



**Ryzyko Nadużyć**

Wybrane nadużycia związane z COVID-19

Lipiec 2020

# Jak COVID-19 oddziałuje na ogólny poziom nadużyć

Szanowni Państwo,

Pandemia koronawirusa wpłynęła na nasze życie i będzie miała na nie znaczący wpływ także w przyszłości. Zmianom mogły ulec nie tylko nasze relacje, ale także całe postrzeganie świata gospodarczego. Wiele firm odkryło, że praca zdalna obniża koszty, a pracownicy mogą w ten sposób pracować efektywniej... ale również wiele firm odkryło, że ich pracownicy nie są wystarczająco zdyscyplinowani.

Niezależnie od tego, praca zdalna, ograniczenia w podróżowaniu, większe uzależnienie od technologii oraz niepewność ekonomiczna stały się ostatnio rzeczywistością dla wielu przedsiębiorstw. Musiały one skupić się na wyzwaniach logistycznych i operacyjnych w celu zaspokojenia potrzeb wszystkich interesariuszy. Nie są to jednak jedyne wyzwania, przed którymi stoimy. Kryzys ten otworzył również drzwi dla zwiększonej presji, możliwości i racjonalizacji, które mogą prowadzić do nadużyć.

Według badania przeprowadzonego przez Stowarzyszenie Biegłych ds. Przepływów i Nadużyć Gospodarczych ACFE ("ACFE") w okresie od końca kwietnia do połowy maja 2020 r. wśród jego członków, od maja 2020 r. 68% specjalistów ds. zwalczania nadużyć doświadczyło już lub zaobserwowało wzrost poziomu nadużyć, przy czym jedna czwarta stwierdziła, że zaobserwowany wzrost był znaczny. Patrząc w przyszłość, specjaliści ds. zwalczania nadużyć oczekują jeszcze większych zmian w ogólnym poziomie nadużyć. Prawie wszyscy ankietowani (93%) stwierdzili, że spodziewają się wzrostu liczby oszustw w następnym roku (tzn. do maja 2021), przy czym ponad połowa respondentów przewiduje znaczny wzrost. Wydaje się, że sytuacja rozwija się bardzo szybko, a oszuści nadal się dostosowują. Biorąc pod uwagę wiele czynników, które sprawiają, że wykrywanie oszustw jest jeszcze trudniejsze niż zwykle, niezbędne jest wyposażenie przedsiębiorstw w zaawansowane rozwiązania.

W niniejszym Newsletterze pragniemy poinformować Państwa, w jaki sposób dotknięty został łańcuch dostaw, jaki jest możliwy wpływ Covid-19 na nadużycia w sprawozdawczości finansowej, co może być potencjalnie niebezpieczne dla Państwa pracowników w kontekście phishingu oraz w jaki sposób organizacje mogą chronić się przed takimi zagrożeniami.

Życzymy ciekawej lektury.



# Wpływ COVID-19 na nadużycia w sprawozdawczości finansowej

# Wpływ COVID-19 na nadużycia w sprawozdawczości finansowej

Pandemia COVID-19 dotknęła niemal wszystkie państwa na świecie i **wywiera wpływ na prawie wszystkie organizacje**. Nie tylko zaburzyła działalność biznesową i łańcuchy dostaw ale także zwiększyła ryzyko nadużyć, w szczególności ryzyko fałszowania sprawozdań finansowych.

## Według analiz ACFE:



Głównym czynnikiem ryzyka w **22%** przypadków fałszywej sprawozdawczości finansowej jest niewłaściwy ton przekazywany przez wyższą kadram kierowniczą.



Pracownicy w większym stopniu pracują obecnie z domu, co stanowi nowe, nieoczekiwane wyzwanie dla systemu kontroli wewnętrznej przeciwdziałającego nadużyciom. Przyczynia się to do przewidywanego w kolejnych 12 miesiącach wzrostu liczby przypadków fałszowania sprawozdań finansowych.



Nadużycia związane z fałszowaniem sprawozdań finansowych charakteryzują się największym poziomem strat. Ich mediana wyniosła **878 tys. euro**.

## Manipulacje wysokością przychodów

Organizacje mogą manipulować wysokością przychodów w celu ograniczenia raportowanego wpływu na ich działalność restrykcji związanych z COVID-19.

