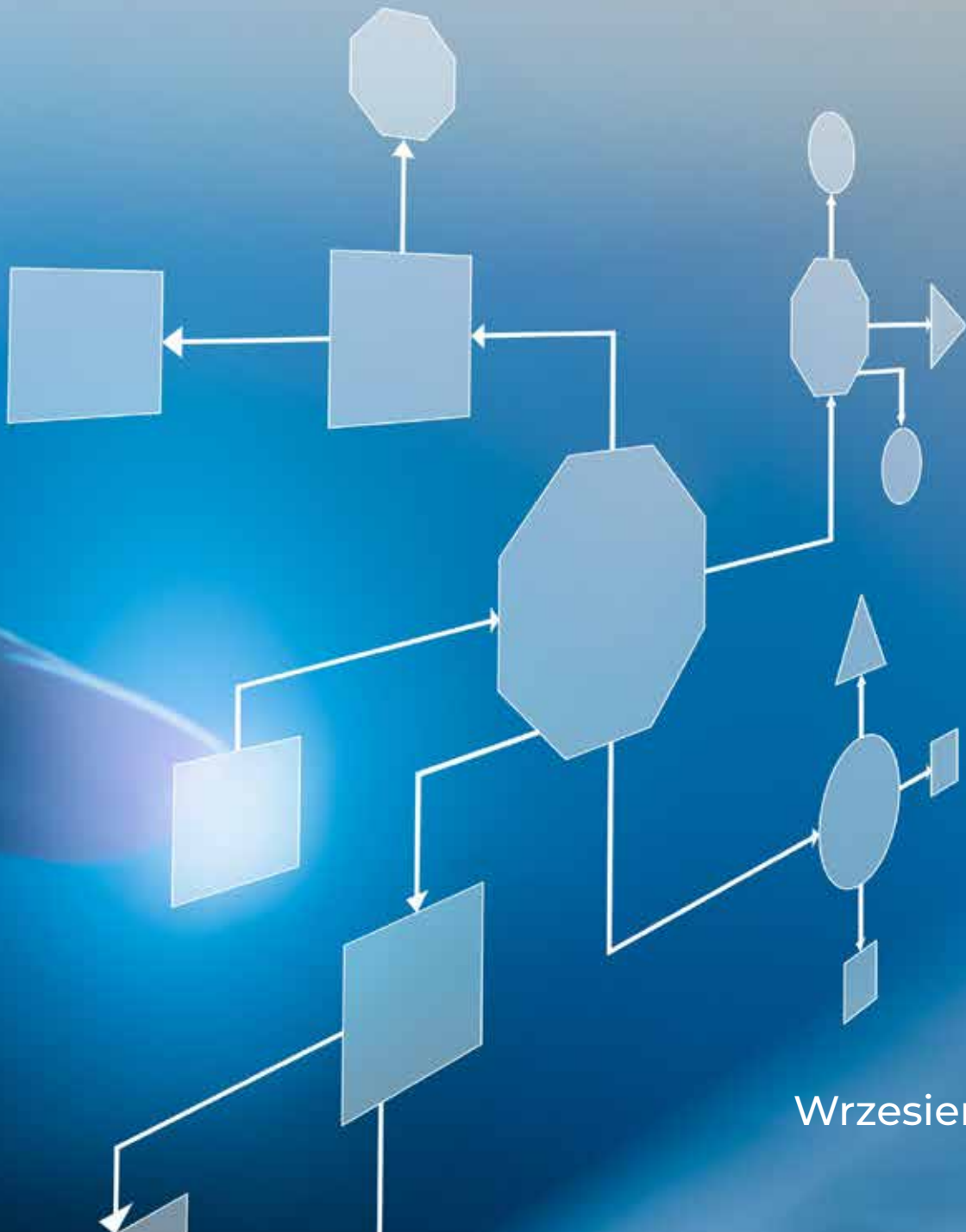


C-Suite *NEWS*



dla **70%**

organizacji kierowanie wielopokoleniowym zespołem jest ważne lub bardzo ważne z perspektywy odniesienia sukcesu w ciągu najbliższych 12-18 miesięcy, ale tylko 10% wyraża pełną gotowość do wdrożenia tego podejścia.

Źródło: Deloitte, „TRENDY: Wielopokoleniowy zespół”



5

Cyberbezpieczeństwo –
diagnoza ryzyka i zabezpieczenie
ciągłości operacyjnej w celu
minimalizacji kosztów

9

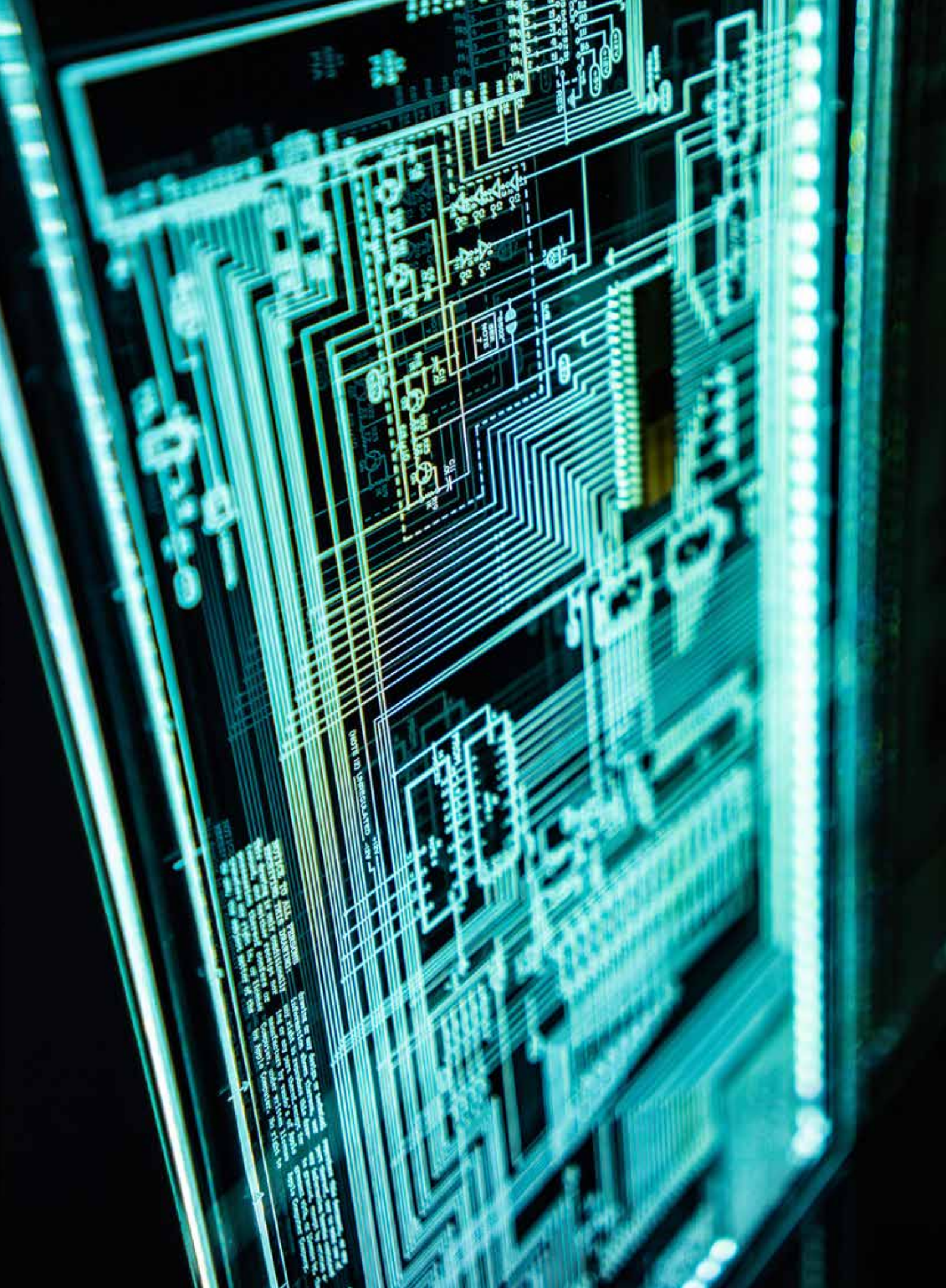
#nieudawany LEADERSHIP –
czyli o atrakcyjnej 5D, zwycięskiej
połówce i magicznym trójkącie!

12

Transformacja cyfrowa w controllingu
- wykorzystanie sztucznej inteligencji
i automatyzacji do prognozowania
i efektywnego zarządzania danymi
finansowymi

16

Ceny transferowe w liczbach.
Jakim wyzwaniem przychodzi sprostać
w przypadku kontroli?



