych.

B. Lokalni agenci są instalowani na serwerach.

C. Agenci przekazują dane do dostawcy chmury zamiast do lokalnych serwerów.

D. Wszystkie powyższe odpowiedzi są poprawne.

7. Co można wykonać za pomocą oceny bezpieczeństwa SecaaS?

A. Tradycyjna ocena sieci

B. Ocena instancji serwera w chmurze

C. Ocena aplikacji

D. Wszystkie powyższe odpowiedzi

8. Co robi rozwiązanie SecaaS bramy bezpieczeństwa sieci?

A. Kontroluje ruch sieciowy

B. Ogranicza witryny internetowe, do których użytkownicy mają dostęp

C. Szyfruje połączenia

D. A i B

9. Co NIE jest wadą SecaaS?

A. Brak wielodostępności

B. Obsługa regulowanych danych

C. Migracja do SecaaS

D. Brak widoczności

10. Jak można przyspieszyć transfery danych podczas korzystania z BC/DR SecaaS?

A. Korzystanie z kompresji dostarczanej przez dostawcę

B. Implementacja lokalnego urządzenia bramy

C. Korzystanie z technik deduplikacji dostarczanych przez dostawcę

D. A i C

ODPOWIEDZI

1. B. Zapory aplikacji internetowych (WAF) mogą sprawdzać ruch sieciowy na warstwie 7 i w rezultacie rozumieć ruch HTTP.

2. D. Wszystkie powyższe odpowiedzi są prawidłowe. SecaaS zazwyczaj umożliwia egzekwowanie zasad za pomocą systemów dostawcy.

3. A. Jeśli dostawca zmusza Cię do korzystania z jego platformy w celu odczytu danych dziennika, prawdopodobnie doprowadzi to do scenariusza blokady. Będziesz musiał utrzymywać relację, aby uzyskać dostęp do danych, które prawdopodobnie będą potrzebne do wykazania zgodności i/lub spełnienia wymogów prawnych. Pozostałe odpowiedzi mogą być prawdziwe lub nie.

4. D. Aby usługa SecaaS była uważana za usługę, dostawca musi mieć produkt lub usługę bezpieczeństwa dostarczoną jako usługa w chmurze i musi spełniać podstawowe cechy chmury. SOC lub ISO/IEC nie jest wymienione jako wymóg.

5. B. Tak, to trudna odpowiedź. Należy zauważyć, że korzyść „kosztowa” nie oznacza, że zaoszczędzisz pieniądze, korzystając z usługi SecaaS. Oznacza ona, że możesz „płacić w miarę rozwoju”. Czy to oznacza, że SecaaS jest tańszy? Niekoniecznie. W rzeczywistości może być droższy niż wewnętrzne systemy, z których korzystasz obecnie.

6. C. Systemy IDS/IPS pobierają dane od agentów i analizują takie dane w środowisku dostawcy.

7. D. Wszystkie wymienione czynności można wykonać w ramach oceny bezpieczeństwa SecaaS.

8. D. Bramy bezpieczeństwa sieci oferują kontrolę ochronną, która może sprawdzać ruch sieciowy pod kątem złośliwego oprogramowania i ograniczać witryny internetowe, do których użytkownicy mogą uzyskać dostęp. Nie wykonują szyfrowania.

9. A. Silna multitenancy to coś, co należy sprawdzić podczas przeprowadzania należytej staranności u dostawcy, ponieważ jej brak może powodować problemy, szczególnie jeśli dane innego dzierżawcy zostaną naruszone w wyniku żądania ediscovery wobec innego dzierżawcy.

10. B. Prawidłowa odpowiedź to zaimplementowanie lokalnego urządzenia bramy. Chociaż lokalna brama może przyspieszyć transfery danych, korzystając z innych technik, nie są one identyfikowane bezpośrednio.