## Ukrywanie skutków innych nadużyć

COVID-19 przyczynia się do nadużyć poprzez presję finansową i osłabienie systemu kontroli wewnętrznej (praca zdalna, ograniczenia zatrudnienia). Księgi rachunkowe mogą być fałszowane w celu ukrycia strat spowodowanych różnymi rodzajami nadużyć (np. kradzieży). Dlatego fałszywa sprawozdawczość finansowa może być tylko symptomem występowania innych nadużyć.

## Aktywowanie kosztów

Przedsiębiorstwa odczuwają presję aby aktywować koszty bieżącej działalności, zamiast uznawać je w rachunku wyników, w celu poprawy wyniku finansowego prezentowanego w bieżących sprawozdaniach finansowych.

**Manipulacje wyceną aktywów (w tym wartością firmy / goodwill) oraz odpisami na utratę ich wartości.**

W obliczu istotnych nieprzewidzianych zakłóceń działalności niektóre aktywa, zarówno rzeczowe jak i niematerialne, mogą doznać trwałej utraty wartości. To z kolei może prowadzić do zniekształconej prezentacji aktywów w sprawozdaniach finansowych jeżeli ich wyceny nie zostaną skorygowane odpowiednimi odpisami.

## Zniekształcenia w notach objaśniających

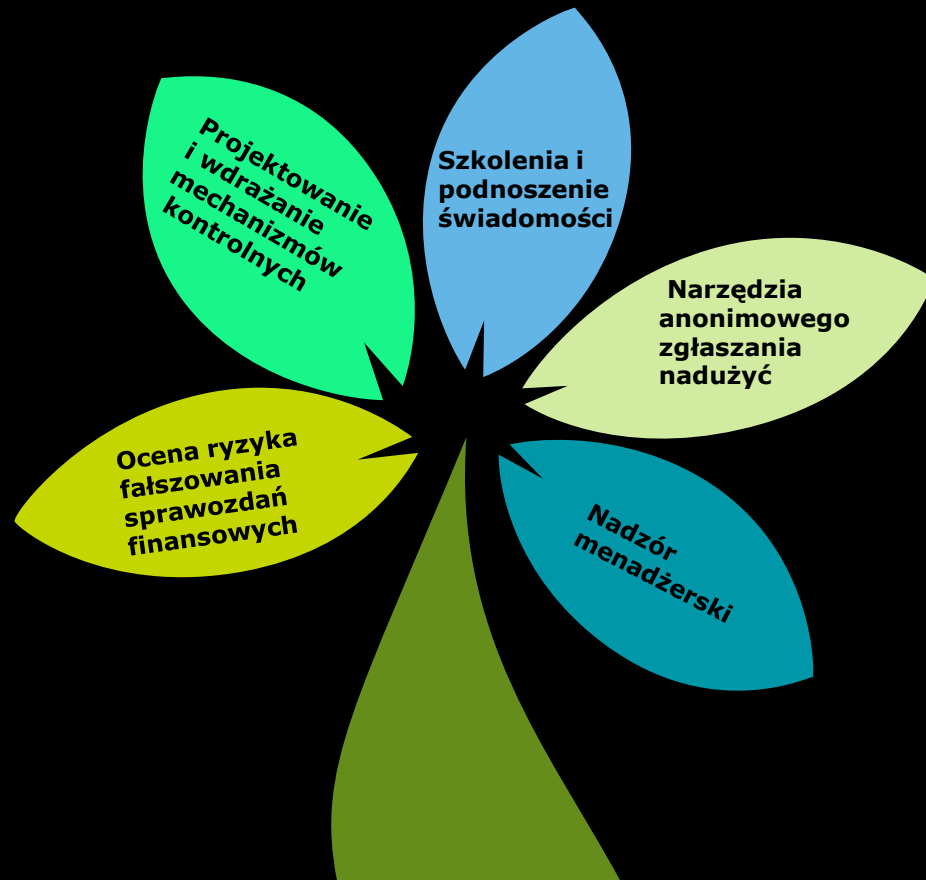
Organizacje mogą unikać ujawniania w notach objaśniających pełnego wpływu COVID-19 na ich działalność i sytuację.

## Płynność i kontynuacja działalności

W związku z silnym spadkiem przychodów ze sprzedaży przedsiębiorstwa zmuszone były korzystać z ich rezerw finansowych aby móc kontynuować działalność, wypłacać wynagrodzenia i wywiązywać się z innych zobowiązań. Ewentualne wykorzystanie rezerw finansowych stworzyło ryzyko utraty płynności i zdolności do kontynuacji działalności.