Cyberbezpieczeństwo firmy – diagnoza ryzyka i zabezpieczenie ciągłości operacyjnej w celu minimalizacji kosztów

Dużo mówi się o hakerach, którzy czają się w wirtualnym świecie, gotowi zaatakować niewystarczająco przygotowane firmy. Codziennie mają miejsce skuteczne cyberataki w celu kradzieży danych firmowych. Eksperti stale podkreślają, jak ważna jest przemyślana ochrona przed cyberprzestępcami. Jednak w sporej liczbie przedsiębiorstw aspekt ten wciąż kuleje – a to nie ma wystarczających środków w budżecie, a to brakuje na rynku specjalistów od bezpieczeństwa IT, a to kadra zarządzająca wychodzi z założenia, że jakoś to będzie...

Niestety cyberatak na organizację, która nie skupiła się na diagnozie ryzyka i nie zadbała o zabezpieczenie ciągłości operacyjnej, jest **dużo bardziej brzemienny w skutkach** (nie tylko finansowo!) niż w przypadku organizacji, która się przygotowała do niego z wyprzedzeniem. Zobacz, jak do tematu cyberbezpieczeństwa firmy podejść z głową.

Czy każda firma powinna się obawiać cyberzagrożeń?

Niektórzy przedsiębiorcy, myśląc o cyberzagrozeniach, pokładają wiarę w łut szczęścia. Usilnie wyznają zasadę „mnie to na pewno nie spotka”. Uważają, że skoro w ogromnym morzu, jakim jest internet, pływają miliony rybek, istnieje znikoma szansa, że haker zarzuci wędkę właśnie na nich. Nie widzą sensu inwestowania czasu, energii i pieniędzy w zabezpieczenia, skoro atak może nigdy nie nastąpić.

Takie podejście jest podsycane przez popularne przekonanie, że cyberprzestępcy atakują tylko duże firmy i korporacje obracające milionami złotych. **Nic bardziej mylnego!** Myślenie, że mniejsza organizacja nie stanowi atrakcyjnego celu w sieci, to mit! Z danych raportu ESET Digital Security Sentiment wynika, że 59 proc. polskich firm z sektora MŚP stanowiło w 2022 roku cel cyberataku. Małe i średnie przedsiębiorstwa doświadczają około połowy wszystkich cyberataków na firmy.

Skąd zatem wziął się taki mit? Przede wszystkim z tego, że ataki na duże przedsiębiorstwa są znacznie bardziej medialne, więc chętniej się o nich mówi i pisze. Nic tak nie działa na emocje odbiorców jak spektakularna sprawa, która dotyczy powszechnie znanego podmiotu i wiąże się ze stratami wynoszącymi grube miliony dolarów.



Dariusz Piaścik

Sales&Development Director
Sagenso

Pamiętaj, żadna organizacja nie jest w pełni bezpieczna w sieci. Dlatego jeśli prowadzisz firmę – nieważne jak dużą – **potraktuj cyberbezpieczeństwo priorytetowo**. Nigdy nie wiadomo, kiedy haker weźmie na celownik właśnie Ciebie. Mleko zawsze może się rozlać. Jednak dojdzie do tego, zanim zdążysz się wcześniej przygotować, naprawdę trudno będzie to wszystko posprzątać.

Przestój działalności w wyniku cyberataku generuje ogromne koszty

Co grozi przedsiębiorstwu w sieci? Do grona najpopularniejszych cyberzagrożeń należą: **phishing, ransomware, złośliwe oprogramowanie oraz ataki DDoS**. Poza tym firma powinna się liczyć z takimi problemami jak: kradzież tożsamości, kradzież lub zgubienie sprzętu firmowego, naruszenie poufności danych, zagrożenia wewnętrzne wywołane działaniem (celowym lub nie) pracowników.

Statystyki są bardzo alarmujące. Do CERT Polska w 2022 roku wpłynęło około 322 tys. zgłoszeń odnośnie incydentów. To wzrost o niemal 178 proc. w porównaniu z rokiem poprzednim. Najczęściej zgłaszano phishing, który stanowił 64 proc. incydentów. Z kolei według badania Sophos w 2021 roku **ofiarą ransomware padło aż 77 proc. polskich firm**. Połowa zaatakowanych zdecydowała się na zapłacenie okupu.

Co właściwie czeka firmę, jeżeli atak ze strony hakerów nastąpi? Przede wszystkim trzeba się przygotować na **poważne straty finansowe**. Jeżeli dojdzie do przerwania ciągłości operacyjnej w wyniku cyberataku, na przykład systemy IT przestaną działać, firma musi na jakiś czas wstrzymać działalność. Niemal 80 proc. przedsiębiorstw biorących udział w badaniu ITIC poinformowało, że godzina przestoju to szacowany koszt 300 tys. dolarów! Oczywiście

wiele zależy od branży i wielkości organizacji. Dla przykładu, gdy w 2016 roku Delta Airlines doświadczyła 5-godzinnego przestoju, straciła blisko 150 milionów dolarów.

Nie tylko straty finansowe, czyli opłakane skutki cyberataku na firmę

Zaatakowana firma powinna się przygotować, że straty finansowe w wyniku przerwania ciągłości biznesowej to dopiero początek trudnej i wyboistej drogi. Gdy przedsiębiorstwo nie wywiąże się z kontraktów lub w ręce hakerów trafią dane klientów, trzeba się liczyć z zerwanymi umowami, a nawet **kosztami procesowymi**. W parze z czymś takim idzie utrata reputacji firmy, drastyczne zmniejszenie zaufania ze strony partnerów biznesowych i mniejsza szansa na pozyskanie nowych kontrahentów.

Jeżeli doszło do wycieku wrażliwych danych, przed firmą zamajaczy **ryzyko kary RODO**. Co więcej, cyberprzestępcy mogą sprzedać pozyskane informacje konkurencji, więc przedsiębiorstwo straci przewagę konkurencyjną. A jeśli dane firmowe zostały zaszyfrowane przez oprogramowanie ransomware, organizacja stanie przed trudną decyzją, czy zapłacić okup.

Do tego dochodzi jeszcze kwestia uszkodzonego sprzętu oraz infrastruktury IT. **Naprawienie takich zniszczeń to kolejne koszty**. W dodatku nigdy do końca nie wiadomo, jak rozległy atak przypuścili hakerzy – ile danych wykradli, co postanowili zrobić z pozyskanymi informacjami, czy nie zostawili po sobie oprogramowania szpiegowskiego...

Dlatego lepiej **zadbać o cyberbezpieczeństwo, zanim incydent nastąpi**. Taka inwestycja wymaga mniejszych nakładów finansowych niż rozpaczliwa walka ze skutkami działań hakerskich. W znacznym stopniu minimalizuje ryzyko zagrożenia. A jeśli mimo wszystko dojdzie do ataku – przyspiesza czas reakcji i poważnie ogranicza straty.

Poznaj swoje silne i słabe strony, czyli jak zdiagnozować ryzyko cyberataku

Czy wiesz, że w 2022 roku hakerzy z Wietnamu niemal bezwysiłkowo włamali się do systemu Holiday Inn, a dokładniej na konto właściciela? „Dla zabawy” wpisywali najpopularniejsze hasła. Udało im się zdobyć dostęp za pomocą prostej kombinacji “Qwerty1234”. Tę jakże świetną rozrywkę zakończyli, usuwając dużą część

danych i pozostawiając firmę z problemami.

Czy wiesz, że w 2022 roku hakerzy z Wietnamu niemal bezwysiłkowo włamali się do systemu Holiday Inn, a dokładniej na konto właściciela? „Dla zabawy” wpisywali najpopularniejsze hasła. Udało im się zdobyć dostęp za pomocą prostej kombinacji “Qwerty1234”. Tę jakże świetną rozrywkę zakończyli, usuwając dużą część danych i pozostawiając firmę z problemami.

Wskazany przykład pokazuje, jak ważne jest wzięcie pod lupę całej organizacji, a więc staranne **prześledzenie zarówno silnych, jak i słabych stron pod kątem cyberbezpieczeństwa**. Może się okazać, że hakerzy wcale nie muszą używać łomu czy dorabiać klucza, żeby wejść przez drzwi. Czasem te drzwi po prostu stoją otworem...

Jak się zabrać za diagnozę ryzyka? Krokiem, który warto postawić jak najszybciej, jest **audyt bezpieczeństwa IT**. Takie działanie pozwoli dogłębnie przeanalizować i ocenić stan infrastruktury informatycznej, serwerów czy sieci, a także jakość stosowanych procedur i zgodność z regulacjami. Wszystko po to, żeby dowiedzieć się, jak wygląda obecna sytuacja, co szwankuje, co wymaga poprawek, co można zrobić lepiej, a o czym zapomniano. Audyt IT zawiera zestaw wskazówek i rekomendacji, które warto wdrożyć, żeby podnieść poziom cyberochrony w firmie, a także zoptymalizować procesy. To przekłada się na niższe koszty w przyszłości.

