



2(11)/2023

# SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

## Cyberbezpieczeństwo bez budżetu

Będzie polska odpowiedź  
na ChatGPT dla biznesu

Nowa era bezpieczeństwa w UE  
Nowe prawo i obowiązki firm

Chwyt marketingowy czy  
poprawa bezpieczeństwa?

Zarobki w sektorach Security & AI

# SPIS TREŚCI

Będzie polska odpowiedź na ChatGPT dla biznesu	4
Wyzwania i osiągnięcia pierwszego roku działania CBZC	12
Podstawy diagnostyki dysków twardych	21
Chwyt marketingowy czy poprawa bezpieczeństwa?	29
10 największych ataków hakerskich w historii	36
Cyberbezpieczeństwo bez budżetu	45
Cyfrowy „sejf” na dane, zapobieganie atakom i logowanie bez haseł	55
Nowa era bezpieczeństwa w UE. Nowe prawo i obowiązki firm	60
Zarobki w sektorach Security & AI	69
Pięć trendów w cybersecurity w 2023	75
Eksperci wydania	83
Partnerzy wydania	85

**CyberTek**  
**Tech Festival**

Szczegóły s. 19

**10% ZNIŻKI DLA NASZYCH CZYTELNIKÓW**

Skontaktuj się z organizatorem mailowo aby otrzymać rabat:  
[konferencja@cybertek.com.pl](mailto:konferencja@cybertek.com.pl)

## SZANOWNI PAŃSTWO,

przed chwilą swoją rocznicę świętowało Centralne Biuro Zwalczania Cyberprzestępczości. O tym że taka jednostka policji powstać musiała nikt nie ma wątpliwości. Zresztą już pierwszy rok funkcjonowania CBZC pokazało, jak bardzo potrzebny jest taki zespół nie tylko w strukturach wojska, ale również policji.

Przez ostatni rok Biuro rozwiązało niemal 100 spraw na terenie całego kraju, w wyniku których zarzuty karne przedstawiono 234 osobom, a 46 z nich zostało tymczasowo aresztowanych. W kilku przypadkach udało się zablokować znaczące kwoty, ponadto policjanci CBZC zabezpieczyli mienie na łączną sumę 33 mln zł.

My, jako wydawnictwo, swoją rocznicę obchodzić będziemy już za miesiąc. Prawie rok temu, kiedy rozpoczynała się wojna za naszą wschodnią granicą, stanęliśmy przed dylematem, czy "Security Magazine" udźwignie ciężar spływających z Ukrainy informacji, czy misja "w służbie bezpieczeństwu" trafi do Czytelników, do których trafić miała. Zaryzykowaliśmy i... udało się.

Przez ten rok z naszymi ekspertami zapisaliśmy niemal 1100 stron rzetelnych, unikalnych, profesjonalnych treści, z którymi dotarliśmy do ponad 270 tysięcy osób, głównie tych, które w firmach zajmują się szeroko pojętym bezpieczeństwem i za nie odpowiadają.

Z okazji naszej pierwszej rocznicy przygotowaliśmy nie tylko masę wartościowych tematów, ale również prezentów oraz ciekawostek. Dlatego zachęcam już dziś do śledzenia naszych kanałów, by nie ominąć informacji o dwunastym wydaniu "Security Magazine".

Rafał  
Ślepiewski





ZAPISZ SIĘ NA  
**NEWSLETTER**  
BY NIE PRZEOCZYĆ  
KOLEJNEGO WYDANIA

**SECURITY MAGAZINE**  
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



**ZAPISZ SIĘ**

**NEWSLETTER**



YOUR EMAIL HERE

**SUBSCRIBE**



# BĘDZIE POLSKA ODPOWIEDŹ NA CHATGPT DLA BIZNESU



Redakcja  
SECURITY MAGAZINE

we współpracy z



**W ciągu ostatniego roku polski SentiOne stworzył silnik rozumienia języka naturalnego dla języka arabskiego i pracuje nad silnikami dla francuskiego, włoskiego i ukraińskiego. Rozwiniął możliwość integracji botów z m.in. Facebookiem, Messengerem i WhatsAppem. Dziś monitoruje ponad 69,5 tys. źródeł w Internecie i przetwarza ponad 150 mln wzmianek dziennie, co przekłada się na wyższą skuteczność ich modeli AI. I właśnie taki model dla biznesu chce stworzyć jako europejską odpowiedź na ChatGPT.**



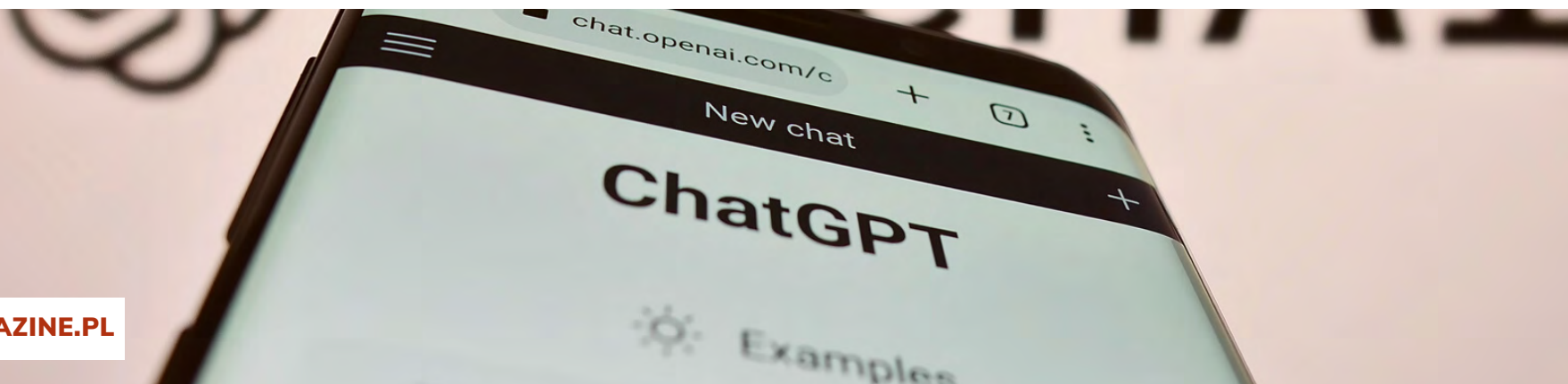
## MODEL JĘZYKOWY - WARUNKI POWSTANIA

Model językowy, mimo ogromnej popularności, jest jednak modelem tzw. blackbox („czarna skrzynka”), botem typu „pytanie - odpowiedź”. Oznacza to, że jest w stanie wygenerować ładnie zbudowane odpowiedzi, ale zupełnie nie rozumie, o co został zapytany - nie orientuje się w rzeczywistości, nie osadza informacji w kontekście. Łączą się z nim też inne kontrowersje, np. tania siła robocza z Afryki wykorzystywana do manualnego sprawdzania modeli.

Magazyn Time raportował, że Open AI, firma, która stworzyła ChatGPT, outsource’owała manualne anotowanie tekstów i nadawanie im tagów do firmy z Kenii i płaciła pracownikom mniej niż 2 dolary za godzinę. Pracownicy ci narażeni byli narażeni na kontakt z drastycznymi treściami.

"Wydaje się, że większość tego tekstu została wyciągnięta z najciemniejszych zakamarków internetu. Niektóre z nich szczegółowo opisywały sytuacje, takie jak wykorzystywanie seksualne dzieci, bestialstwo, morderstwo, samobójstwo, tortury, samookaleczenie i kazirodztwo" - podał Time.

- ChatGPT robi wrażenie, jednak przez to, jak został zbudowany, może wprowadzać w błąd lub szerzyć dezinformację, co jest nieakceptowalne, szczególnie w zastosowaniu biznesowym - mówił Bartosz Baziński, COO i współzałożyciel SentiOne, dodając: - Technologia musi służyć ludziom, a nie działać przeciwko nim. Algorytmy sztucznej inteligencji powinny być pomocne, nie mogą szerzyć dezinformacji, wprowadzać błąd, przeklinać lub szerzyć obraźliwych opinii - ksenofobicznych, rasistowskich itp., co już się zdarzało. Po co nam technologia, która wprowadza w błąd lub nas obraża? To bez sensu.



## **Aby stworzyć model językowy jak ChatGPT, należy spełnić kilka warunków, w tym:**

- **dostępność dużej ilości danych treningowych:** modele językowe opierają się na uczeniu maszynowym, co wymaga dużej ilości danych tekstowych do nauki,
- **zasoby obliczeniowe:** modele językowe są bardzo złożone i wymagają dużych zasobów obliczeniowych, takich jak procesory graficzne (GPU) lub chmury obliczeniowe, aby móc efektywnie trenować modele,
- **zespół ekspertów:** stworzenie modelu językowego wymaga zespołu ekspertów w dziedzinach takich jak uczenie maszynowe, językoznawstwo czy informatyka,
- **czas i budżet:** trenowanie modelu językowego jest czasochłonne i kosztowne, dlatego ważne jest, aby mieć odpowiednie zasoby, aby móc to zrobić skutecznie,
- **otwarte źródła i biblioteki:** dostępność otwartych źródeł i bibliotek umożliwiających budowanie i trenowanie modeli językowych, takich jak TensorFlow lub PyTorch, jest kluczowa dla sukcesu projektu,
- **wiedza i doświadczenie w projektowaniu modeli językowych:** Projektowanie i trenowanie wymaga wiedzy i doświadczenia w zakresie ar-

chitektur sieci neuronowych, hiperparametrów oraz metod uczenia,

- **dostęp do różnorodnych źródeł danych:** modele językowe uczą się od danych, dlatego ważne jest, aby mieć dostęp do różnorodnych i reprezentatywnych źródeł danych, takich jak teksty, dialogi czy artykuły,
- **ocena i testowanie modelu:** po stworzeniu modelu językowego ważne jest, aby przeprowadzić szereg testów i ocen, aby upewnić się, że jest on wystarczająco dobry i gotowy do użycia,
- **częste aktualizacje i ulepszenia:** modele językowe muszą być regularnie aktualizowane i ulepszone, aby umożliwić im uczenie się i dostosowywanie do zmieniających się potrzeb i wymagań rynku,
- **integracja z innymi systemami i narzędziami:** modele językowe muszą być zintegrowane z innymi systemami i narzędziami, takimi jak CRM, e-commerce i systemy baz danych, aby były jak najbardziej efektywne i użyteczne.

