KnowBe4 PREMIER PARTNER

K4 CONSULTING

ZESTAW BEZPŁATNYCH NARZĘDZI

DO TESTÓW BEZPIECZEŃSTWA

Wstęp

W niniejszym opracowaniu znajdą Państwo opis kilku, bardzo przydatnych, często unikalnych i całkowicie bezpłatnych narzędzi. Dzięki nim możecie przetestować bezpieczeństwo w Waszej organizacji. Wszystkie opisane narzędzia są produktami albo realizowane są na bazie produktów światowego lidera, firmy KnowBe4.

W dzisiejszych czasach wiedza jest w cenie, a wiedza o słabościach naszej organizacji jest bezcenna. Zachęcamy do realizacji testów wymienionych w niniejszym dokumencie, gdyż w sposób prosty, łatwy i szybki możecie poznać słabości i zareagować zanim zrobią to przestępcy!

Gwarantujemy, że ***wszystkie odnośniki w tym dokumencie są bezpieczne*** a dają Państwu wygodę w dostępie do narzędzi i dodatkowych materiałów. Wyjątkowo proszę je klikać.

Wybraliśmy tylko kilka z dostępnych narzędzi. Pełną listę mogą Państwo zobaczyć pod adresem: https://www.knowbe4.com/free-it-security-tools

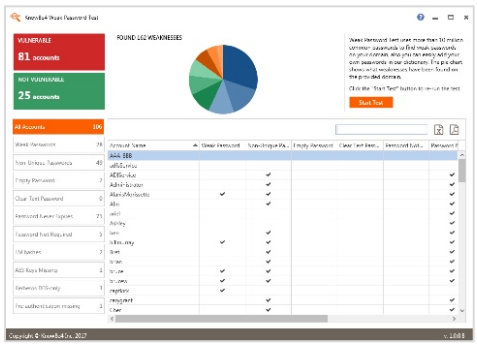
Skontaktuj się z nami a uzyskasz pełne informacje, wsparcie i pomoc w przeprowadzeniu opisanych testów. Pisz na adres: info@k4consulting.pl

Życzymy Państwu jak najkrótszych raportów z jak najmniejszą ilością problemów.

Zespół K4 Consulting

1 PASSWORD TOOLS

WEAK PASSWORD TEST (WPT)



W ostatnim raporcie firmy Verizon możemy przeczytać, że aż 81% naruszeń bezpieczeństwa związanych z włamaniami wykorzystywało skradzione lub słabe hasła. Warto więc zawczasu sprawdzić siłę i jakość haseł pracowników. Jak to zrobić?

Mamy bezpłatne, proste w użyciu i bardzo przydatne narzędzie do testu siły i jakości haseł w domenie. Wystarczy je pobrać, zainstalować i zobaczyć, jak wygląda rzeczywistość w Twojej sieci.

Oprogramowanie testuje hasła pod kątem 10 typów zagrożeń związanych ze słabymi hasłami, takich jak np. niska siła, zduplikowane hasła, brak hasła, hasło nigdy nie wygasa. Instalacja i przeprowadzenie testu zajmą Ci 5 minut po których otrzymasz kompletny raport!

Jak pobrać oprogramowanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i pobrać oprogramowanie.
https://info.knowbe4.com/weak-password-test-partner?partnerid=0010c000022DcIPAA0

Jak zainstalować narzędzie?

Pod poniższymi adresami znajdziesz przejrzystą instrukcję instalacji oraz film. Nic prostszego.
Instrukcja: https://support.knowbe4.com/hc/en-us/articles/115006118227-Weak-Password-Test-WPT-
Film instruktażowy: https://support.knowbe4.com/hc/en-us/articles/360001529147-Video-Weak-Password-Test-WPT-

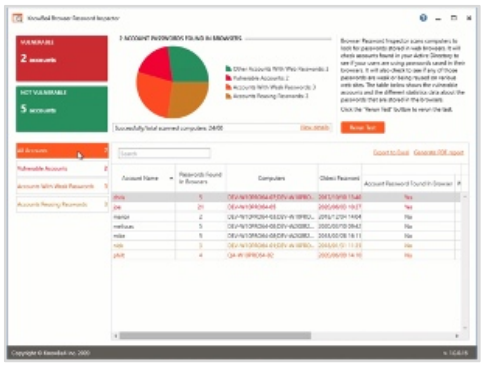
Wymagania

Active Directory, Windows 7 lub wyższy (32 lub 64 bit)

Czy to bezpieczne?