# Jak organizacje mogą chronić się przed ryzykiem



## Ocena ryzyka fałszowania sprawozdań finansowych

Organizacje potrzebują zaktualizować wcześniejsze oceny ryzyka fałszywej sprawozdawczości finansowej, w tym zidentyfikować nowe zagrożenia i zaktualizować oceny poziomów ryzyka stosowanie do nowej sytuacji wywołanej COVID-19.

## Projektowanie i wdrażanie mechanizmów kontrolnych

Koncentracja na działalności operacyjnej oraz praca zdalna skutkują obniżeniem skuteczności kontroli wewnętrznej. W sytuacji kryzysowej może dochodzić do omijania mechanizmów kontrolnych w celu ułatwienia działania procesów biznesowych. Może to stwarzać dogodne warunki do działania oszustów. Dlatego organizacje potrzebują aktualizacji i oceny ich mechanizmów kontrolnych.

## Szkolenia i podnoszenie świadomości wśród pracowników

Zapoznaj pracowników z przykładami nadużyć oraz ich symptomami, na które powinni zwracać uwagę. Uczyni ich to bardziej czujnymi w codziennej pracy i zwiększy szanse na wczesne wykrycie potencjalnych nadużyć.

## Narzędzia anonimowego zgłaszania nadużyć

Zawiadomienia od sygnalistów pozostają najskuteczniejszą metodą wykrywania nadużyć. Organizacje mogą usprawnić ten proces poprzez udostępnienie pracownikom i stronom trzecim narzędzi pozwalających na anonimowe zgłaszanie nieprawidłowości. Organizacje powinny zapewnić, że wszystkie zgłoszenia są należycie rozpatrywane i w uzasadnionych przypadkach wyjaśniane poprzez przeprowadzanie audytów śledczych.

## Nadzór menadżerski

Kierownictwo może ograniczać potencjalne szkody poprzez przywiązywanie uwagi do prawidłowego funkcjonowania systemu kontroli wewnętrznej oraz audytu wewnętrznego i zewnętrznego.



# Wpływ COVID-19 na łańcuchy dostaw

# Wpływ COVID-19 na łańcuchy dostaw

## Łańcuch dostaw

### Przegląd zakłóceń

Organizacje zmuszone są dostosować swoje obecne, ugruntowane łańcuchy dostaw, logistykę i procesy produkcyjne do nowych, utrudnionych warunków globalnej współpracy gospodarczej. Jest to próba szybkiego zareagowania na zmiany i skutecznego łagodzenia wpływu blokad i upadłości na procesy biznesowe.

Przedsiębiorstwa muszą podejmować odpowiednie, terminowe i skuteczne działania w celu kontynuacji działalności gospodarczej i dalszego zaspokajania potrzeb swoich klientów oraz odpowiedniego wspierania swoich pracowników.



Poza zakłóceniami w łańcuchu dostaw, organizacje muszą odpowiedzieć na zakłócenia w kanałach dystrybucji. Magazynowanie zapasów, opakowań i kluczowych surowców staje się ważne dla utrzymania kontynuacji działalności przedsiębiorstw.

Integracja wielu organizacji w regionie Europy Środkowo-Wschodniej z otwartymi gospodarkami Europy sprawia, że są one narażone na zakłócenia w łańcuchu dostaw.



Duże skale zwolnień w II kw. 2020 r. w

Europie szacowana na **7.8% lub 12 milionów** pełnoetatowych pracowników.



**93%**

ludności świata mieszka w krajach, w których obowiązują ograniczenia w zakresie podróży lub eksportu.



Do sektorów najbardziej narażonych na ryzyko należą: hotelarstwo, gastronomia, produkcja, handel detaliczny, usługi biznesowe i administracyjne.



Eksport stanowi około **55%** polskiego PKB.



Związek Polskich Pracodawców Handlu i Usług stwierdził wśród swoich członków spadek obrotów o **45%** w Warszawie i o **37%** poza Warszawą w pierwszym miesiącu po rozluźnieniu kwarantanny (w porównaniu do analogicznego okresu przed rokiem).

# Wpływ COVID-19 na łańcuchy dostaw

## Budowanie nowych relacji łańcucha dostaw i mapowanie łańcucha dostaw

Ogólnoświatowe zamknięcie gospodarek istotnie zakłóciło dostawy towarów drogą morską, lotniczą i lądową. W efekcie dostawy niezbędnych dla produkcji materiałów zostały poważnie ograniczone.

