EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA

4CF

Surf the future

nieoczekiwana przyszłość:

CYBERBEZPIECZEŃSTWO

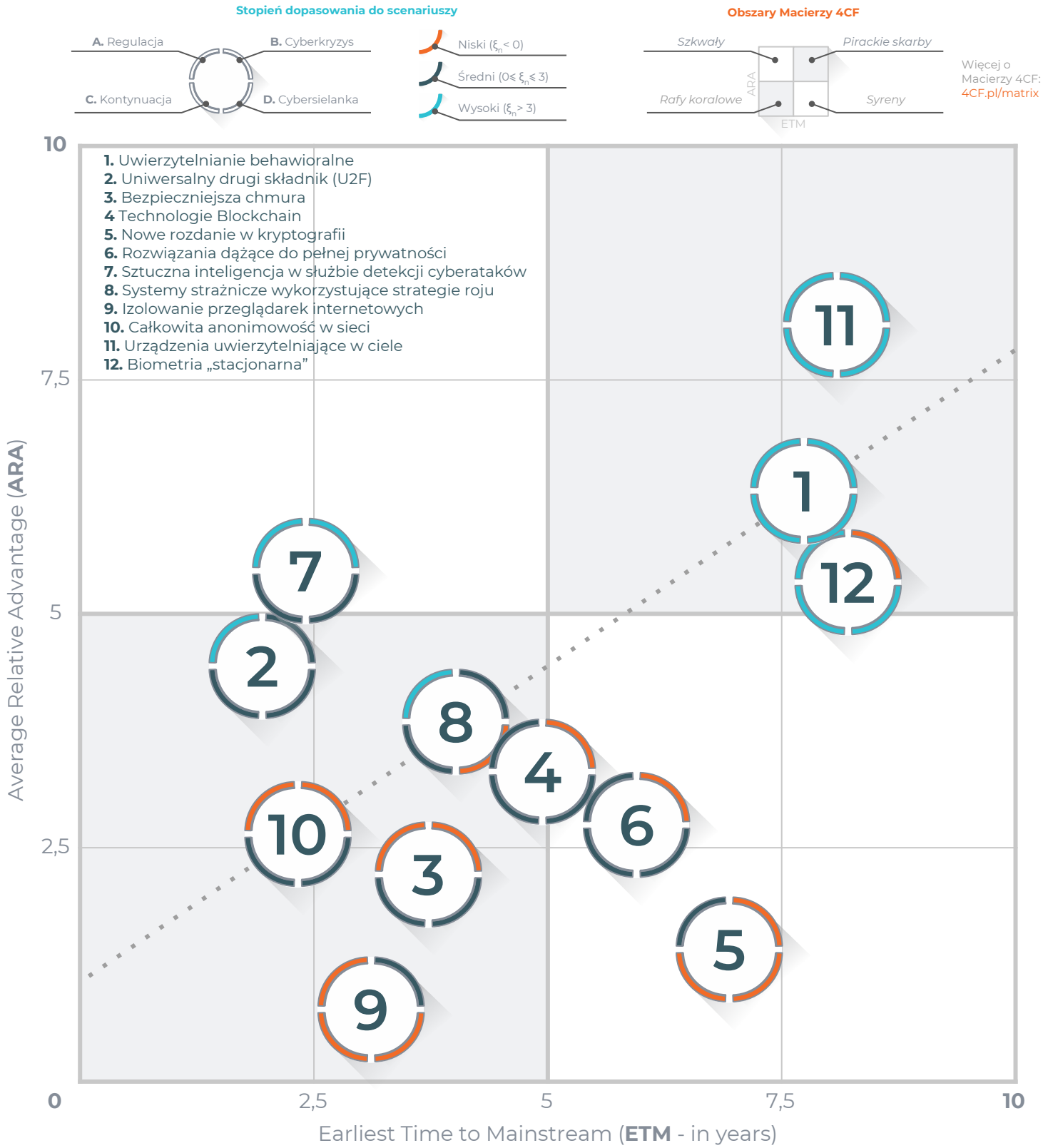
MACIERZ 4CF

2018+10

MACIERZ 4CF: **CYBERSEC 2018+10**

Przyszłość cyberbezpieczeństwa nie jest przesądzona - kształtuje ją wspólnie wiele podmiotów. Jak więc uzyskać przewagę strategiczną i zaskakiwać konkurencję, jednocześnie samemu nie dając się zaskoczyć? Macierz 4CF to sprawdzone w szerokim wachlarzu dziedzin (od FMCG, branży medycznej i bankowości po zastosowania wojskowe) narzędzie wsparcia długoterminowej analizy strategicznej. Zazwyczaj stosuje się ją do analizy konkretnej organizacji, w odniesieniu do jej celów strategicznych, segmentów rynku i potrzeb. Pomaga wypracować plan rozwoju oparty na niedostępnych konkurencji wglądach w przyszłość. Poniższa wersja jest jawna i uniwersalna, ale mimo tego zawiera wiele informacji o rozwiązaniach, których nie powinno się ignorować - warto potraktować ją jako zaproszenie do pogłębionej analizy z perspektywy własnej firmy.

Macierz 4CF określają dwie osie: Średnia Względna Korzyść (**ARA** - *Average Relative Advantage*) oraz Najkrótszy Czas do Upowszechnienia (**ETM** - *Earliest Time to Mainstream*). ARA to uśredniona dla scenariuszy przyszłości złożona miara, uwzględniająca zalety i wady danego rozwiązania względem alternatywnych rozwiązań w stosunku do przyszłych potrzeb. ETM podany jest w latach od roku 2018 i wyraża najwcześniejszy możliwy czas upowszechnienia. ETM nie jest więc prognozą, ale trzeba się liczyć z tym, że w terminie określonym przez ETM może być już za późno na reakcję.



SCENARIUSZE: CYBERSEC 2028

Myśląc o przyszłości mamy tendencję do ekstrapolowania dzisiejszych trendów podświadomie zakładając, że nie zostaną one zaburzone w kolejnych latach. Jednak przyszłość nie jest przesądzona, a jej rozwój podążać może wieloma różnymi ścieżkami. Cyberbezpieczeństwo w kolejnej dekadzie podlegać będzie