Czy taka diagnoza musi być przeprowadzona przez osobę mającą rozległe kwalifikacje z zakresu cyberbezpieczeństwa? Niekoniecznie. To zależy od tego, na które rozwiązanie się zdecydujesz. Na przykład **Telescope, czyli audyt bezpieczeństwa IT** stworzony przez Sagenso, nie wymaga specjalistycznej wiedzy. Możesz go **przeprowadzić samodzielnie**. Intuicyjne narzędzie poprowadzi Cię za rękę przez cały proces. Na koniec uzyskasz raport identyfikujący obszary wymagające natychmiastowych działań. Możesz szczegółowo omówić te wyniki z dedykowanym ekspertem. Powie, co zrobić w następnej kolejności, by firma stała się bardziej bezpieczna.

Ryzyko zdiagnozowane, błędy naprawione... Co dalej?

Poznanie stanu obecnego i naprawienie niedociągnięć to dopiero początek. Miej na uwadze, że hakerzy wykazują się ogromną kreatywnością, żeby osiągnąć swój cel. Nie dość, że zgromadzili spory arsenał skutecznych działań, to wciąż go ulepsza-

“

Jeżeli doszło do wycieku wrażliwych danych, przed firmą zamajaczy ryzyko kary RODO. Co więcej, cyberprzestępcy mogą sprzedać pozyskane informacje konkurencji.

”

ją i rozbudowują. Dlatego zabezpieczenia, jakie do tej pory się w firmie sprawdzały, kiedyś mogą nie wystarczyć. **Cyberbezpieczeństwo to proces, który stale zmienia się i przekształca**, więc musisz regularnie weryfikować dotychczasowe rozwiązania, aby upewnić się, czy wciąż działają tak, jak powinny.

Chcesz stale trzymać rękę na pulsie i stać się godnym przeciwnikiem dla cyberprzestępców? Zadbaj o stworzenie **kompleksowej strategii cyberbezpieczeństwa**. Żeby odpowiednio do tego podejść, możesz zasięgnąć porady eksperta – na przykład umówić się na bezpłatne konsultacje na temat cyberbezpieczeństwa ze specjalistą [Sagenso](#).

W porozumieniu z fachowcem **dobierz odpowiednie procedury zwiększające bezpieczeństwo firmy** i minimalizujące koszty wynikłe z potencjalnego cyberataku. Przygotuj scenariusze działań na różne okazje. Kogo w firmie powiadomić, gdy doszło do próby wyłudzenia danych? Jakie kroki podjąć po ataku ransomware? Jakie procedury zastosować po wycieku danych? Kto jest odpowiedzialny za wykonywanie kopii zapasowych? Kto zarządza dostępami do systemu IT? Między innymi na takie pytania trzeba sobie odpowiedzieć. Spisz wszystko w dokumencie, do którego wgląd powinni mieć wszyscy pracownicy.

Jasna strategia jest niezwykle ważna w kontekście zapewnienia ciągłości biznesowej. Dzięki niej możesz sprawnie uniknąć wielu zagrożeń. A jeżeli do jakiegoś incydentu, każdy członek zespołu będzie wiedział, co i jak robić. W takich momen-

tach szybkość reakcji stanowi czynnik, który w dużej mierze decyduje o wielkości poniesionych strat. Niestety wiele firm próbuje działać bez takiego dokumentu. Według danych z badania przeprowadzonego przez UpCity **tylko połowa organizacji posiada wdrożony plan bezpieczeństwa IT**. W dodatku 1/3 tych podmiotów nie modyfikuje stworzonego już planu.

Jeżeli chcesz, żeby Twoja firma uniknęła olbrzymich kosztów wynikłych z cyberzagrożeń, odrzuć w kącie zasadę „mnie to nie spotka” i zacznij działać. Stwórz zabezpieczenia, przez które hakerom będzie trudno się przedrzeć. Taka inwestycja czasu i środków **pozwoli Ci spać spokojnie**.

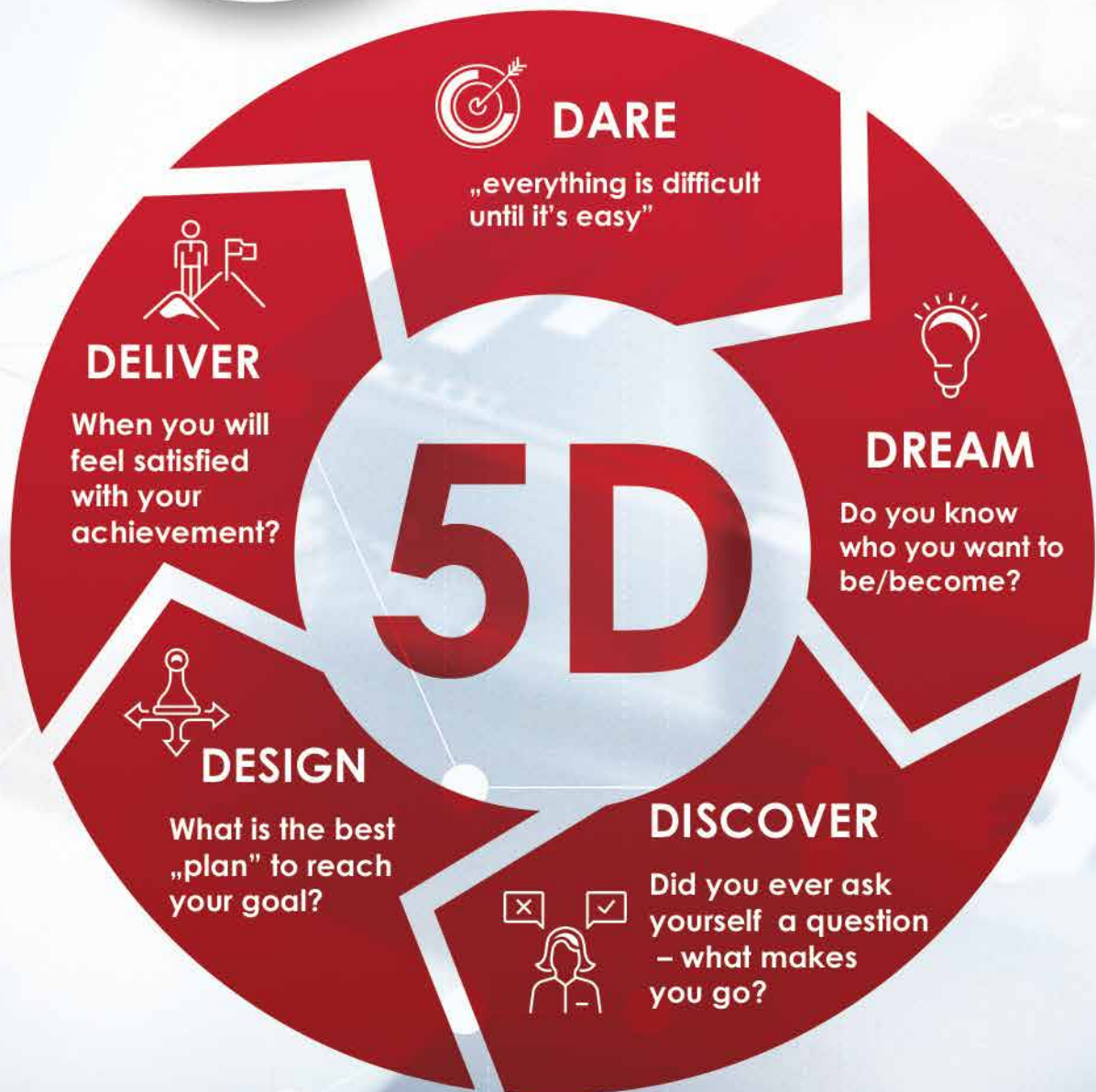
Sagenso Sp. z o.o. realizuje projekt „Opracowanie i walidacja opartego na sztucznej inteligencji systemu do ochrony przed złośliwym oprogramowaniem typu ransomware” POIR.01.01.01-00-0228/22 współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Inteligentny Rozwój, realizowany w ramach konkursu Narodowego Centrum Badań i Rozwoju: „Szybka Ścieżka – Innowacje Cyfrowe”.





DARE TO DELIVER YOUR DREAMS!

Violetta Malek, MBA
Absolvent VIP
& Mentor of Łódź University
Global Business Mentor of Everwise,
Co-Founder of Gekko advisoryNOW
& controllingNOW



mentorNOW by

Gekko
advisoryNOW

#nieudawany LEADERSHIP – czyli o atrakcyjnej 5D, zwycięskiej połówce i magicznej trójkącie!

Nie! Nie będę dziś pisać o stylach zarządzania i przywoływać cech liderów autokratycznych, demokratycznych czy charyzmatycznych. Nie będę wskazywać różnic między liderem a menadżerem i nie będę, o zgrozo!, doszukiwać się powodów, dla których półć miałaby odgrywać kluczową rolę w byciu #nieudawanym liderem! Będę natomiast omawiać i dzielić się skutecznym podejściem do budowania silnych zespołów, które nie cierpią udawania i stawiają na prawdziwość w codziennej realizacji zadań. Zadań, które angażują i rozwijają, a ich realizacja daje satysfakcję i przyczynia się do sukcesu zespołu, jego członków i firmy.