## **Model językowy może zostać stworzony przez wiele różnych firm i organizacji, w tym:**

- Duże korporacje technologiczne, jak Google, Amazon, Microsoft czy Apple, które mają wiedzę, zasoby i doświadczenie w dziedzinie ucze-





nia maszynowego i technologii językowej.

- Start-upy specjalizujące się w uczeniu maszynowym i sztucznej inteligencji, które inwestują w rozwój modeli językowych.
- Instytuty naukowe i akademickie, które mają programy badawcze i duże zasoby obliczeniowe, a także specjalistów z dziedziny uczenia maszynowego i językoznawstwa.
- Firmy z branży IT i oprogramowania, które chcą wykorzystać modele językowe w swoich produktach i usługach.
- Agencje rządowe i organizacje non-profit, które szukają nowych rozwiązań do zastosowań w sektorze publicznym lub dla dobra społeczeństwa.

## **POLSKA FIRMA ZBUDUJE MODEL JĘZYKOWY DLA BIZNESU**

Rozpoczęły się prace nad stworzeniem europejskiej odpowiedzi na ChatGPT, a jej twórcą będzie polski SentiOne.

- Nasze modele sztucznej inteligencji są na bieżąco douczane na specjalnie przygotowanych tekstach i wiedzy dziedzinowej, testowane m.in. na zapisach rzeczywistych rozmów klientów z call center. Patrząc na nasze zasoby – zbiory danych i zespół – jestem przekonany, że nikt nie zbuduje lepszego modelu dla języka polskiego, a następnie dla innych języków euro-

pejskich, niż my. Chcemy stać się liderem w dostarczaniu technologii AI dla biznesu, a konkretnie dla branż: finansowej, ubezpieczeniowej, medycznej, telekomunikacyjnej. Od początku powstania SentiOne zainwestowaliśmy w rozwój technologii oraz modeli sztucznej inteligencji ponad 42 mln złotych i cały czas ją rozwijamy. Ze względu na duże zainteresowanie zarówno naszymi modelami, jak i ChatGPT, rozważamy, czy udostępnić próbki naszego modelu do testów dla szerszego grona odbiorców - damy znać - zaznaczył Bartosz Baziński.

- SentiOne spełnia warunki, pozwalające zbudować takie narzędzie. Dzięki 11 latom monitorowania Internetu ma dostęp do nieprzebranej ilości danych publicznych, tekstów oraz wypowiedzi. Ma również doświadczenie w budowaniu skutecznego, autorskiego modelu AI opartego o sieci neuronowe, który rozumie ludzkie intencje na poziomie 96 procentach. Dzięki licznym skutecznym wdrożeniom chatbotów i voicebotów u klientów biznesowych eksperci z SentiOne dysponują również dużym know-how oraz mają dostęp do danych dziedzinowych. Narzędzie SentiOne będzie równie łatwe do obsługi, jak ChatGPT, bo jest tworzone w systemie low-code / no-code, który nie wymaga od użytkowników umiejętności kodowania - dowiedzieliśmy się od firmy, która od 11 lat wspiera marki w zakresie automatyzacji obsługi klienta z wykorzystaniem technologii AI.





Warto też wiedzieć, że w 2021 roku firma otrzymała od Narodowego Centrum Badań i Rozwoju grant wysokości niemal 19 mln zł na rozwój konwersacyjnej sztucznej inteligencji, a w 2020 roku zdobyła tytuł finalisty EIT Digital Challenge i znalazła się wśród 20 najlepszych spółek technologicznych w Europie.

## ŻYCIE Z TECHNOLOGIĄ

- Wobec ChatGPT pojawiają się również zarzuty związane z tym, że jest wykorzystywany do zadań, które powinny być wykonywane samodzielnie, np. pisanie wypracowań i prac zaliczeniowych przez uczniów i studentów. Jednak to nie zawsze jest złe rozwiązanie. Przykładowo, nauczyciel może zlecić technologii, by wymyśliła i napisała test na temat wojen z zakonem krzyżackim z 10 propozycjami pytań wielokrotnego wyboru. Czy to oznacza, że sztuczna inteligencja zastąpi nauczyciela? Nie, bo test będzie wymagał weryfikacji, a do wykorzystania będzie się nadawało zapewne 50-70 procent zaproponowanych pytań. Czy to przyspieszy pracę nauczyciela? Tak, o te 50-70 procent - przekonywał SentiOne.

- Do tego, że modele AI zachęcają do pracy nie-samodzielnej, podszedłbym od drugiej strony - za-

chęcą, by wszyscy wspierali swoją pracę AI - mówił Bartosz Baziński, dodając: - Nie obronimy się przed technologią, więc radzę, by nauczyć się z nią żyć i z niej korzystać, a nie dać się jej wykorzystać. Technologia AI może znacząco przyspieszyć pracę wielu, wielu osób. I w mojej opinii sztuczna inteligencja nie zastąpi ludzi, ale zastąpi tych, którzy jej nie używają.

# PATRONAT

## SECURITY MAGAZINE

# POLSECURE 2023

## MIĘDZYNARODOWE TARGI 25-27 KWIETNIA



Debiut wystawy poświęconej bezpieczeństwu publicznemu gwarantowanemu przez służby mundurowe był niezwykle udany. Kolejna edycja **Międzynarodowych Targów POLSECURE** odbędzie się w Targach Kielce w kwietniu 2023 roku.

Międzynarodowe Targi to efekt współpracy Targów Kielce z Komendą Główną Policji. Specjalistyczne wydarzenia wymaga merytorycznego i taktycznego wsparcia. W projekt zaangażowane są: Komenda Główna Policji, Komenda Główna Straży Granicznej, Państwowa Straż Pożarna, Służba Więzienna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Komisja Nadzoru Finansowego, Główny Inspektor Transportu Drogowego, Lotnicze Pogotowie Ratunkowe, Narodowe Centrum Badań i Rozwoju, a także Rządowe Centrum Bezpieczeństwa.

W pierwszej edycji wystawy uczestniczyło blisko 100 wystawców. Partnerem Strategicznym Targów POLSECURE była firma WB Group, jeden z największych polskich koncernów, specjalizujący się w projektowaniu i produkcji rozwiązań w sektorze obronnym i cywilnym.

**POLSECURE 23** pod Honorowym Patronatem Ministra Spraw Wewnętrznych i Administracji, po raz kolejny będzie w pełni poświęcone bezpieczeństwu publicznemu. Wydarzenie będzie doskonałą okazją do zaprezentowania oferty firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania służącego łączności, dowodzeniu czy kontroli, ale także do wymiany doświadczeń i rozmów o potrzebach służb mundurowych.

Obok ekspozycji kluczowym elementem wydarzenia będzie Międzynarodowa **Konferencja Policyjna** organizowana przez Komendę Główną Policji. Podczas drugiej edycji Targów spotkanie koncentrowało się będzie na trzech głównych tematach: cyberbezpieczeństwo, laboratorium kryminalistyczne oraz logistyka.



 **polsecure**

**II Międzynarodowe Targi  
POLSECURE**

**25-27.04.2023**

**WYDARZENIA TOWARZYSZĄCE**

- **Międzynarodowa Konferencja Policyjna**  
Zakres tematyczny: cyberbezpieczeństwo, laboratorium kryminalistyczne, logistyka
- **Pokazy dynamiczne**
- **Prezentacje sprzętu**

Więcej informacji na [polsecure.targikielce.pl](https://polsecure.targikielce.pl)

Patronat Honorowy



Minister Spraw  
Wewnętrznych i Administracji



SLUŻBA  
WIĘZIENNA

RCB



**NCBR**  
Narodowe Centrum Badań i Rozwoju



# WYZWANIA I OSIĄGNIĘCIA PIERWSZEGO ROKU DZIAŁANIA CBZC



Marcin Zagórski

Centralne Biuro Zwalczania Cyberprzestępczości

**Minął rok od powołania Centralnego Biura Zwalczania Cyberprzestępczości, nowej jednostki Policji, której zadaniem ma być walka z cyberzagrożeniami. Stworzenie centralnej, wyspecjalizowanej komórki miało być odpowiedzią na stale rosnącą skalę cyberzagrożeń. Jak wyglądał ten rok? Jakie efekty uzyskało nowe Biuro? Jakie wyzwania czekają nas w nadchodzącym czasie?**

