KPMG

COVID-19

Co mogą zrobić CIO i CISO, aby pomóc swojej firmie

Marzec 2020

Rosnące obawy dotyczące skali i wpływu pandemii COVID-19, skłaniają przedsiębiorców do wdrożenia natychmiastowych działań, aby firma mogła dalej funkcjonować. CIO i CISO odgrywają istotną rolę w zapewnieniu, aby organizacja mogła działać także w sytuacji, gdy władze wdrażają środki mające na celu przeciwdziałanie pandemii.

Czy Twoja firma potrafi skutecznie funkcjonować dzięki pracy zdalnej?

Dobrze jest się upewnić, że Twoja firma potrafi funkcjonować zdalnie, a także, że pracownicy są świadomi, iż mogą w ten sposób pracować. Może to wymagać skorygowania zasad zarządzania uprawnieniami dostępowymi oraz zarządzania ryzykiem. Kwestie, które należy rozważyć:

- Czy koncentratory VPN, zapory ogniowe i inne rozwiązania sieciowe zostały dostosowane tak, aby mogły obsłużyć dużą liczbę pracowników, którzy będą pracować zdalnie?
- Czy zastanawiałeś się nad tym, kto z potencjalnych kluczowych dostawców, wykonawców i sprzedawców będzie musiał uzyskać dostęp do sieci oraz z jakim obciążeniem dla systemu będzie się to wiązało?
- Czy infrastruktura została przetestowana tak, aby zweryfikować czy może obsłużyć przewidywane obciążenie?
- Czy istnieją pojedyncze elementy infrastruktury mogące powodować awarie i czy jest możliwość zapewnienia odporności na nie?
- Czy jest potrzeba, aby poluzować mechanizmy kontroli dostępu? Albo może, aby dostarczyć dodatkowych kont do zdalnego dostępu?
- Czy dział pomocy technicznej ma wystarczające zasoby do obsługi wszystkich zapytań użytkowników, którzy nie mogą się zalogować lub nie są zapoznani z pracą zdalną?
- Jeżeli pracownicy potrzebują laptopów do pracy zdalnej, czy istnieje odpowiednia pula dostępnych laptopów lub czy można je zamówić, a także w jaki sposób należy rozdysponować laptopy, które już są w posiadaniu firmy?
- W przypadkach, w których pula urządzeń jest ograniczona, czy rozważałeś, które z nich są najważniejsze i próbowałeś przydzielić dostęp za pomocą alternatywnych rozwiązań (np. O365 i One Drive vs aplikacje własne firmy)?
- Czy rozważałeś możliwość dodania w tym okresie do „białej listy oprogramowania" tylko określonych aplikacji i zablokowania wszystkich pozostałych, nieistotnych usług?
- Czy w firmie są jakieś ograniczenia dotyczące włączania się do mostków telekonferencyjnych, oraz czy możesz zrobić coś, aby wyskalować tę infrastrukturę?
- Czy rozważałeś alternatywne rozwiązania w chmurze do przeprowadzania konferencji i telepracy?
- Czy wszyscy pracownicy dysponują niezbędnym oprogramowaniem do telekonferencji, numerami dostępu/łączami potrzebnymi do włączenia się do telekonferencji? A także czy materiały szkoleniowe są łatwo dostępne i czy może nie należałoby ustanowić osobnego numeru do działu pomocy technicznej w związku z uruchomieniem pracy zdalnej?
- Czy jest możliwość zdalnej realizacji pomocy technicznej, w przypadku gdy pracownicy pomocy technicznej będą musieli pracować z domu?
- Czy są przygotowane przewodniki z odpowiedziami na kluczowe pytania dotyczące pomocy technicznej, tj.:
  - Jak się zalogować?
  - Jak zmienić hasło?
  - Jak uzyskać dostęp do kluczowych usług?
  - Jak uzyskać pomoc z działu pomocy?
  - Jakie są najważniejsze kontakty, w przypadku sytuacji kryzysowej?

Czy jesteś w stanie wyskalować wszystkie cyfrowe kanały komunikacji firmy, aby sprostać wzrostowi zapotrzebowania?

Ograniczenia w podróżowaniu, które są wymagane aby zatrzymać rozprzestrzenianie się wirusa, mogą spowodować zwiększenie ruchu we wszystkich tradycyjnych i cyfrowych kanałach komunikacyjnych firmy.