Skłoniło to wiele przedsiębiorstw do rozpoczęcia poszukiwań lokalnych rozwiązań w celu wypełnienia pojawiających się luk w ich łańcuchach dostaw. Wiele przedsiębiorstw w krótkim czasie nawiązało nowe relacje biznesowe z podmiotami lokalnymi.

Szybkie nawiązywanie nowych relacji biznesowych wiąże się z ryzykiem. Wynika ono głównie z braku odpowiedniej weryfikacji potencjalnych partnerów biznesowych i ich możliwości.

Podczas gdy bezpieczeństwo pracowników i klientów jest sprawą najwyższej wagi w sytuacjach kryzysowych, firmy muszą również zapewnić, w możliwym zakresie, ciągłość ich działalności. Epidemia COVID-19 wywołała potrzebę dystansu społecznego, skłaniając przedsiębiorstwa do stosowania rozwiązań w zakresie pracy zdalnej. Firmy utrzymujące dotychczas bezpośrednie interakcje z klientami zaczynają patrzeć na swoją działalność pod różnymi kątami i szukają nowych metod funkcjonowania.



Ponad **312 mld PLN** przeznaczone przez rząd na walkę kryzysem wywołanym pandemią.



NBP obniżył stopę procentową o 40 punktów bazowych do **0.1%**.



Federacja Przedsiębiorców Polskich szacuje, że w samym okresie między 16 marca i 20 kwietnia polska gospodarka straciła z powodu restrykcji **79 mld PLN**. 24 mld przypada na przemysł, 20 mld PLN na handel, 5 mld PLN na budownictwo, a 30 mld PLN na pozostałe branże usługowe.



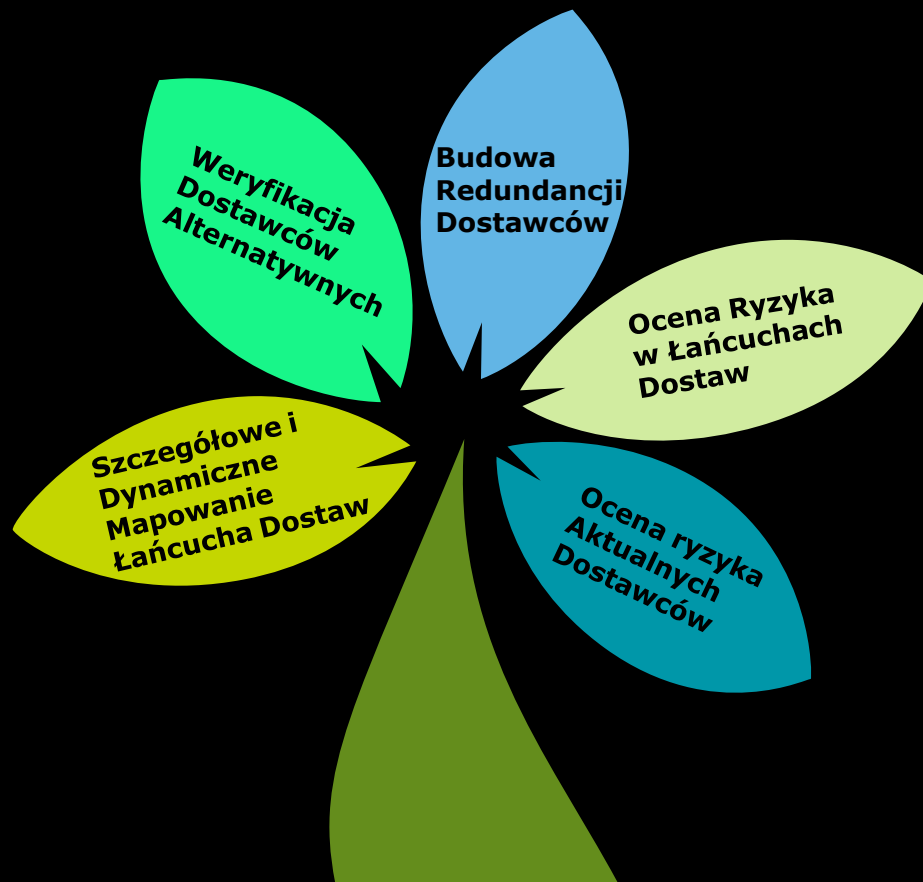
MFW prognozuje, że gospodarki 19 krajów strefy euro zmniejszą się łącznie o **7.5%**.