wpływowi szeregu czynników zmian, z których najważniejsze zostały przeanalizowane i zgrupowane w klastry określające cztery scenariusze przyszłości. Jeden z nich, to scenariusz kontynuacji, odpowiadający prostej ekstrapolacji trendów. Trzy pozostałe opisują wersje przyszłości, w których jeden bądź więcej z aktualnych trendów ulegnie istotnej zmianie. Odnosząc poszczególne rozwiązania do możliwych scenariuszy przyszłości można ocenić czy rozwiązania te są odporne na zmiany warunków otoczenia oraz w jakich warunkach sprawdzą się najlepiej.

A. REGULACJA

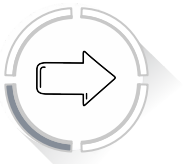
Widząc efekty działań podjętych w 2018 roku, m.in. wprowadzenia regulacji RODO na terenie UE, czy tzw. ACTA2, państwa oraz organizacje międzynarodowe przystąpiły do dalszego regulowania cyberprzestrzeni. Przez trzecią dekadę XXI wieku wprowadzano kolejne regulacje, nakładające prawny kaganiec na działania w sieci. Wymóg prawny tworzenia sprzętu bezpieczniejszego i odpornego na cyberataki (stosowanie filozofii „secure by design"), zobowiązanie firm do zwiększania nakładów na cyberbezpieczeństwo, tworzenie agencji państwowych i międzynarodowych zajmujących się bezpieczeństwem w sieci - te kolejne rozwiązania wraz z upływem lat stają się rzeczywistością. Rozwój rynku wyhamowuje, a usługi sieciowe drożeją. W 2028 roku, mimo intensywnych protestów internautów, ofensywa regulacyjna zostaje zwieńczona tzw. Internetem 2.0, w którym każdy użytkownik jest identyfikowalny i wykrywalny, a boty i sztuczne inteligencje mają przypisanych właścicieli, którzy ponoszą odpowiedzialność za ich działania.

Wygląda na to, że era dzikiego dzikiego zachodu w sieci dobiegła końca, ale nie wszystkim konsumentom się to podoba. Część osób cieszy się z bezpieczeństwa zapewnionego restrykcyjnymi regulacjami, ale wielu - zniechęconych poczuciem powszechnej inwigilacji i podrożeniem usług sieciowych - szuka prywatności w nie do końca legalnych alternatywach do Internetu 2.0.