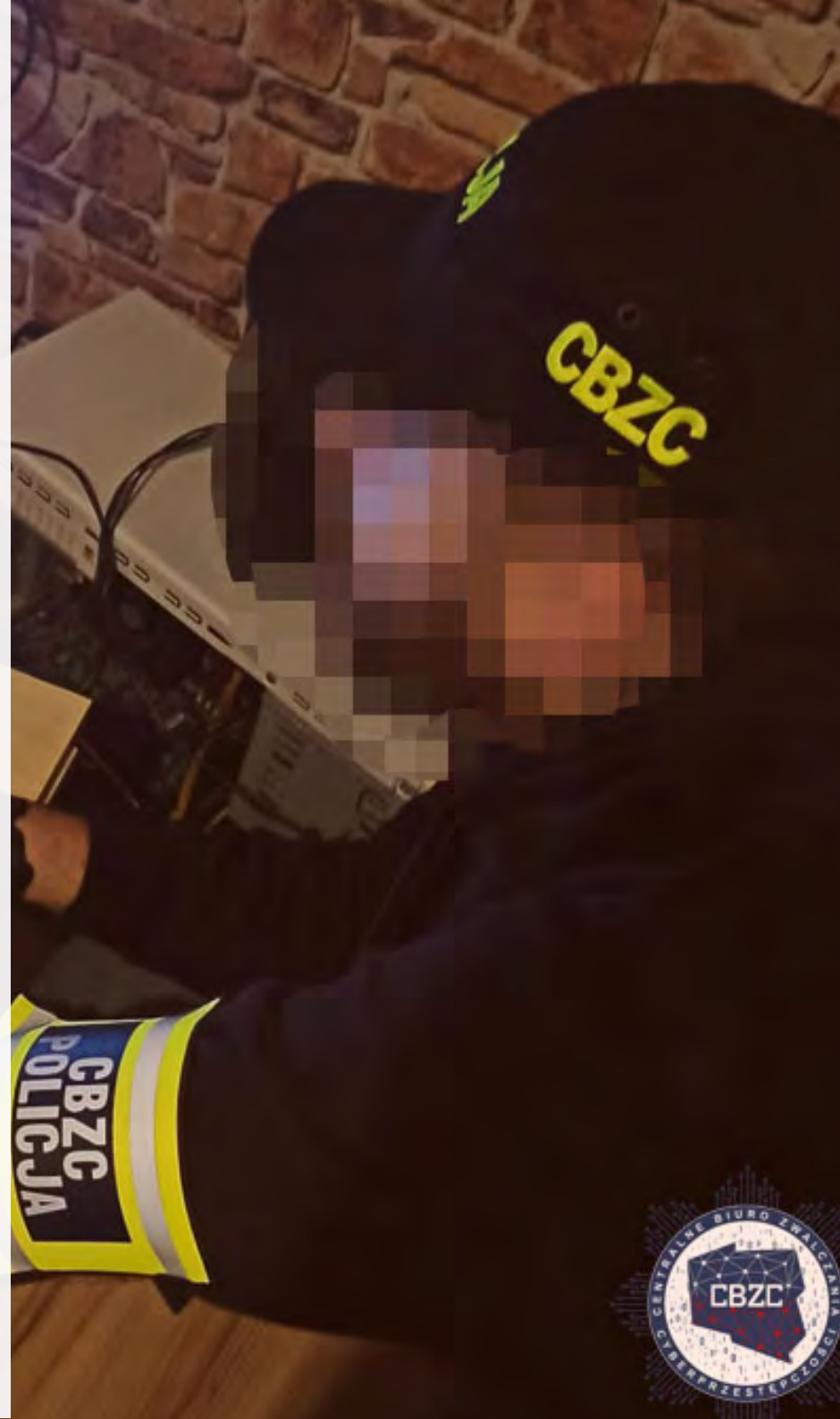


## ZAŁOŻENIA

12 stycznia ubiegłego roku weszła w życie ustawa, która powołała nową jednostkę Policji – Centralne Biuro Zwalczania Cyberprzestępczości. Jednostka, której zadaniem jest walka z cyberzagrożeniami, jest odpowiedzią na stale rosnącą skalę cyberprzestępstw i pojawiające się nowe zagrożenia w sieci.

Biuro z wysoko wyspecjalizowaną kadrą, wyposażone w najnowocześniejszy sprzęt teleinformatyczny i wykorzystujące w pełni możliwości informatyki śledczej ma stanowić o sile i skuteczności w walce z cyberprzestępczością.

Tworzenie CBZC rozpoczęło powołanie w dniu 1 listopada 2021 pełnomocnika Komendanta Głównego Policji do przygotowania rozwiązań organizacyjnych i prawnych związanych z planowanym utworzeniem nowej jednostki. Od tego momentu rozpoczął się proces formowania nowych struktur przyszłego Biura, zmiany obowiązujących przepisów prawa i opracowywanie rozwiązań logistycznych. 1 maja ub. r. decyzją Ministra SWiA na stanowisko Komendanta CBZC powołano dotychczasowego pełnomocnika KGP - inspektora Adama Cieślaka.



Istotnym elementem budowania nowych struktur Biura, była rekrutacja funkcjonariuszy pełniących dotychczas służbę w komórkach ds. zwalczania cyberprzestępczości w Komendzie Głównej Policji, w komendach wojewódzkich policji i Komendzie Stołecznej Policji oraz w innych jednostkach policji do CBZC. Ten okres był bardzo intensywny. Swoją chęć przejścia do CBZC zadeklarowało łącznie prawie 900 policjantów. Po wstępnej weryfikacji dokumentów, przeprowadzono bardzo wiele rozmów z policjantami – niemal 650 osób. Proces rekrutacji pozytywnie przeszło ponad 320 funkcjonariuszy. 12 lipca 2022 to ważna data w funkcjonowaniu CBZC. Tego dnia policjanci pełniący służbę w komórkach do spraw zwalczania cyberprzestępczości w KGP i w komendach wojewódzkich przeszli do CBZC, a wraz z nimi większość prowadzonych przez nich spraw. To ten moment można uznać za faktyczny start Biura.

## CO DALEJ?

1 lipca uruchomiliśmy stronę internetową jednostki, na której systematycznie zamieszczano informacje związane z działaniami podejmowanymi przez policjantów CBZC oraz szeroko rozumianą profilaktyką w zakresie walki z cyberzagrożeniami, a także porady, jak nie stać się ofiarą cyberprzestępców.

Rozwój kadry Biura to jedno z ważniejszych wyzwań na kolejne lata. W związku z tym wraz z rozwojem Biura, na stronie internetowej CBZC pojawiały się kolejne zakładki „Rekrutacja” czy „Zagrożenia w sieci”, ale także informacje dotyczące doboru do Biura. W zakładkach tych pojawiały się stosowne komunikaty i profilaktyczne materiały do pobrania. 13 listopada założono konto Biura na portalu społecznościowym Facebook. Narzędzia te wykorzystywane są do komunikacji ze społeczeństwem, mediami i innymi instytucjami.







## ROZWIĄZANE SPRAWY

W sumie od momentu powołania CBZC, funkcjonariusze przeprowadzili niemal 100 realizacji na terenie całego kraju, w wyniku których zarzuty karne przedstawiono 234 osobom, a 46 z nich zostało tymczasowo aresztowanych. W kilku przypadkach udało się zablokować znaczące kwoty pieniędzy, ponadto policjanci CBZC zabezpieczyli mienie na łączną sumę 33 mln złotych.

Jednym z najważniejszych i szeroko komentowanych w mediach wydarzeniem była pierwsza duża realizacja Biura. 3 listopada 2022 roku podczas konferencji prasowej przedstawiono szczegóły akcji: zatrzymanie 44 podejrzanych, 82 przeszukania na terenie niemal całego kraju, zabezpieczonych około 350 nośników cyfrowych na których ujawniono ok. 15,5 tys. plików przedstawiających seksualne wykorzystywanie dzieci to efekt kilkudniowych działań policjantów Centralnego Biura Zwalczania Cyberprzestępczości we współpracy m.in. z prokuraturą i Europol.

Po tej realizacji przyszły kolejne, skierowane głównie wobec oszustów internetowych. Jest to jedna z ważniejszych kwestii, na której skupiają się działania CBZC. W połowie listopada policjanci rozbili 6-osobową grupę osób podejrzaną o dokonanie szeregu oszustw internetowych na szkodę jednego z międzynarodowych portali sprzedażowych na łączną sumę strat 250 tys. zł. Oszuści internetowi poprzez mechanizm fikcyjnego zwrotu zamówionych urządzeń elektronicznych pobierali środki pieniężne ze zwrotów jak i same urządzenia. W wyniku przeprowadzonych działań zatrzymano 6 osób, zabezpieczając szereg urządzeń elektronicznych, karty SIM oraz dokumentację bankową.



Podejrzani usłyszeli zarzuty karne szeregu oszustw i podrobienia dokumentów, pięciu mężczyzn zostało tymczasowo aresztowanych.

Pod koniec listopada zatrzymano na gorącym uczynku po popełnienia przestępstwa kolejne osoby podejrzane o popełnienie przestępstw internetowych. Dwóch mężczyzn w wieku 32 i 34 lat, zamieszczało ogłoszenia na jednym z portali społecznościowych, które dotyczyły możliwości podjęcia pracy poza granicami RP. Dysponując danymi personalnymi potencjalnych zainteresowanych pracą, rejestrowali szereg numerów telefonów, zakładali w różnych bankach rachunki oraz konta na jednym z serwisów aukcyjnych w wyniku czego możliwe było zawieranie umów kredytowych. W wyniku działalności przestępczej, w okresie od 1 lipca 2022 r. do 21 listopada 2022 r. sprawcy zawarli co najmniej 120 umów na łączną kwotę około 150 tysięcy złotych oraz usiłowali zawrzeć ponad 100 umów na kwotę około 350 tysięcy złotych. Wobec jednego z mężczyzn zastosowano środek zapobiegawczy w postaci tymczasowego aresztowania.

Kolejna akcja miała miejsce pod koniec grudnia. Funkcjonariusze zatrzymali pięć osób w wieku od 23 do 32 lat podejrzanych o działanie w grupie przestępczej i popełnianie szeregu oszustw w tym oszustw komputerowych. W wyniku działań policjantów w dwóch warszawskich mieszkaniach ujawniono i zabezpieczono aktywną, nielegalną infrastrukturę teleinformatyczną składającą się z komputerów,



terminali komputerowych sterujących tzw. sim-boxami, telefonów komórkowych, routerów, switchy i modemów. Urządzenia te były wykorzystywane do tworzenia na dużą skalę fikcyjnych kont w mediach społecznościowych, komunikatorach i na platformach sprzedażowych. W wyniku przeprowadzonych czynności ujawniono blisko 20 tys. kart SIM. Trzech z podejrzanych również zostało tymczasowo aresztowanych.

## WSPÓŁPRACA I KOMUNIKACJA

Ważną kwestią w tworzeniu Biura było opracowanie znaku graficznego, który identyfikowałby nową jednostkę i stanowił znak rozpoznawczy. W tym celu ogłoszono konkurs na logo CBZC, który został rozstrzygnięty 12 września ubiegłego roku. Od tamtej chwili zwycięski projekt jest umieszczany na różnego rodzaju materiałach promocyjnych oraz w oficjalnych dokumentach podnosząc tym samym rangę i prestiż Biura.

Istotną rolę w walce z cyberprzestępcami jest ścisła współpraca z instytucjami krajowymi oraz międzynarodowymi, jak Interpol, Europol czy J-CAT, czyli Wspólna Grupa Zadaniowa ds. Cyberprzestępczości przy EUROPOL-u. Przykłada-

my wielką wagę do współpracy transgranicznej nie tylko z tak oczywistymi krajami jak USA, ale np. Singapurem czy Koreą.

W przypadku naszego kraju ta współpraca odbywa się m. in. z NASK-iem, CEPOL-em, CSIRT KNF, ZBP i innymi organizacjami policyjnymi oraz pozapolicyjnymi. W tym zakresie wspólnie prowadziliśmy i prowadzimy różnego rodzaju przedsięwzięcia, spotkania czy szkolenia, których tematem jest cyberbezpieczeństwo i walka z cyberzagrożeniami.

Bierzemy aktywny udział w procesie tworzenia międzynarodowych ram prawnych, które mają na celu zwiększenie skuteczności działań organów ścigania i przeciwdziałania popełnianiu przestępstw w cyberprzestrzeni. CBZC przewodniczy międzynarodowemu zespołowi zadaniowemu, w którego skład wchodzi przedstawiciele 22 organów ścigania z 18 krajów członkowskich Europolu.

