CIONET DIGITAL EXCELLENCE

SECURITY EXCELLENCE

RAPORT 2019/20

Badanie przeprowadziliśmy wśród dyrektorów IT
i bezpieczeństwa, tworzących strategię cybersecurity
w firmach i instytucjach z całej Polski

SPIS TREŚCI

CZYNNIKI BEZPIECZEŃSTWA

KOSZTY/RYZYKA/INCYDENTY/ROI

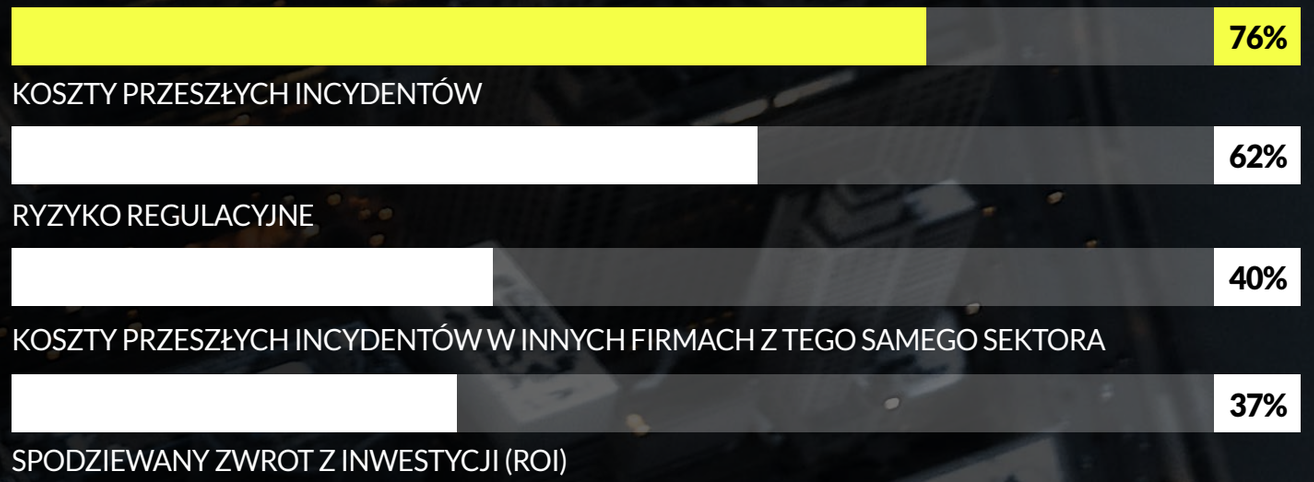
+

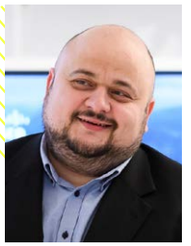
Jak tworzony jest budżet bezpieczeństwa i co tak naprawdę sprawia, że organizacja jest dobrze zabezpieczona?

>>>

Nauka na błędach – własnych i innych organizacji – jest najważniejszym czynnikiem decydującym o wysokości budżetu na bezpieczeństwo w przyszłości. Firmy analizują dane historyczne własne i firm o podobnych parametrach. Wciąż bardzo istotne jest ryzyko związane ze zgodnością z przepisami.

PROJEKTY ZWIĄZANE Z BEZPIECZEŃSTWEM – JAKIE CZYNNIKI UWZGLĘDNIASZ?





ŁUKASZ BROMIRSKI,
SECURITY PRODUCT MANAGER,
SECURITY BU, CISCO

Dobrą informacją jest, że firmy w Polsce przy szacowaniu zapotrzebowania na budżet oraz czas swoich pracowników biorą pod uwagę koszty dotychczasowych włamań (76% ankietowanych). Dane dotyczące rzeczywistych kosztów dopiero zaczynają być w Polsce dostępne, ale istotnie zmieniają optykę decydentów biznesowych. Co prawda nadal większość ankietowanych wskazuje, że nakłady na bezpieczeństwo są za niskie i wynoszą zaledwie parę procent całego budżetu IT, ale stale od wielu lat rosną. To dobrze, ponieważ za świadomością powinny podążać nakłady finansowe – inaczej w organizacjach może pojawić się frustracja i wypalenie zawodowe.

MARCIN KRZEMIENIEWSKI,
BUSINESS LINE MANAGER SECURITY, NTT POLAND

Brak inwestycji w obszar bezpieczeństwa jest postrzegany jako ryzyko, narażenie na niepotrzebne koszty obsługi incydentu. Inwestycje w tym obszarze są też często wymuszone przez regulacje. Chętniej uczymy się na swoich błędach, zamiast wyciągać wnioski z wpadek innych. Wyniki badania pokazują, że najważniejszy jest budżet i ściśle z nim związany dobór rozwiązań technicznych, czyli zakup odpowiednich metod zabezpieczeń. Warto stosować szeroką perspektywę, pamiętać o zakupach i projektowaniu infrastruktury, ale nie pomijać aspektu szkoleniowego.

TOMASZ ŁUŻAK,
PRODUCT OWNER IT SECURITY, T-MOBILE POLSKA

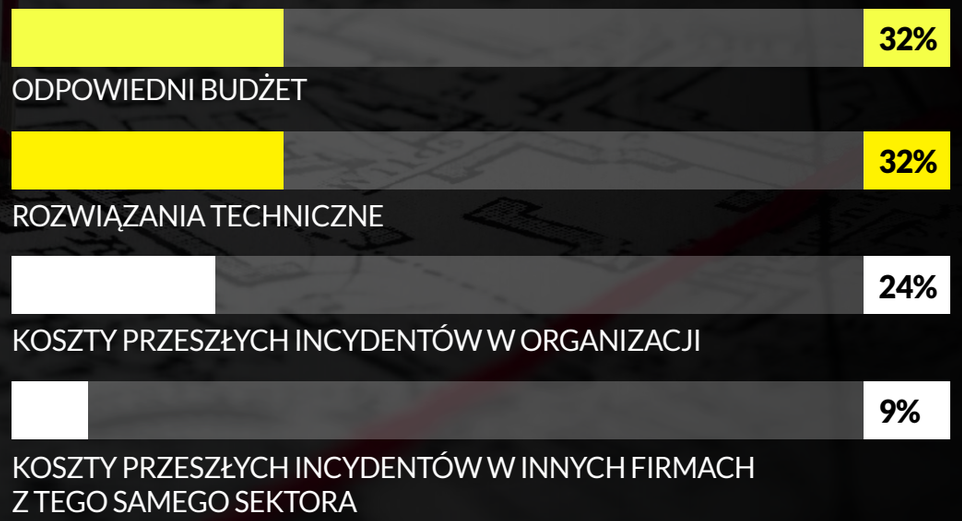
Praktyka niestety dowodzi, że głównymi motywatorami do inwestycji w obszarze bezpieczeństwa IT są: wystąpienie incydentu we własnej organizacji oraz regulacje prawne. W budżecie firmy nakłady na cyberbezpieczeństwo często schodzą na dalszy plan i traktowane są jako zło konieczne – np. jako nieobowiązkowa polisa ubezpieczeniowa, która redukuje ryzyko wystąpienia incydentu, ale nie przynosi korzyści finansowych. Dopiero doświadczenie przykrych skutków incydentu uświadamia zarządzającym, że bezpieczeństwo powinno być traktowane na równi z innymi obszarami, ponieważ ma znaczący wpływ na ciągłość biznesową organizacji.

Jak twierdzą respondenci, należyty poziom bezpieczeństwa teleinformatycznego zapewnić może odpowiedni budżet. Powinien on być stałą częścią wydatków IT, adekwatną do przeprowadzonej analizy ryzyka i branżowych benchmarków. Zatrważający jest fakt, że spora grupa organizacji nie jest w stanie w ogóle określić jaki procent budżetu IT przeznacza na cyberbezpieczeństwo. Z odpowiedzi wynika także, że na bezpieczeństwo organizacji, w równym stopniu mają wpływ rozwiązania techniczne, które powinny być dobrane z rozwagą i adekwatnie do budżetu, wielkość firmy, specyfika działalności oraz katalog zagrożeń organizacji. Warto zawsze pomyśleć o pozyskaniu inżynierów bezpieczeństwa. Jeden wykwalifikowany specjalista może przynieść firmie więcej korzyści niż wielomilionowe nakłady na technologie teleinformatyczne.

>>>

Budżet i odpowiednie technologie to najważniejsze czynniki, zapewniające bezpieczeństwo w firmie – nie jest to zaskakujący wynik.

CO ZAPEWNIA BEZPIECZEŃSTWO ORGANIZACJI?



MARCIN SAFRANOW,
DYRETKTOR IT, VECTRA

Nie warto skupiać się na braku budżetu czy nowych narzędzi, znacznie lepiej skoncentrować się na własnych kompetencjach i już posiadanych rozwiązaniach.

Odpowiedni budżet i rozwiązania techniczne to zdaniem jednej trzeciej uczestników badania najistotniejsze elementy w zapewnieniu bezpieczeństwa organizacji. Pytanie tylko, czy istnieje coś takiego, jak odpowiedni budżet w obszarze bezpieczeństwa, w którym wciąż pojawiają się nowe narzędzia i wyzwania, nowe potencjalne koszty? Dlatego ważne jest, aby w pełni wykorzystać już posiadane zasoby – przede wszystkim dobrze poznać narzędzia dostępne w organizacji, ich możliwości. Specjaliści IT są gadżeciarzami, uwielbiamy wszelkie nowinki techniczne i chętnie decydujemy się na kolejne zakupy, zwłaszcza, że dostawcy posiadają ogromną ekspercką wiedzę, doświadczenie i potrafią nas do tych zakupów zainspirować. Trzeba jednak być pragmatycznym i w pierwszej kolejności wykorzystać już zakupione zasoby.

Kilka praktycznych wskazówek:

Definiujemy potrzeby biznesowe, a dopiero potem zaczynamy rozważać zakup narzędzi

Trzeba sprawdzić jak dostępne narzędzia są obecnie wykorzystywane - czy nie ma błędnych wdrożeń, czy ludzie są wystarczająco dobrze przeszkoleni, czy potrafimy w pełni wykorzystać możliwości posiadanych zasobów

Warto zwrócić się z prośbą do vendora o audyt i sprawdzenie narzędzi, które od niego kupiliśmy

Warto mieć w zespole osobę, która jest pragmatyczna i jest przeciwwagą dla gadżeciarzy.

ŁUKASZ BROMIRSKI,
SECURITY PRODUCT MANAGER, SECURITY BU, CISCO

W trakcie dyskusji podczas spotkań Security Excellence, zwracaliśmy dużą uwagę na aspekt ludzki – specjalistów w działach bezpieczeństwa, oraz zespołach monitoringu i reagowania. Tym bardziej cieszy fakt, że coraz więcej firm (32%) docenia wagę dobrych narzędzi pozwalających zmniejszyć obciążenie analityków bezpieczeństwa.