Powiązane technologie

1. Czym jest przypinanie certyfikatu?

A. Instalowanie certyfikatu na urządzeniu mobilnym

B. Przechowywanie certyfikatu w otwartym rejestrze certyfikatów, który może być używany lub walidowany

C. Kojarzenie hosta z certyfikatem

D. Wszystkie powyższe

2. Gdzie należy wykonać szyfrowanie danych w systemie big data?

A. Pamięć podstawowa

B. Pamięć pośrednia

C. W pamięci

D. A i B

3. Do czego służy Spark w big data?

A. Spark to system plików do przechowywania big data.

B. Spark to moduł uczenia maszynowego.

C. Spark to moduł przetwarzania big data.

D. Spark służy do przechowywania big data.

4. Które z poniższych zdarzeń doprowadziło w przeszłości do problemów z bezpieczeństwem urządzeń IoT?

A. Osadzanie poświadczeń w urządzeniu

B. Brak szyfrowania

C. Brak mechanizmów aktualizacji dla urządzeń IoT

D. Wszystkie powyższe

5. Dlaczego macierze uprawnień mogą być skomplikowane podczas korzystania z nich w systemach big data?

A. Z implementacjami big data powiązanych jest wiele komponentów.

B. Kilka komponentów nie pozwala na szczegółowe uprawnienia.

C. Komponenty środowiska chmurowego są wykorzystywane jako część implementacji big data.

D. Prawidłowe są odpowiedzi A i C.

6. Jakie są typowe komponenty powiązane z systemem big data?

A. Rozproszone gromadzenie danych

B. Rozproszone przechowywanie danych

C. Rozproszone przetwarzanie danych

D. Wszystkie powyższe

7. Jakie są trzy V big data według CSA?

A. Duża prędkość, duża objętość, duża wariancja

B. Duża prędkość, duża objętość, duża różnorodność

C. Duża walidacja, duża objętość, duża różnorodność

D. Duża wartość, duża wariancja, duża prędkość

8. Które z poniższych nie jest uważane za platformę bezserwerową według CSA?

A. Moduł równoważenia obciążenia

B. Serwer DNS

C. Usługa powiadomień

D. Przechowywanie obiektów

9. Kiedy należy wykonać walidację danych wejściowych?

A. W przypadku korzystania z chmury jako zaplecza dla aplikacji mobilnych

B. W przypadku korzystania z chmury jako zaplecza dla urządzeń IoT

C. W przypadku korzystania z usług w chmurze w celu obsługi systemu big data

D. Wszystkie powyższe

10. Według CSA, jaki jest/są atrybut(y) chmury, które sprawiają, że idealnie nadaje się ona do obsługi aplikacji mobilnych?

A. Koszt uruchomienia wymaganej infrastruktury

B. Rozproszony geograficzny charakter chmury

C. Nieodłączne bezpieczeństwo związane z usługami w chmurze

D. B i C

ODPOWIEDZI

1. D. Przypinanie certyfikatu polega na skojarzeniu certyfikatu z hostem. Może to być przydatne, aby uniemożliwić atakującym korzystanie z serwera proxy w celu przeglądania niezaszyfrowanej aktywności sieciowej, która może zostać wykorzystana do identyfikacji luk w zabezpieczeniach. Żadna z pozostałych odpowiedzi nie jest prawidłowa.

2. D. Szyfrowanie (jeśli jest wymagane) dużych danych musi zostać wykonane we wszystkich lokalizacjach przechowywania, w tym w lokalizacjach podstawowych i pośrednich.

3. C. Spark to moduł przetwarzania dla Hadoop, który jest uważany za następną generację MapReduce. Chociaż Hadoop został omówiony tylko jako część tła dużych danych, jest on wyraźnie wymieniony w tekście głównym tej książki i wytycznych CSA jako moduł przetwarzania dużych danych.

4. D. Wszystkie wymienione odpowiedzi w przeszłości prowadziły do problemów z bezpieczeństwem urządzeń IoT.

5. D. CSA stwierdza, że macierze uprawnień mogą być skomplikowane zarówno przez liczbę komponentów w systemie dużych danych, jak i zasoby w chmurze, które mogą być wykorzystywane jako część implementacji dużych danych.

6. D. System big data składa się z rozproszonego gromadzenia, rozproszonego przechowywania i rozproszonego przetwarzania.

7. B. Trzy V to duża objętość, duża prędkość i duża różnorodność. Oznacza to, że system big data musi przetwarzać dużą objętość danych, które przychodzą z dużą szybkością i mogą być w wielu formatach (ustrukturyzowanych, nieustrukturyzowanych i strumieniowych).

8. B. Serwer DNS nie jest opcją bezserwerową według CSA. Poczekaj, ponieważ jest tu pewna lekcja do wyciągnięcia. Dostawcy mogą oferować klientom usługę DNS. Jednak nie o tym jest tutaj napisane. Poświęć trochę czasu na przeczytanie pytań na egzaminie, aby upewnić się, że nie zostaniesz oszukany przez sformułowania. Możesz absolutnie zbudować własny serwer DNS w środowisku IaaS lub możesz skorzystać z usługi DNS, jeśli dostawca ją oferuje. Inne możliwe odpowiedzi są wymienione jako platformy bezserwerowe.

9. D. Najlepszą praktyką bezpieczeństwa jest zawsze przeprowadzanie walidacji danych wejściowych dla każdego przychodzącego ruchu sieciowego. Obejmuje to wszystkie wymienione technologie.