MFW prognozuje, że PKB Polski spadnie w 2020 r. o **4.6%**.



# Jak organizacje mogą się chronić przed zidentyfikowanymi zagrożeniami



## Szczegółowe i Dynamiczne Mapowanie Łańcucha Dostaw

Ocena wpływu zagrożeń wynikających z COVID-19 na dostawców pierwszego i drugiego poziomu (tier 1, tier 2) oraz opracowanie pełnego obrazu zmian w łańcuchu dostaw, tych które już nastąpiły i tych które prawdopodobnie nastąpią w krótkim i długim okresie.

## Weryfikacja Alternatywnych Dostawców

Identyfikacja potencjalnych alternatywnych źródeł dostaw, mniej podatnych na zakłócenia wynikające z Covid-19. Weryfikacja potencjalnych nowych dostawców pod kątem ich możliwości i reputacji w celu zminimalizowania ryzyka nawiązania niekorzystnych relacji biznesowych.

## Budowanie Redundancji Dostawców

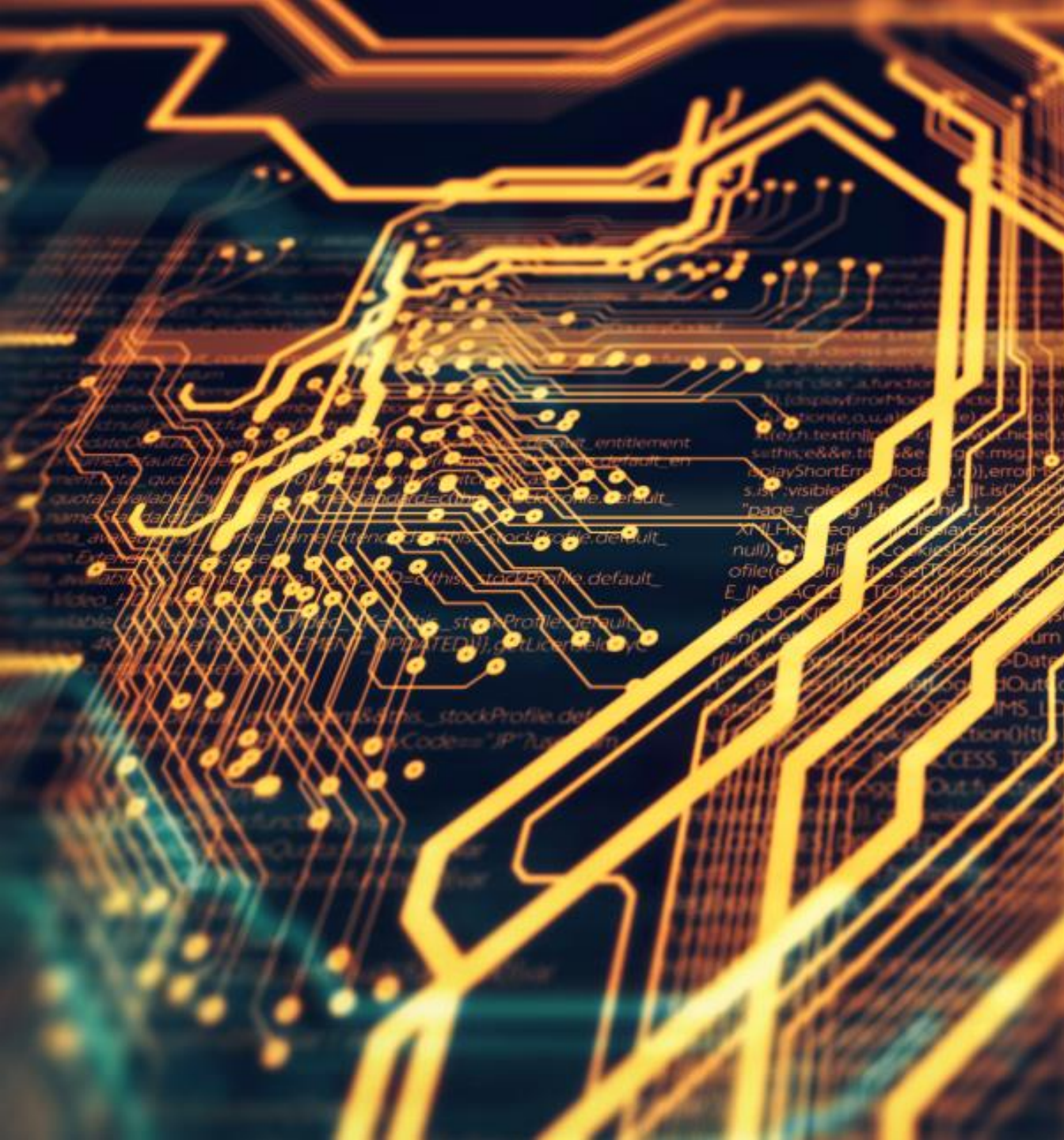
W ramach rozwiązań długoterminowych organizacje powinny budować redundancje w ramach swoich łańcuchów dostaw, tak aby minimalizować ryzyko przerwania łańcuchów dostaw istotnych dla kontynuacji procesów biznesowych.