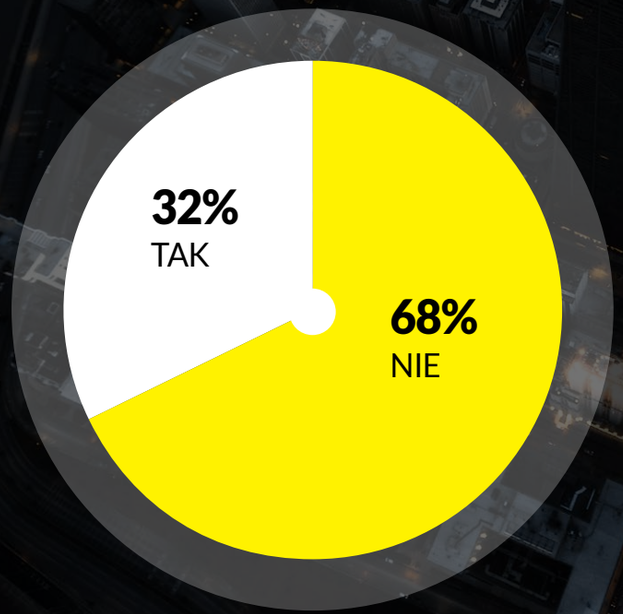
TOMASZ MATUŁA,
EKSPERT I MENEDŻER RYNKU ICT ORAZ TELCO, DYREKTOR PROGRAMOWY

Tylko 9% uważa, że istotne w zapewnieniu bezpieczeństwa firmy są koszty incydentów w innych firmach z tego samego sektora. Można odnieść wrażenie, że nie lubimy się uczyć na błędach innych. Szkoda, bo to najtańszy i najskuteczniejszy sposób nauki.

ALEKSANDER SURMA,
IT DIRECTOR, CMC POLAND

Koszty przyszłych incydentów (zarówno wewnątrz organizacji, jak również w organizacjach tego samego sektora) wprost wynikają z zagrożeń, a te z kolei determinują poziom ryzyka w konkretnych środowiskach, firmach i procesach. Wyniki ankiety w zakresie najistotniejszych elementów w zapewnieniu bezpieczeństwa, równo rozkładają głosy pomiędzy ryzyko, rozwiązania techniczne oraz ich finansowanie (budżet). Mamy jasną odpowiedź, że nie ma jednego magicznego elementu, który decyduje o zapewnieniu (cyber)bezpieczeństwa.

Tradycyjne podejście do cyberbezpieczeństwa nie sprawdza się w naszej rzeczywistości – trzeba je stale zmieniać i uaktualniać.



CZY TRADYCYJNE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA STANOWI DOBRĄ ODPOWIEDŹ NA NOWĄ RZECZYWISTOŚĆ?

SEBASTIAN GRABSKI,
SALES ENGINEER, ZSCALER

Kolejna edycja Security Excellence pokazuje, że temat cyberbezpieczeństwa jest tematem chętnie dyskutowanym. Potwierdza to frekwencja oraz aktywność uczestników. Z punktu widzenia Zscaler, bardzo istotne było jednoznaczne potwierdzenie, że tradycyjne podejście do cyberbezpieczeństwa nie adresuje obecnej rzeczywistości. Rzeczywistości, w której konsumpcja usług chmurowych jest codziennością. Dotyczy to w szczególności pokolenia „millenialsów", które jest typem użytkownika, dla którego praca to nie jest miejsce bądź lokalizacja. Dla pokolenia „millenialsów" praca to stan, w którym przebywamy od czasu do czasu i może być wykonywana z dowolnego miejsca na dowolnym urządzeniu. Skoro praca nie jest związana z miejscem, to w takim razie tradycyjne podejście do cyberbezpieczeństwa przestaje spełniać swoją funkcję. Skoro nasze aplikacje już są w chmurze to przed czym chroni nas cyberbezpieczeństwo oparte o urządzenia klasy appliance?

BEZPIECZEŃSTWO
CORAZ DOJRZALSZE

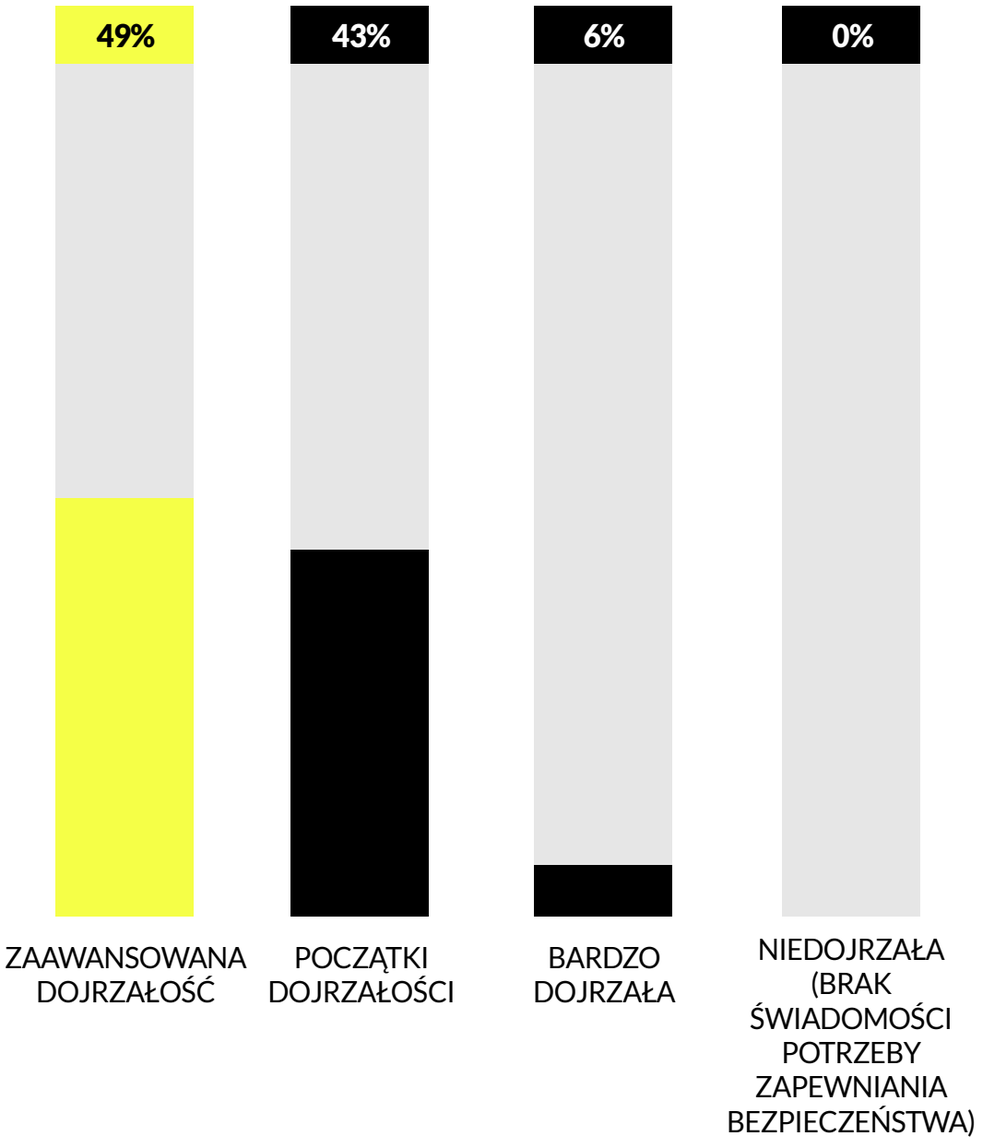
Konsekwencja, pragmatyzm i ciągłe aktualizowanie posiadanych rozwiązań to konieczność – w kwestii bezpieczeństwa nie wolno popadać w samozadowolenie

55% organizacji chwali się dojrzałą kulturą bezpieczeństwa

Niemal połowa uczestników uczestników badania optymistycznie uważa, że ich organizacja osiągnęła zaawansowany stopień bezpieczeństwa – czyli istnieje pełna świadomość potrzeb i trwa implementacja odpowiednich rozwiązań.

Nieco mniejszy odsetek uważa, że jest na początku drogi do dojrzałości – czyli już wie, jakie ma potrzeby i zaczyna wdrażać rozwiązania. Elita bezpieczeństwa to 6%, które ma już w pełni wdrożone wszystkie istotne rozwiązania, wciąż je ewaluuje i aktualizuje. Nikt nie przyznał się do niedojrzałości w obszarze bezpieczeństwa.

DOJRZAŁOŚĆ ORGANIZACJI POD KĄTEM KULTURY BEZPIECZEŃSTWA



TOMASZ ŁUŻAK,
PRODUCT OWNER IT SECURITY,
T-MOBILE POLSKA

Interesujący wydaje się wynik badania w zakresie dojrzałości firmy, pod kątem kultury cyberbezpieczeństwa. Odpowiedzi większości respondentów wskazują, że firmy są świadome potrzeb, a w wielu z nich są już wdrażane procedury i rozwiązania bezpieczeństwa teleinformatycznego. Jednak do osiągnięcia pełnej dojrzałości w postaci ustabilizowanego, ciągłego procesu bezpieczeństwa IT, jeszcze trochę brakuje. Najsłabszym ogniwem wciąż pozostaje człowiek. Dlatego przedsiębiorstwa jednoznacznie wskazują edukację wszystkich użytkowników, jako najważniejszy element wspierający budowanie kultury bezpieczeństwa w firmie.

MACIEJ IWANICKI,
SYSTEMS ENGINEER , F5

Obawy przed kosztami wycieku danych, jakie ma większość badanych, są słuszne, bo zagrożenie przed atakami i coraz bardziej wyrafinowane działania hakerów są faktem. Atak może skutecznie załamać działanie firmy oraz wpłynąć na nas wszystkich. Wyobraźmy sobie, że dochodzi do ataku na dostawców energii, wówczas sami możemy być odcięci od dostaw w domu, a okoliczne zakłady produkcyjne przestaną działać. Z pewnością z obawą tą wiąże się również konieczność zapłacenia wielotysięcznych kar.

ARKADIUSZ OLCHAWA,
CIO, ITAKA

Wyniki badania pokazują, że przedsiębiorstwa podchodzą do kwestii bezpieczeństwa w sposób bardzo pragmatyczny, są w swoich działaniach konsekwentne i dzięki temu skuteczne. Głównym czynnikiem, uwzględnianym w ocenie projektów związanych z bezpieczeństwem, są koszty przyszłych incydentów, a najważniejszym elementem zapewnienia bezpieczeństwa odpowiedni i odpowiednio wykorzystany budżet oraz kultura bezpieczeństwa budowana przez edukację wszystkich użytkowników. Zdecydowana większość oceniła swoją organizację jako dojrzałą w stopniu zaawansowanym lub początkowym pod kątem kultury bezpieczeństwa, co z jednej strony mogłoby wskazywać, że w tym obszarze mamy jeszcze wiele do zrobienia. Z drugiej strony, może jest jasnym wskazaniem istnienia świadomości, że budowa kultury bezpieczeństwa jest procesem ciągłym i dojście na poziom najwyższej samooceny może skutkować ryzykiem zbytniego „samozadowolenia" i samo w sobie stanowić czynnik ryzyka.

SKUTECZNA KULTURA

CZYLI CZŁOWIEK W CENTRUM

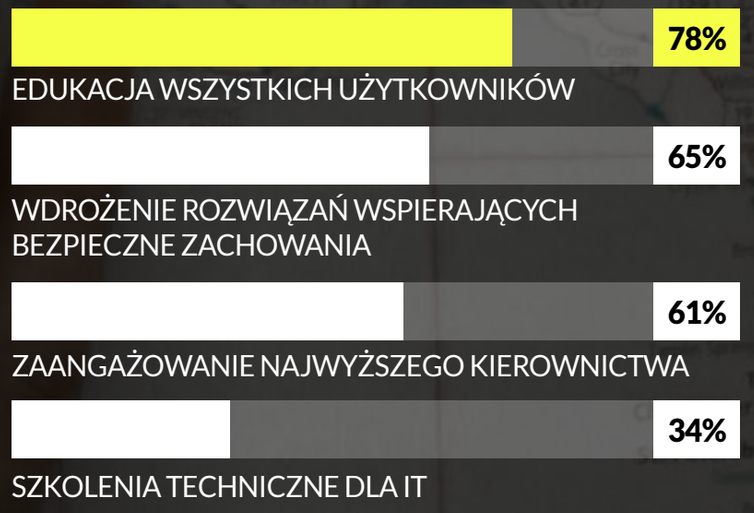
EDUKACJA/TECHNOLOGIA/SECURITY BY DESIGN

Bez zaangażowania wszystkich w organizacji – od zarządu po szeregowych pracowników – nie da się zbudować kultury bezpieczeństwa w firmie.