Dzisiejszy świat biznesu, który w swym pędzie jest zmienny, niepewny, złożony i nieprzewidywalny (VUCA), potrzebuje jak nigdy dotąd prawdziwych, autentycznych i #nieudawanych liderów. Czy rzeczywiście jak nigdy dotąd? Jack Welch już dawno temu zauważył, że „kiedy tempo zmian zachodzących na zewnątrz firmy jest większe niż tempo zmian wewnątrz - zbliża się koniec”. Ja uważam, że tak, mamy do czynienia z sytuacją jak nigdy dotąd, ponieważ nigdy dotąd w takim wymiarze nie pracowaliśmy zdalnie oraz nie korzystaliśmy z nowoczesnych rozwiązań technologicznych i narzędzi robotyzujących tak wiele aspektów pracy ludzkiej. Nigdy dotąd nie napisano tylu poradników biznesowych na temat leadershipu, nigdy dotąd nie było tak bogatej oferty szkoleniowej i nigdy dotąd nie doświadczaliśmy tak wielkiego deficytu #nieudawanego przywództwa!

Kim jest #nieudawany lider?

Na *synonym.net* czytamy, że nieudawany to: niepozowany, rzetelny, realny, zgodny z rzeczywistością, autentyczny, rzeczywisty, szczery, właściwy, będący oryginałem, niekłamany, samodzielny, nienaśladowczy, niesfałszowany, niepozorowany, naturalny, prawdziwy, nieobłudny, niefałszywy, niewymuszony, z krwi i kości, wiarygodny, faktyczny.

Czy taki lider istnieje? Oczywiście tak, ale należy do niezwykle niewielkiego grona!

Z różnych badań dotyczących oczekiwań co do postawy lidera wynika, że około 20% osób pełniących role menadżerskie przejawia cechy autentycznego lidera (m.in. badanie Gallupa mówi, że jedynie 18% menadżerów posiada kompetencje zarządzania talentem).



Violetta Małek

Co-Founder & CEO
Gekko advisoryNOW,
Co-Founder controllingNOW

Dlaczego zatem aż 80% (Gallup 82%) zarządzających tak trudno jest dostać się do tego grona? Co powoduje, że zarządzanie kapitałem ludzkim jest dla nich tak trudne? Ja uważam, że nie o trudność tutaj chodzi, a raczej o podejście, o metodykę, o sprawdzone przez garstkę skutecznych liderów style i schematy oraz - co jest krytycznym aspektem - o niedopuszczenie do usypiania empatii wraz z rosnącą władzą. I tutaj pojawia się czynnik ludzki, niezwykle ważny aspekt, który nabiera coraz większych rozmiarów w czasach #vuca, #rpa, #remotework, #multigenerations oraz #wellbeing w kontekście nowych wartości, o których przypomniła pandemia C-19.

Dla mnie #nieudawany lider to ktoś, kto potrafi wydobyć z każdego członka zespołu potencjał „ukryty” i zagospodarować „jawny”, potrafi zbudować zespół, który jest zgrany i niezwykły, bo jest inspirowany i motywowany do poszukiwania skutecznych rozwiązań, których osiągnięcie daje ogromną satysfakcję. #nieudawany lider prowadzi swój zespół przez meandry biznesu, będąc wymagającym coachem i mentorem. Jest to taki ktoś, kto określa obowiązki, daje odpowiedzialność, wyposaża w odpowiednie narzędzia i strategie oraz zaraża pasją, aby zmaksymalizować sukces organizacji, jednostki i zespołu!

Odkąd sama stałam się #nieudawanym liderem, aktywnie udzielam się w dyskusjach na temat „odejść” członków zespołu. Nie tylko dlatego, że dzieje się tak, jak to mówi słynne już powiedzenie, że „ludzie przychodzą do firmy, a odchodzą od menadżera”, ale głównie dlatego, że można tego uniknąć. Według mnie o wiele lepiej brzmi, że „ludzie przychodzą do firmy i do menadżera, i nie odchodzą”, co wspaniale ujął Richard Branson: „wyszkol

ludzi na tyle dobrze, żeby mogli odejść, traktuj ich na tyle dobrze, żeby nie chcieli!“ A jeśli odchodzą, to jest to ich kolejny krok w rozwoju zawodowym, wypracowany wspólnie z #nieudawanym liderem! Nowe powiedzenie staje się rzeczywistością, jeśli zastosowane zostaną 3 podejścia/metodyki do zarządzania talentem/kapitałem ludzkim/zespołem: atrakcyjna **5D**, zwycięskie **50%** i magiczny **Trójkąt**.

Atrakcyjna 5D „Odważ się realizować marzenia” (eng. „Dare to Deliver your Dreams”)



Metodyka pozwalająca zdiagnozować potencjał, określić długoterminowy cel rozwoju i plan realizacji dla każdego członka zespołu. Pierwszy krok to - **ODWAŻ** się, mierz wysoko, daleko (**DARE**), bo - zgodnie z powiedzeniem Thomasa Fullera - „wszystko jest trudne, zanim stanie się łatwe”. W tym kroku następuje zwolnienie hamulców, nabranie wiatru w żagle, zbudowanie wewnętrznej siły i wzmocnienie wiary w siebie. Drugi krok to - **WYOBRAŹ** sobie siebie za kilka lub kilkanaście lat (**DREAM**), bo każdy, w którymś momencie swojego życia, myślał o tym, kim chciałby zostać w swoim zawodowym życiu.

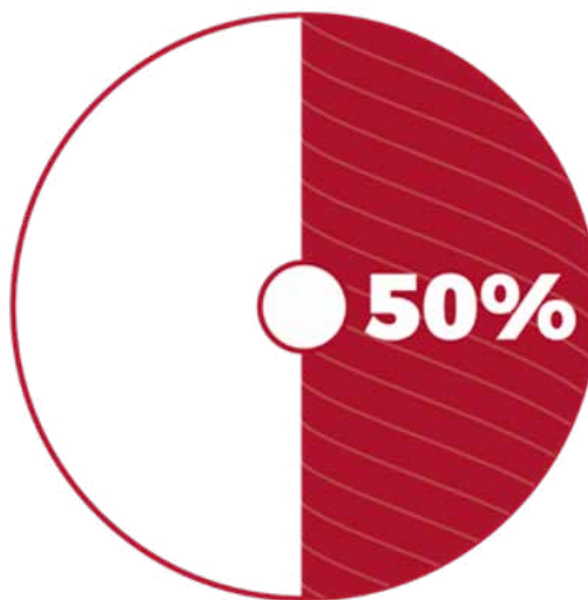
Dzieci marzą, aby zostać kosmonautą, nauczycielem czy prezesem. Jako nastolatki wybierają kierunki studiów, które przybliżają ich do tego celu. Studenci natomiast, bogatsi o nowe doświadczenia życiowe i projektowe, utwierdzają się w swoim pierwotnym wyborze lub wręcz gubią w gąszczu możliwości, jakie daje dzisiejszy biznes. #nieudawany lider, który niejednokrotnie zarządza zespołem wielopokoleniowym, ma za zadanie dotarcie do tych celów lub ich wypracowanie z każdym członkiem zespołu. W tym miejscu pojawia się krok trzeci – **ODKRYJ** swój potencjał (**DISCOVER**), którego identyfikacja pozwala jak najlepiej dopasować talent do zadań na aktualnym lub przyszłym stanowisku pracy. **ZAPROJEKTUJ** drogę do celu (**DESIGN**).

Tutaj mamy do czynienia z dwoma podejściami: 1) brak długoterminowego celu rozwoju i przyjmowanie tego „co życie podrzuci” oraz 2) określenie celu długoterminowego. Chociaż dla wielu osób podejście nr 1 wydaje się bardzo dynamiczne, elastyczne czy wręcz zwinne, to niesie ze sobą ryzyko „zapędzenia w kozły róg”, bo oddajemy kontrolę przypadkowi i krótkotrwałym preferencjom czy chwilowej słabości.

O wiele bardziej skutecznym jest podejście nr 2, które pozwala na utrzymanie kontroli nad naszym rozwojem i na dotarcie do celu lub świadomą jego zmianę. Tylko wtedy, kiedy mamy długoterminowy cel, jesteśmy w pełni przygotowani do reagowania na wszelkie okoliczności, które życie nam przynosi. Po określeniu celu dochodzi do zdefiniowania planu dotarcia, czyli do 5 kroku - **OSIĄGNIJ** swój cel (**DELIVER**).