## Ocena Ryzyka dla Łańcucha Dostaw

Organizacje powinny opracować oparty na ryzyku proces identyfikacji i oceny pojawiających się zagrożeń dla ich łańcucha dostaw. Zidentyfikowane istotne ryzyka powinny być na bieżąco monitorowane. Zmiany ryzyka wynikające ze zmian w łańcuchu dostaw powinny być identyfikowane i oceniane.

## Ocena ryzyka Aktualnych Dostawców

Ryzyko zerwania łańcucha dostaw powinno być oceniane w odniesieniu do istniejących bezpośrednich dostawców, jak również dostawców znajdujących się niżej w łańcuchu dostaw (dostawcy dostawców).



# Wpływ COVID-19 na **Phishing**

# Phishing

Managerowie **zgodzili się na obniżenie wynagrodzeń** podczas kryzysu... Aby uzyskać więcej informacji kliknij tutaj. **Twój HR.**

## Przypomnijmy, czym jest phishing?

Phishing jest rodzajem oszustwa, w którym impulsywna lub nieostrożna osoba nieświadomie ujawnia poufne dane osobowe / firmowe i dane te są następnie wykorzystywane przez oszustów. Najczęściej dokonywany jest za pośrednictwem wiadomości e-mail lub SMS (smishing), czasem także przez kanały telefoniczne (vishing).

Dlaczego oszustwo nazywane jest phishingiem? Ponieważ oszust zarzuca „wędkę” i po prostu czeka, aż złowią się jakieś ofiary.

Warunki kryzysu ułatwiają oszustom atakowanie pracowników poprzez wysyłanie „pilnych” wiadomości e-mail podszywając się pod członków kierownictwa wyższego szczebla, co prowadzi do ujawnienia poufnych informacji lub wykonania przelewu.

W ciągu miesiąca od wybuchu epidemii w Chinach firmy zajmujące się cyberbezpieczeństwem zaczęły zgłaszać przypadki phishingu związane z COVID-19.



**100 000 000** e-maili

związanych z phishingiem blokowanych jest przez Google **codziennie**



**20%** z nich jest powiązanych COVID-19\*

\*13-17 kwietnia 2020r.

## Phishing w czasie COVID-19

Znany czeski producent oprogramowania antywirusowego ostrzega przed zwiększoną ilością fałszywych wiadomości e-mail i witryn, które próbują przekonać użytkowników do zakupu sprzętu ochronnego, testerów antywirusowych lub przekazania pieniędzy wskazanym organizacjom. Informacje te są nieprawdziwe. Po kliknięciu przez ofiarę zamieszczonego w wiadomości przycisku zostaje ona przekierowana na stronę internetową, na której wprowadza swoje dane osobowe. Dane te są następnie wykorzystywane przez oszustów.

Sprawca wykorzystuje brak uwagi ofiar. Może na przykład zamienić miejscami lub pominąć literę w domenie e-mail. Przykładem może być domena „@gmal.com”. Czy zareagowałbyś na e-mail z adresu deloittece@gmal.com?

Wykorzystywane są również znane nazwy, zwłaszcza WHO („Światowa Organizacja Zdrowia”), które są dodawane do adresu e-mail. Może to przybrać formę na przykład [who.alerts@global.org](mailto:who.alerts@global.org)

Oszuści mogą również wykorzystać domenę twojej firmy. Mogą na przykład podszyć się pod dział HR lub kierownictwo firmy wysyłając wiadomość do pracowników o wynagrodzeniach i bonusach w czasie pandemii. Mogą również podszyć się pod twojego przełożonego, który pilnie potrzebuje dowiedzieć się czegoś z załączonego pliku. Plik będzie miał nazwę „COVID19\_threats\_for\_companies.pdf.exe” i po otwarciu uruchomi inny plik (pdf) z informacjami. Jednakże zainstaluje także konia trojańskiego. Niektórzy użytkownicy mają ukryte rozszerzenia końcowe w nazwach plików, więc widzieć będą tylko rozszerzenie „pdf”.