>>>

Szkolenia dostosowane do poszczególnych grup użytkowników, jasny katalog bezpiecznych zachowań, poparty odpowiednimi rozwiązaniami i wsparcie ze strony menedżerów – **to najważniejsze elementy**.

CZYNNIKI WSPIERAJĄCE BUDOWANIE KULTURY BEZPIECZEŃSTWA W FIRMIE



TOMASZ LASKOWSKI,
KIEROWNIK DZIAŁU
INFORMATYKI, PORT SZCZECIN

Po raz kolejny przekonujemy się, że to człowiek jest najważniejszym ogniwem łańcucha bezpieczeństwa w naszych organizacjach. To jego wiedza, a zwłaszcza świadomość zagrożeń, stanowi o cyfrowym bezpieczeństwie całości organizacji i my jako CIO to nareszcie widzimy. Praca jaką mamy do wykonania to właśnie zbudowanie tej świadomości i uświadomienie wszystkim, jaka odpowiedzialność ciąży również (jak nie przede wszystkim) na nich. Uświadomienie nie tylko poprzez procedury i sztywno określone ramy zachowań, a przez pracę u podstaw budującą w każdym przekonanie o jego znaczącej roli w nowym, cyfrowym świecie.

Za tym, co wskazuje badanie, powinny iść rozwiązania wspierające te zachowania. Nie tylko w wymiarze technicznym i technologicznym ale i w obszarze miękkim, promowania postaw i działań bezpiecznych. Budowanie zaangażowania w tej dziedzinie musi być jednak spójne dla całości organizacji i uwzględniać zaangażowanie najwyższego kierownictwa – stąd powinien iść przykład. Szkolenia techniczne IT zamykają peleton, bo IT wie. Wie i działa.

MARCIN KRZEMIENIEWSKI,
BUSINESS LINE MANAGER
SECURITY, NTT POLAND

Edukacja, edukacja i jeszcze raz edukacja - nie ma takich narzędzi które zastąpią myślenie. Potrzebna jest strategia budowania świadomości security awareness. Pracownicy powinni wiedzieć, jakich zachowań mają unikać, np. bezrefleksyjnego klikania w załączniki. Organizacja powinna mieć wypracowaną metodykę szkoleń i nie powinno być grup z niej wyłączonych – zarząd nie powinien stanowić wyjątku, bo to źle wpływa na ogólne morale. Przykład musi iść z góry i w wielu dojrzałych organizacjach to świetnie działa.

JACEK SAMUJŁO,
CSO, LUFTHANSA SYSTEMS

Mówi się, że ryba psuje się od głowy – podobnie jest z kulturami w organizacjach. Aby zbudować właściwą kulturę bezpieczeństwa należy zacząć od samej góry, czyli najwyższego kierownictwa. To prezes, zarząd i dyrekcja muszą zrozumieć i czuć potrzebę zabezpieczenia interesów firmy w świecie cyfrowym. To oczywiście wiąże się z bezpieczeństwem informacji a w szczególności cyberbezpieczeństwem. Najwyższe kierownictwo służy przykładem dla reszty firmy – jeśli słowa (slogany) nie idą w parze z czynami, reszta organizacji nie będzie podążała tą ścieżką. Dopiero w kolejnym etapie edukacja użytkowników nabiera kluczowego znaczenia lecz pod warunkiem, że tzw. góra realizuje deklaracje w zakresie bezpieczeństwa i wspiera pracowników w tym aspekcie. Za tym muszą iść wydatki na rozwiązania wspierające bezpieczne zachowania oraz szkolenia bezpieczeństwa zarówno dla IT jak i reszty obszarów – bardziej dostosowane do ich potrzeb. Z czasem buduje się kultura, która wspiera organizację w prowadzeniu biznesu. Security staje się częścią DNA organizacji.

MACIEJ IWANICKI,
SYSTEMS ENGINEER , F5

Blisko połowa firm rozpoczyna wdrażanie strategii cyberbezpieczeństwa, co świadczy o wzroście świadomości i chęci rozbudowy tej gałęzi infrastruktury – to cieszy. Nasza firma angażuje się w szereg działań mających za zadanie edukowanie poprzez warsztaty, webinaria, dzielenie się wynikami prowadzonych badań, np. informacje o tym, na co przedsiębiorstwa zwracają uwagę i co jest dla nich najistotniejsze w publikowanych co roku raportach o Stanie Aplikacji (State of Application Services Report).

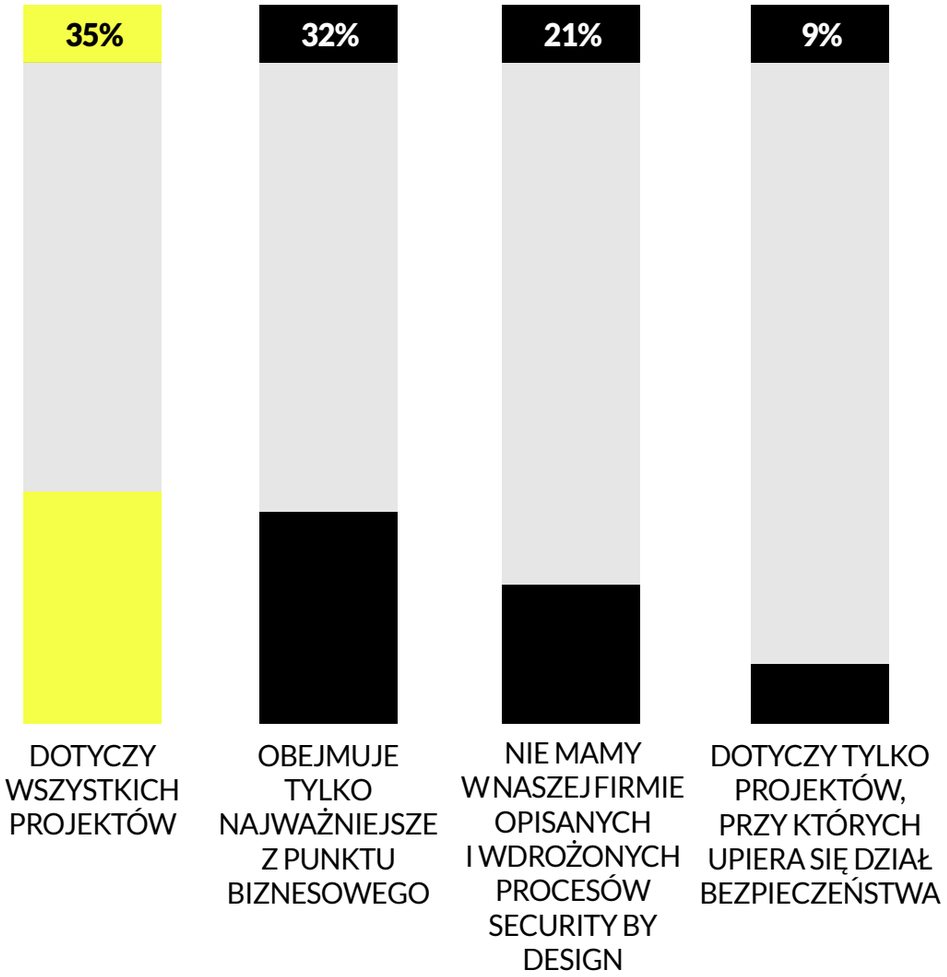
ALEKSANDER SURMA,
IT DIRECTOR, CMC POLAND

Z przedstawionego podejścia do budowania w naszych organizacjach kultury bezpieczeństwa w oparciu o pracowników, współpracę z dostawcami, wsparcie kierownictwa płynie pozytywny wniosek. To ludzie są jednym z najważniejszych ogniw.

SECURITY BY DESIGN

TYLKO CO 3. ORGANIZACJA STOSUJE PODEJŚCIE SECURITY BY DESIGN ORAZ PRIVACY BY DESIGN. W 20% WCIĄŻ NIE MA JESZCZE TAKICH PROCESÓW.

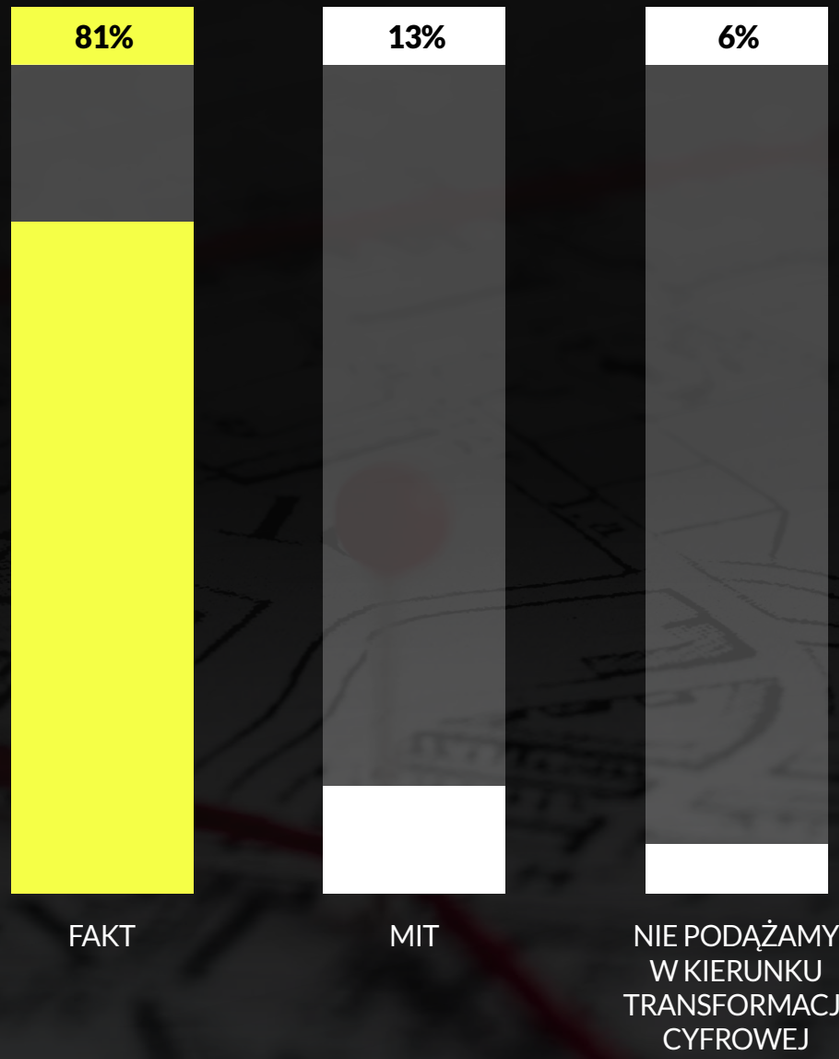
CYBERBEZPIECZEŃSTWO JAKO INTEGRALNY ELEMENT METODYKI PROJEKTÓW (WDROŻONO PODEJŚCIE SECURITY BY DESIGN ORAZ PRIVACY BY DESIGN)