Zastępca Komendanta Centralnego Biura Zwalczania Cyberprzestępczości nadkom. Marcin Bednarz jest przewodniczącym Rady ECTEG – Europejskiej Grupy ds. Szkoleń i Edukacji w Ob-



szarze Cyberprzestępczości, oraz przewodniczy Wspólnej Grupie Zadaniowej ds. Zwalczania Cyberprzestępczości J-CAT.

Pod koniec ubiegłego roku ogłosiliśmy rozpoczęcie pierwszej rekrutacji do CBZC dla osób nie będących policjantami. Informacja o rozpoczęciu naboru pojawiła się w mediach ogólnopolskich, na stronach internetowych jednostek policji, a także w social mediach. Do dzisiejszego dnia dokumenty rekrutacyjne złożyło 144 osoby. Dobór do CBZC ma charakter ciągły i na ten rok również wyznaczono kolejne terminy przyjęć.

## WYZWANIA

Jeśli chodzi o wyzwania stojące przed Centralnym Biurem Zwalczania Cyberprzestępczości, to z całą pewnością będzie to stały rozwój struktur Biura, rozbudowa zaplecza logistycznego, budowa nowych siedzib dla zarządów i wydziałów w kraju, oraz adaptacja tych już istniejących i wyposażanie ich w nowoczesny sprzęt teleinformatyczny.

Skupiać się także będziemy na podnoszeniu umiejętności i udział w szkoleniach z zakresu wykorzystywania nowoczesnych metod przy prowadzeniu spraw dotyczących cyberprzestępstw.





# PATRONAT SECURITY MAGAZINE

## DRUGA EDYCJA

### CYBERTEK TECH FESTIVAL

**DOŁĄCZ DO NAS**  
**I ENJOY THE CYBER!**

**CyberTek**  
**Tech Festival**

**SAVE THE DATE**  
**& ENJOY THE CYBER**

📅 24-26.05.2023

📍 Muzeum Śląskie,  
Katowice

**CyberTek Tech Festival to II edycja profesjonalnego, międzynarodowego, wyjątkowego wydarzenia budującego społeczność specjalistów w zakresie cyberbezpieczeństwa sieci przemysłowych. Tegoroczna konferencja odbędzie się pod hasłem: ENJOY THE CYBER.**

Wymieniaj doświadczenia, dyskutuj o dobrych praktykach w doborowym towarzystwie i atmosferze sprzyjającej kreatywności oraz nawiązywaniu znajomości, które zaprocentują.

CyberTek Tech Festival jest w całości poświęcony cyberbezpieczeństwu systemów przemysłowych, natomiast jego nadrzędnym celem jest upowszechnianie wiedzy i budowanie partnerstwa wokół idei „Ekosystemu cyberbezpieczeństwa”, która promuje pryncypia współpracy na rzecz cyberbezpiecznego przemysłu, w tym kontekście wdrażania w życie Ustawy o KSC.

Wydarzenie kierowane jest przede wszystkim do osób, na których spoczywa odpowiedzialność za stworzenie, skuteczne wdrożenie lub realizację programów bezpieczeństwa obejmujących sieci i systemy przemysłowe.

To konferencja tworzona dla ekspertów przez ekspertów w dziedzinie cyberbezpieczeństwa.

#### **Tematyka poruszana podczas konferencji:**

- Red Team, Pentesty, Offensive Security w OT
- Blue Team (GRA, branżowe scenariusze)
- Incident Response, Security Operations Center

(SOC), Security, Orchestration and Automation (SOAR) dla OT

- Specyfika Digital Forensics/Incident Response dla elementów systemów automatyki (PLC, HMI)
- Śledzenie zagrożeń w OT, szacowanie ryzyka i ciągłość działania
- Zapewnienie zgodności, Audyt Cyber w OT, KSC, NIS2, IEC62443
- Nadzór i zarządzanie bezpieczeństwem OT/IT; Cyberprogram w firmie
- Architektura i narzędzia (cyber)bezpieczeństwa w OT
- Monitorowanie OT; #SBOM
- Dostęp zdalny
- Historie i wpadki z obszaru bezpieczeństwa IT/OT, doświadczenia z wdrożeń
- Trendy i technologie, zmieniające sieci przemysłowe, czyli jak na paradygmaty cyber w OT wpływają: chmura, 5G, IoT
- Zero Trust vs. IoT
- Software Defined Network (SDN) w ICS
- Migracja z SDH – MPLS-TP
- i wiele innych.

# CyberTek Tech Festival

 Muzeum Śląskie, Katowice

 24-26.05.2023



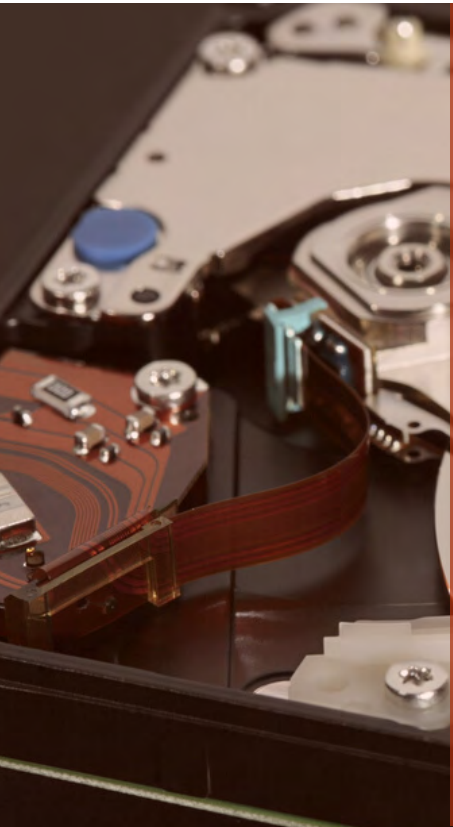


# PODSTAWY DIAGNOSTYKI DYSKÓW TWARDYCH

---



Paweł Kaczmarzyk  
Serwis komputerowy Kaleron



**W przypadku utraty dostępu do danych często podejmujemy samodzielne próby odzyskania informacji. Nierzadko korzystamy przy tym z różnego rodzaju poradników, instrukcji lub szukamy pomocy na forach internetowych. I bardzo często znajdujemy kogoś, kto chce nam pomóc, ale nie zawsze potrafi. Często też podejmujemy działania, które zamiast rozwiązać problem jedynie pogarszają sytuację. Dlaczego tak się dzieje? Bo często działamy na oślep, zapominając o diagnostyce i stosujemy metody nieadekwatne do usterek, jakie dotknęły nasz dysk.**

## CO SIĘ MOŻE ZEPSUĆ W DYSKU?

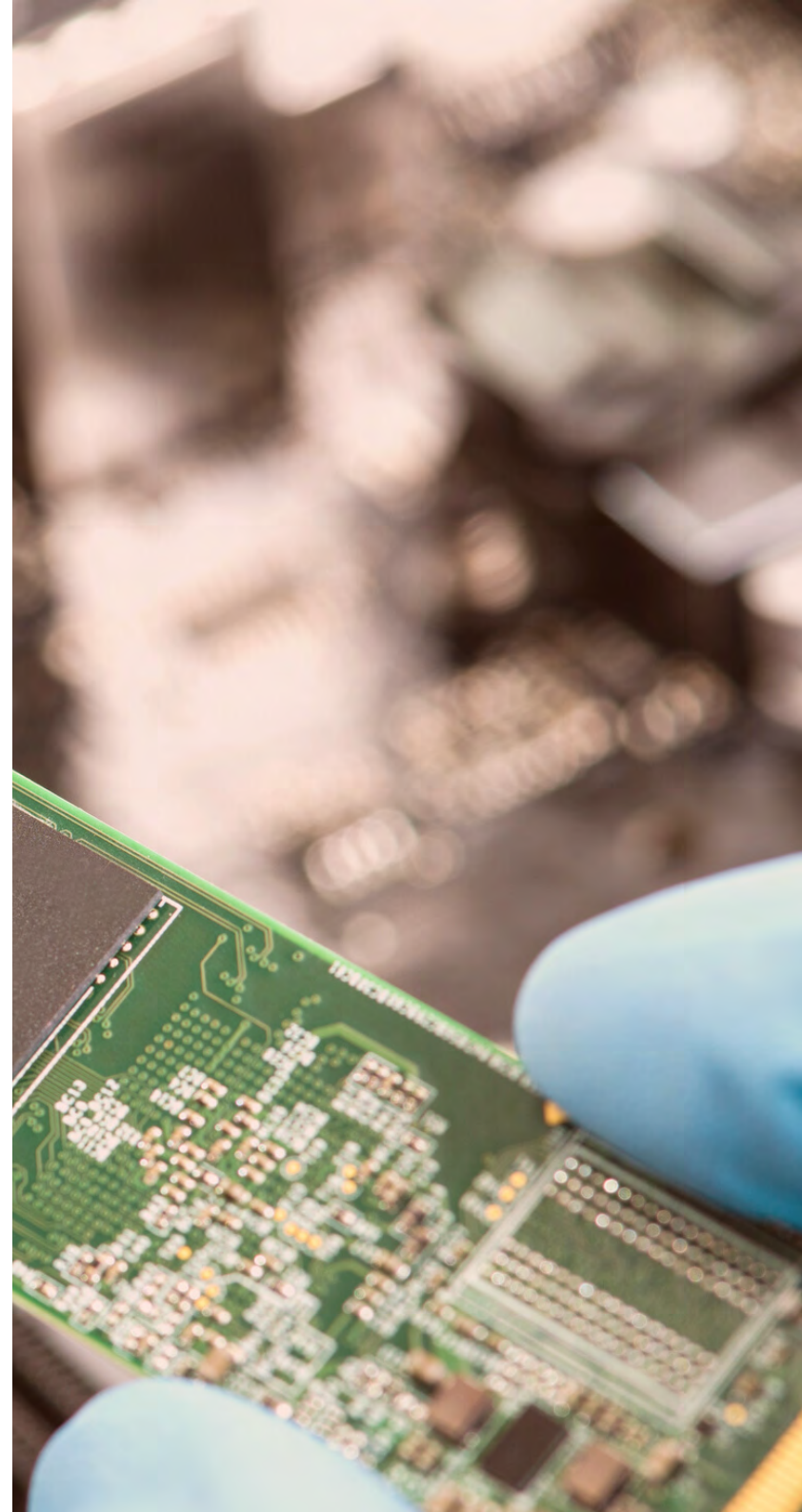
Dyski twarde są bardzo skomplikowanymi urządzeniami. Bardziej skomplikowanymi od całej reszty komputera. Oprócz elementów elektronicznych składają się także z podsystemu mechanicznego, a całość jest zarządzana przez rozbudowane oprogramowanie układowe. Niewiele osób wie, że w przypadku dysków twardych oprogramowanie układowe jest przechowywane nie tylko w EEPROMie na płycie elektronicznej, ale też na talerzach, w niewidocznym dla użytkownika obszarze zwanym strefą serwisową.