Jestem wielkim zwolennikiem dążenia do ciągłego inwestowania około 50% czasu lidera/menadżera w kapitał ludzki/talent. Inwestorzy giełdowi doskonale wiedzą, co mam na myśli - sam pieniądz niczego nie zdziała, chyba, że dostanie się w dobre ręce i ponadprzeciętna wartość zostanie wygenerowana. To samo dzieje się z talentem/potencjałem zespołu! Tylko prawdziwy i #nieudawany lider potrafi **zastosować** **podejście 5D**, aby „obracać” skutecznie kapitałem, niejednokrotnie go powiększając, rozwijając i szlifując!

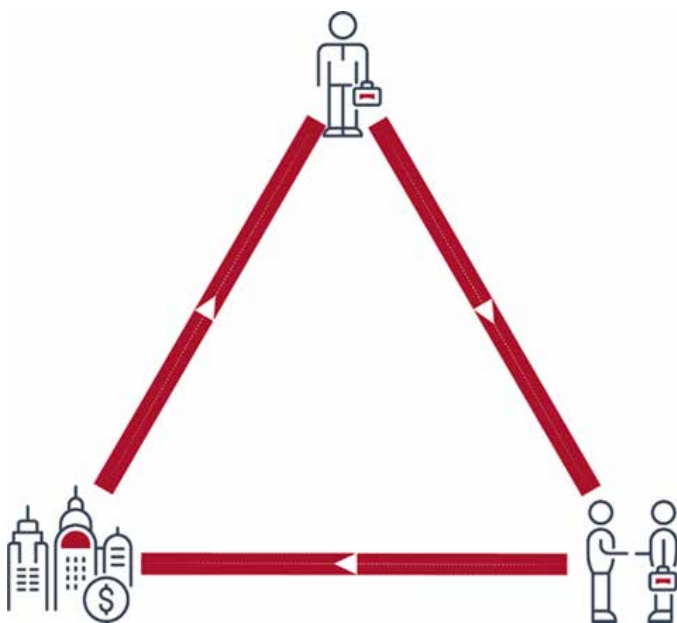
Zwycięska POŁÓWKA



Co jeszcze wchodzi w skład podejścia „50%”? W zależności od **dojrzałości zespołu** (może być na przykład „młody”, nowo powstały z opracowanymi opisami stanowisk, celami i ścieżkami kariery lub „stary”, bez aktualnych/relevantnych opisów stanowisk, teoretycznymi/oderwanymi od rzeczywistości, i wcale nie SMART celami oraz brakiem planów rozwoju) i **kultury organizacyjnej firmy** należy:

1. odpowiednio dobrać i „uszyć na miarę” strukturę organizacyjną zespołu,
2. opracować drzewo sukcesji dla każdego pracownika,
3. wypracować/określić potencjał „jawny” i „ukryty”,
4. dążyć do „poznania” aspektów wpływających na dobrostan każdego członka zespołu.

Magiczny TRÓJKĄT



Magia trójkąta polega głównie na tym, że jest i powinien pozostać równoboczny (zapewniający równowagę)! Na wierzchołkach są: **jednostka** (członek zespołu), **zespół** oraz **firma**. To oznacza, że tylko wtedy, kiedy cele jednostki (i te rozwojowe, i te operacyjne), cele zespołu i cele firmy są spójne, współgrające, skorelowane, harmonijne i tak samo ważne, jest szansa na ich pełną realizację. Zwykle skaskadowanie celów operacyjnych firmy „top-down” nie zapewni pełnej równowagi, której osiągnięcie jest w rękach #nieudawanego lidera! Bo to on doprowadza do odkrycia drzemiącego potencjału w każdym członku zespołu, bo to on wspólnie z zespołem wypracowuje cele operacyjne zespołu, których spełnienie (a w tak zarządzanym zespole często przekroczenie) przyczynia się do sukcesu i

realizacji celów operacyjnych i biznesowych firmy.

Krytyczne warunki zapewniające równowagę:

1. każdy członek zespołu utożsamia się ze swoimi celami operacyjnymi, bo ich realizacja wspiera rozwój zawodowy (praca według metodyki 5D),
2. wszyscy członkowie zespołu dobrze wiedzą, jak realizacja ich celów operacyjnych przyczynia się do osiągnięcia wyników przez firmę (przydatne jest tutaj np. drzewo strategiczne),
3. #nieudawany lider upewnia się, że cele operacyjne (często też rozwojowe) każdego członka zespołu są dobrze znane koleżankom i kolegom z zespołu (komunikacja pozioma, wewnątrz-zespołowa), co pozwala na spójną i optymalną ich realizację (warsztaty robocze, na których omawiane są cele indywidualne, ich oddziaływanie na siebie i sposoby optymalizacji tych, które się zazębiają),
4. zespół wypracowuje własną misję i wizję (spójną ze strategią firmy), co pozwala każdemu pracownikowi utożsamiać się, zaangażować i dawać z siebie to, co najlepsze. Najważniejszym faktorem sukcesu w tej relacji jednostka - zespół jest świadomość tego, jak realizacja celów operacyjnych zespołu sprzyja rozwojowi zawodowemu każdego z jego członków,
5. kultura firmy zorientowana jest na talent, na prawidłowy rozwój kompetencji i na mądre „obracanie” kapitałem ludzkim, który stanowi cenny i główny zasób firmy!

Świat, w którym żyjemy i prowadzimy biznes, wymaga od zarządzających większej koncentracji na człowieku, jego potencjale i potrzebach, mimo że (albo właśnie dlatego) poziom automatyzacji procesów sięga swoich historycznych wyżyn (a z racji zwiększania, z roku na rok, inwestycji w nowoczesne technologie będzie jeszcze wyżej). Przedstawione powyżej, moje 3 autorskie metodyki/podejścia są bardzo skuteczne, jeśli są wdrażane przez #nieudawanego lidera o wysokim ilorazie EQ. Jego sekretem jest to, w jaki sposób tworzy zespół => stawiając na różnorodność, entuzjazm i nieograniczoną energię. Wydobywa z każdego członka zespołu to, co najlepsze, rozwija i obserwuje, jak praca staje się jego pasją, a firma i on sam odnosi sukces!

“

Zwykle skaskadowanie celów operacyjnych firmy „top-down” nie zapewni pełnej równowagi, której osiągnięcie jest w rękach #nieudawanego lidera!

”

Transformacja cyfrowa w controllingu

- wykorzystanie sztucznej inteligencji i automatyzacji do prognozowania i efektywnego zarządzania danymi finansowymi

W dynamicznym i coraz bardziej globalnym środowisku biznesowym skuteczne zarządzanie danymi finansowymi i umiejętność dokonywania prognoz stanowią fundamentalny element sukcesu organizacji. W związku z tym funkcja controllingowa jest jednym z tych obszarów biznesowych, które w nadchodzących latach powinny być szczególnie otwarte na cyfrową transformację, wykorzystującą narzędzia sztucznej inteligencji (AI) i automatyzację.

Korzyści z wykorzystywania AI w controllingu

W uproszczeniu sztuczna inteligencja umożliwia komputerom i systemom IT wykonywanie zadań, które normalnie wymagałyby ludzkiego myślenia. W obszarze controllingu AI może być wykorzystywana do analizy dużych zbiorów danych finansowych w celu identyfikacji trendów, wykrywania anomalii oraz prognozowania przyszłych wyników finansowych. Algorytmy uczenia maszynowego mogą analizować historyczne dane finansowe i na ich podstawie tworzyć modele predykcyjne, które wspierają proces budżetowania i planowania długookresowego oraz podejmowanie strategicznych decyzji finansowych i biznesowych. Ponadto sztuczna inteligencja może pomóc w automatyzacji procesów controllingu, takich jak analiza kosztów, zarządzanie ryzykiem czy raportowanie finansowe. Dzięki temu pracownicy działu finansowego mogą skupić się na bardziej wartościowych zadaniach, takich jak interpretacja wyników analiz i opracowywanie strategii poprawy wyników.



Paweł Młyński

Partner, Gekko advisoryNOW

Potencjalnych korzyści z transformacji cyfrowej z wykorzystaniem AI jest wiele, do kluczowych należą:

- 1. Szybkość i efektywność** - automatyzacja i zaangażowanie AI do analizy raportów pozwala na szybsze przetwarzanie danych i generowanie raportów w czasie rzeczywistym, umożliwiając szybsze podejmowanie decyzji.
- 2. Większa precyzja** - algorytmy SI mogą dokładnie analizować duże ilości danych, eliminując błędy ludzkie i poprawiając precyzję analiz finansowych.
- 3. Lepsze prognozowanie** - dzięki analizie dużych zbiorów historycznych danych i wykorzystaniu modeli predykcyjnych opartych na AI, organizacje mogą dokładniej przewidywać przyszłe wyniki finansowe.
- 4. Oszczędność czasu i zasobów** - dzięki automatyzacji rutynowych zadań, pracownicy mogą skupić się na bardziej wartościowych aspektach controllingu, takich jak interpretacja danych, zostawiając przetwarzanie i częściowo analizę danych robotom i AI.
- 5. Lepsze rozumienie danych** - AI może na podstawie złożonych danych wygenerować pogłębione wnioski, ujawniając trendy i zależności, które mogłyby umknąć ludzkiemu oku.
- 6. Minimalizacja błędów** - wykorzystanie AI i robotów eliminuje ryzyko ludzkich pomyłek, a także pozwala znacznie szybciej wykrywać anomalie i nieprawidłowości w danych.