Oczywiście. Należy pamiętać, że to narzędzie nigdy nie wyświetli ani nie zgłosi rzeczywistych haseł do kont użytkowników w Twojej usłudze AD. Hasła w AD są zaszyfrowane i nigdy nie będą widoczne. Wyniki testu identyfikują tylko konta użytkowników, które nie przeszły testu, abyś mógł podjąć działania naprawcze. Dodatkowo, dane pobierane ze skanowanych maszyn są szyfrowane. Informacje uzyskane podczas testu są zapisywane w pamięci lokalnej, a nie na dysku. Żadne informacje z Twojej usługi Active Directory nie zostaną nigdzie wysłane na żadnym etapie testu. Oprogramowanie to jest rozwiązaniem on-premise a za jego bezpieczeństwo gwarantuje firma KnowBe4.

BROWSER PASSWORD INSPECTOR (BPI)



Gdy użytkownicy zapisują hasła w przeglądarce, ułatwiają tym samym zadanie cyberprzestępcom, aby włamać się do Twojej sieci. Atakujący odnoszą coraz większe sukcesy, wykorzystując kombinację złośliwego oprogramowania służącego do wyłudzania informacji i zrzucania haseł w celu kradzieży danych uwierzytelniających użytkowników. Ponieważ 50% pracowników używa tego samego hasła do kont służbowych i osobistych, ryzyko kradzieży danych uwierzytelniających i przejęcia kont jest jeszcze większe!

Bezpłatne narzędzie KnowBe4 Browser Password Inspector (BPI) pomoże Ci zidentyfikować użytkowników, porównując hasła zapisane w przeglądarkach z hasłami z Active Directory. Dzięki temu masz natychmiast informację, gdzie może wystąpić problem, możesz podjąć działania naprawcze oraz masz jasny obraz ryzyka w Twojej organizacji.

Wystarczy, że poświęcisz 5 minut na instalację i uruchomienie testu a za chwilę dostaniesz miarodajny i precyzyjny raport!

Jak pobrać oprogramowanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i pobrać oprogramowanie.
https://info.knowbe4.com/browser-password-inspector-partner?partnerid=0010c000022DcIPAA0

Jak zainstalować narzędzie?

Pod poniższymi adresami znajdziesz przejrzystą instrukcję instalacji oraz film. Nic prostszego.
Instrukcja: https://support.knowbe4.com/hc/en-us/articles/360048423413-Browser-Password-Inspector-BPI-
Film instruktażowy: https://support.knowbe4.com/hc/en-us/articles/360051383673-Video-Browser-Password-Inspector-BPI-

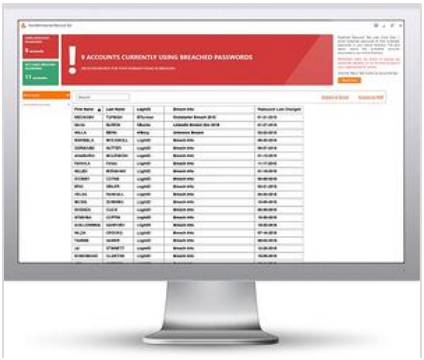
Wymagania

Active Directory, Windows 7 lub wyższy (32 lub 64 bit), 2GB RAM

Czy to bezpieczne?

Oczywiście. Analiza jest wykonywana na stacji roboczej, na której zainstalowano BPI, żadne poufne dane nie opuszczają Twojej sieci, a rzeczywiste hasła nigdy nie są ujawniane. BPI skanuje tylko komputery z systemem Windows. Żadne informacje z Twojej usługi Active Directory nie zostaną nigdzie wysłane na żadnym etapie testu. Oprogramowanie to jest rozwiązaniem on-premise a za jego bezpieczeństwo gwarantuje firma KnowBe4.