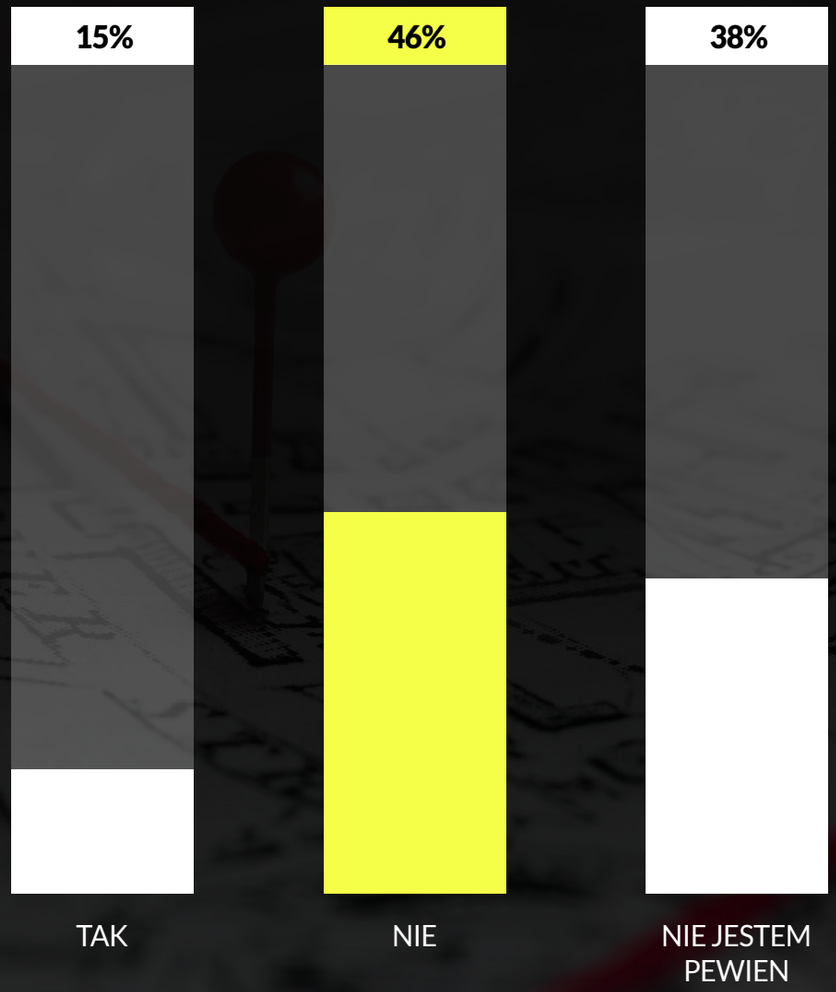
TOMASZ ŁUŻAK,
PRODUCT OWNER IT SECURITY,
T-MOBILE POLSKA

Optymizmem napawa fakt, że ponad 60% firm uważa, iż cyberbezpieczeństwo jest integralnym elementem projektów, a przynajmniej tych najważniejszych z perspektywy biznesowej. Dbałość o aspekty bezpieczeństwa już na samym początku projektu sprawia, że na późniejszym etapie jego realizacji minimalizujemy liczbę poprawek i eliminujemy potencjalne konflikty między biznesem a zespołami technicznymi.

CZY SZEROKO ROZUMIANA TRANSFORMACJA CYFROWA W TWOJEJ ORGANIZACJI TO W FAKT CZY MIT?



CZY UWAŻASZ, ŻE APLIKACJE W TWOJEJ ORGANIZACJI SĄ BARDZO DOBRZE ZABEZPIECZONE?



MACIEJ IWANICKI,
SYSTEM ENGINEER, F5

Należy uznać, że transformacja cyfrowa w naszym kraju to fakt. Ciekawostką może być informacja, że wynik jest identyczny jak ten, który uzyskaliśmy w najnowszym badaniu na temat Stanu Aplikacji w 2020 roku*, otrzymanym od 2600 respondentów z całego świata. Otrzymane wyniki są również zbieżne z głównymi dzisiejszymi wyzwaniami, które stoją przed przedsiębiorstwami w zakresie ochrony aplikacji, czyli zarządzaniem bezpieczeństwem, politykami i szeroko rozumianej zgodności z obowiązującymi regulacjami prawnymi. Przedsiębiorstwa nie wyobrażają sobie tworzenia i publikacji aplikacji, które nie skupiają się na bezpieczeństwie, jednocześnie oferując łatwe z nich korzystanie.

Obserwowany przez nas trend w automatyzacji operacji sieciowych w celu zwiększenia efektywności działania IT i przez to biznesu, nadal postępuje. Już prawie 3/4 organizacji wykorzystuje automatyzację by transformacja cyfrowa przebiegała sprawniej i bezpieczniej.

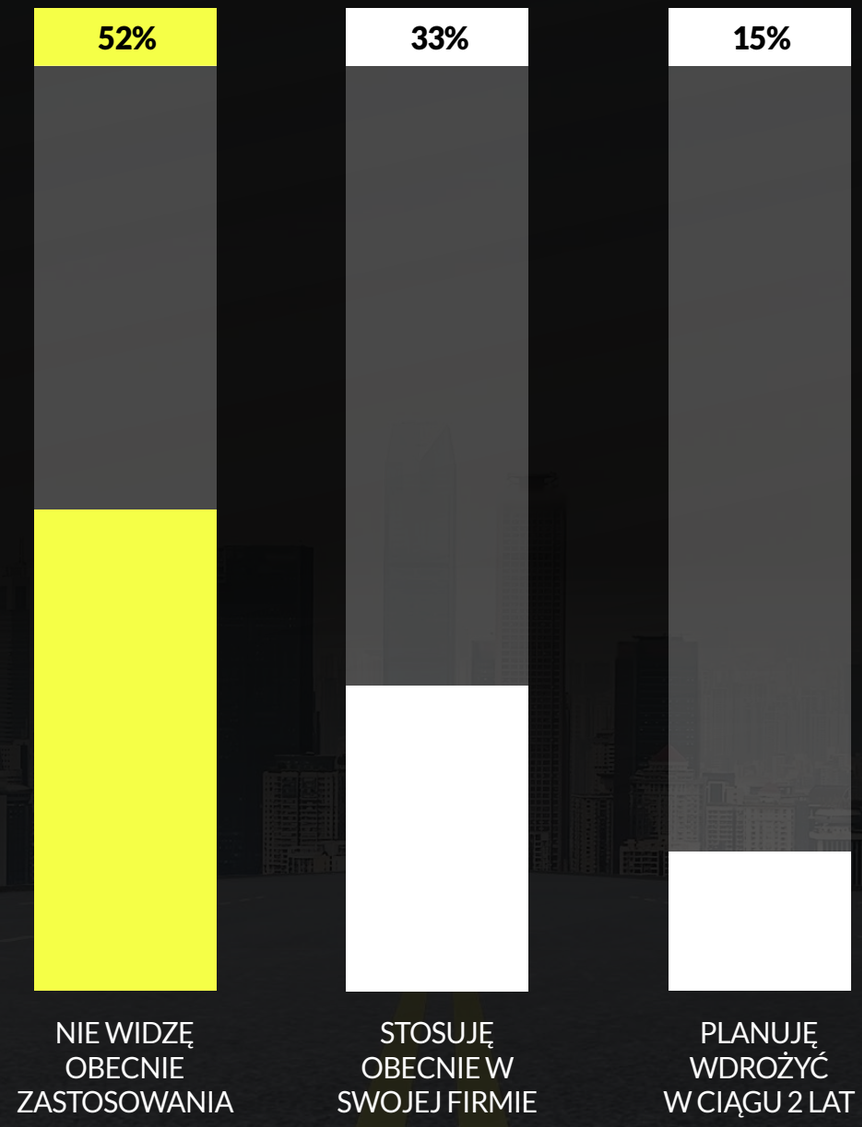
*** https://www.f5.com/state-of-application-services-report**

MARCIN KRZEMIENIEWSKI,
BUSINESS LINE MANAGER SECURITY, NTT POLAND

Systemy biometryczne mają tyle samo zwolenników co przeciwników, rynek podzielony jest mniej więcej po równo. Biometria to ciągle dla nieznacznej większości miła ciekawostka lub też technologia przyszłości. Większość naszych klientów, nie widzi jej zastosowania, bądź też dopiero rozważa takie możliwości w przyszłości.

Z drugiej jednak strony prawie połowa naszych klientów bądź już stosuje technologie biometryczne w swoich infrastrukturach lub też planuje je wdrożyć w ciągu 24 miesięcy. Wygląda na to, że na rynku szykuje się zmiana.

JAK WYKORZYSTUJESZ TECHNOLOGIE BIOMETRYCZNE?



NAJLEPSZE PRAKTYKI

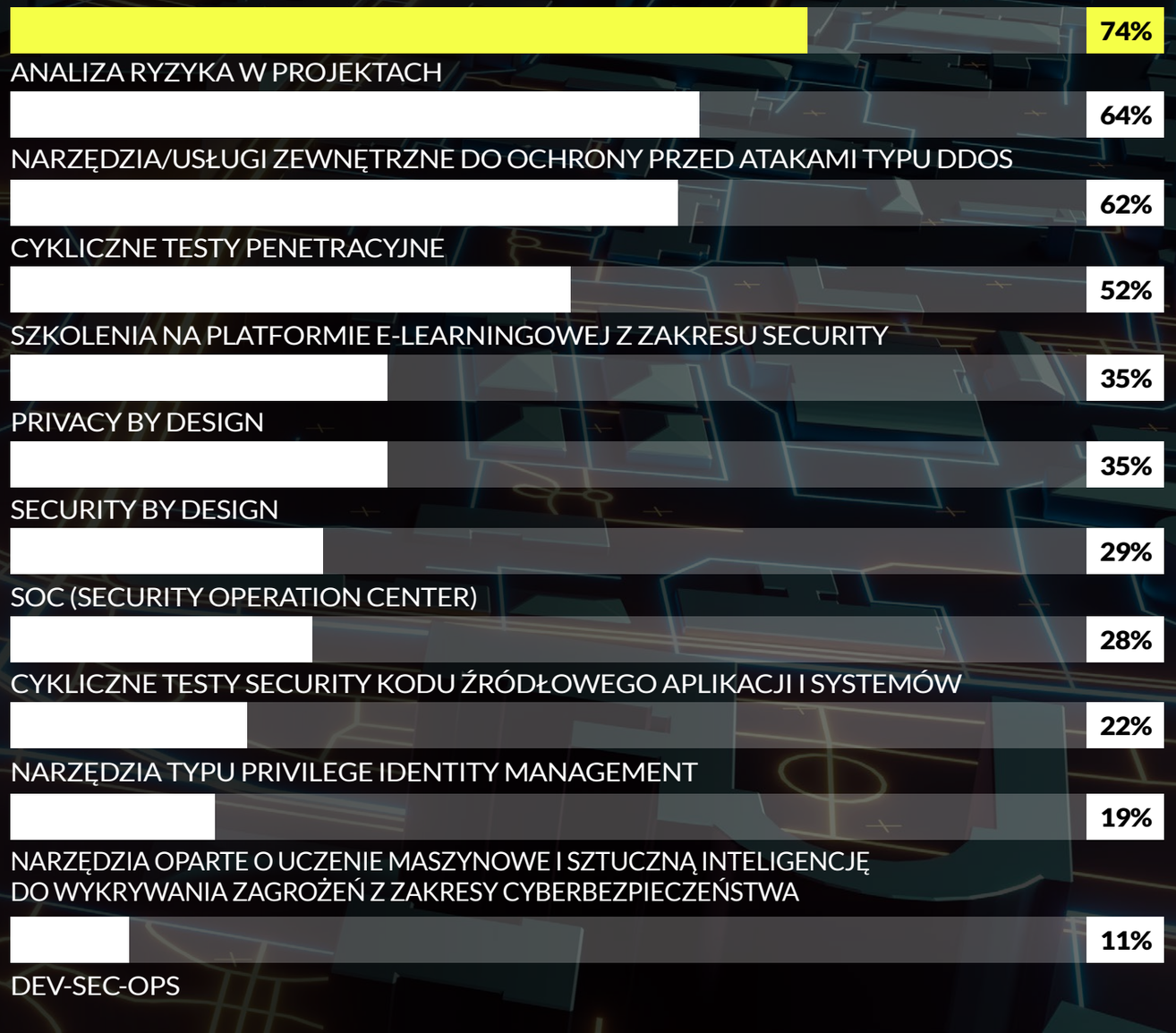
METODOLOGIE/FINANSE/CLOUD

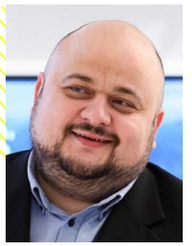
Które metodologie sprawdzają się najlepiej i czy przyszłość bezpieczeństwa to cloud?