B. CYBERKRYZYS

Po dziesiątkach lat wytężonych prac w latach 20. XXI wieku została definitywnie udowodniona hipoteza Riemanna - klucz do efektywnego odkrywania liczb pierwszych, stanowiących podstawę obecnej kryptografii. W połączeniu z coraz większą mocą obliczeniową dostępną cyberprzestępcom oraz wciąż powszechnymi dziurami w oprogramowaniu, sprawia to, że nad światem zawisła groźba chaosu związanego z niemożnością połączenia wygody dostępu do danych z bezpieczeństwem. Rozpoczął się globalny wyścig o stworzenie nowych, skutecznych metod szyfrowania i uwierzytelniania. Niestety, za późno - w 2028 następuje seria spektakularnych cyberataków, a poziom bezpieczeństwa w internecie radykalnie spada. Instytucje finansowe z dnia na dzień odcinają się od sieci. Wybucha kryzys gospodarczy, sparaliżowane są instytucje finansowe i giganci technologiczni, a rządy państw wzajemnie oskarżają się o wspieranie cyberataków. Świat znajduje się o włos od trzeciej wojny światowej.

Konsumenci panicznie boją się utraty danych i środków finansowych. Gotowi są w dużej mierze zrezygnować z wygody w imię zwiększenia bezpieczeństwa, co w wielu przypadkach owocuje - przynajmniej częściowym - powrotem do rozwiązań niesieciowych.



C. KONTYNUACJA

Branża IT rozwija się. Giganci IT, a także głodne sukcesu start-upy zalały rynek sprzętem IoT, w efekcie w 2028 roku wprowadzając ludzkość w pełnoprawną erę *smart*. Większość urządzeń codziennego użytku zaopatrzona jest w moduły zbierania i wysyłania danych, które analizowane przez zaawansowane algorytmy sztucznej inteligencji stają się podwalinami nowych produktów. Ta technologiczna *prosperity* ma jednak swoją cenę - wraz ze wzrostem liczby urządzeń IoT rośnie liczba cyberataków, w tym uciążliwych ataków DDoS. Zagrożenie nie rośnie jedynie ze strony grup przestępczych - cyfrowe siły zbrojne są nieodzownym elementem armii państwowych, dochodzi też do pierwszych otwartych konfliktów w cyberprzestrzeni. Internet przestał być tak swobodnym miejscem jak niegdyś - internauci są ostrożniejsi, a firmy IT traktują bezpieczeństwo priorytetowo. Działanie różnych sił utrzymuje się w stanie chybotliwej równowagi sprawiając, że cyberprzestrzeń trzeszczy od napięć i tylko czeka na rozłam lub wybuch globalnego konfliktu.

Konsumenci miotają się pomiędzy obawami związanymi z bezpieczeństwem danych, prywatnością i wygodą. Większość korzysta z powszechnych usług sieciowych w przeświadczeniu, że są one względnie bezpieczne. Regularne doniesienia o spektakularnych atakach hakerskich uwrażliwiają jednak konsumentów na kwestie związane z cyberbezpieczeństwem.

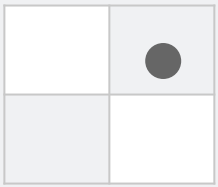
D. CYBERSIELANKA

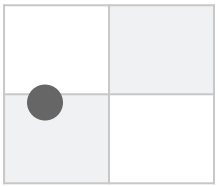
Społeczność naukowa oraz biznesowa związana z branżą IT, dostrzegłszy spowolnienie wzrostu mocy obliczeniowej, skierowała swoje wysiłki ku poszukiwaniu nowych rozwiązań. W 2028 następuje przełom - oparte na technologiach fotonicznych i kwantowych rozwiązania IT są niezawodne i dostępne w cenie przystępnej dla biznesu, przez co szybko zyskują użytkowników. Co prawda do posiadania komputera kwantowego w telefonie potrzeba jeszcze kilku dobrych lat, ale drastyczne zwiększenie mocy obliczeniowej, połączone z nowym - kwantowym - podejściem do szyfrowania sprawia, że bezpieczeństwo wrażliwych danych cyfrowych gwałtownie rośnie. Dysponenci rozwiązań kwantowych ograniczają ich dostępność do konkretnych zastosowań tj. badań naukowych i mechanizmów bezpieczeństwa w finansach, bez dostępu dla prywatnych osób, by nie dawać cyberprzestępcom broni do ręki. Wygląda na to, że przynajmniej na kilka najbliższych lat widmo kryzysu cyberbezpieczeństwa zostaje zażegnane.