- Klienci i odbiorcy mogą częściej oczekiwać, że transakcje z Twoją firmą odbywać się będą za pośrednictwem kanałów cyfrowych. Czy jesteś w stanie dostosować Wasze systemy i usługi tak, aby sprostać rosnącym potrzebom?
- W jaki sposób będziesz monitorować wydajność systemów? A także, kto będzie mógł podjąć decyzje o dostosowaniu przepustowości systemu lub stworzeniu dynamicznych mechanizmów priorytetyzacji w przypadku gdy przepustowość systemu będzie stanowić problem?
- Czy wiesz, w przypadku przeciążenia systemów, które usługi mogą zostać wyłączone, lub w jaki sposób dostęp klientów do systemu może zostać zmieniony?
- Czy Twoja firma jest zależna od działania centrów obsługi telefonicznej (call center)? A w przypadku, gdy te centra obsługi zostaną zamknięte lub będą niedostępne, czy klienci i odbiorcy będą mogli skontaktować się z Twoją firmą za pośrednictwem innych kanałów?
- Czy istnieje możliwość zezwolenia na pracę zdalną pracownikom centrum obsługi telefonicznej lub przeniesienia ich zadań do innego centrum obsługi telefonicznej?
- Czy zastanawiałeś się nad powiązaniami między centrami obsługi telefonicznej a punktami obsługi klientów oraz wpływem na nie jakichkolwiek parametrów usług outsourcingowych?
- Czy omawiałeś parametry usług outsourcingowych z kluczowymi dostawcami tych usług i w jaki sposób priorytetyzują oni potrzeby Twojej firmy względem potrzeb innych swoich klientów?

Czy Twoja firma jest zależna od kluczowych pracowników działu IT?

Może zdarzyć się tak, że pracownicy zostaną zarażeni, będą objęci kwarantanną lub będą musieli opiekować się członkami rodziny. Z tego powodu Twoja firma powinna przygotować się na znaczący poziom absencji w pracy.

- Co by się stało, gdyby kluczowi pracownicy działu IT (w tym podwykonawcy) byli objęci kwarantanną lub zachorowali na wirusa? Należy ustalić, czy firma nie jest przypadkiem zależna od niewielkiej liczby kluczowych osób zarówno w ramach swojego personelu jak i personelu głównych dostawców lub wykonawców usług.
- W jaki sposób można zmniejszyć tę zależność? Czy na przykład w ramach procedur awaryjnych można umożliwić innym administratorom dostęp do najważniejszych systemów?
- Kto należy do zespołu ds. bezpieczeństwa firmy? Kim są kluczowe osoby dla bezpieczeństwa informatycznego firmy? A jeśli CISO nie będzie mógł wykonywać swojej pracy, to kto wówczas zadba o bezpieczeństwo firmy?

Co by się stało, gdyby nastąpiło zakłócenie działania centrum przetwarzania danych?

Epidemia koronawirusa może wpłynąć także na działanie centrum przetwarzania danych. Pozytywny wynik testu na obecność koronawirusa u pracownika może doprowadzić do ewakuacji i przymusu dezynfekcji budynku. Co więcej, zmniejszony dostęp do infrastruktury transportowej może uniemożliwić dotarcie do budynku, a w rezultacie pracownicy centrum przetwarzania danych mogą nie być w stanie pracować.

- W przypadku ewakuacji jednego z twoich centrów przetwarzania danych, czy Twoja firma ma plany odtwarzania systemów informatycznych na wypadek katastrofy? Czy te plany zostały przetestowane?
- Jak szybko Twoja firma może przejść do pracy w trybie awaryjnym i kto zarządza tym procesem?
- Czy Twoja firma jest zależna od kluczowych osób (w tym wsparcia podwykonawcy) w zakresie obsługi centrum przetwarzania danych i jak możesz zarządzać tą zależnością?

Czy jesteś w stanie dostosować możliwości swojej chmury?

Może pojawić się zwiększone zapotrzebowanie na usługi chmurowe, które potrzebują dodatkowej mocy obliczeniowej. Wiązać się to może z dodatkowymi kosztami. Z kolei na inne usługi może zmniejszyć się zapotrzebowanie.

- Czy jesteś w stanie monitorować zapotrzebowanie na usługi przetwarzania w chmurze i skutecznie zarządzać rozdysponowaniem zasobów?
- Czy podjęto decyzje dotyczące pokrycia dodatkowych kosztów, które mogą zostać poniesione w związku z dostosowywaniem lub udostępnianiem innych usług w chmurze?

Czy Twoja firma jest zależna od dostawców?

Dostawcy i partnerzy biznesowi Twojej firmy również mogą znaleźć się w sytuacji awaryjnej, a ich działalność również może zostać zakłócona.

- Czy jesteś w stanie określić kluczowych dostawców Twojej firmy? Jak poradziłaby sobie Twoja firma, gdyby dostawcy nie mogli funkcjonować (w tym np. kluczowi dostawcy usług wsparcia i utrzymania)?
- Czy można teraz podjąć kroki w celu zmniejszenia tej zależności? Na przykład przy użyciu zasobów Twojego zespołu?
- Czy omawiasz ewentualne następstwa sytuacji awaryjnej ze swoimi kluczowymi dostawcami? Czy jesteś w stanie szybko się skontaktować z tymi dostawcami?
- Czy określiłeś, którzy dostawcy IT Twojej firmy mogą znaleźć się pod presją finansową? Jaka byłaby Twoja alternatywna strategia zarządzania infrastrukturą IT, gdyby dostawcy musieli zakończyć działalność?

Co by się stało, gdyby doszło do incydentu cyberbezpieczeństwa?