Oczywiście, uszkodzeniu może ulec każdy z komponentów dysku. Nasze myśli najczęściej biegną w kierunku „fizycznym” - elementów elektronicznych i mechanicznych, które nieraz próbujemy losowo przekładać z innych dysków w nadziei, że to pomoże, ale współcześnie coraz więcej awarii jest związanych z błędami oprogramowania układowego. A te błędy bardzo rzadko możemy naprawić, wykorzystując oprogramowanie zgrane od innego dysku.

Szczegółowe omówienie architektury oprogramowania układowego dysków twardych znacznie wykracza poza ramy tego artykułu, dlatego zostanie ona przedstawiona w dużym uproszczeniu.

Oprogramowanie układowe dysków jest podzielone na różnie nazywane przez różnych producentów bloki funkcjonalne. Niektóre z nich, jak fragmenty mikrokodu, powtarzają się w wielu egzemplarzach nie tylko tego samego modelu. Inne, jak np. logi SMART, nie mają istotnego znaczenia dla uruchomienia dysku i dostępu do danych. Jednak są pewne bloki, które są indywidualne dla każdego egzemplarza.

Wśród tych indywidualnych bloków największe znaczenie mają tzw. adaptawy parametryzujące pracę bloku głowic magnetycznych i odpowiednie wzmocnienie







odczytywanego przez głowice sygnału oraz bloki odpowiadające za zarządzanie defektami powierzchni i prawidłowe tłumaczenie adresów adresacji LBA wykorzystywanej przez dysk w komunikacji ze światem zewnętrznym na wewnętrzne adresy fizyczne. W praktyce to właśnie te ostatnie fragmenty oprogramowania układowego najczęściej ulegają awariom.

Prócz tego uszkodzeniom mogą ulec powierzchnia magnetyczna (tzw. uszkodzone sektory) oraz struktury logiczne systemu plików. Destabilizacja struktur logicznych może wynikać z wystąpienia uszkodzonych sektorów, błędów użytkownika lub oprogramowania, a także działania złośliwego oprogramowania. Do pogłębienia uszkodzeń struktur logicznych może dojść też w rezultacie uruchomienia zautomatyzowanych procedur naprawczych, o czym pisałem w poprzednim numerze.

## DIAGNOSTYCZNE WYKORZYSTANIE PROCEDURY STARTOWEJ DYSKU TWARDEGO

Ważne! Przed przystąpieniem do diagnostyki dysku twardego należy go uważnie obejrzeć pod kątem śladów usterek mechanicznych, zalania (zacieki na obudowie, korozja), uszkodzonych elementów elektronicznych, wcześniejszych ingerencji, w szczególności połączonych z otwieraniem hermobloku. Uruchomienie dysku wiąże się z ryzykiem pogorszenia jego stanu, zwłaszcza w przypadku zanieczyszczenia wnętrza hermobloku, nieumiejętnego montażu lub demontażu podzespołów, brakujących podzespołów albo pozostawienia wewnątrz niezabezpieczonych elementów. Dopiero po zweryfikowaniu stanu dysku można go bezpiecznie podłączyć.

## USTERKI ELEKTRONICZNE

Pierwszym etapem inicjalizacji dysku twardego po podaniu zasilania jest rozpakowanie zawartej w EEPROM-ie części oprogramowania układowego do bufora RAM oraz test układów elektronicznych. Jeśli dysk nie reaguje na podłączone zasilanie, najprawdopodobniej uszkodzony jest któryś z układów. W przypadku dysków hybrydowych SSHD częstą przyczyną awarii jest zużycie bufora NAND. Uszkodzenie może dotyczyć nie tylko układów na PCB, ale też np. komutatora-przedwzmacniacza znajdującego się wewnątrz hermobloku.

Brak reakcji na zasilanie może również wynikać z podstawienia obcej PCB. Jeśli oprogramowanie układowe w EEPROM-ie nie obsługuje danego przedwzmacniacza, inicjalizacja zostaje przerwana na tym etapie. Podobnie w przypadku podstawienia obcej elektroniki w dyskach SSHD bez odpowiedniej inicjalizacji bufora NAND niezgodność zawartości bufora spowoduje przerwanie procedury startowej.

W niektórych dyskach jako elementy zabezpieczające stosowane są diody Zenera. W przypadku podania nieprawidłowych napięć, diody Ze-





nera ulegają uszkodzeniu i przejmują przepływ prądu chroniąc przed uszkodzeniem pozostałe elementy elektroniczne dysku. W przypadku dobrej klasy zasilacza zabezpieczenie przeciwzwarciowe powinno wykryć zwarcie i spowodować odcięcie zasilania.

## USTERKI MECHANICZNE

Jeśli dysk podejmuje próbę rozpędzenia talerzy, możemy w praktyce wykluczyć uszkodzenia elektroniczne. Po uruchomieniu silnika obracającego talerze następuje uwolnienie bloku głowic magnetycznych ze strefy parkowania. Głowice powinny odczytać sygnał serwo, następnie odnaleźć strefę serwisową oraz doczytać z niej pozostałą część oprogramowania układowego. Przerwanie inicjalizacji na tym etapie wskazuje na uszkodzenia mechaniczne.

Nieudane próby rozpędzenia talerzy współcześnie często wynikają z nieprawidłowego zaparkowania głowic na powierzchni talerzy. Głowice najczęściej są parkowane na rampie poza obrębem talerza lub w specjalnie przygotowanej strefie parkowania. Dla zapewnienia laminarnego przepływu powietrza i stabilnej wysokości lotu głowicy nad powierzchnią tale-

rza producenci starają się, aby zarówno ta powierzchnia, jak i powierzchnia samych głowic były jak najgładsze. W konsekwencji zaparkowanie głowic w obszarze przechowującym dane skutkuje pojawieniem się oddziaływań molekularnych zdolnych do zablokowania rozruchu talerzy.

Pozostałe przyczyny problemów z rozpędzeniem talerzy w większości przypadków dotyczą bezpośrednio silnika. Może to być uszkodzenie uzwojeń lub łożyska. Uszkodzenia stosowanych współcześnie łożysk hydrodynamicznych są znacznie rzadsze niż w przypadku używanych w przeszłości łożysk kulkowych. Na problemy silnika może też wskazywać uszkodzenie sterownika silnika, tzw. drivera. W przypadku dużych oporów mechanicznych na łożysku silnika może dojść do przegrzania tranzystorów w sterowniku i uszkodzenia układu.

Najbardziej typowym objawem uszkodzeń mechanicznych dysków twardych jest dźwięk stukających głowic. Blok głowic magnetycznych uderza o ograniczniki, gdy głowice nie mogą odnaleźć sygnału serwo.



Oprócz uszkodzenia samych głowic objaw taki może spowodować podstawienie obcej elektroniki zawierającej w EEPROMie niezgodne adaptawy lub zdemagnetyzowanie dysku.

Szczególnie niepokojące są dźwięki świadczące o tarciu głowic o powierzchnię talerzy. W takich sytuacjach może dojść do degradacji powierzchni w stopniu uniemożliwiającym odzyskanie danych. W nowszych dyskach, w celu zabezpieczenia przed wystąpieniem usterek wtórnych, w przypadku braku możliwości odczytania sygnału serwo oprogramowanie układowe po kilku sekundach wyłącza głowice, odsyłając je do strefy parkowania i wyłącza silnik obracający talerze.

## USTERKI OPROGRAMOWANIA UKŁADOWEGO

Jeżeli dysk uruchamia się poprawnie, talerze obracają się równomiernie, a głowice nie stukają, dysk powinien odczytać zawartość strefy serwisowej, przedstawić się prawidłowym modelem i pełną pojemnością oraz wyjść w gotowość. Zatrzymanie inicjalizacji na tym etapie wskazuje na błędy oprogramowania układowego. Najprostszą wskazówką związaną z błędami tej kategorii może być przywieszenie BIOS-u podczas uruchomienia komputera na ok. 20-30 sekund. Takie zachowanie związane jest z oczekiwaniem BIOS-u na wystawienie przez dysk identyfikatora.



W zależności od modelu i usterki dyski z problemami oprogramowania układowego mogą się zachowywać w różny sposób. Najczęściej zawieszają się (ustawiony bit BSY w rejestrze stanu), nie wystawiając identyfikatora czy przedstawiają się zerową albo nietypowo małą pojemnością. Niektórym problemom towarzyszą nietypowe kombinacje bitów w rejestrze stanu i rejestrze błędów. Jeśli dysk jest wykrywany poprawnie, ale odmawia wykonania jakichkolwiek poleceń związanych z dostępem do sektorów użytkownika, prawdopodobnie jest zabezpieczony hasłem ATA.

## DEFEKTY POWIERZCHNI

W przypadku dysków, które przechodzą poprawnie inicjalizację oraz są rozpoznawane przez BIOS i system operacyjny, jest możliwość oceny jego stanu technicznego przez wewnętrzny system monitorowania stanu SMART. Przy czym trzeba mieć na uwadze, że jest to system bardzo niedoskonały i o ile raportując zły stan dysku zazwyczaj ma rację, to zgłaszając, że dysk jest w dobrej formie, SMART często się myli. Status SMART można sprawdzić przy pomocy dowolnego programu diagnostycznego.

Największą wartość diagnostyczną SMART ma wtedy, gdy można porównać jego parametry w czasie i zaobserwować ewentualne pogarszanie stanu na wczesnym etapie.

Stan powierzchni najlepiej ocenić na podstawie jej skanu. Najlepiej do tego celu wybrać programy sprawdzające czasy odczytu poszczególnych sektorów oraz monitorujące rejestr błędów, co pozwala uszkodzonym/nieodczytanym sektorom przypisać odpowiednie kody błędów. Takie programy pozwalają na wcześniejsze wykrycie niestabilnych i wolniej czytających się obszarów, które mogą wskazywać na pogorszenie się stanu dysku. W przypadku wystąpienia uszkodzonych sektorów znajomość kodów błędów pozwala na wyciągnięcie wniosków co do ich charakteru oraz najlepszego sposobu dalszego postępowania.