>>>

Ocena ryzyka, odpowiednie narzędzia i testy penetracyjne to najczęściej stosowane metodologie.

WDROŻONE METODYKI/TECHNOLOGIE I DOBRE PRAKTYKI





ŁUKASZ BROMIRSKI,
SECURITY PRODUCT MANAGER,
SECURITY BU, CISCO

Firmy w Polsce same oceniają się jako próbujące zbudować świadomość potrzeb i w efekcie uzyskać potrzebne zasoby – w tym finansowe – do implementacji efektywnych rozwiązań bezpieczeństwa. Niestety, pracownicy tych zespołów tylko w 35% ankietowanych firm angażowani są w procesy projektowania systemów i procesów. Oznacza to, że 2/3 firm nadal mimo wysokiej świadomości, traktuje bezpieczeństwo informatyczne jako dodatek a nie elementarną część wszystkich procesów oraz kultury firmy.

ALEKSANDER SURMA,
IT DIRECTOR,
CMC POLAND

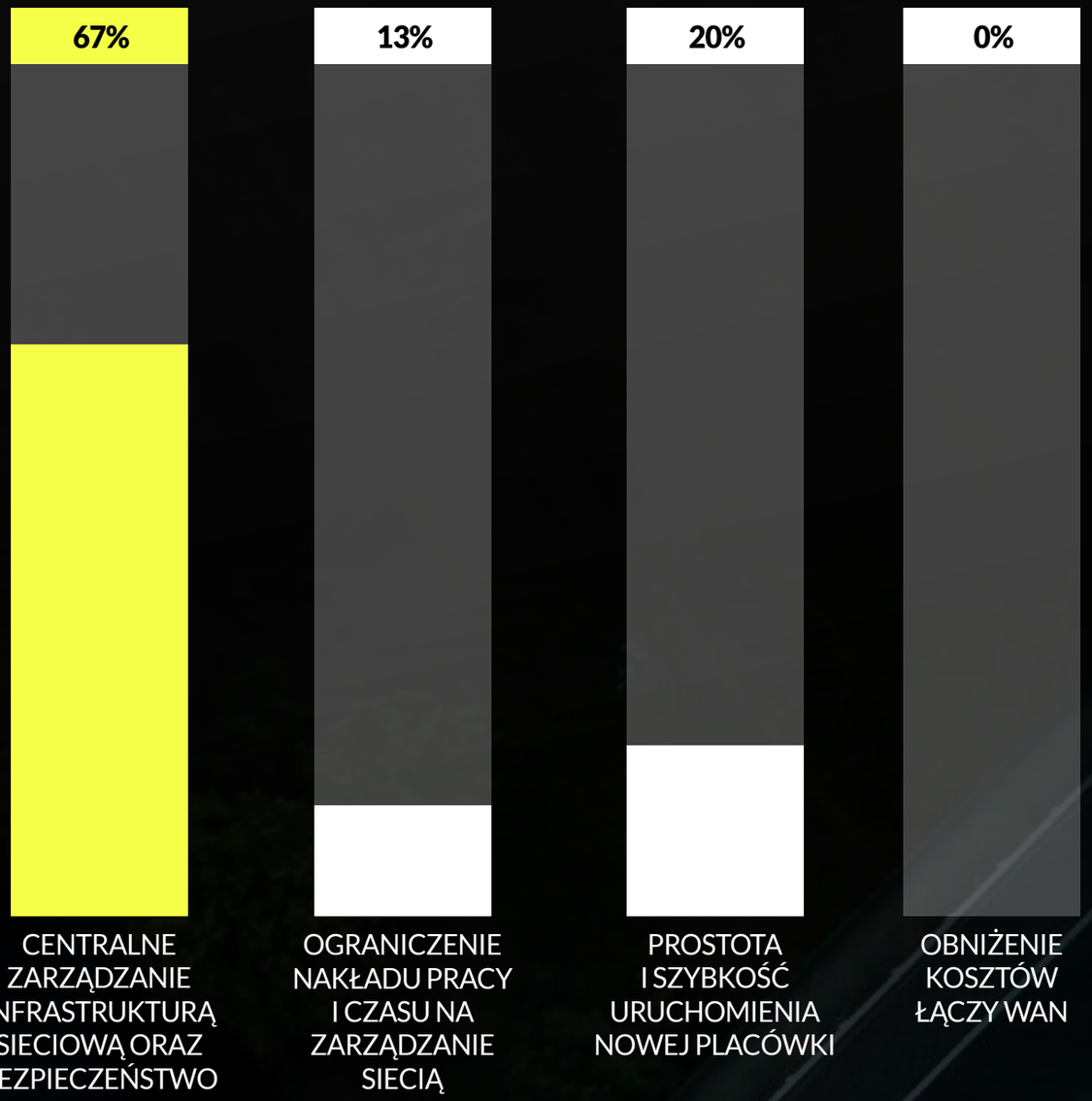
Wskazanie na zarządzanie ryzykiem pojawia się wyraźnie w ocenie bezpieczeństwa firmy oraz wykorzystywanych metodykach i dobrych praktykach. Istotne jest, że oprócz wykorzystywania wewnętrznych procesów w firmach (analiza ryzyka, testy kodu i aplikacji, szkolenia, audyty), w znaczącej liczbie firm korzystamy z testów penetracyjnych dla potwierdzenia skuteczności swoich rozwiązań w zakresie bezpieczeństwa. Rekomendacje z testów pomagają nam aktualizować ryzyka, opisać i ustawić priorytety następnych działań.

TOMASZ MATUŁA,
EKSPERT I MENEDŻER RYNKU ICT
ORAZ TELCO, DYREKTOR PROGRAMOWY

Cieszy, że ponad jedna trzecia ankietowanych deklaruje, że ma wdrożone w organizacji Security/Privacy by Design. Z drugiej strony oznacza, że 65% powinno uruchomić inicjatywę wdrożenia podejścia procesowego do security, nawet w uproszczonej formie ASAP. Być może wina za taki stan rzeczy leży po stronie dostawców technologii, którzy obiecują, że ich „cudowne pudełka" czy systemy rozwiążą wszystkie problemy z bezpieczeństwem?

75% ankietowanych deklaruje, że ma wdrożoną analizę ryzyka. Z moich bardzo wielu rozmów podczas wiosennego i jesiennego Roadshow wynika, że managerowie IT w bardzo niewielkim, niewystarczającym stopniu korzystają w praktyce z analizy ryzyka. Szkoda, ponieważ to potężne, wyjątkowo użyteczne narzędzie! Mieć pasy bezpieczeństwa w samochodzie a mieć i je zapinać podczas jazdy to jednak zasadnicza różnica ;-)

KTÓRY CZYNNIK WPŁYWA NA WYBÓR ROZWIĄZANIA SOFTWARE DEFINED WAN?

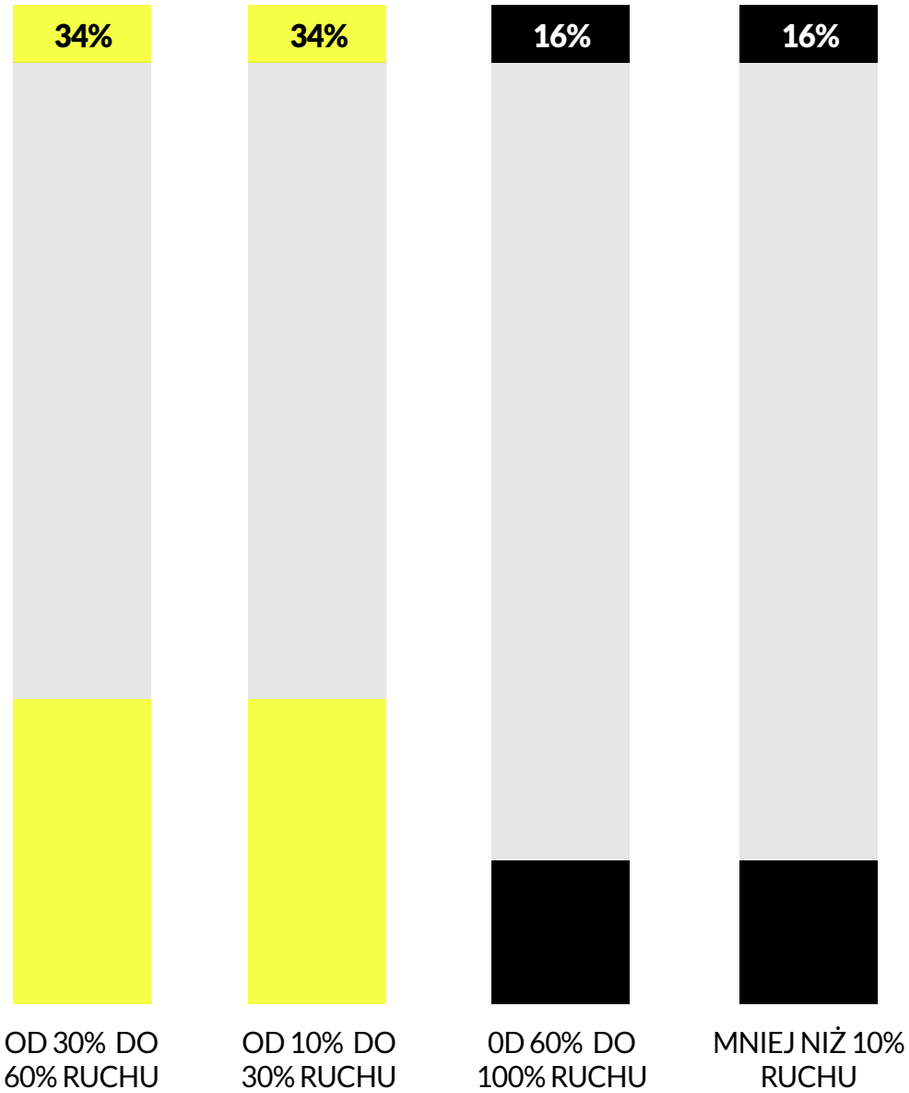


MARCIN KRZEMIENIEWSKI,
BUSINESS LINE MANAGER SECURITY, NTT POLAND

Producenci oraz integratorzy wdrażający rozwiązania SD-WAN często postrzegali tę technologię w kontekście optymalizacji kosztów. Ten pogląd okazuje się słuszny, ale absolutnie nie w obszarze prosto liczonych kosztów łączy telekomunikacyjnych, tylko po stronie nieoczywistych kosztów związanych z zarządzaniem, utrzymaniem oraz bezpieczeństwem środowiska IT.