BREACHED PASSWORD TEST (BPT)



Gdy użytkownicy zapisują hasła w przeglądarce, ułatwiają tym samym zadanie przestępcom. Aż 25% pracowników używa tego samego hasła do wszystkich loginów. A jeśli to hasło jest już skompromitowane i dostępne w „Dark Web"? Używanie haseł, które zostały złamane, naraża Twoją sieć na ryzyko. Zmuszanie użytkowników do częstej zmiany haseł również nie jest dobrym rozwiązaniem. Wystarczy jedno złamane hasło, aby hakerzy uzyskali dostęp do Twojej sieci.

Chcesz sprawdzić, czy w Twojej organizacji są używane skompromitowane hasła? Użyj narzędzia KnowBe4 Breached Password Test (BPT), które sprawdzi hasła powiązane z Twoją domeną w bazach naruszeń a następnie porówna je z aktualnie używanymi hasłami przez użytkowników w Active Directory.

Wystarczy, że poświęcisz 5 minut na instalację i uruchomienie testu a za chwilę dostaniesz miarodajny i precyzyjny raport!

Jak pobrać oprogramowanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i pobrać oprogramowanie.
https://info.knowbe4.com/breached-password-test-partner?partnerid=0010c000022DcIPAA0

Jak zainstalować narzędzie?

Pod poniższymi adresami znajdziesz przejrzystą instrukcję instalacji oraz film. Nic prostszego.
https://support.knowbe4.com/hc/en-us/articles/360001508408-Breached-Password-Test-BPT-

Wymagania

Active Directory, Windows 7 lub wyższy (32 lub 64 bit)

Czy to bezpieczne?

Oczywiście. Analiza jest wykonywana na stacji roboczej, na której zainstalowano BPT, żadne poufne dane nie opuszczają Twojej sieci, a rzeczywiste hasła nigdy nie są ujawniane. Oprogramowanie to jest rozwiązaniem on-premise a za jego bezpieczeństwo gwarantuje firma KnowBe4.

2 EMAIL SECURITY TOOLS

EMAIL EXPOSURE CHECK PRO (EEC PRO)

Kampanie phishingowe typu BEC i Spear Phishing przestępcy rozpoczynają zawsze od zebrania informacji o celu ataku. Od tego, ile informacji na nasz temat znajduje się w sieci, zależy jak dobrze i precyzyjnie atak zostanie zaplanowany. Jakie informacje są wartościowe dla przestępców? Praktycznie każda informacja jest cenna i można ją wykorzystać.

Wiele adresów e-mail i tożsamości pracowników Twojej organizacji jest już dostępnych w Internecie i łatwo je znaleźć cyberprzestępcom. Dzięki temu mogą łatwo przeprowadzać ataki socjotechniczne na Twoją organizację.

Badanie KnowBe4's Email Exposure Check Pro (EEC) identyfikuje zagrożonych użytkowników w Twojej organizacji. Korzystając z nowej generacji bazy danych o wyciekach od SpyCloud, EEC Pro wykorzystuje jedno z największych i najbardziej aktualnych źródeł, aby pomóc Ci aktywnie chronić Twoją organizację przed naruszeniem poświadczeń

Na koniec otrzymasz e-mailem z raport w formacie PDF z liczbą ujawnionych wiadomości e-mail, tożsamości i znalezionych poziomów ryzyka. Otrzymasz również link do pełnego, szczegółowego raportu rzeczywistych znalezionych użytkowników, w tym nazwy wycieku i informacji o ujawnieniu hasła. Wypełnienie formularza zajmie Ci 2 minuty a w efekcie otrzymasz wartościowy raport!

Jak zamówić badanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i czekać na raport!
https://info.knowbe4.com/email-exposure-check-pro-partner?partnerid=0010c000022DcIPAA0

Chcesz wiedzieć więcej?

Pod poniższym adresem znajdziesz więcej informacji na temat badania:
https://support.knowbe4.com/hc/en-us/articles/210465178-Email-Exposure-Check-Pro-EEC-Pro-

Wymagania

Wypełnienie formularza. Badanie realizowane jest automatycznie a wynik ogólny przesyłany jest na adres e-mail wraz z linkiem dostępowym do szczegółowych danych.

Czy to bezpieczne?

Oczywiście. Te informacje już są dostępne w sieci, więc i tak niczego nie ryzykujesz.