Konsumenci bez problemu odnajdują się w tym nowym, wspaniałym świecie - chętniej niż dotychczas powierzają swoje dane zewnętrznym podmiotom i masowo korzystają z coraz bardziej zaawansowanych usług sieciowych, w tym z opartych o sztuczną inteligencję wirtualnych asystentów, dysponujących nawet najintymniejszymi informacjami o swoich użytkownikach.

1. Uwierzytelnianie behawioralne

Identyfikacja użytkownika na podstawie odruchu lub zachowania (trudność jego kontrolowania zwiększa bezpieczeństwo całej procedury) - np. użytkownik wprowadza tekst do komputera na klawiaturze, a system porównuje ten sposób pisania ze wzorcem. Przyszłe możliwości są jeszcze ciekawsze - badanie refleksu, reakcji źrenicy na impuls świetlny, czy skoku ciśnienia po przekazaniu treści wizualnych. Metoda ta w długiej perspektywie uzyskała bardzo wysoką ocenę.



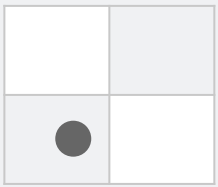


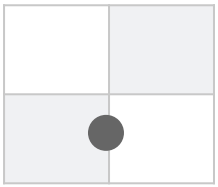
2. Uniwersalny drugi składnik (U2F)

Identyfikacja użytkownika przy pomocy dodatkowego sprzętu, przeznaczonego wyłącznie do tego celu. Standardy tego typu rozwiązań opracowuje konsorcjum FIDO Alliance (Fast IDentity Online), a przykładem jest YubiKey firmy Yubico. Aby uniknąć problemu wykorzystania takiego klucza przez osoby niepowołane (np. wskutek jego zgubienia), powinien on być połączony z dodatkowym zabezpieczeniem np. PINem lub biometrią.

3. Bezpieczniejsza chmura

Użytkownicy mają możliwość przekazania swoich danych pod ochronę wyspecjalizowanym firmom w ramach usługi opartej o chmurę. Przykładem takiej ochrony jest m.in. szyfrowanie homomorficzne/*lattice cryptography* - rozwiązanie, które maskuje dane przeliczane w udostępnianych przez strony trzecie chmurach.



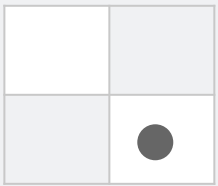


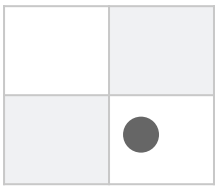
4. Powszechny Blockchain do kontroli nadużyć

Zachowanie anonimowości oraz unikalności danych poprzez stosowanie blockchaina (systemu weryfikacji danych przy wykorzystaniu poprzednich danych w łańcuchu transakcji) może pomóc zarówno przy kontroli nadużyć wykonywanych przez poddostawców (poziom *supply chain*), jak i ułatwić walkę z fake newsami. W porównaniu do alternatyw uzyskał umiarkowaną ocenę ARA.

5. Nowe rozdanie w kryptografii

Kolejne pokolenie algorytmów szyfrujących dane - np. następne wydanie obecnego standardu SHA (SHA-4). Korzystając z rosnącej w czasie mocy obliczeniowej urządzeń dostępnych typowym użytkownikom specjaliści od cyberbezpieczeństwa opracowują bardziej złożone i trudniejsze do złamania algorytmy szyfrujące. Przełomem w tej dziedzinie może być szyfrowanie oparte o kod DNA. Mimo nadziei, jest to tylko rozwiązanie zaradcze, bez potencjału na trwałą zmianę obrazu cyberbezpieczeństwa.



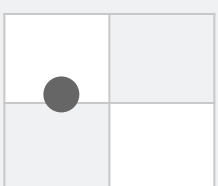


6. Rozwiązania dążące do pełnej prywatności

Rozwiązania, które mają zapewnić użytkownikowi pełną kontrolę nad jego danymi w sieci (np. platforma SOLID - *social linked data*) i tym samym zmniejszyć wrażliwość na ataki z ich wykorzystaniem. Dane użytkownika znajdowałyby się w konkretnych, znanych mu miejscach sieci, a każda usługa chcąca je wykorzystać musiałaby mieć na to udzieloną zgodę. Rozwiązanie dobre dla prywatności, ale bez wpływu na inne zagadnienia cyberbezpieczeństwa.