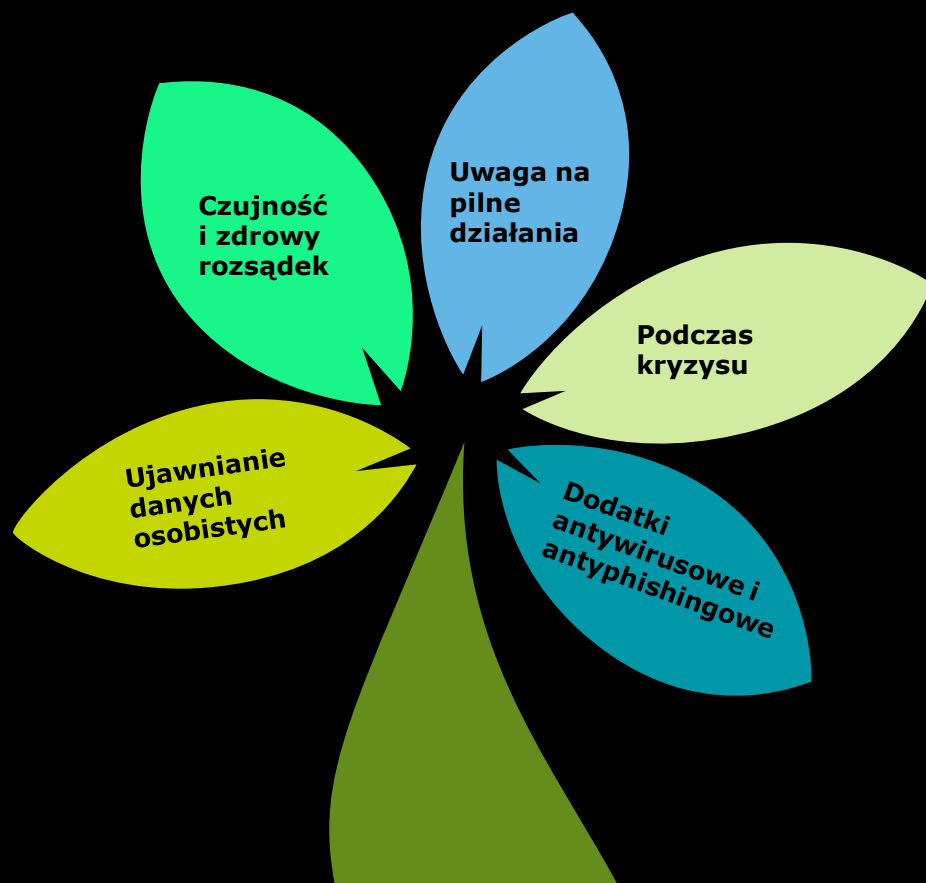


**...każdorazowo zachowaj spokój i usuń e-mail!**

Aby zwiększyć świadomość pracowników na temat zagrożeń związanych z phishingiem, można wysłać do pracowników symulowaną wiadomość e-mail wyłudżającą informacje, a następnie dostarczyć informacje szkoleniowe dla tych pracowników, którzy nie rozpoznali w otrzymanej wiadomości próby phishingu.

Bądź ostrożny! Nieostrożne stosowanie tej techniki może stanowić naruszenie prawa!

# Jak organizacje mogą się chronić przed zidentyfikowanymi zagrożeniami



## Zachowaj czujność i kieruj się zdrowym rozsądkiem

Kieruj się zdrowym rozsądkiem aby zidentyfikować podejrzaną wiadomości e-mail. Zawsze sprawdzaj adres nadawcy pod kątem błędów pisowni i nie klikaj podejrzanym linków, ani nie otwieraj załączników z nieznanymi lub niezweryfikowanymi źródłami. Może to bowiem skutkować pobraniem wirusa. Jeśli chcesz sprawdzić link, zawsze możesz skorzystać z Google lub przejść bezpośrednio do strony internetowej firmy. Wiadomości phishingowe z reguły zawierają bezosobowe formy powitania, ponieważ są kierowane dla ogółu odbiorców.