Wraz z e-mailem otrzymujesz tylko zbiorczy raport z ogólną informacją a szczegółowe informacje otrzymasz dopiero jak skorzystasz z załączonego linka.

DOMAIN SPOOF TEST

Czy zdajesz sobie sprawę, że jedną z pierwszych rzeczy, które próbują hakerzy, jest sprawdzenie, czy mogą sfałszować adres e-mail kogoś z Twojej własnej domeny?

Dzięki temu mogą przeprowadzić atak na Twoją organizację podszywając się pod kierownictwo firmy.

Przed takim atakiem trudno jest się obronić, chyba że użytkownicy są przeszkoleni w zakresie „świadomości bezpieczeństwa" (Security Awareness Program).

Bezpłatne badanie KnowBe4 Domain Spoof Test da ci w szybki i łatwy informacje, czy Twój serwer e-mail jest poprawnie skonfigurowany.

Jest to prosty, nieinwazyjny test typu „pass / fail". Wysyłany jest sfałszowany e-mail „od Ciebie do Ciebie". Jeśli dotrze do Twojej skrzynki odbiorczej, wiesz, że masz problem. Dowiesz się tego w ciągu 48 godzin!

Jak zamówić badanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i czekać na efekty!
https://info.knowbe4.com/domain-spoof-test-partner?partnerid=0010c000022DcIPAA0

Chcesz wiedzieć więcej?

Pod poniższymi adresami znajdziesz więcej informacji na temat badania oraz informacje jak zabezpieczyć swój serwer przed tego typu atakami.
Opis: https://support.knowbe4.com/hc/en-us/articles/204671908-Domain-Spoof-Test-DST-
Instrukcja jak zabezpieczyć serwer: https://support.knowbe4.com/hc/en-us/articles/212679977-Domain-Spoof-Prevention-in-Exchange-2013-2016-Office-365

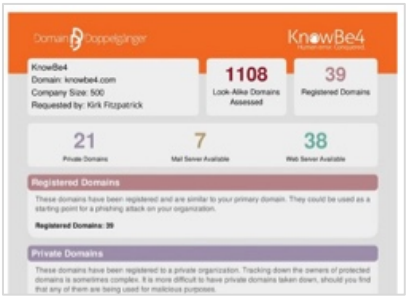
Wymagania

Wypełnienie formularza. Badanie realizowane jest automatycznie a wynik przesyłany jest na twój adres e-mail.

Czy to bezpieczne?

Oczywiście. E-mail zostanie wysłany tylko do Ciebie. Za bezpieczeństwo gwarantuje firma KnowBe4, która zrealizowała już tysiące takich testów dla swoich Klientów.

DOMAIN DOPPELGÄNGER



Według badań przeprowadzonych przez Farsight Security, fałszywe nazwy domen internetowych używane do wyłudzeń danych osobowych są bardziej rozpowszechnione niż początkowo sądzili eksperci.

Farsight Security informuje, że dla każdej zarejestrowanej dzisiaj globalnej marki, istnieje prawie 20 fałszywych domen internetowych.

Spośród tych sfałszowanych stron ponad dziewięćdziesiąt procent oferuje jakąś legalnie wyglądającą stronę internetową w celu realizacji działań przestępczych.

Podobnie brzmiące nazwy domen są bardzo często wykorzystywane do ataków phishingowych. Im są bardziej zbliżone do nazwy Twojej domeny tym bardziej mogą być skuteczne w działalności przestępczej (w odniesieniu do Twojej organizacji jak i Twoich kooperantów). Czy chciałbyś wiedzieć, ile takich domen w chwili obecnej jest zarejestrowanych na świecie?

Firma KnowBe4 oferuje bezpłatne narzędzie, z którego wyniki otrzymasz w raporcie PDF. Narzędzie o nazwie Doppelgänger jest przeznaczone do analizy takich domen. Dzięki uzyskanym informacjom możesz uaktualnić reguły systemu antyspamowego lub podjąć kroki prawne. Te informacje możesz też wykorzystać do opracowania testów phishingowych dla swoich pracowników. Będzie to świetny, praktyczny sprawdzian dla pracowników bazujący na możliwych w rzeczywistości scenariuszach.

Jak zamówić badanie?