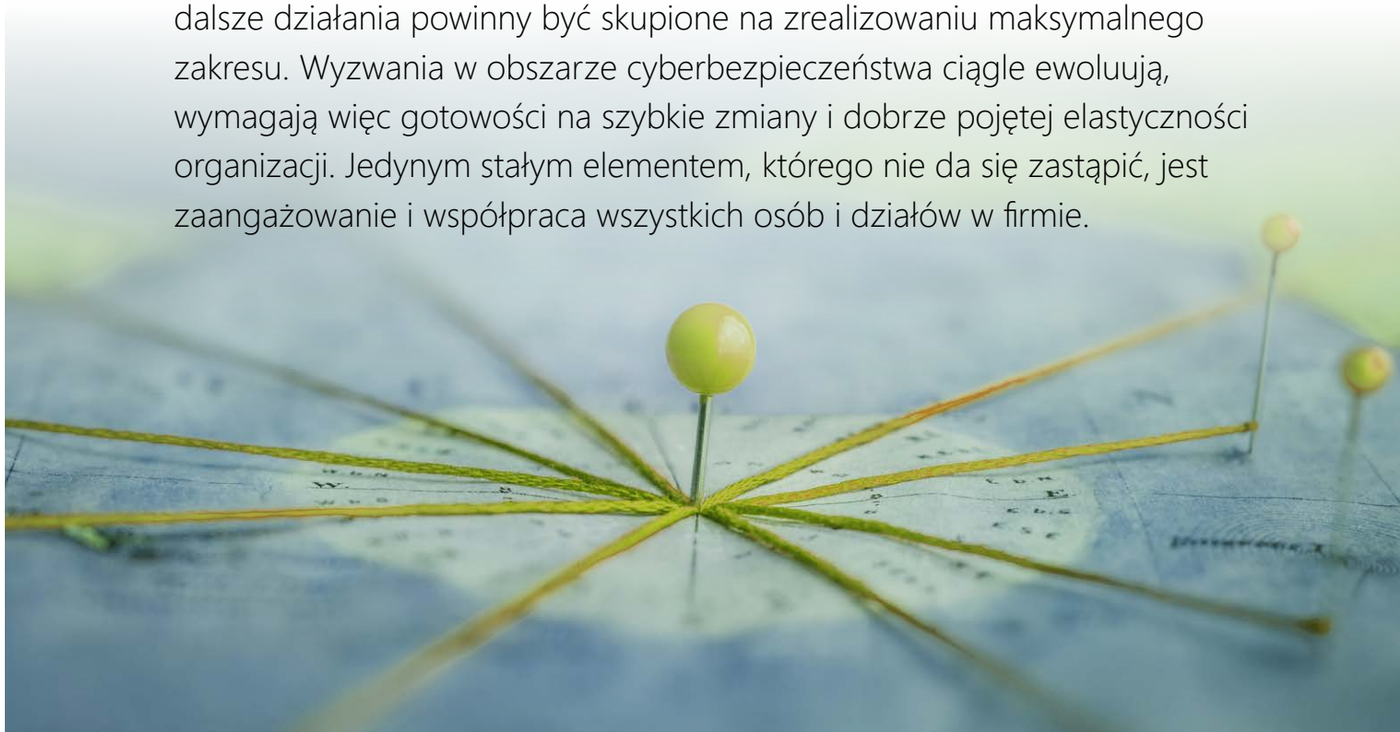
Dla aż 67% naszych klientów to właśnie centralne zarządzanie oraz bezpieczeństwo są głównymi wyzwalaczami decyzji o wejściu w technologię SD-WAN, podczas gdy żaden z nich nie wspomina o obniżeniu kosztów utrzymania łączy WAN, co jest dla nas dość zaskakujące. Organizacje w mniejszym stopniu zaczynają zwracać uwagę na obniżenie kosztów łącza, a ważniejsze okazuje się bezpieczeństwo, lepsze wykorzystanie posiadanych zasobów i czasu pracy administratorów.

JAKI PROCENT RUCHU APLIKACJI PRACOWNIKÓW WIDZI CSO? (LUB SĄDZI, ŻE WIDZI)



ARKADIUSZ OLCHAWA,
CIO, ITAKA

Po przeanalizowaniu wyników utwierdzam się w przekonaniu, że w kwestii zapewnienia bezpieczeństwa w organizacji, czy w projektach, najwłaściwszym podejściem jest wykorzystanie metodyk zwinnych. Po określeniu najważniejszych celów jak np. zapewnienie ciągłości działania, zapobieganie utracie poufnych danych, zapobieganie utracie pieniędzy, a następnie przypisanie odpowiedniego budżetu (który zawsze będzie niewystarczający), dalsze działania powinny być skupione na zrealizowaniu maksymalnego zakresu. Wyzwania w obszarze cyberbezpieczeństwa ciągle ewoluują, wymagają więc gotowości na szybkie zmiany i dobrze pojętej elastyczności organizacji. Jedynym stałym elementem, którego nie da się zastąpić, jest zaangażowanie i współpraca wszystkich osób i działów w firmie.



ŁUKASZ BROMIRSKI,
SECURITY PRODUCT MANAGER,
SECURITY BU, CISCO

Spotkania i rozmowy w trakcie Security Excellence Roadshow pozwoliły nam potwierdzić wyniki badań, które prowadzimy jako Cisco co roku, ale przyniosły również pewne ciekawe niespodzianki.

Zgodnie z naszymi badaniami z ostatnich dwóch lat, w tym prowadzonymi w Polsce, świadomość braku widoczności w ruchu szyfrowanym i jednocześnie wzrostu udziału tego ruchu w ogólnym ruchu internetowym danego przedsiębiorstwa wzrasta. Z reguły poniżej ¼ ankietowanych twierdzi, że jest świadoma i obserwuje na bieżąco między 80 a 100% ruchu internetowego swoich pracowników i aplikacji, co daje jeszcze pole do popisu, ale świadczy dobrze o samoświadomości. Wraz z pojawieniem się protokołu TLS 1.3, problem braku widoczności ruchu szyfrowanego między odbiorcą a serwerem będzie coraz poważniejszy i już dzisiaj należy przedsięwziąć kroki aby tą widoczność sobie zapewnić.

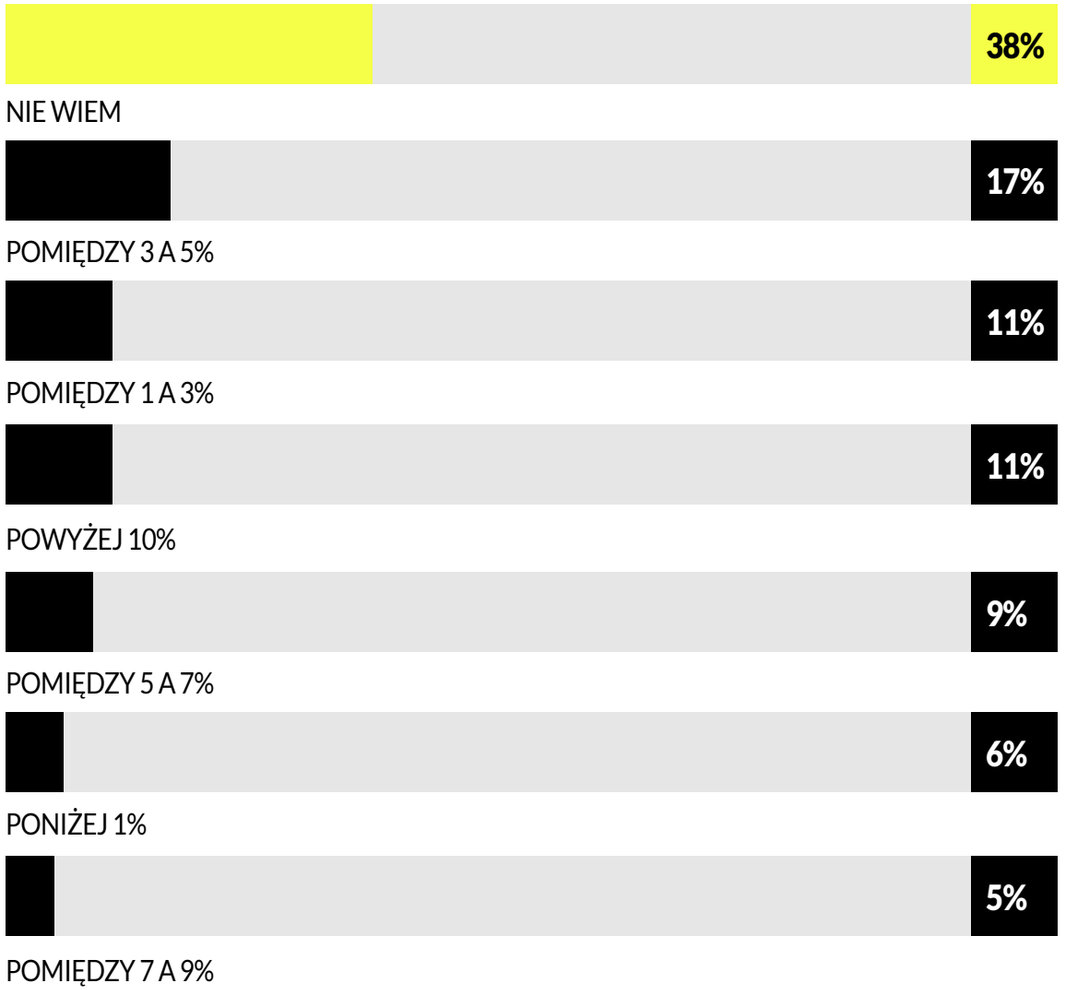
Kolejny trend z naszych badań, który znalazł potwierdzenie w odpowiedziach w trakcie spotkań Security Excellence, to malejąca ilość używanych systemów bezpieczeństwa. Ewidentnie Polska stanowi tu czołówkę europejską – zdecydowana większość wskazywała do maksymalnie pięciu różnych systemów i należy podkreślić że jest to znaczący spadek – jeszcze rok temu, podobne badanie wskazywało na 8-10. To dobrze wróży zarówno efektywności operacyjnej jak i pozytywnemu wpływowi na koszty związane z integracją i treningami.