Jeśli na dysku mamy ważne dane, priorytetem jest zabezpieczenie informacji. Nadmierne zaangażowanie w diagnostykę wiąże się z ryzykiem pogorszenia stanu dysku. Przy podejrzeniu degradacji powierzchni dysku skany należy wykonywać fragmentarycznie, w minimalnym zakresie pozwalającym na ocenę stanu dysku.



# DOŁĄCZ DO GRONA EKSPERTÓW

---

BUDUJ SWOJĄ MARKĘ  
I ROZPOZNAWALNOŚĆ  
SWOJEJ FIRMY

SECURITY MAGAZINE

[WWW.SECURITYMAGAZINE.PL](http://WWW.SECURITYMAGAZINE.PL)





# CHWYT MARKETINGOWY CZY POPRAWA BEZPIECZEŃSTWA?



Kris Durski  
Vault Security



**Czym tak naprawdę jest multifactor authentication, inaczej zwany MFA (Multi-Factor Authentication)? Aby to wyjaśnić, potrzebujemy określić czynniki uwierzytelniania i ile z nich znamy? Ogólnie rzecz biorąc, nie tylko w cyberprzestrzeni, ale także w prawdziwym życiu, czynnik uwierzytelniający jest kategorią dowodu, że ktoś jest tym, za kogo się podaje.**

## CO WIESZ, CO MASZ, KIM JESTEŚ

Istnieją trzy podstawowe czynniki uwierzytelniania: co wiesz, co masz, i kim jesteś. Coś, co wiesz, to hasło, data urodzenia, jakiś fakt z czyjegoś życia lub inne dane osobowe. Coś, co masz, jest artefaktem w twoim posiadaniu, niekoniecznie fizycznym, takim jak token cyfrowy, karta dostępowa, klucz do zamka lub cokolwiek, co jest unikalne dla danej osoby.

Coś, kim jesteś, to biometryczna tożsamość osoby, taka jak odcisk palca, skan siatkówki, wzór mowy, skan twarzy lub jakakolwiek inna tożsamość ciała, która prawdopodobnie jest unikalna dla konkretnej osoby. Od niedawna w cyfrowym świecie za czynnik uwierzytelniający można uznać również lokalizację wirtualną lub fizyczną, taką jak adres IP (Internet Protocol) czy współrzędne geograficzne dostarczane poprzez GPS (Global Positioning System) czy triangulację źródeł sygnału bezprzewodowego sygnały.

Aby proces uwierzytelniania można było uznać za MFA, musi on wykorzystywać co najmniej dwa z wymienionych podstawowych czynników i każdy powinien należeć do innej kategorii. Chociaż uważa się, że przy większej liczbie wymaganych czynników intruz prawdopodobnie nie wiedziałby, nie domyśliłby się ani nie posiadałby sekretnych danych, w dzisiejszym świecie najbardziej tajne fakty osobiste szybko przedostają się do domeny publicznej.

Dlatego konieczne jest wykorzystanie czynników, które mają bardzo niskie prawdopodobieństwo wycieku do publicznie dostępnych zasobów lub łatwej kradzieży. Ważne jest również, aby zdać sobie sprawę, że jeśli dana osoba nie jest celem wysokiego poziomu dla „profesjonalnego” hakowania, MFA nawet przy słabych czynnikach może znacznie poprawić bezpieczeństwo przed naruszeniami popełnianymi przez oszustów - amatorów.







Jeśli jednak dana osoba kontroluje dane lub inne środki, które mogą mieć dużą wartość dla innej strony dysponującej praktycznie nieograniczonymi zasobami, szanse na przełamanie tych czynników mogą być znacznie większe. Tak więc, rozważając czynniki uwierzytelniania, należy wziąć pod uwagę dwa główne elementy: wartość, którą chronią oraz koszt ich złamania, przy czym koszt to nie tylko pieniądze, ale także czas potrzebny na pomyślne naruszenie.



W środowiskach bezpieczniejszych dotychczas wybraną metodą jest logowanie hasłem rozszerzonym o token cyfrowy, w środowisku publicznym najbardziej popularne jest logowanie hasłem powiązaniem z dowodem posiadania urządzenia lub usługi poprzez zwrot kodu weryfikacyjnego wysłanego przez serwer uwierzytelniający za pośrednictwem wiadomości SMS lub e-mail. Przyjrzyjmy się teraz, czy te metody są skuteczne.

## SKUTECZNOŚĆ LOGOWANIA HASŁEM

Bezpieczne tokeny identyfikacyjne sprzętowe lub programowe, generują nowy kod w ustalonych odstępach czasu na podstawie wewnętrznego zegara i wartości początkowej współdzielonej z serwerem, dzięki czemu serwer może wygenerować ten sam kod dla określonego użytkownika i w określonym czasie. Podczas logowania użytkownik wpisuje swoje hasło i rozszerza je o kod wygenerowany przez bezpieczny token identyfikacyjny, w ten sposób tworząc dłuższe i nieco losowe hasło. Podejście to zawiera w sobie dwa krytyczne elementy: dobrą synchronizację zegarów i ochronę wartości początkowej, jako ich wspólnego sekretu. Choć algorytm był przez jakiś czas utrzymywany w tajemnicy, ostatecznie został złamany, więc wartości początkowe pozostają kluczem do unikalności kodu dla konkretnego użytkownika.

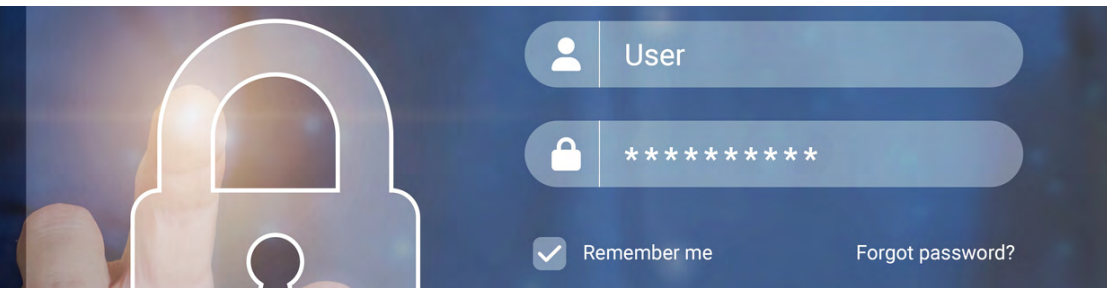
Choć tokeny sprzętowe zwykle zapewniają lepszą ochronę przed włamaniem ze względu na ich

fizyczną separację, mają też wady, ponieważ można je ukraść, a kiedy to nastąpi, oszust może swobodnie z nich korzystać, dopóki ich właściciel nie zgłosi kradzieży.

Innym problemem związanym z tokenami sprzętowymi jest to, że nie są dostępne, kiedy są potrzebne - mogą być zagubione, zapomniane lub po prostu wadliwe.

Koncepcja tokenów cyfrowych ma również kilka słabych punktów, bo generowane kody nie są efemeryczne, zatem można je ponownie wykorzystać w okresie ich ważności, a ponieważ podróżują razem z hasłem, można je wyłudzić w taki sam sposób, jak hasła.

Należy również zauważyć, że wspólny sekret to wszystko, co jest potrzebne do replikacji kodów, tym samym wraz z wyłudzonym hasłem otwiera drogę do podszywania się pod uprawnionego użytkownika.





Innym ważnym faktem jest to, że metoda nie jest typem Zero Knowledge Proof, bo serwer ma już pełną wiedzę na temat sekretu, więc aby uzyskać sekret do podszywania się pod użytkownika, haker może zaatakować użytkownika lub serwer i tylko od niego zależy, z którego wejścia skorzysta. Więc tak, metoda MFA jest lepsza niż samo hasło, i nie, ponieważ nie daje znaczącej poprawy bezpieczeństwa w stosunku do samego hasła.

## KODY WERYFIKACYJNE

Przyjrzyjmy się teraz kodom weryfikacyjnym wysyłanych e-mailem lub SMS-em (Short Messaging System). Zarówno e-mail, jak i SMS są podatne na podsłuchiwanie ich transakcji. W przypadku wiadomości e-mail, jeśli obie komunikujące się strony korzystają z usług różnych dostawców, wiadomości są wysyłane do siebie za pośrednictwem protokołu SMTP (Simple Mail Transfer Protocol) przy użyciu tak zwanych serwerów HOP, które przekazują wiadomości i w tym tkwi luka. Serwery HOP nie są szczególnie bezpieczne, ponieważ wiele z nich używa certyfikatów z podpisem własnym lub nie używa ich wcale. Bez względu na to, jak bezpieczne jest połączenie między klientem poczty e-mail a serwerem dostawcy poczty, dopóki wiadomości trafiają do innej usługi, co ma miejs-

ce w większości przypadków, ochrona jest słaba.

Podobny problem dotyczy SMS, który wykorzystuje protokół SS7 między różnymi dostawcami, natomiast protokół ten nie ma praktycznie żadnych wbudowanych środków do zabezpieczenia ruchu. Jeśli wiadomość z kodem weryfikacyjnym nie dotrze od firmy telefonicznej do jej abonenta, kody najprawdopodobniej zostaną przesłane za pośrednictwem protokołu SS7, skąd oszuści będą mogli je wydobyć. Kolejnym problemem związanym z poleganiem na tożsamości urządzenia jest możliwość jego sklonowania, a tym samym umożliwienie oszustowi otrzymania kodów na sklonowanym urządzeniu.