Wystarczy wpisać poniższy adres, wypełnić formularz i czekać na raport!
https://info.knowbe4.com/domain-doppelganger-partner?partnerid=0010c000022DcIPAA0

Chcesz wiedzieć więcej?

Pod poniższymi adresami znajdziesz więcej informacji na temat badania, analizy rezultatów oraz film.
Opis: https://support.knowbe4.com/hc/en-us/articles/360008865254-Domain-Doppelgänger-Product-Manual
Film: https://support.knowbe4.com/hc/en-us/articles/360011615933

Wymagania

Wypełnienie formularza. Badanie realizowane jest automatycznie a wynik ogólny przesyłany jest na adres e-mail wraz z linkiem dostępowym do szczegółowych danych.

Czy to bezpieczne?

Oczywiście. Te informacje już są dostępne w sieci, więc i tak niczego nie ryzykujesz. Wraz z e-mailem otrzymujesz tylko zbiorczy raport z ogólną informacją a szczegółowe informacje otrzymasz dopiero jak skorzystasz z załączonego linka.

3

PHISHING TOOLS

PHISHING SECURITY TEST (PST)

Czy wiesz, że za 92% infekcji złośliwym oprogramowaniem oraz 76% naruszeń bezpieczeństwa odpowiada phishing? Tak, zwykły e-mail z odnośnikiem lub/i załącznikiem.

Teraz bezpłatnie, w prosty i szybki sposób możesz dowiedzieć się, jaki odsetek Twoich pracowników jest podatny na phishing dzięki bezpłatnemu testowi bezpieczeństwa przeprowadzonemu przez naszego partnera KnowBe4.

Zobacz też, jak wypadasz na tle innych użytkowników z Twojej branży i podobnej wielkości firmy. Sam przekonasz się jaki to może być problem w Twojej organizacji. Oczywiście mamy wzorce phishingowe w języku polskim. KnowBe4 Phishing Security Test (PST) to narzędzie, dzięki któremu możesz samodzielnie lub najlepiej z pomocą partnera KnowBe4, przetestować swoich użytkowników. W ten sposób przekonasz się jaka naprawdę jest jej odporność na zagrożenia typu phishing. Pamiętaj, każde kliknięcie to potencjalny incydent bezpieczeństwa!

badanie wymaga pewnego przygotowania oraz poświęcenia odpowiedniej ilości czasu (kilka godzin) dlatego zaplanuj je w okresie, w którym będziesz dysponował wolną chwilą. To świetne narzędzie w rozmowie z kierownictwem firmy.

Jak zamówić test?

Wystarczy wpisać poniższy adres i wypełnić formularz aby rozpocząć test!
https://www.knowbe4.com/partner-phishing-security-test-intl?partnerid=0010c000022DcIPAA0

Co dalej?

Pod poniższymi adresami znajdziesz szczegółowy opis testy i kolejnych jego kroków oraz film.
Opis: https://support.knowbe4.com/hc/en-us/articles/204843728-Phishing-Security-Test-PST-
Film: https://support.knowbe4.com/hc/en-us/articles/360000939307-Video-Free-Phishing-Security-Test-PST-

Wymagania

Zanim przystąpisz do testu musisz się odpowiednio przygotować. Pierwszą kwestią jest dodanie domen KnowBe4 wykorzystywanych w testach na „białą listę" systemu antyspamowego (tym razem testujemy ludzi a nie systemy techniczne). Przygotuj też listę adresów e-mail użytkowników, których chciałbyś w ten sposób przetestować. Lista nie powinna być większa niż 100 adresów. Najlepiej skontaktuj się z autoryzowanym partnerem KnowBe4 a uzyskasz pełne informacje, wsparcie i pomoc w przeprowadzeniu testów. Pisz na adres: info@k4consulting.pl

Czy to bezpieczne?

Oczywiście. Ty zarządzasz całym testem i poszczególnymi jego elementami. Za bezpieczeństwo gwarantuje firma KnowBe4, która zrealizowała już tysiące takich testów dla swoich Klientów. Test będzie realizowany z serwerów zainstalowanych na terenie EU a żadne dane nie opuszczą tej strefy.