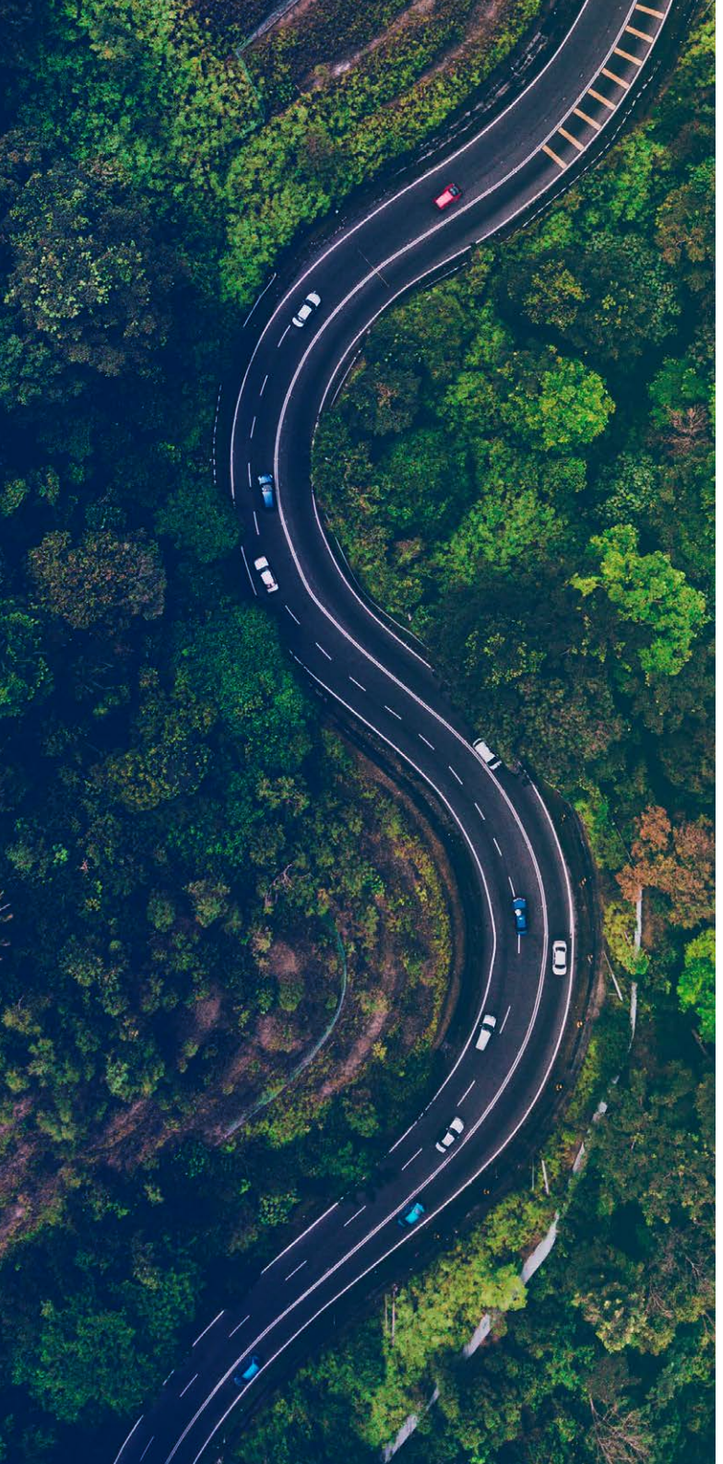
BUDŻET BEZPIECZEŃSTWA

\+

FINANSE NA BEZPIECZEŃSTWO OKREŚLONE Z GÓRY, TRAKTOWANE INCYDENTALNIE, CZY WBUDOWANE WE WSZYSTKIE PROJEKTY?

PROCENT CAŁKOWITEGO BUDŻETU IT PRZEZNACZANY NA CYBERBEZPIECZEŃSTWO





MAREK PIOTROWSKI,
DYREKTOR IT, KOMPUTRONIK

Zaskakujące jest to, że ponad 1/3 badanych odpowiada, że nie wie, jaki jest procent budżetu na bezpieczeństwo w ramach budżetu IT. To wskazuje na to, że wydatki na bezpieczeństwo traktowane są incydentalnie, a nie systemowo lub nie są klasyfikowane jako te wynikające z potrzeb bezpieczeństwa. Tymczasem bezpieczeństwo informacji w praktyce jest obecne prawie we wszystkich wydatkach na IT. Skoro podstawą sensu istnienia IT jest wspieranie biznesu, który w zasadzie coraz częściej polega na elektronicznym przepływie informacji, to można w ten sposób wykazać, że w praktyce wydatki na IT zawsze w jakiejś części będą dotyczyć wydatków na bezpieczeństwo. W tym miejscu koniecznie trzeba dodać, że coraz popularniejszy trend w projektowaniu IT, polegający na zapewnieniu analizy ryzyka w obszarze bezpieczeństwa informacji od samego początku projektu (security by design) w praktyce powoduje, że wnioski płynące z prac analitycznych wprost mają wpływ na biznes od samego początku jego projektowania.

W ten sposób wydatki na bezpieczeństwo będą zaimplementowane w biznes, co więcej, na etapie projektowania zarówno strona biznesowa jak i IT, zdając sobie sprawę z możliwości i wymagań, powinny wspólnie dążyć do wypracowania takiego planu, by był on konkurencyjny zarówno poprzez efektywność biznesową jak i optymalizację kosztów po stronie IT.

Istotne jest to, by taki proces współpracy był również uwzględniony na etapie budowania strategii przedsiębiorstwa. Wówczas będzie można mówić o budżecie na IT i bezpieczeństwo, jako elemencie utrzymania zawartych kontraktów oraz zapewnieniu finansowania nowych potrzeb w zakresie wsparcia biznesu i wszyscy powinni wiedzieć, czy i ile na ten cel przeznaczono.

BEZPIECZEŃSTWO MOBILNE

Mobilna transformacja wymaga jednoczesnego zapewnienia użytkownikom pełnej swobody i wygody i totalnego bezpieczeństwa firmowych danych.

KAROL GRABARCZYK,
PRINCIPAL B2B TECH EXPERT
BUSINESS & CLOUD, SAMSUNG

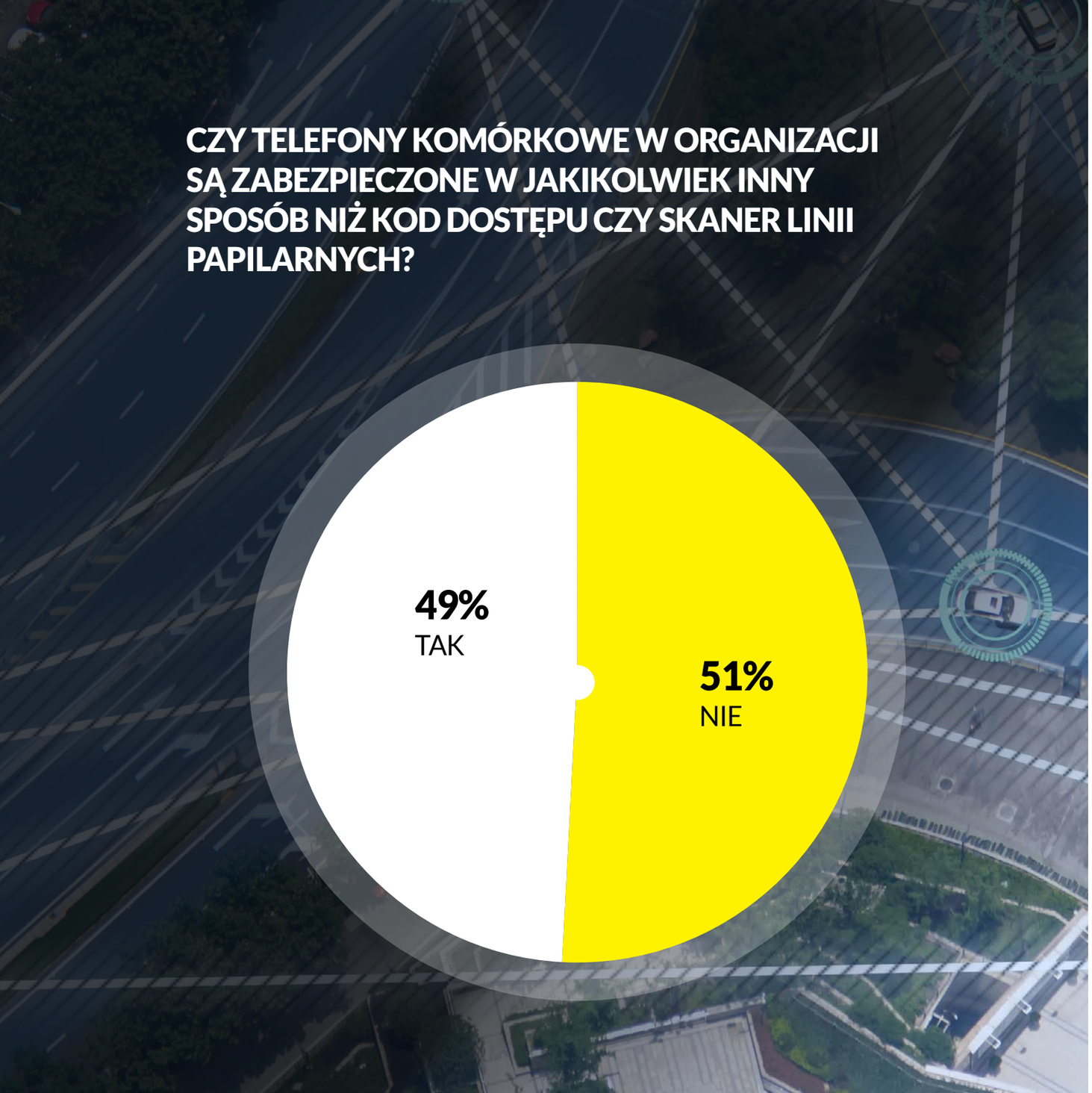
Każda organizacja chciałaby usprawnić mobilność pracy w terenie i dostępne narzędzia, urządzenia mobilne. Platforma Samsung Knox, może użytkownikom zapewnić wygodny, płynny dostęp do danych służbowych, poczty, aplikacji służbowych. Coraz więcej organizacji wykorzystuje funkcjonalności takie jak podpis biometryczny i możliwość tworzenia własnych elektronicznych formularzy. To sprawdza się zwłaszcza w obsłudze klienta, skraca proces i czyni go bardziej efektywnym.

Portfolio urządzeń i usług mobilnych rośnie w szybkim tempie, każda organizacja może dostosować rozwiązania do swoich potrzeb. W wielu firmach coraz większym powodzeniem cieszą się urządzenia klasy ruggedized, które dają możliwość bezpiecznej pracy w trudnych warunkach, w rękawiczkach czy z uszkodzonym ekranem.

W obsłudze sprzedaży stacjonarnej, mamy możliwość zmiany urządzenia mobilnego w system interakcji z klientem, np. sprzedawca wyświetla na swoim ekranie wariant oferty dopasowany do klienta, a ten może od razu przejrzeć, zaakceptować i podpisać umowę podpisem biometrycznym lub kwalifikowanym. To wszystko jest zamknięte w bezpiecznej przestrzeni roboczej, którą zarządza dział IT.