Korzyści z AI i automatyzacji w controllingu

- 1** Szybkość i efektywność
- 2** Większa precyzja
- 3** Lepsze prognozowanie
- 4** Oszczędność czasu i zasobów
- 5** Lepsze rozumienie danych
- 6** Minimalizacja błędów

W jakich obszarach controllingu warto „zatrudnić” sztuczną inteligencję?

Decyzja o wykorzystaniu AI powinna być oparta o analizę sytuacji konkretnych organizacji – ich potrzeb, celów i możliwości. AI działa na danych, kluczowe jest więc określenie, na jakich danych pracuje (może pracować) dana organizacja i czy ich rodzaj i struktura są odpowiednie do uczenia maszynowego i innych technik AI. Wyniki takiej analizy powinny zostać zderzone z dostępnymi na rynku rozwiązaniami – wielu dostawców może zaoferować rozwiązania wykorzystujące AI dostosowywane czy wręcz tworzone w oparciu o specyfikę poszczególnych organizacji i jej procesów. Dostępnych jest również wiele sprawdzonych gotowych narzędzi i systemów, które rozwinęły swoje funkcjonalności dzięki AI (kilka przykładów z bardzo dużej oferty rynkowej: IBM Cognos Analytics - wykorzystuje AI do automatyzacji procesów generowania raportów i przewidywania trendów finansowych, SAP S/4HANA Finance - wykorzystuje AI do automatyzacji procesów finansowych oraz do tworzenia prognoz, narzędzia Oracle wykorzystują sztuczną inteligencję m.in. do analizy danych finansowych, identyfikacji trendów i dostarczania spersonalizowanych analiz kontrolingowych, Anodot - wykorzystuje uczenie maszynowe i sztuczną inteligencję do monitorowania biznesu i wykrywania anomalii).

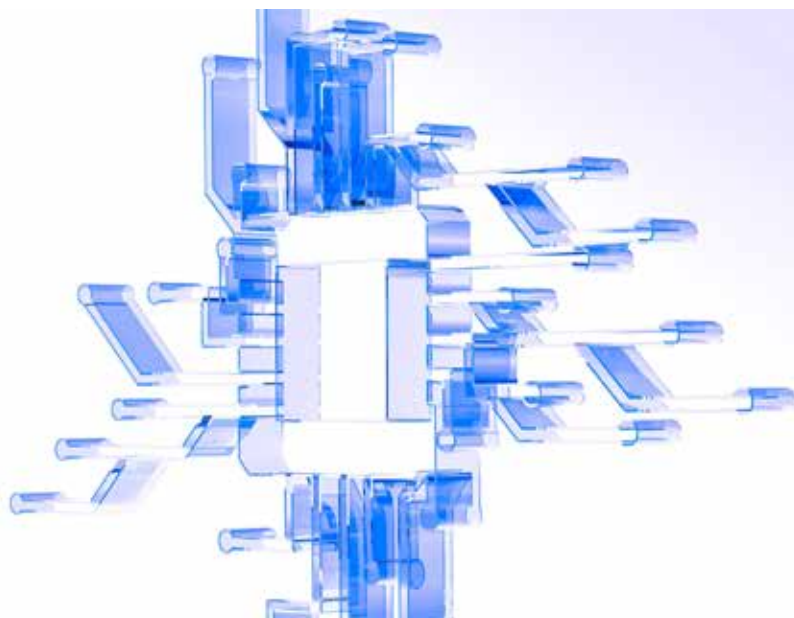
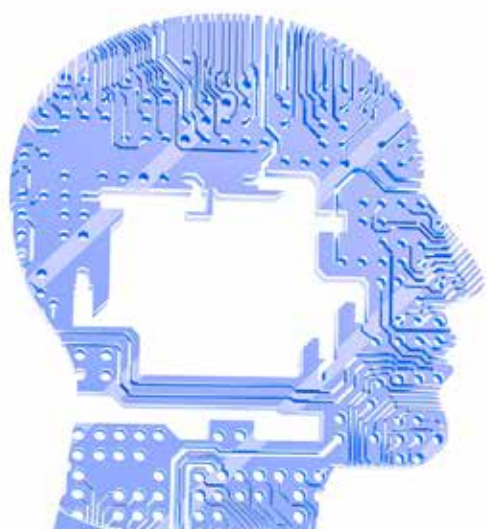
Nawet nie wchodząc w analizę potrzeb poszczególnych organizacji, można zidentyfikować te obszary controllingowe, w których AI jest już wykorzystywany w największym stopniu lub w których wzrostu stosowania narzędzi z elementami AI można się spodziewać w najbliższych latach:

- **prognozowanie** - jeden z obszarów kontrolingowych, w którym o AI mówi się najwięcej, m.in. dzięki możliwościom analizowania dużej ilości danych i tworzenia dynamicznych (i „samouczących się”) modeli predykcyjnych. Ostatnie lata pokazały nam, jak trudne do przewidzenia jest otoczenie (obecnie mówi się wręcz o świecie

BANI, czyli: B (*Brittle*) – kruchy, A (*Anxious*) – niepokojny, (*Non-linear*) – nieliniowy i I (*Incomprehensible*) – niezrozumiały), stąd też presja na wykorzystanie zaawansowanych, przekraczających możliwości ludzkiego umysłu narzędzi do prognozowania rośnie,

- **analizy i raportowanie zarządcze** - narzędzia z wbudowanym AI mogą nie tylko przygotowywać złożone analizy w oparciu o wiele kompleksowych źródeł danych (niezależnie od obszaru), ale również wyciągać na ich podstawie wnioski i formułować rekomendacje biznesowe (przy wykorzystaniu *machine learning*),
- **zarządzanie ryzykiem i funkcje kontrolne** - część zadań związanych z identyfikowaniem ryzyk (w tym finansowych) i ich oceną znajduje się często w funkcji controllingowej. Narzędzia wykorzystujące AI mogą pomagać w wykrywaniu anomalii, ostrzegać o potencjalnych zagrożeniach, znajdować w danych nieprawidłowości i niestandardowe przypadki, kontrolować koszty, wykorzystanie zasobów i kluczowe wskaźniki,
- **monitorowanie działalności biznesowej** - metody sztucznej inteligencji mogą przyczynić się na wiele sposobów do bardziej efektywnego i precyzyjnego monitorowania działalności biznesowej (np. wykrywania migracji klientów na dużych zbiorach danych),
- **analizy rynkowe** - sztuczna inteligencja jest w stanie zbierać i przetwarzać dane rynkowe, prognozować ewolucję trendów i wspomagać proces podejmowania decyzji związanych ze strategią marketingową, rozwojem produktów czy polityką cenową.

Oczywiście obszarów wykorzystania narzędzi z elementami AI jest znacznie więcej, biorąc pod uwagę jak duży potencjał automatyzacyjny oferuje sztuczna inteligencja. Czy w takim razie nadchodzi kres funkcji controllingowej obsługiwanej przez człowieka?



Czy AI zastąpi kontrolerów finansowych?

Aby spróbować odpowiedzieć sobie na pytanie o skalę „zagrożenia” dla kontrolerów finansowych ze strony AI, warto najpierw uświadomić sobie, jakie przewagi sztuczna inteligencja może posiadać nad człowiekiem w obszarze controllingowym.



Co do zasady, mózg ludzki pracuje dużo wolniej niż maszyna, jego prędkość i wydajność uzależniona jest od rodzaju problemu, z jakim się styka, ma też bardzo ograniczoną w stosunku do najnowszych technologii prędkość i wydajność gromadzenia oraz procesowania informacji. Sztuczna inteligencja może przetwarzać ogromne ilości danych na raz. Co więcej, człowiek na wysokim poziomie efektywności (wysokim dla człowieka, nie AI) może pracować w ograniczonym czasie, wymaga przerw i odpoczynku, zbyt długa praca zwiększa ryzyko błędów. W przypadku człowieka pojawia się również skłonność do optymizmu (skłonność do nierealistycznych prognoz i oceny faktów). Dodatkowo, ludzie często podświadomie dostosowują swoje prognozy do konkretnego punktu odniesienia (w przypadku prognozy taką „kotwicą” może być na przykład wartość z budżetu lub z poprzedniego roku), bywają nieobiektywni, a także ulegają naciskom, uprzedzeniom i emocjom. Sztuczna inteligencja i ucze-

nie maszynowe nie są tak podatne na ludzkie emocje ani subiektywne opinie, co prowadzi do bardziej precyzyjnych prognoz (choć oczywiście modele uczenia maszynowego również mogą być „obciążone” subiektywizmem ich twórców i zasilanymi danymi). AI jest również mniej podatne na manipulację – uczenie maszynowe opiera się na algorytmach w celu dokonywania prognoz i manipulowanie tymi prognozami jest znacznie trudniejsze niż w tradycyjnych metodach prognostycznych opartych o pracę ludzką. AI może również dostosowywać się na bieżąco do zmian w zbiorze danych, podczas gdy zmiana założeń, podejścia czy dostosowanie się do nowego zbioru danych człowiekowi zajmuje znacznie więcej czasu.