Zorganizowane grupy przestępcze wykorzystują strach przed COVID-19 do prowadzenia ukierunkowanych kampanii phishingowych typu spear-phishing i zakładania fałszywych stron internetowych. Wszystko to sprawia, że ryzyko incydentu związanego z cyberbezpieczeństwem jest większe.

- Czy pracownicy Twojej firmy otrzymali informację, gdzie uzyskać dostęp do wiarygodnych wiadomości na temat pandemii COVID-19, a także na temat działań Twojej firmy mających na celu przeciwdziałanie rozprzestrzenianiu się wirusa?
- Czy pracownicy zostali ostrzeżeni o zwiększonym ryzyku ataków phishingowych z wiadomościami na temat COVID-19?
- Jeśli jesteś zależny od zewnętrznych systemów lub rozwiązań, w tym tych zamówionych jako usługi w chmurze, komu powierzyłbyś obsługę incydentów związanych z bezpieczeństwem tych systemów?
- Czy nie powinieneś zmienić w czasie pandemii swojego podejścia do zarządzania procesami bezpieczeństwa w Twojej firmie? W tym np. do monitorowania zdarzeń związanych z bezpieczeństwem?

Co by się stało, gdyby doszło do incydentu informatycznego?

Podczas gdy w wiadomościach dominują informacje nt. COVID-19, nadal powinieneś zdawać sobie sprawę z możliwości awarii infrastruktury IT. Szczególnie pod uwagę należy brać zmieniające się wymagania dotyczące infrastruktury lub cyberataki.

- Czy byłbyś w stanie zdalnie koordynować incydent? A także, czy masz niezbędne zaplecze konferencyjne oraz dostęp do stron/procesów i przewodników zarządzania incydentami?
- Czy masz skonfigurowane wirtualne centrum zarządzania kryzysowego na wypadek, gdyby fizyczny dostęp był ograniczony?
- Czy Twoja firma jest zależna od kluczowych osób odpowiedzialnych za reakcję na incydent, a jeśli tak, to co możesz zrobić, aby zmniejszyć tę zależność?
- Jak zmienia się struktura zarządzania kryzysowego/ reagowania na incydenty, jeśli kluczowi menedżerowie ds. obsługi incydentów są niedostępni?
- Czy masz pewność, że kopie zapasowe Twojej firmy są aktualne, a w najgorszym przypadku że możesz przywrócić krytyczne dane i systemy firmy?
- Jak Twoja firma poradziłaby sobie z incydentem wywołanym przez złośliwe oprogramowanie typu ransomware, gdy duża część pracowników pracuje zdalnie?

Czy Twoja firma w optymalny sposób wykorzystuje swoje zasoby?

Musisz być w stanie funkcjonować z ograniczoną liczbą pracowników i mieć jasność, które zadania Twojego zespołu są priorytetowe.

- Czy nadałeś odpowiedni priorytet poszczególnym działaniom Twojego zespołu? Czy są jakieś zadania, które możesz odroczyć, a pracowników oddelegować do planowania awaryjnego i najważniejszych działań?
- Czy masz możliwość rozporządzać dodatkowym budżetem, na wypadek gdy będziesz potrzebować szybko zdobyć sprzęt lub zatrudnić dodatkowego podwykonawcę, czy zdobyć specjalistyczne wsparcie?
- Jeśli znajdujesz się pod presją ograniczenia wydatków, czy wiesz, które z nich należy utrzymać, a na których można teraz oszczędzić?

Czy dajesz przykład swojemu zespołowi?

Pomimo wszystkich powyższych kwestii organizacyjnych, nadal jesteś menedżerem wyższego szczebla, a Twój zespół będzie liczył na Ciebie w zakresie przywództwa i wsparcia.

- Czy upewniłeś się, że Twój zespół wdraża odpowiednie praktyki higieniczne? Czy zaoferowałeś swojemu zespołowi elastyczną i zdalną pracę w celu spełnienia zmieniających się potrzeb?
- Czy masz aktualne dane kontaktowe do całego swojego zespołu? Czy Twój zespół wie, z kim się skontaktować w nagłym wypadku?
- Czy prezentujesz Twojemu zespołowi zachowania, których od nich oczekujesz? Co by się stało, gdybyś był niezdolny do pracy? Kto by Cię wówczas zastępował?

Życzymy bezpieczeństwa i zdrowia!

W razie pytań lub potrzeby dodatkowej porady, skontaktuj się z nami.

Krzysztof Radziwon
Partner
Doradztwo biznesowe
T: +48 508 047 500
E: kradziwon@kpmg.pl

Michał Kurek
Partner
Doradztwo biznesowe
T: +48 660 440 041
E: michalkurek@kpmg.pl

Marek Gzowski
Dyrektor
Doradztwo biznesowe
T: +48 664 080 095
E: mgzowski@kpmg.pl

Materiał jest tłumaczeniem broszury KPMG International pt. "COVID-19. What the CIO and CISO can do to help" opublikowanej w marcu 2020 r.
Skład i modyfikacja treści w języku polskim KPMG w Polsce. © 2020 KPMG in Poland.