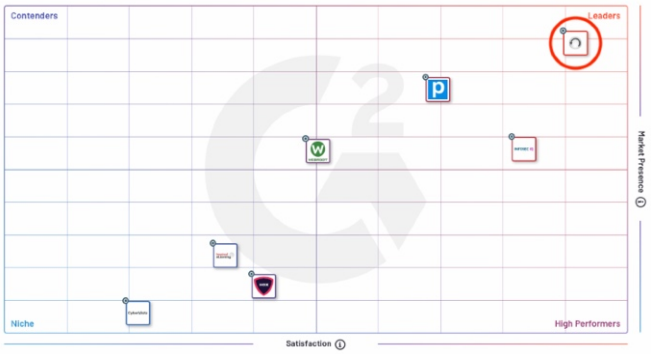
4

KNOWBE4

KnowBe4 – lider rozwiązań Security Awareness

KnowBe4 jest firmą z USA a jednym z jej założycieli jest Kevin Mitnick, legenda zastosowania socjotechniki do przestępstw cybernetycznych. Firma rozwija się bardzo dynamicznie i jest w chwili obecnej światowym liderem w rozwiązaniach Security Awareness co od kilku lat potwierdza firma Gartner w swoich raportach.

KnowBe4 posiada ponad 36 tys. klientów z ponad 6 milionami użytkowników na całym świecie z dostępnymi łącznie 32 wersjami językowymi, w tym oczywiście języku polskim.



KnowBe4 jest od kilku ostatnich lat niekwestionowanym liderem na rynku rozwiązań do wspierania kształtowania Kultury Bezpieczeństwa w organizacjach i realizacji programów do minimalizacji zagrożeń czynnika ludzkiego – Security Awareness Program – co potwierdzają wszystkie ukazujące się raporty rynkowe uznanych, światowych organizacji.

Bezpieczeństwo

Narzędzia KnowBe4 dostępne są w oparciu o rozwiązanie chmurowe i wykorzystuje usługi Amazon Web Services (AWS), zapewniające właściwą skalowalność, dostępność, nadmiarowość i bezpieczeństwo. Dla klientów zlokalizowanych na obszarze Unii Europejskiej wydzielona jest dodatkowa infrastruktura, zlokalizowana fizycznie w Irlandii, odseparowana od serwerów zlokalizowanych w USA. Zapewnia to zgodność z GDPR i gwarancję, że dane osobowe obywateli EU nie opuszczą jej i nie będą przetwarzane poza jej granicami (co oficjalnie potwierdza na swoich stronach KnowBe4). Narzędzia w postaci oprogramowania wymienionego w niniejszym dokumencie są dostępne w formie on-premise.

FedRAMP Li-SaaS authorized

Platforma KnowBe4 posiada Certyfikat Federalnego programu zarządzania ryzykiem i autoryzacją (FedRAMP) obejmujący cały rząd USA. FedRAMP określa wymagania bezpieczeństwa i dostawcy usług przetwarzania w chmurze muszą przestrzegać, aby rząd mógł korzystać z ich usług.

SOC 2 & SOC 3

Wszystkie produkty KnowBe4 posiadają certyfikat SSAE18 SOC2 Type 2. Oceny KnowBe4 SOC2 obejmują wszystkie kryteria usług zaufania takie jak: bezpieczeństwo, dostępność, integralność przetwarzania, poufność i prywatność.

Szczegółowe i najbardziej aktualne informacje dotyczące bezpieczeństwa, zgodności oraz zapewnionej nadmiarowości znajdują się pod adresem: https://www.knowbe4.com/security

5

K4 CONSULTING

K4 CONSULTING

Specjalizacja

Udowadniamy, że człowiek z najsłabszego ogniwa może stać się dodatkowym i kluczowym elementem systemu bezpieczeństwa każdej organizacji – „human firewall" - współtworząc silną kulturę bezpieczeństwa, podwyższającą znacząco odporność organizacji na cyberzagrożenia.

Skuteczność naszych programów tworzymy w oparciu o najnowsze badania naukowe z dziedziny psychologii behawioralnej, kognitywistyki oraz zastosowanie najlepszych, często unikalnych narzędzi. Wykorzystujemy wiedzę o człowieku, żeby regularnym i długofalowym działaniem tworzyć trwałą zmianę zachowań oraz budować współodpowiedzialność i zaangażowanie w bezpieczeństwo firmy. W naszej pracy analizujemy, diagnozujemy, przygotowujemy i wdrażamy programy dopasowane do specyfiki organizacji i pracujących w niej ludzi. Wykorzystujemy najlepsze metodologie i praktyki uznane i stosowane na całym świecie, rozwijając je, aby działały jeszcze lepiej.