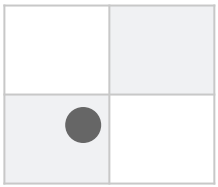
7. Sztuczna inteligencja w służbie detekcji cyberataków

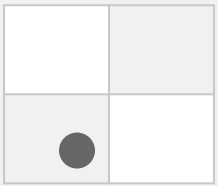
Przy atakach DDoS podstawową obroną jest ich wczesna detekcja. Tu z pomocą mogą przyjść narzędzia sztucznej inteligencji (deep learning, machine learning, neural networks), skuteczniej rozpoznające wzorce zachowań charakterystyczne dla ataków *malware* na bardzo wczesnym etapie i dławiące je w zarodku. To rozwiązanie to potencjalny *game-changer*.



8. Systemy strażnicze wykorzystujące strategie roju

Źródłem potencjalnych, skutecznych rozwiązań do detekcji cyberataków mogą być strategie stosowane przez gatunki zwierząt, które tworzą zaawansowane struktury społeczne. Przykładem takiego algorytmu jest HONIED (Hive Oversight for Network Intrusion Early Warning using DIAMoND) - wykorzystujący efektywną strategię informowania o pojawieniu się anomalii w systemie, zainspirowaną zachowaniem pszczół.



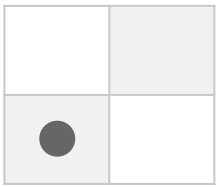


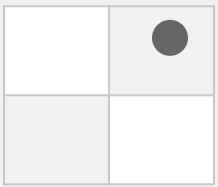
9. Izolowanie przeglądarek internetowych

Fizyczna izolacja przeglądarek internetowych/połączeń internetowych od infrastruktury danych i sieci wewnętrznych (organizacji). Podatność na ataki internetowe systemu spada wtedy prawie do zera. Nieco mniej bezpiecznym, acz wygodniejszym rozwiązaniem jest też zdalna izolacja w formie usługi. Firma może wykupić dostęp do serwerów, na których będzie korzystać z przeglądarek. Gdy dojdzie do zainfekowania, w pierwszej kolejności narażone są maszyny usługodawcy.

10. Całkowita anonimowość w sieci

Możliwość ukrycia swojej tożsamości w sieci przy jednoczesnym zachowaniu zdolności autoryzacji mogłaby drastycznie zwiększyć bezpieczeństwo internautów. Jednym z narzędzi do osiągnięcia tego stanu może być rozwijany obecnie algorytm zk-SNARK - oparty o *zero-knowledge proof* czy anonimizacja/pseudonimizacja danych. Ale czy całkowita anonimowość nie ośmieli cyberprzestępców do bardziej agresywnych działań? To ryzyko istotnie wpływa na ocenę rozwiązania.



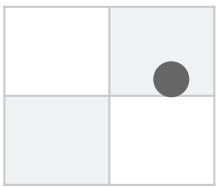


11. Urządzenia uwierzytelniające w ciele

W najprostszej wersji jest to implant, który pozwala na uwierzytelnianie i autoryzację płatności w sposób podobny do popularnych obecnie płatności bezstykowych. W wersji bardziej zaawansowanej weryfikuje dodatkowo tożsamość „nosiciela", a także aktywuje się tylko w określonym momencie, np. po wykonaniu ręką gestu, który stanowi oświadczenie woli. Zdecydowany lider w badaniu, ale wciąż potrzebuje dużo czasu do wejścia na szeroki rynek.

12. Biometria „stacjonarna"

Mimo wejścia biometrii do mainstreamu (sprawdzanie linii papilarnych w smartfonach czy bardziej zaawansowane skanowanie twarzy), wciąż nie możemy płacić za zakupy „samymi sobą" - bez portfela, telefonu, ani żadnych innych akcesoriów przy sobie. Biometria stacjonarna może być odpowiedzią na ten problem, ale by do tego doszło musi zapewnić użytkownikom dostateczny poziom poczucia bezpieczeństwa („Skan mojej tęczówki/wzór siatki naczyń kapilarnych nie jest przechowywany w terminalu, w którym płaciłam"), ale także zwiększyć wygodę użytkowania (biometria dziejąca się „w tle").