Lista przewag AI nad człowiekiem jest długa. Jednakże są obszary, w których przewaga człowieka wciąż jest bezsprzeczna. AI pracuje na danych i algorytmach, dlatego w trudnych sytuacjach sztucznej inteligencji może brakować ludzkiego zrozumienia kontekstu. Kontrolerzy mogą korzystać w swojej pracy z intuicji i doświadczenia, co jest trudne do odwzorowania przez maszyny. Ma to szczególnie istotne znaczenie w sytuacji ograniczonego dostępu do danych czy też błędnych danych. W przypadku AI trudniej też jest sprawować kontrole nad procesem decyzyjnym, gdyż często decyzje są podejmowane na podstawie skomplikowanych modeli, trudnych do zrozumienia przez ludzi.

Sztuczna inteligencja wciąż posiada wiele ograniczeń, generuje dodatkowe ryzyka związane np. z bezpieczeństwem i prywatnością danych, a w wielu przypadkach jest jeszcze rozwiązaniem zbyt drogim dla organizacji. Dlatego należy ją traktować jako rozwiązanie komplementarne do pracy kontrolerów – ich zadania muszą być przeformułowywane w związku z wykorzystaniem AI, natomiast do tego, aby AI stało się pełnoprawnym partnerem w zakresie finansów i controllingu wciąż bardzo daleka droga. Nie zmienia to faktu, że transformacja cyfrowa w controllingu związana ze sztuczną inteligencją i automatyzacją to nieunikniony kierunek dla organizacji dążących do osiągnięcia lepszej efektywności, precyzji i szybkości w zarządzaniu danymi finansowymi.

“

Decyzja o wykorzystaniu AI powinna być oparta o analizę sytuacji konkretnych organizacji – ich potrzeb, celów i możliwości.

”



Ceny transferowe w liczbach. Jakim wyzwaniom przychodzi sprostać w przypadku kontroli?

Ceny transferowe – obszar zwykle utożsamiany z corocznymi obowiązkami formalnymi: przygotowaniem dokumentacji cen transferowych i analiz danych porównawczych (tzw. benchmarków) oraz złożeniem wymaganych oświadczeń i informacji. Czy jednak ceny transferowe kończą się na etapie wypełnienia obowiązków dokumentacyjnych i sprawozdawczych, czy to może dopiero początek wyzwań?

Jak tematykę tę postrzegają organy skarbowe? Jakim wyzwaniom przychodzi sprostać w przypadku kontroli? I wreszcie, jak kontrole cen transferowych przekładają się na wyniki fiskalne tak istotne z perspektywy Ministerstwa Finansów?

Ceny transferowe – obszar nieodgadniomy?

Istotę cen transferowych można sprowadzić do prostego stwierdzenia – udowodnienie rynkowości transakcji wewnątrzgrupowej. Czy to z perspektywy organów skarbowych czy podatników, warunek pozostaje ten sam – spełnienie kryterium tzw. ceny rynkowej. Sporne pozostaje natomiast to, czym jest owa „cena rynkowa”. Obydwie strony mają tu spreczny interes – celem organów skarbowych jest zapewnienie jak największych wpływów Skarbowi Państwa (czyt. pozostawienie w Polsce możliwie wysokiej marży), z drugiej jednak strony trudno oczekiwać od przedsiębiorców aby ci, w czasach obciążania coraz to nowymi daninami, nie poszukiwali źródeł oszczędności.

Oszczędności, które mogą jednak przełożyć się na zadeklarowanie podstawy opodatkowania w niższej wysokości.



Agnieszka Bieńkowska
Partner Zarządzający,
Doradca Podatkowy



Maciej Gierada
Lider Praktyki Cen
Transferowych i Wycen

Sprzeczny interes stron dobrze obrazują przykłady wewnątrzgrupowych transakcji transgranicznych. Zderzają się w nich kolizyjne interesy fiskalne nie tylko na linii podatnik – fiskus, ale także na poziomie poszczególnych krajów oraz ich wpływów podatkowych. Przykładowo, patrząc z perspektywy polskiej – jakie miałyby być powody udzielenia przez polską spółkę taniego finansowania jej siostrzanemu odpowiednikowi w Niemczech, skoro na lokalnym rynku mogłaby z łatwością odnaleźć lepsze źródła inwestycji, które przyniosłyby wyższe stopy zwrotu? Patrząc z kolei z perspektywy podmiotu niemieckiego jako beneficjenta finansowania – jakie przyczyny miałyby stać za zapłatą zbyt wysokiego oprocentowania na rzecz spółki polskiej, skoro od niemieckich banków mógłby on otrzymać pożyczkę na znacznie lepszych warunkach?

W praktyce takim właśnie pytaniom przychodzi stawić czoła w trakcie kontroli z zakresu cen transferowych. Charakter dyskusowanych w ich toku zagadnień pokazuje wyraźnie, że problematyka ta wykracza znacząco poza proste obowiązki sprawozdawcze, w praktyce wymagając nie tylko multidyscyplinarnej wiedzy z obszaru podatków, ekonomii, statystyki czy prawa międzynarodowego, ale także – co nie mniej ważne – dostrzegania i

“ Istotę cen transferowych można sprowadzić do prostego stwierdzenia – udowodnienie rynkowości transakcji wewnątrzgrupowej. ”

dostosowywania się do zmieniających się trendów co do zakresu i sposobu weryfikowania cen transferowych przez organy podatkowe.

Ceny transferowe obszarem różnych wyzwań

Cele w obszarach podatkowych, w tym cen transferowych, wyznacza ustawodawca poprzez tworzenie odpowiednich przepisów prawa. To w ich ramach muszą poruszać się podatnicy, ale także – a może przede wszystkim – organy podatkowe. Oprócz górnolotnych sformułowań pt. „zamknięcie luki CIT”, „zamknięcie luki TP”, w praktyce widoczne są jednak pewne prawidłowości, których poprawne zidentyfikowanie może wpłynąć na bezpieczeństwo podatkowe firmy. Jaki zatem obraz tematyki cen transferowych wyłania się ostatnimi laty?

A. Chaos regulacyjny – w latach 2016-2020 w zakresie cen transferowych funkcjonowały trzy odmiennie stany prawne: w roku 2016 obowiązywały przepisy odmiennie niż w roku 2018, rok 2018 z kolei to zupełnie inna rzeczywistość regulacyjna niż rok 2020.

B. Niepewność – skutkiem tak częstych zmian była duża niepewność co do kolejnych modyfikacji stawianych przed podatnikami wymagań.

C. Koszty – chaos i niepewność regulacyjna oraz nakładające się na nie wyzwania makroekonomiczne prowadziły do znacznego wzrostu kosztów wypełnienia podstawowych obowiązków w zakresie cen transferowych i podatków w ogóle.

Czynniki te – choć dla podatników fundamentalne – nie są niestety brane pod uwagę w toku czynności sprawdzających czy kontroli podatkowych. Organy podatkowe koncentrują się zwykle na jednym, wybranym roku finansowym, zapominając, że z perspektywy podatnika planowanie budżetowe i fiskalne następuje w znacznie dłuższych horyzontach czasowych. Co zatem stanowi obecnie najpowszechniejszy obszar kontroli?

A. Straty podatkowe – szczególnie te wieloletnie, to obecnie niemal gwarancja, że podatnik zostanie poddany tzw. czynnościom sprawdzającym z zakresu cen transferowych, które w przypadku zidentyfikowania nieprawidłowości mogą przerozdzić się w kontrolę podatkową.

B. Zmiany makroekonomiczne – które dla podatnika mogą stanowić bazę dla uzasadnienia gorszych wyników finansowych (i podatkowych) firmy, dla fiskusa natomiast fundament do wniosku, że w realiach ówczesnej koniunktury podatnik powinien wygenerować znacznie wyższą rentowność na tle swojej konkurencji. Konkurencji, do której porównanie go przy pomocy wspomnianego już raportowania TPR, stanowi dla organów niezwykle proste i sprawne do wykonania zadanie.

C. Restrukturyzacje – dynamiczne czasy wymagają podejmowania dynamicznych decyzji, co przekłada się na bardziej liczne niż kiedykolwiek fuzje, reorganizacje przedsiębiorstw czy też zmiany w zakresie prowadzonych działań gospodarczych. Wszystkie te czynności to niezwykle „ciekawe” dla organów podatkowych obszary, w obrębie których weryfikacji podlega m.in. to, czy aby na pewno podatnik zastosował odpowiednie marże.