POTENCJALNE OBSZARY TRANSFORMACJI MOBILNEJ W ORGANIZACJI

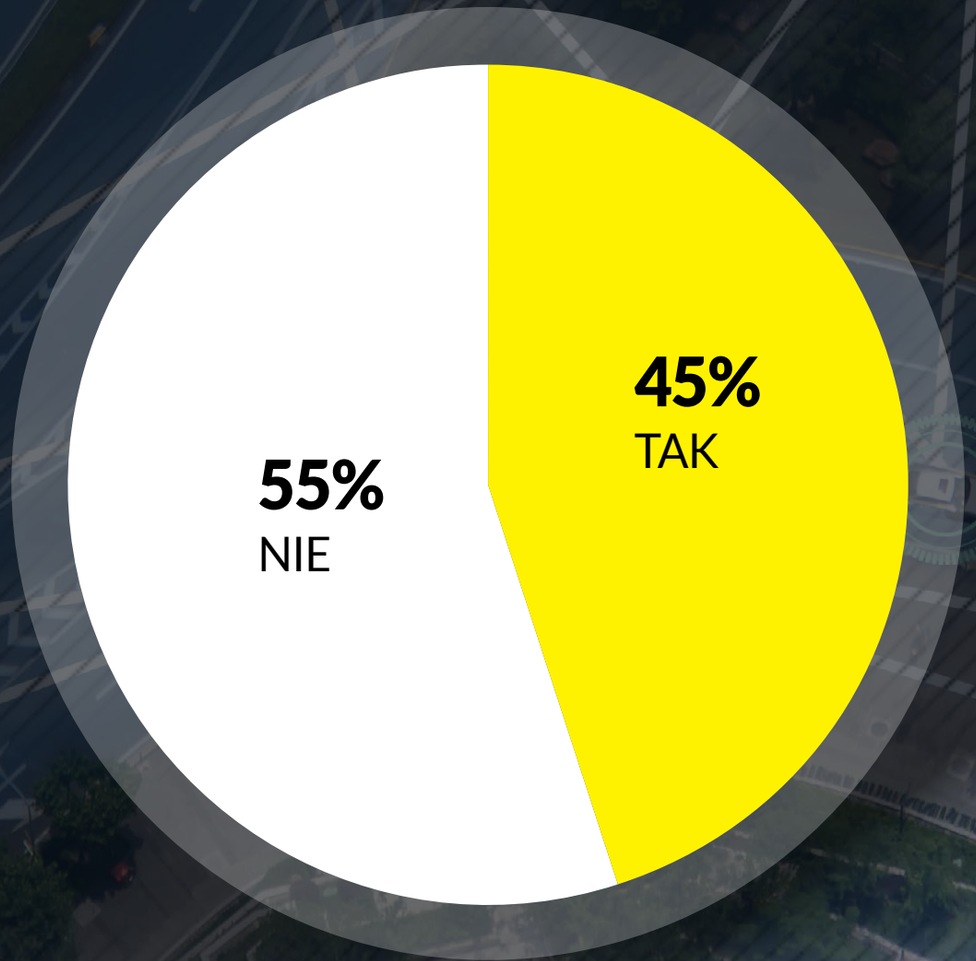
CZY TELEFONY KOMÓRKOWE W ORGANIZACJI SĄ ZABEZPIECZONE W JAKIKOLWIEK INNY SPOSÓB NIŻ KOD DOSTĘPU CZY SKANER LINII PAPILARNYCH?



TOMASZ ŁUŻAK,
PRODUCT OWNER - IT SECURITY
W T-MOBILE POLSKA

Wyniki badania wskazują, że połowa firm nie stosuje zabezpieczeń innych niż kod dostępu czy skaner linii papilarnych. W praktyce oznacza to, że w zabezpieczaniu infrastruktury IT wciąż zapomina się o tak ważnym elemencie, jakim są firmowe telefony komórkowe. Urządzenia te stały się nieodłącznym elementem pracy wielu z nas, drugim komputerem. Dzięki nim mamy dostęp do poczty elektronicznej czy z aplikacji firmowych z dowolnego miejsca. Dynamicznie rosnący ruch generowany przez urządzenia mobilne, a także liczba podatności w mobilnych systemach operacyjnych, w połączeniu ze wspomnianym brakiem zabezpieczeń, prowokują cyberprzestępców do coraz częstszych ataków na te urządzenia. Udany atak może prowadzić do kradzieży danych, inwigilacji użytkownika, czy nieświadomej aktywności w sieciach botnetowych. Odpowiedzią na tego typu zagrożenia są rozwiązania dostarczane przez operatorów telekomunikacyjnych. Szczególnie te niewymagające instalacji oprogramowania na urządzeniach końcowych, np. Cyber Guard od T-Mobile Polska.

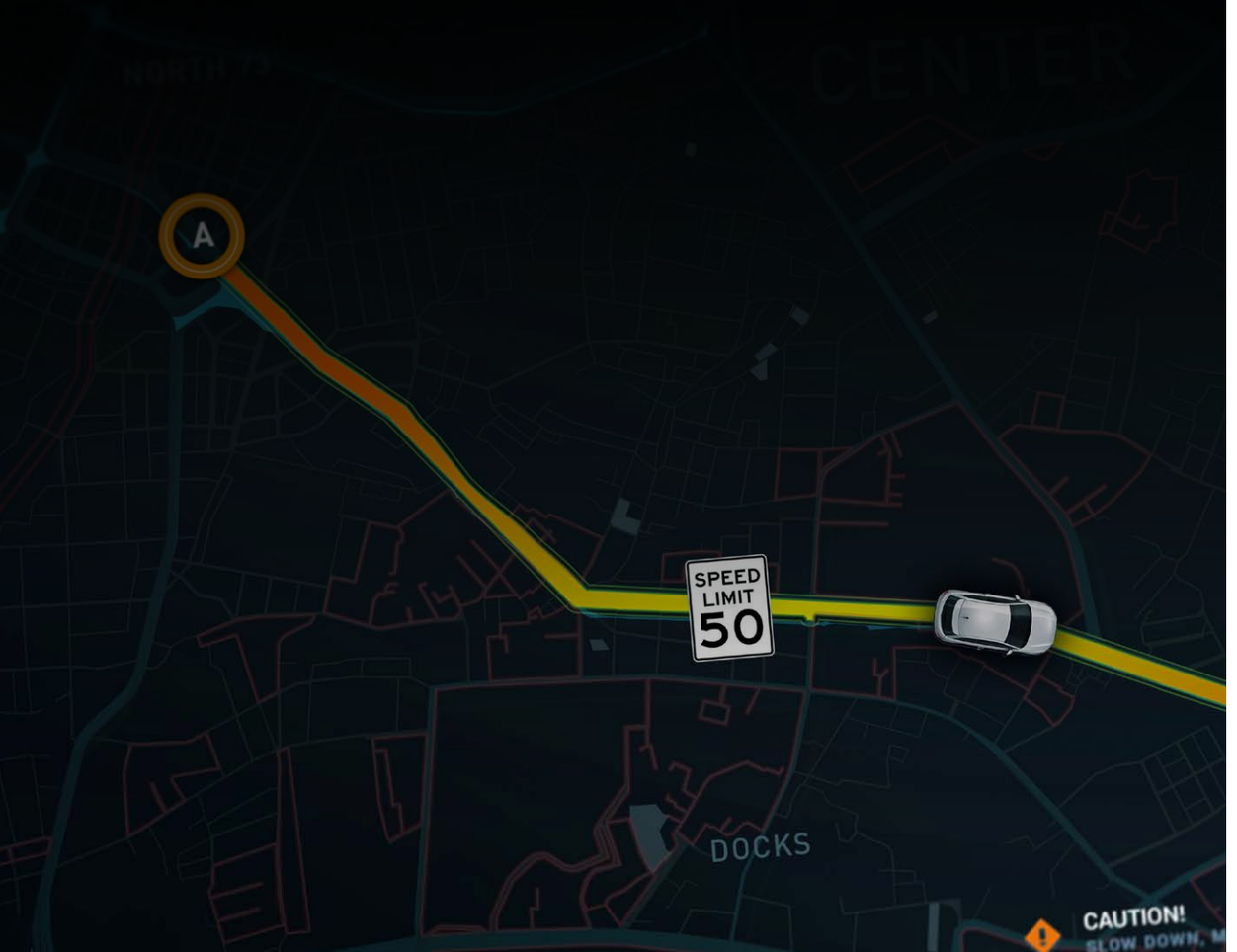
CZY W ORGANIZACJI INCYDENTY BEZPIECZEŃSTWA MONITOROWANE SĄ PRZEZ CAŁĄ DOBĘ?



TOMASZ ŁUŻAK,
PRODUCT OWNER - IT SECURITY
W T-MOBILE POLSKA

Z badania wynika że 45% firm nie monitoruje incydentów w trybie 24x7x365. Przyczyną może być wysoki koszt inwestycji w narzędzia do monitorowania, np. systemy klasy SIEM. Może również konieczność utrzymywania zespołu Security Operations Center (SOC), składającego się z dobrze opłacanych specjalistów bezpieczeństwa IT, a których notorycznie brakuje na rynku. Alternatywę mogą stanowić propozycje firm, zwłaszcza operatorów telekomunikacyjnych. Ci ostatni oferują zaawansowane usługi SOC, realizujące monitoring czy zaawansowane usługi informatyki śledczej.

CLOUD I BEZPIECZEŃSTWO



OBAWY PRZED KORZYSTANIEM W WIĘKSZYM ZAKRESIE Z CHMURY PUBLICZNEJ (SAAS, AZURE, AMAZON ITP.)

72%

STOSUJĘ MODEL HYBRYDOWY: CHMURĘ PRYWATNĄ I WŁASNE ROZWIĄZANIA ORAZ CHMURĘ PUBLICZNĄ. Z CZEGO I W JAKIM ZAKRESIE KORZYSTAM ZALEŻY WYŁĄCZNIE OD KORZYŚCI BIZNESOWYCH ORAZ ANALIZY RYZYKA.

17%

WOLĘ KORZYSTAĆ Z ROZWIĄZAŃ I APLIKACJI, KTÓRE SAM WDRAŻAM I KTÓRYMI ZARZĄDZAM. DZIĘKI TEMU LEPIEJ ZARZĄDZAM BUDŻETEM I MNIEJ WYDAJĘ NA IT. TYLKO JEŚLI NIE MAM WYJŚCIA (NP. OFFICE 365) KORZYSTAM Z CHMURY.

6%

BARDZO CHĘTNIE KORZYSTAM Z CHMURY PUBLICZNEJ I NIE MAM ŻADNYCH OBAW PRZED KORZYSTANIEM Z NIEJ. GDYBY NIE DŁUG TECHNOLOGICZNY TO W CAŁOŚCI PRZESZEDŁ BYM NA ROZWIĄZANIA Z CHMURY PUBLICZNEJ.

2%

CHMURA PUBLICZNA BĘDZIE ZAWSZE MNIEJ BEZPIECZNA NIŻ MOJE WŁASNE ROZWIĄZANIA W MOIM DC. NIE UFAM TYM ROZWIĄZANIOM.

TOMASZ MATUŁA,
EKSPERT I MENEDŻER RYNKU ICT ORAZ
TELCO, DYREKTOR PROGRAMOWY

19% woli własne DC oraz aplikacje i nie ufa chmurze. To całkiem dużo ale może też wynikać ze specyfiki pewnych branż (np. obronność, produkcja i OT). 72% stosuje model hybrydowy co jest pragmatycznym wyborem i jeszcze przez wiele lat racjonalnym dla wielu firm, chociażby ze względu na „dług technologiczny". Pamiętajmy tylko o tym, że wieloletni dłużnicy sumarycznie zawsze płacą więcej a czasami bankrutują...

TOMASZ ŁUŻAK,
PRODUCT OWNER - IT SECURITY
W T-MOBILE POLSKA

Polskie firmy powszechnie sięgają po usługi chmurowe, które coraz częściej nie tylko uzupełniają, ale wręcz zastępują tradycyjne rozwiązania. Wydaje się to zrozumiałe w kontekście kosztów i trudności w utrzymywaniu i zabezpieczaniu własnych środowisk teleinformatycznych. Popyt na rozwiązania chmurowe stymuluje też rosnąca podaż produktów bezpieczeństwa, świadczonych poprzez chmury publiczne. Przedsiębiorstwa podchodzą jednocześnie do tematu w sposób bardzo pragmatyczny – proporcja wykorzystania rozwiązań w obu modelach zależy głównie od analizy ryzyka i korzyści biznesowych.


DIGITAL EXCELLENCE
CIONET
WWW.SECURITYEXCELLENCE.PL
cisco
NTT
SAMSUNG
zscaler