SHA - *Secure Hash Algorithms* - dosł. „algorytmy siekanki bezpieczeństwa" - rodzina reguł (funkcji kryptograficznych), które zamieniają wprowadzone przez użytkownika treści (np. hasło, login, numer karty kredytowej) na 40 cyfrową liczbę zapisaną w kodzie szesnastkowym. Trzecia z kolei iteracja tej rodziny, SHA-3, jest obecnie głównym standardem szyfrowania danych w Internecie.

Zero-knowledge proof - protokół komunikacji, który umożliwiałby jednej stronie dialogu (Rozmówcy A) udowodnienie drugiej stronie (Rozmówcy B) faktu posiadania wiedzy na temat wartości pewnej danej X, bez ujawniania żadnych dodatkowych faktów poza właśnie samym faktem posiadania tej wiedzy. Co ważne - Rozmówca A nie ujawnia Rozmówcy B wartości danej X. Informuje go jedynie o tym, że wie jaka jest ta wartość - i w tym tkwi siła tego protokołu.

Anonimizacja - metoda zapewniania prywatności polegająca na oczyszczeniu wprowadzanych przez użytkownika danych ze wszystkich informacji, mogących go zidentyfikować.

Pseudonimizacja - metoda podobna do anonimizacji, różniąca się tym, że dane identyfikujące użytkownika nie są usuwane, a ukrywane pod pseudonimem.

DDoS - *Distributed Denial of Service* - dosł. „rozproszona odmowa obsługi" - rodzaj cyberataku polegający na „zapchaniu" serwera np. ze stroną internetową milionami próśb o dostęp, generowanymi przez przejęte przez cyberprzestępcę urządzenia (boty, zombie-boty), co w efekcie powoduje czasowy brak dostępu do danej usługi.

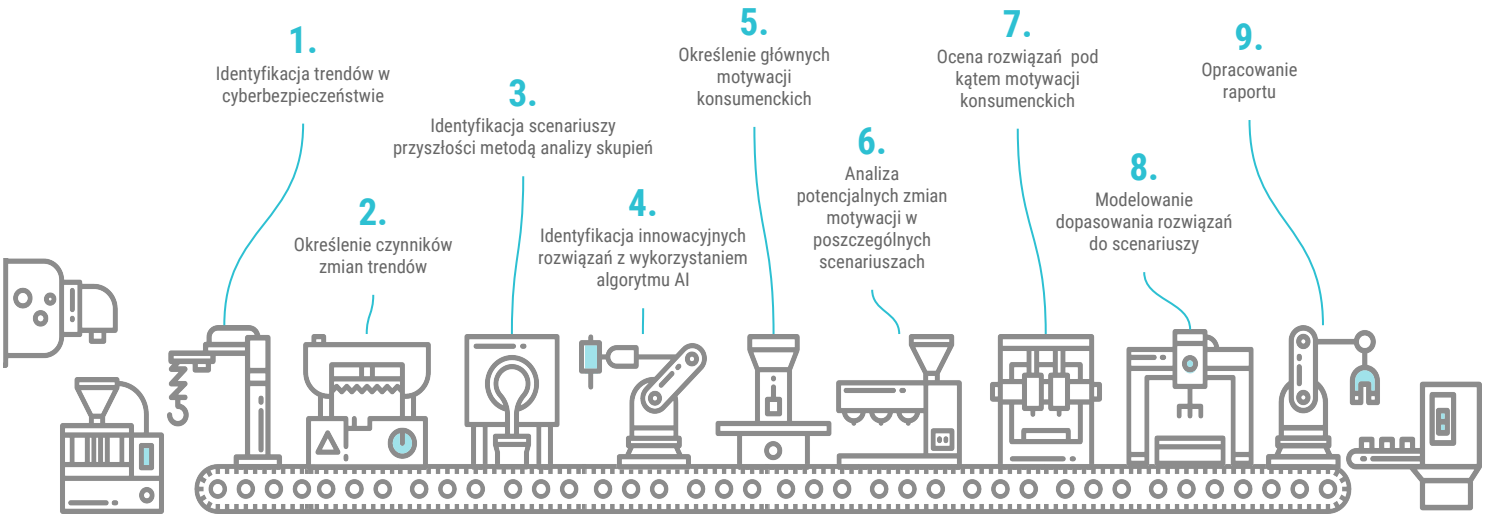
IoT - *Internet of Things* - Internet rzeczy. Pojęcie, które opisuje zjawisko „podłączania" do Internetu przedmiotów codziennego użytku, których podstawowa funkcja nie ma nic wspólnego z komunikowaniem się ludzi (szczoteczki do zębów, lodówki, różnego rodzaju znaczniki do zbierania i przesyłania informacji). Przedmioty te zbierają wszelakie dane i za pośrednictwem sieci przesyłają je do dalszej analizy, ale także komunikują się między sobą (np. zawieszka przy kluczach „rozmawia" z zamkiem w drzwiach). W 2017 do sieci było podłączonych prawie 9 miliardów takich urządzeń. Szacuje się, że w 2020 roku ich liczba przekroczy 20 miliardów.