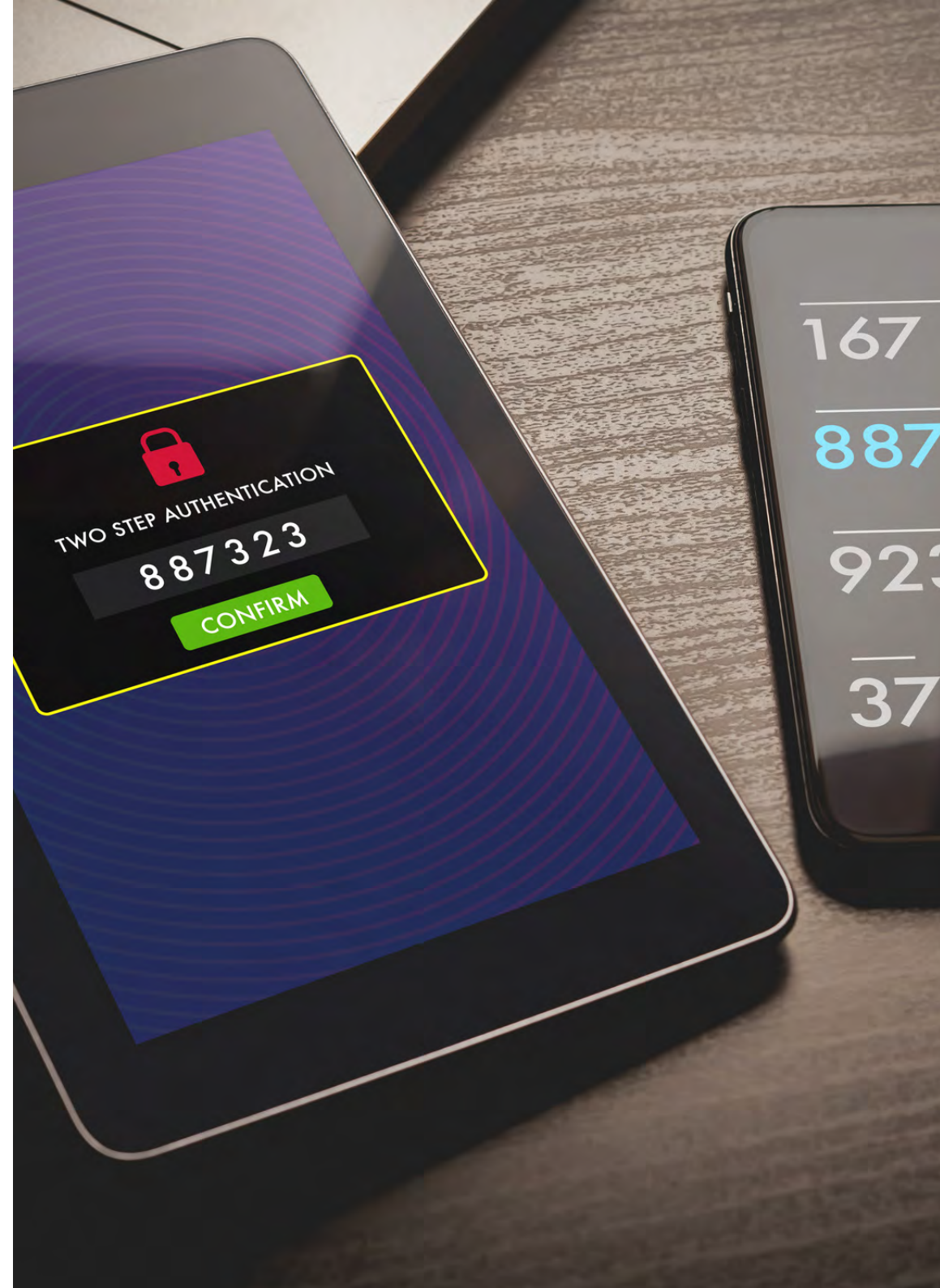
Prawdziwa poprawa bezpieczeństwa polega nie tylko na zwiększeniu liczby czynników uwierzytliwiających, ale na zmianie tych czynników na te, które są trudniejsze do złamania. Również przedstawienie czynników podmiotowi weryfikującemu, czyli serwerowi, nie powinno wiązać się z przesyłaniem ich przez sieć w takiej postaci, w jakiej są, ale z wykorzystaniem pośrednich sposobów udowodnienia ich znajomości lub posiadania.

Wybierając metody bezpieczeństwa, należy sku-

pić się nie tylko na serwerze, ale na obu komunikujących się stronach, serwerze i kliencie.

Klient może być hakerem, ale to samo można powiedzieć o serwerze, który jest używany do podszywania się pod dostawcę serwisu. Wiele razy protokoły uwierzytelniania ignorują klientów, jako mających takie same prawa, aby wiedzieć, kim jest druga strona i czy jest to naprawdę uzasadnione, aby uniknąć wysyłania danych na serwer fałszujący.

Niestety, uwierzytelnianie wieloskładnikowe (MFA) w obecnej formie, w jakiej jest wdrażane i stosowane, nie jest tutaj odpowiedzią, chociaż istnieją technologie, które zapewniają takie możliwości.







Polityka®  
Bezpieczeństwa



# SZKOLENIA Z OCHRONY DANYCH OSOBOWYCH

**SPRAWDŹ OFERTĘ**

# 10 NAJWIĘKSZYCH ATAKÓW HAKERSKICH W HISTORII

---



Redakcja  
SECURITY MAGAZINE

**Ataki hackerskie mają tak długą historię, jaką ma internet. Poznaj naszą subiektywną listę dziesięciu największych ataków hackerskich w historii, które odcisnęły solidne piętno na firmach i organizacjach działających na całym świecie.**



## 1 **ROBAK MORRISA**

Robak Morrisa to dzisiaj w zasadzie legenda. Dyskietka zawierająca oryginalny kod robaka Morrisa mieści się obecnie w Museum of Science w Stanach Zjednoczonych. W 1988 r. student informatyki Robert Tappan Morris stworzył samopowielający się kod. Ten służył mu początkowo tylko do wykazywania błędów w działaniach systemów 4 BSD Unix.

Problem jednak w tym, że kiedy Morris wypuścił go do sieci 2 listopada 1988 r., to nie zadziałało zabezpieczenie uniemożliwiające robakowi powielanie się. Ofiarą robaka Morrisa padło ok. 6 tys. maszyn, stanowiących wówczas ok. 10% wszystkich urządzeń podłączonych do internetu. Straty oszacowano na 100 mln dolarów.

Morris początkowo starał się anonimowo zapobiec sytuacji. Rozwój robaka starali się też ukrócić informatycy z Uniwersytetu Kalifornijskiego i Massachusetts Institute of Technology. Wszystko wróciło do normy dopiero po 8 dniach. Morris przyznał się potem do stworzenia robaka i skazano go na 3 lata obserwacji sądowej, 10 tys. dolarów grzywny i 400 godzin prac społecznych oraz zwrócenie kosztów sądowych.

## 2 **MAFIABOY**

W lutym 2000 r. przeprowadzono serię ataków DDoS na serwery jednych z największych serwisów w internecie. Mowa tutaj o takich gigantach jak Yahoo!, CNN, eBay czy Amazon. Okazało się, że za atakami stał... 15-letni uczeń szkoły średniej z Montrealu w Kanadzie,





niejaki Michael Calce. Ten, jak sam twierdzi, hakowaniem zajął się już w wieku 9 lat.

Pierwszą ofiarą MafiaBoya (bo takim pseudonimem się posługiwał) padło Yahoo!. 15-latek nazwał swój projekt „Rivolta” (zamieszki po włosku) i przypuścił atak DDoS. Jego ataki były na tyle skuteczne, że doprowadziły do przerwania pracy wyszukiwarki. W wywiadach, których później udzielił, twierdził, że atak przeprowadził „przez pomyłkę”. Miał on wprowadzać adresy IP do scenariusza, a następnie udać się do szkoły i zapomnieć, że wszystko nadal działa.

Później jednak przypuścił identyczny atak na CNN, a następnie na eBay i Amazona. Do swojej cyberprzestępczej działalności MafiaBoy miał używać programu Tribe Flood Network, stworzonego przez innego hakera. W 2001 r. został skazany przez sąd na 8 miesięcy aresztu otwartego i ograniczono mu dostęp do internetu. Calce już w dorosłym wieku zaczął pisać książki, a obecnie pracuje jako konsultant ds. cyberbezpieczeństwa.

## 3 WANNACRY

W 2017 r. przeprowadzono serię ataków ransomware za pomocą oprogramowania WannaCry. Ofiarą padło aż 300 tys. komputerów z systemem Windows w 99 krajach. Grupa przestępcza posługująca się tym programem – używała go do szantażu – oczywiście w celu wyłudzenia sporych sum pieniędzy.

WannaCry wykorzystywała exploit o nazwie EternalBlue, blokując komputery czy szyfrując dane, a następnie żądając okupu za ich odblokowanie. Ofiarami tego oprogramowania padły m.in. korporacja telekomunikacyjna Telefónica, Deutsch Bahn, Nissan, FedEx czy Departament Usług Zdrowotnych w Wielkiej Brytanii (NHS).



Jednak mimo przeprowadzenia cyberataku na tak szeroką skalę – hakerom do maja 17 maja 2017 r. udało się wyłudzić jedynie nieco ponad 79 tys. dolarów w bitcoinach. Mimo to atak wygenerował olbrzymie straty dla poszczególnych organizacji. Wspomniane NHS przyznało, że zakłócenia spowodowane włamaniem, odwołały ok. 19 tys. spotkań, co kosztowało 20 mln funtów. Późniejsze koszty zostały oszacowane na dodatkowe 72 mln funtów.

Winnych upatruje się w północnokoreańskich grupach hakerów na usługach tamtejszego reżimu. Oczywiście, tamtejsze MSZ zaprzeczało doniesieniom. O atak oskarżano też niejakiego Park Dzin Kioka, który miał mieć powiązania z północnokoreańskim reżimem. A samego Kioka rząd amerykański objął sankcjami bankowymi. Od 2017 r. ataki za pomocą programu WannaCry są niezwykle rzadkie, ale ciągle się zdarzają.

4

## CYBERATAK NA BANK W BANGLADESZU

W 2016 r. Bank Centralny Bangladeszu doświadczył cyberataku. W jego wyniku stracił kilkadziesiąt mln dolarów. Co ciekawe – konto, z którego skradziono pieniądze utworzono w oddziale Rezerwy

Federalnej w Nowym Jorku i zostały przelane na anonimowe konta na Sri Lance i Filipinach.

Cyberprzestępcy włamali się do globalnego systemu finansowego transferu gotówki SWIFT, co umożliwiło im przeprowadzenie ataku. Wykonali oni 30 poleceń przelewów, ale tylko 5 z nich zakończyło się sukcesem. Hakerzy próbowali wypłacić ok. 850 mln dolarów. Ostatecznie z bangladeskiego banku wyprowadzili „jedynie” ok. 81 milionów dolarów, z czego 18 mln udało się odzyskać.

Cybernaruszenie uznano za część jednego, szerszego cyberataku przeprowadzonego na różne banki w Azji. O cyberatak oskarżano chińskich hakerów oraz wspomnianego wcześniej Park Dzin Kioka. Rząd filipiński okazał solidarność z Bangladeszem, a tamtejszy sąd nakazał zamrożenie środków, które wpłynęły na filipińskie konto do czasu zakończenia śledztwa. Był to jeden z największych cyberataków w historii bankowości.