Jesteśmy skuteczni, ponieważ oprócz dużej wiedzy, jesteśmy wyposażeni w najlepsze dostępne narzędzia, dzięki którym potrafimy nie tylko zaadresować, ale i mierzyć kluczowe aspekty kultury bezpieczeństwa. Bazujemy na 7-wymiarowym modelu, który zapewnia precyzyjną kontrolę nad całym procesem kształtowania ludzkich postaw i zachowań. Model ten posiada rekomendację Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji ENISA®. Programy wdrażane u naszych klientów pozwalają na obniżenie ryzyka dla czynnika ludzkiego nawet o 90%, co przekłada się na 15-krotny wzrost odporności organizacji na zagrożenia w tym obszarze.

Nasza historia

Firma K4 Consulting założona została w 2001 roku. Od samego początku zajmowaliśmy się bezpieczeństwem w obszarze IT. Przez lata doświadczeń i uczestnictwa w dużych projektach informatycznych mieliśmy okazję obserwować zmieniający się krajobraz zagrożeń. W ostatnich latach, pomimo stosowania coraz nowszych, doskonalszych rozwiązań technologicznych, obserwowaliśmy rosnącą liczbę skutecznych ataków cyberprzestępców i incydentów bezpieczeństwa. Zrozumieliśmy wtedy, że na bezpieczeństwo należy spojrzeć z szerszej perspektywy. Poza technologią i procedurami, bezpieczeństwo zaczyna się i kończy na ludziach: ich zachowaniach, motywacjach i nawykach. Dlatego już 5 lat temu postanowiliśmy skupić się na czynniku ludzkim w bezpieczeństwie.

Dzisiaj łącząc pasję, doświadczenie i zaangażowanie, pomagamy naszym klientom podwyższać odporność na cyberzagrożenia, wdrażając skuteczne rozwiązania wzmacniające kulturę bezpieczeństwa w organizacji (Security Awareness Program).

Strategiczne partnerstwo z KnowBe4

Od 2018 roku jesteśmy partnerem firmy KnowBe4. W chwili obecnej jako pierwsza i jedyna firm w Polsce posiadamy najwyższy status partnerski KnowBe4 Premier Partner. Firma KnowBe4 jest niekwestionowanym światowym liderem na rynku narzędzi do realizacji programów Security Awareness. Oferuje kompletne rozwiązanie skupiające w jednym miejscu wszystkie potrzebne narzędzia, takie jak: obszerna biblioteka szkoleń e-learningowych, automatyzację i pomiar kampanii szkoleniowych, automatyzację i pomiar testowych kampanii phishingowych, pomiar ryzyka czynnika ludzkiego, pomiar kultury bezpieczeństwa, narzędzia do zgłaszania zagrożeń czy automatyzację procesu analizy zagrożeń zgłaszanych przez użytkowników.

Nieustanny rozwój i wprowadzanie nowych funkcjonalności oferowanego produktu oraz pionierskie podejście KnowBe4 do tematyki bezpieczeństwa - co roku potwierdzane najwyższymi notami w międzynarodowych rankingach rozwiązań Security Awareness - zdecydowały o tym, że to właśnie tę firmę wybraliśmy na naszego partnera.

Miarą naszej wiedzy i doświadczenia jest to, jak efektywnie potrafimy się nimi dzielić z innymi. Dlatego w roku 2020 utworzyliśmy Centrum Kompetencyjne, gdzie otrzymać można pomoc merytoryczną, procesową oraz techniczną dotyczącą realizacji programów Security Awareness na bazie narzędzi oferowanych przez KnowBe4.

Kontakt

Krzysztof Kozłowski
Tel +48 577 207 607
e-mail: krzysztof.kozlowski@k4consulting.pl

K4 CONSULTING
Biuro handlowe:
Ul. Reduta Wyskok 4
80-741 Gdańsk
https://k4consulting.pl