## Nie ujawniaj danych osobistych

To ogólna zasada w Internecie. Nie należy ujawniać danych osobowych ani finansowych za pośrednictwem poczty elektronicznej. Wejdź na stronę firmy, która żąda tych danych i sprawdź ich działalność oraz dane kontaktowe. Możesz do nich zadzwonić lub przyjść osobiście.

## Unikaj pilnych działań

Oszuści mogą nakłaniać do natychmiastowych działań, np. do kliknięcia lub wypełnienia ankiety w ograniczonym czasie. Czynności te mogą mieć na celu np. ponowne wysłanie polisy ubezpieczeniowej od firmy ubezpieczeniowej lub przekazanie darowizny na pomoc w walce z kryzysem. Zazwyczaj prowadzą jednak do witryn służących do wyłudzenia danych. Pamiętaj, aby zwracać uwagę na wszystkie pilne prośby e-mail!

## Podczas kryzysu

Uważaj na fałszywe organizacje lub sklepy internetowe sprzedające niezbędne towary (maski, płyny dezynfekujące...). Sprawdź stronę internetową, infolinię i recenzje na temat konkretnej firmy, a także opłaty za przesyłkę itp. Oszuści wykorzystują strach i emocje wywołane kryzysem aby skłaniać do robienia zakupów.

## Aktualizuj oprogramowanie antywirusowe

Upewnij się, że oprogramowanie antywirusowe i anty-malware na twoim komputerze działa i jest aktualne. Firmy antywirusowe posiadają obszerną wiedzę o cyberatakach. Czy wiesz, że możesz zainstalować dodatek anty-phishingowy w swojej przeglądarce?



Skontaktuj się z nami, jeśli masz pytania dotyczące zagadnień omawianych w prezentacji lub inne pytania z zakresu zapobiegania, wykrywania i dochodzenia w sprawie nieetycznych i nieuczciwych działań w organizacjach:

**Aaron Goldfinch**

Partner | Forensic Poland

Deloitte Advisory sp. z o.o. sp. k.

Al. Jana Pawła II 22, 00-133 Warszawa

Mobile: +48 662 155 399

agoldfinch@deloittece.com | www.deloitte.com

Nazwa Deloitte odnosi się do jednego lub kilku podmiotów Deloitte Touche Tohmatsu Limited („DTTL”), jej firm członkowskich oraz ich podmiotów powiązanych (zwanymi łącznie „organizacją Deloitte”). DTTL (zwana również „Deloitte Global”), każda z jej firm członkowskich i podmiotów z nimi powiązanych są prawnie odrębnymi, niezależnymi podmiotami, które nie mogą podejmować decyzji ani zobowiązań za inne podmioty wobec osób trzecich. DTTL, każda z jej firm członkowskich i podmiotów powiązanych ponoszą odpowiedzialność wyłącznie za własne działania i zaniechania, a nie za działania i zaniechania innych firm członkowskich i podmiotów powiązanych. DTTL nie świadczy usług na rzecz klientów. Zapraszamy na stronę [www.deloitte.com/pl/onas](http://www.deloitte.com/pl/onas) w celu uzyskania dalszych informacji.

Deloitte to wiodąca, międzynarodowa firma świadcząca klientom usługi obejmujące m.in. audyt, konsulting, doradztwo finansowe, zarządzanie ryzykiem, doradztwo podatkowe.

Nasza globalna sieć firm członkowskich i podmiotów powiązanych (zwana łącznie „organizacją Deloitte”) obejmuje ponad 150 krajów i terytoriów i świadczy usługi na rzecz czterech na każde pięć spółek z rankingu Fortune Global 500®. Aby dowiedzieć się, w jaki sposób około 312 000 pracowników Deloitte realizuje misję firmy, zachęcamy do odwiedzenia strony: [www.deloitte.com](http://www.deloitte.com).

Deloitte Central Europe to regionalna organizacja podmiotów działających w grupie Deloitte Central Europe Holdings Limited, firmy członkowskiej Deloitte Touche Tohmatsu Limited w Europie Środkowej. Usługi świadczą spółki zależne i powiązane z Deloitte Central Europe Holdings Limited, które stanowią odrębne i niezależne podmioty prawa. Spółki zależne i powiązane z Deloitte Central Europe Holdings Limited znajdują się w grupie wiodących firm, świadczących usługi profesjonalne w regionie Europy Środkowej; zatrudniają łącznie niemal 7 000 pracowników w 44 biurach, działających w 18 krajach.

© 2020. Wszelkich informacji udziela Deloitte Polska.