D. Transakcje finansowe – rosnąca inflacja to rosnące stopy procentowe, a rosnące stopy procentowe to wzrost kosztów finansowania. Wzrost kosztów finansowania to z kolei idealny obszar do podjęcia działań przez organy skarbowe, które z jednej strony weryfikują, czy aby na pewno nie został poniesiony zbyt wysoki koszt, a z drugiej, patrząc z perspektywy podatnika udzielającego finansowania, czy jego wynagrodzenie aby na pewno nie zostało ustalone na zbyt niskim poziomie.

E. Wartości niematerialne – kto jest właścicielem praw niematerialnych w grupie? W którym kraju podlegają one ochronie prawnej, a w którym zostały wytworzone? Czy opłata za udzielenie zgody na korzystanie z prawa ochronnego na znak towarowy została poniesiona w rynkowej wartości? Czy podatnik powinien w ogóle ponieść opłatę za znak czy może był to po prostu zakup usługi, która w celu zwiększenia kosztu (i tym samym obniżenia podstawy opodatkowania) została ubrana w „szaty” licencyjne? To kolejne z pytań regularnie stawianych firmom przez organy skarbowe, które postrzegają transakcje w obszarze wartości niematerialnych jako podstawowy element występowania wspomnianej już „luki CIT”.

Krytycznym obszarem weryfikacji przez organy podatkowe niezmiennie pozostają straty podatkowe, zwłaszcza wieloletnie. Szczególnej uwadze poddawani są także podatnicy, którzy strat podatkowych co prawda nie osiągają, ale ich rentowności na tle bezpośredniej konkurencji pozostaje na obniżonym poziomie. Istotne ryzyko generuje także wysoki poziom kosztów ponoszonych przez polskiego podatnika w obszarze transakcji finansowych i usługowych nabywanych od kontrahentów powiązanych.

Kontrole w obszarze CIT i cen transferowych – jaki obraz przedstawiają liczby?

Ceny transferowe – multidyscyplinarny obszar podatkowy, łączący zagadnienia z pogranicza prawa i ekonomii, w którym na podatnika czyhają liczne wyzwania związane z obroną osiągniętej rentowności. Czy podsumowanie to broni się statystykami z kontroli podatkowych? Spójrzmy na najważniejsze z liczb¹.

¹ Wartości pozyskane w trybie dostępu do informacji publicznej z Ministerstwa Finansów oraz z artykułu „Fiskus trafia z kontrolami w punkt”, opublikowanym w Dzienniku Gazeta Prawna, 27.04.2023 r.

WARTOŚĆ	CHARAKTERYSTYKA
14 %	O tyle wzrosła w 2022 r. liczba podatników w porównaniu do pandemicznego roku 2020
15 %	O tyle kontroli więcej organy skarbowe przeprowadziły w 2022 r. w porównaniu do roku 2021
~18 000	Tyle kontroli przeprowadziły w roku 2022 urzędy skarbowe. To wzrost o 2,3 tys. w porównaniu do roku 2021 i o 2,8 tys. w porównaniu do roku 2020
97,1%	Tyle kontroli w 2022 r. zakończyło się ustaleniem domiaru podatkowego
85,8%	Tyle kontroli w 2020 r. zakończyło się ustaleniem domiaru podatkowego
9 mld zł	Ponad 9 miliardów zł uszczupień budżetowych wykryły organy skarbowe w trakcie czynności sprawdzających i kontroli przeprowadzonych w 2022 r.
3,3 mld zł	Ponad 3,3 miliarda zł uszczupień budżetowych wykryła Izba Administracji Skarbowej w Warszawie w trakcie czynności sprawdzających i kontroli przeprowadzonych w 2022 r.
850 mln zł	Tyle należnego fiskusowi dochodu doszacowano w pierwszej połowie 2022 r. wyłącznie w obszarze cen transferowych

Jaki obraz kontroli w obszarze CIT i cen transferowych ilustrują przytoczone liczby oraz toczące się obecnie kontrole podatkowe?

1. Liczba kontroli rośnie współmiernie do wzrostu liczby podatników.

2. Drastycznemu wzrostowi (do 97,1% w 2022 r.) uległa liczba kontroli zakończonych domiarem na poziomie pierwszej lub drugiej instancji. Spowodowane jest to coraz lepszymi narzędziami, którymi organy skarbowe dysponują w ramach typowania podatników do kontroli (takimi jak np. raportowanie elektroniczne cen transferowych TPR). Aczkolwiek należy mieć na uwadze, że dla celów statystycznych Ministerstwa Finansów jego wartość pozostaje bez znaczenia, tj. domiar w wysokości 1 tys. zł będzie z perspektywy „statystycznej” równie pozytywnym rozstrzygnięciem jak doszacowanie 1 mln zł.

3. Ponad 35% wszystkich polskich uszczupień budżetowych zostało wykryte w 2022 r. przez Izbę Administracji Skarbowej w Warszawie.

4. Około 20% domiaru podatkowego w obszarze CIT w 2022 r. dotyczyło wyłącznie cen transferowych.

5. Organы zajmują się kontrolą w pierwszej kolejności lat podatkowych, które zbliżają się do przedawnienia. Celem jest przerwanie jego biegu.

6. Szczególnie newralgiczne z perspektywy organów skarbowych, jak i późniejszego prowadzenia czynności będzie typowanie po-

datników do kontroli za lata 2020 i 2021, tj. lata dotknięte skutkami pandemii COVID-19. Wybór podmiotów do weryfikacji będzie musiał być prowadzony ze szczególną ostrożnością, co w żadnym stopniu nie wyklucza, że spółki operujące w branżach najbardziej dotkniętych skutkami pandemii nie muszą liczyć się z kontrolą. Szczególnej uwadze należy poddać podmioty, które w latach 2020 i 2021 korzystały z rządowych programów wsparcia, co mogło prowadzić do przejściowej poprawy ich rentowności.

Jakkolwiek 9 miliardów zł wykrytych w 2022 r. uszczupień budżetowych z tytułu CIT może wydawać się wartością znaczącą, należy pamiętać, że proces prowadzony przez Ministerstwo Finansów, którego celem jest zamknięcie „luki CIT”, wydaje się dopiero na początku drogi. Jej pierwszym etapem jest udostępnienie organom narzędzi, które umożliwią – z jednej strony – skuteczne typowanie podatników do kontroli, z drugiej – ograniczą zaangażowanie organów w weryfikację rozliczeń dokonywanych przez podmioty o relatywnie niewielkim wpływie na należności podatkowe Skarbu Państwa.

Jednym z fundamentalnych kroków na tej drodze było wprowadzenie od 1 stycznia 2019 r. raportowania elektronicznego cen transferowych (TPR). Kolejną graniczną datą będzie rozciągnięcie także na małych i średnich podatników – również tych zwolnionych z VAT – obowiązku korzystania z KSeF (Krajowego System e-Faktur) od 1 stycznia 2025 r. Po tej dacie należy spodziewać się, że typowanie do kontroli będzie nie tylko równie skuteczne jak dzisiaj, ale – co ważniejsze – będzie dotyczyło również podatników, którzy w największym stopniu przyczyniają się do powstawania uszczupień budżetowych Skarbu Państwa.



optymalizujemy
procesy biznesowe
i operacyjne



zarządzamy kosztami
i wartością
przedsiębiorstw



budujemy modele
operacyjne organizacji
z sektora BSS



szukamy potencjału
RPA



przeprowadzamy
zmiany organizacyjne



restrukturyzujemy
operacyjnie
i strategicznie



opracowujemy
raporty rynkowe



zarządzamy projektami



wspieramy ekspercko
na żądanie

Nasz zespół to kompetentni, utalentowani konsultanci wywodzący się z globalnych firm doradczych oraz doświadczeni analitycy finansowi i eksperci biznesowi z wielu branż w Polsce i na świecie.

Z ostatniej chwili!

controllingNOW

- nowy gracz na rynku usług outsourcingowych specjalizujący się w profesjonalnym controllingu dla firm oraz organizacji pozarządowych
www.controllingnow.pl



Anna Boguszevska



Violetta Malek



Paweł Młyński

controllingNOW



5 urodziny
Gekko advisoryNOW!

Nowe biuro **Gekko advisoryNOW!**
Zapraszamy do **Warsaw UNIT!**



W następnym numerze m. in.:

- **Wartość informacji zarządczej** dla organizacji pozarządowych
- **Zarządzanie projektami** – dobór metodyki projektowej i rola lidera projektu!
- **Zespoły wielopokoleniowe** – jak skuteczny lider korzysta z dobrodziejstw różnorodności i jak adresuje pojawiające się wyzwania?



Gekko advisoryNOW Sp. z o.o.
 Spektrum Tower
 ul. Twarda 18 | 00-105 Warszawa
 tel. +48 22 295 69 60
 mob. +48 606 564 406
 www.advisorynow.pl

Gekko
 advisoryNOW