10. B. Jedynym wymienionym atrybutem w wytycznych CSA dotyczących przydatności aplikacji mobilnych do chmury jest geograficzna natura chmury. Tak, środowisko chmury może być bezpieczniejsze, ale to jest oczywiście wspólna odpowiedzialność. Nigdy nie masz gwarancji, że działanie w chmurze będzie tańsze niż działanie systemów w Twoim własnym centrum danych.

ENISA Cloud Computing: Korzyści, zagrożenia i zalecenia dotyczące bezpieczeństwa informacji

1. Które z poniższych rozwiązań jest wymienione przez ENISA jako sposób, w jaki dostawcy SaaS lub PaaS chronią swoich klientów?

A. Dostawcy powinni mieć nadmiarowe miejsce do przechowywania danych.

B. Dostawcy powinni mieć umowę o powiernictwie kodu źródłowego.

C. Klienci powinni mieć umowy kontraktowe, w których wymienione są kary za utratę kodu.

D. Wszystkie powyższe odpowiedzi są poprawne.

2. Zgodnie z dokumentacją ENISA, które z poniższych rozwiązań można wykorzystać w IaaS w celu zapewnienia przenośności?

A. OVF

B. WAF

C. IAM

D. DAM

3. Dlaczego usuwanie danych jest uważane za największe ryzyko bezpieczeństwa według ENISA?

A. Ze względu na współdzielony charakter przechowywania danych

B. Ze względu na brak możliwości zweryfikowania, czy dane są odpowiednio usuwane

C. Ponieważ dyski SSD nie mogą niezawodnie usuwać danych

D. A i B

4. Które z poniższych rozwiązań nie jest przykładem uzależnienia od dostawcy?

A. Umowy z karami za rozwiązanie umowy

B. Dostawca eksportuje dane tylko w zastrzeżonym formacie

C. Niestandardowe aplikacje SaaS

D. Platformy PaaS, które ograniczają dostępne funkcje

5. Przeskakiwanie między maszynami wirtualnymi to atak, który jest możliwy w przypadku jakiej awarii?

A. Awaria kontroli pamięci masowej wirtualnej

B. Awaria segregacji hiperwizora

C. Awaria izolacji hiperwizora

D. Niewystarczające kontrole bezpieczeństwa przez klienta

6. Które z poniższych można uznać za złośliwego insidera zgodnie z „Najważniejszymi zagrożeniami bezpieczeństwa” ENISA?

A. Administrator klienta

B. Audytor dostawcy

C. Audytor klienta

D. Wszystkie powyższe

7. Administrator firmy ustala, że najlepszym podejściem do radzenia sobie z nagłymi wzrostami ruchu sieciowego jest utworzenie grupy skalowania automatycznego, która utworzy nieograniczoną liczbę

serwerów internetowych w celu zaspokojenia zwiększonego zapotrzebowania. Co utworzył administrator?

A. Administrator wdrożył praktykę skalowania automatycznego, która jest powszechnie stosowana w celu wykorzystania elastycznej natury chmury.

B. Administrator wdrożył system równoważenia obciążenia aplikacji.

C. Administrator wdrożył system równoważenia obciążenia sieci.

D. Administrator utworzył scenariusz ekonomicznej odmowy usługi na wypadek ataku odmowy usługi na firmę.

8. Które z poniższych nie jest uważane za lukę związaną z ryzykiem utraty reputacji firmy z powodu działań współnajemców?

A. Brak izolacji zasobów

B. Brak izolacji reputacji

C. Luki w zabezpieczeniach hiperwizora

D. Przechowywanie obiektów

9. Które z poniższych nie jest wymienione w dokumentacji ENISA jako potencjalny obszar, który należy rozważyć i chronić przed wykorzystaniem w odniesieniu do provisioningu użytkowników?

A. Poświadczenia, które mogą być podatne na przechwycenie i odtworzenie

B. Jeśli klient nie może kontrolować procesu provisioningu dostawcy

C. Jeśli tożsamość klienta może nie zostać odpowiednio zweryfikowana podczas rejestracji

D. Możliwość klienta ograniczenia dostępu do systemu IAM dostarczonego przez dostawcę do określonego zakresu adresów IP

10. Co zawsze należy zrobić, aby chronić się przed możliwym naruszeniem interfejsu zarządzania, gdy atakujący uzyska dostęp do środowiska chmury (wybierz najlepszą odpowiedź)?