JAK POWSTAŁ TEN RAPORT?

Niniejszy raport jest efektem złożonego procesu analitycznego, wykorzystującego zaawansowaną metodologię w celu zapewnienia jakości i skali badania, która umożliwia ocenę przyszłych rozwiązań. Za pomoc i konsultację przy opracowaniu raportu zespół 4CF pragnie szczególnie podziękować Karolowi Chwastowskiemu, Grzegorzowi Małeckiemu, Marcinowi Strzeleckiemu, Tomaszowi Jędrkiewiczowi oraz Aleksandrze Świączkowskiej. Raport powstał we współpracy z Polskim Towarzystwem Studiów nad Przyszłością, w ramach Europejskiego Miesiąca Cyberbezpieczeństwa.

ptsp.pl
POLSKIE TOWARZYSTWO STUDIÓW NAD PRZYSZŁOŚCIĄ

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA



CO DALEJ?

Czy coś Państwa w naszej analizie zaskoczyło? A może z czymś się Państwo nie zgadzają? W których scenariuszach widzą Państwo bardziej szansę, a w których zagrożenie? Upowszechnieniu których rozwiązań woleliby Państwo przeciwdziałać, a za których sprawą chcieliby Państwo spróbować zawojować rynek?

Szybkie zmiany rynkowe sprawiają, że znacznie trudniej jest opracować strategię działania odporną na przyszłość. Wnioski zawarte w niniejszym raporcie mogą Państwu pomóc w zidentyfikowaniu obszarów szczególnie interesujących z perspektywy Państwa organizacji. Jednak aby na rynkach przyszłości zaskakiwać konkurencję jednocześnie samemu nie dając się zaskoczyć, potrzeba głębszej analizy, uwzględniającej znacznie więcej rozwiązań, Państwa cele strategiczne, segmenty rynku, możliwości i potrzeby. Taka analiza, wraz ze stałym monitorowaniem otoczenia w poszukiwaniu wczesnych sygnałów ostrzegawczych, to klucz do uzyskania zdolności *surfowania na fali zmian* – kształtowania pożądanych scenariuszy przyszłości i wykorzystywania zmian do skutecznej realizacji długoterminowych celów rozwojowych. Warto mieć świadomość, że wiele organizacji, w tym Państwa konkurenci, dysponuje już podobnymi do niniejszego, lecz niejawnymi i znacznie bardziej rozbudowanymi, opracowaniami, w oparciu o które starają się budować swoją przyszłą przewagę.

4CF
Surf the future

4CF to polska firma o międzynarodowym zasięgu, od ponad dekady pomagająca klientom w podejmowaniu właściwych decyzji strategicznych. Dbamy o to, aby nasi klienci byli zawsze o krok przed konkurencją – by nie tylko utrzymywali się na fali zmian, lecz także wykorzystywali zmiany rynkowe do skuteczniejszej od konkurencji realizacji celów.

Dostarczenie wglądów w przyszłość mogących wesprzeć decyzje rozwojowe to zadanie, które traktujemy bardzo poważnie – stale rozwijamy zaawansowaną metodologię badawczą, dzięki której znajdujemy się w światowej czołówce. To dlatego ufają nam nie tylko klienci korporacyjni tacy jak Asseco, First Data, Skanska, BGŻ BNP Paribas, Deloitte czy Kongsberg, lecz także organizacje międzynarodowe i instytucje rządowe.

www.4CF.pl
info@4cf.pl
(+48) 22 24 72 772
fb.com/4CFuture