A. Połącz się z interfejsem zarządzania za pośrednictwem sieci VPN IPSec.

B. Chroń połączenia za pomocą protokołu TLS.

C. Wdróż uwierzytelnianie wieloskładnikowe na wszystkich kontach uprzywilejowanych.

D. Utwórz oddzielne konta dla administratorów z dostępem do płaszczyzny zarządzania.

ODPOWIEDZI

1. B. Aby mieć pewność, że oprogramowanie SaaS lub PaaS nie zostanie osierocone lub porzucone w przypadku awarii dostawcy, klienci powinni upewnić się, że dostawcy mają umowę o powiernictwie kodu z zewnętrznym agentem powierniczym. Chociaż inne odpowiedzi są dobrymi pomysłami na ochronę klientów, w dokumentacji ENISA wymieniono tylko umowy o powiernictwie kodu.

2. A. Dokument ENISA określa otwarty format wirtualizacji (OVF) jako potencjalnie korzystny w zakresie przenośności w środowisku IaaS.

3. D. Niezabezpieczone lub niekompletne usuwanie danych stanowi ryzyko w chmurze ze względu na współdzielony charakter przechowywania i brak możliwości sprawdzenia, czy dane są odpowiednio usuwane. Chociaż czyszczenie dysków SSD jest możliwe (tylko za pomocą narzędzi dostarczonych przez dostawcę), nie jest to wymienione jako powód w dokumencie. Nie jest również prawdą, że wszyscy dostawcy używają dysków SSD do przechowywania danych klientów.

4. C. Wszystkie produkty SaaS są dostosowanymi aplikacjami. Fakt ten nie jest źródłem uzależnienia od dostawcy. To, co tworzy sytuację blokady w przypadku SaaS, to brak możliwości łatwego przenoszenia danych od jednego dostawcy SaaS do drugiego. Jeśli istnieją narzędzia (zwykle są ograniczone) do przenoszenia od jednego dostawcy SaaS do drugiego, blokada dostawcy może być dość łatwo rozwiązana. Wszystkie pozostałe odpowiedzi to scenariusze blokady.

5. C. Wykonywanie przeskakiwania między maszynami wirtualnymi jest wynikiem awarii izolacji hiperwizora. Żadna z pozostałych odpowiedzi nie jest prawidłowa. Pamiętaj, że segregacja nie jest tym samym, co izolacja.

6. B. Dokument ENISA wymienia pracowników i kontrahentów dostawcy jako potencjalnych złośliwych insiderów. W związku z tym jedyną możliwą poprawną odpowiedzią jest audytor dostawcy.

7. D. Administrator stworzył scenariusz ekonomicznej odmowy usługi, jeśli kiedykolwiek dojdzie do ataku odmowy usługi na firmę. Wynika to z mierzonej charakterystyki usługi chmury obliczeniowej, w której firmy płacą za wykorzystywane zasoby. Równoważenie obciążenia rozłoży ruch tylko na ustaloną liczbę serwerów, więc B i C nie odnoszą się do tego, co ustalił administrator. Wreszcie, chociaż grupy automatycznego skalowania są powszechne, musi istnieć ustalony limit liczby serwerów, które zostaną utworzone.

8. D. Przechowywanie obiektów to jedyna odpowiedź, która nie jest wymieniona jako powiązana podatność na ryzyko utraty reputacji biznesowej z powodu działań współużytkowników.

9. D. Jedyną możliwą odpowiedzią, która nie jest wymieniona, jest to, że klient może ograniczyć dostęp do systemu IAM dostarczonego przez dostawcę do określonego zakresu adresów IP. Wynika to z faktu, że system IAM jest częścią płaszczyzny zarządzania, do której dostęp może uzyskać każdy jako część szerokiej charakterystyki dostępu do sieci chmury. Wszystkie inne wpisy są wymienione jako obszary do rozważenia i ochrony.

10. C. Konta uprzywilejowane powinny zawsze uzyskiwać dostęp do płaszczyzny zarządzania za pomocą MFA. Płaszczyzna zarządzania jest narażona na zwiększone ryzyko naruszenia, ponieważ jest globalnie dostępna; dlatego wdrożenie VPN jakiegokolwiek rodzaju nie jest wymienione jako potencjalne zabezpieczenie. Wszyscy użytkownicy uzyskujący dostęp do płaszczyzny zarządzania powinni zawsze mieć oddzielne konta, ale D dotyczy odrzucenia, a nie bezpieczeństwa kont uzyskujących dostęp do płaszczyzny zarządzania. Mimo że wszystkie połączenia powinny być chronione podczas przesyłu (np. za pomocą protokołu TLS), odpowiedź B nie jest najlepsza.