5

## GOOGLE CHINA

Chińska Republika Ludowa nie słynie z demokratycznego rządu i szanowania praw człowieka. Toteż w tamtejszym kraju (i dookoła niego) istnieje wiele organizacji starających się walczyć o posza-



nowanie wcześniej wymienionych kwestii. Wiele tych organizacji korzysta z kont Google, m.in. do korespondencji.

W grudniu 2009 r. chiński oddział Google wykrył naruszenie cyberbezpieczeństwa w wyniku którego hakerzy uzyskali dostęp do firmowych serwerów oraz skrzynek mailowych m.in. działaczy na rzecz praw człowieka. Bigtech oficjalnie wskazał, że ma dowody, że za cyberatakiem stał chiński rząd i że to właśnie rzeczeni działacze byli jego głównym celem.

Reżim ChRL zaprzeczał tym doniesieniom, choć cały świat wskazywał na naruszenie z ich strony. W marcu 2010 r. Google przeniosło swoje serwery do Hongkongu. Ale obecnie chiński rynek zdominowała tamtejsza rodzima wyszukiwarka – Baidu (70,49%). Z Google w Chinach korzysta ok. 19,6% wszystkich użytkowników internetu i jest to jeden z najniższych wyników tego giganta na świecie.

6

## JEDEN Z NAJWIĘKSZYCH ATAKÓW DDOS W HISTORII

Tak zwany DDoS z 2002 r. jest uznawany za jeden z największych i najbardziej złożonych ataków tego typu w historii internetu. 21 października 2002 r. o godz. 17:00 zaatakowano 9 z 13 serwerów znajdujących się na szczycie hierarchii systemu nazw domen internetowych. W ciągu godziny cyberprzestępcom udało się wyłączyć 7 serwerów i spowodowali wielokrotne wyłączanie 2 innych.

Eksperti ds. cyberbezpieczeństwa wskazywali, że ktoś najwyraźniej próbował „wyłączyć cały internet”. Choć ataku nie odczuli zwykli użytkownicy (poza spowolnieniem działania internetu), to część firm zajmujących się rootowaniem serwerów nie mogło poradzić sobie z atakiem, a władze federalne Stanów Zjednoczonych wskazały, że był to najbardziej złożony cyberatak w historii.

Choć od sprawy minęło prawie 21 lat, to do dziś nie znaleziono sprawcy lub sprawców. Nie

wiadomo więc, co było powodem ataku. I bardzo możliwe, że nigdy się tego nie dowiemy.

## 7 PRZEJĘCIE 77 MILIONÓW KONT UŻYTKOWNIKÓW SONY

Japoński gigant rozrywkowy Sony nie ma łatwego życia z cyberprzestępcami. 17–19 kwietnia 2011 r. Sony PlayStation Network padło ofiarą ataku hakerskiego. W jego wyniku przejęto 77 mln kont użytkowników. A ponadto cyberprzestępcom udało się przerwać działanie serwisu aż na miesiąc. Co więcej – skradziono ponad 12 tys. danych z kart kredytowych należących do klientów Sony.

Ów cyberatak kosztował firmę 140 mln funtów. Jakby tego było mało, brytyjskie Biuro Komisarzy ds. Informacji ukarało Sony za niezachowanie odpowiednich środków bezpieczeństwa. Grzywna wyniosła blisko ćwierć miliona funtów.

Lukę, która umożliwiła hakerom włamanie się do systemów Sony, odkryto już 16 lutego 2011 roku. Choć Sony zaktualizowało swoje serwery Apache, to jak widać – na nic się to zdało. Co ciekawe – na początku kwietnia tego samego roku Sony zostało zaatakowane przez grupę Anonymous, która chciała w ten sposób zaprotestować podjęciu do Geor-

ga Hotza – hakywisty, który tworzył nielegalne oprogramowanie dla konsol.

Jednak grupa nie przyznawała się do późniejszego cyberataku, w którym skradziono dane klientów Sony. Do dziś nie wiadomo, kto stał za atakiem. Oskarża się zarówno grupę Anonymous, jak i byłych pracowników japońskiego giganta.

## 8 WYCIEK DANYCH PRACOWNIKÓW I AKTORÓW SONY

Sony nie ma łatwego życia z cyberprzestępcami. W 2014 r. grupa hakerów zaatakowała Sony Pictures Entertainment. Cyberprzestępcom udało się wyłączyć serwery firmy. Zamiast strony www giganta wyświetlana była trupia czaszka i żądania grupy.

Organizacja ta określiła się jako Strażnicy Pokoju. Cyberprzestępcom udało się uzyskać dostęp do





Hakerzy pozyskali także karty zdrowia aktorów, jak i scenariusze filmów koncernu. Z tego powodu jeden z filmów musiał zostać wycofany z produkcji. Do walki z cyberprzestępcami Sony wydało aż 15 mln dolarów.

Rząd Stanów Zjednoczonych upatrywał się winnych w Korei Północnej. Ponoć grupa Strażników Pokoju była tak naprawdę cyberbrojnym ramieniem reżimu. Eksperci powiązywali atak z filmem z 2014 r. – „Wywiad ze Słońcem Narodu”, w którym ośmieszano północnokoreańską dyktaturę i zaprezentowano zamach na Kim Dzong Una. Firmie ostatecznie udało się odzyskać kontrolę nad swoimi serwerami, ale przypłacili to sporą sumą pieniędzy, wizerunkową plamą i utratą produkcji jednego z dzieł.

## 9 ATAK NA BITCOIN MT GOX

Na świecie funkcjonuje wiele giełd kryptowalutowych. Jedną z nich było Bitcoin MT Go, które swego czasu stało się liderem w tym sektorze. Niestety, kariera tej organizacji zakończyła się stosunkowo szybko. I to głównie za sprawą cyberataku. W lutym 2014 r. Bitcoin Mt Gox nagle przestało handlować. Cyberprzestępcy skradli z niej 460 mln dolarów w bitcoinach.

Nie był to jedyny (udany) cyberatak na tę giełdę, ale ten był zdecydowanie największy. Choć jak upatrują się niektóre media (np. japońska gazeta Yomiuri Shimbun) wyprowadzenie środków z Bitcoin Mt Gox mogło być nie tyle kwestią cyberataku, co oszustwa dokonanego w obrębie samej giełdy. Tak czy siak – Bitcoin Mt Gox zbankrutowało i już nigdy więcej się nie podniosło.

Z kolei francuski deweloper i CEO giełdy – Mark Kerpelès został później aresztowany za oszustwa i defraudacje, o które zresztą był wcześniej oskarżany przez grupę hakywistów.







## 10 ATAK NA CITIGROUP

Banki i fintechy często padają ofiarami cyberprzestępców. W końcu to tam trzymamy nasze środki. I w 2011 r. nie było inaczej. Wówczas to CitiGroup doświadczyło ataku cyberprzestępców. Hakerzy wykorzystali back-door i włamali się na serwery organizacji. W ten sposób pozyskali informacje o 360 tysięcy kont klientów banku, a także wyprowadzili 2,7 mln dolarów.

Co najgorsze, dane tych 200 tys. klientów zostały ujawnione. Mowa tutaj o adresach, nazwiskach i danych finansowych. Cyberatak na CitiGroup uznawany jest za jeden z największych i najbardziej drastycznych w skutkach w historii bankowości. Co ciekawe – firma wykryła naruszenie w trakcie rutynowej kontroli. To pokazuje, że warto regularnie przeprowadzać testy penetracyjne oraz kontrole bezpieczeństwa. Szkoda jednak, że w tym przypadku było to już po fakcie.

Oto cała subiektywna lista TOP 10 największych cyberataków w historii. Podobnych naruszeń w historii internetu było wiele. I niestety, najprawdopodobniej w przyszłości będzie ich tylko więcej, bo cała cyfryzacja stale postępuje. Dlatego ważne jest, aby dbać o swoje cyberbezpieczeństwo.

**Organizujesz wydarzenie związane  
z bezpieczeństwem w firmie  
lub nowymi technologiami?**

**Sprawdź ofertę  
PATRONATU  
MEDIALNEGO**



**Napisz do nas:**

**[redakcja@securitymagazine.pl](mailto:redakcja@securitymagazine.pl)**




# CYBERBEZPIECZEŃSTWO BEZ BUDŻETU

---



Adam Gola  
The Software House



**Klient nie chce lub nie może zainwestować w bezpieczeństwo – brzmi znajomo? Problemów jest wiele i mało kto próbuje je rozwiązać. Pora więc podnieść rękawicę i sprawdzić, czy można zadbać o bezpieczeństwo bez wsparcia klienta, budżetu, a jednocześnie mierząc się z deficytem bezpieczników. Niemożliwe?**

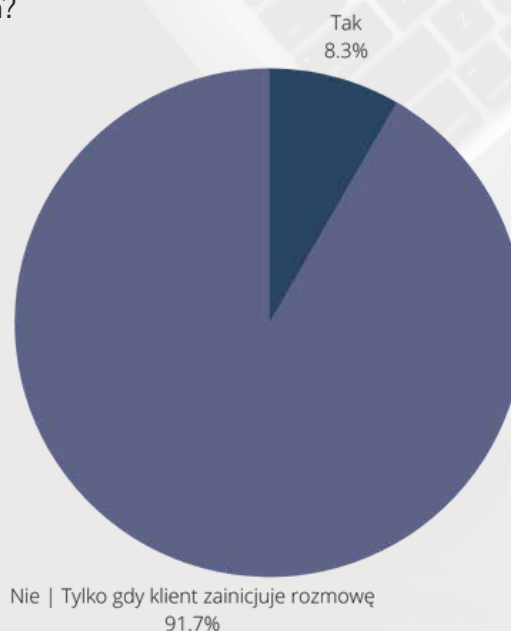
Dziś na każdym kroku możemy usłyszeć o wyciekach danych, własności intelektualnej i innych incydentach bezpieczeństwa. Po jednej stronie szali mamy coraz częstsze ataki, po drugiej biznes, który nie zawsze jest w stanie wygospodarować odpowiedniego budżetu na ochronę. Wraz z zespołem ludzi zaangażowanych w temat bezpieczeństwa, postanowiliśmy sprawdzić czy jesteśmy w stanie wpłynąć na jego wyższy poziom, gdy brakuje środków, specjalistów oraz świadomości.

## WYNIKI BADAŃ

Zanim jednak omówię wnioski na podstawie komercyjnych case study, muszę wspomnieć o pewnych badaniach, które były kluczowe do rozstrzygnięcia tego problemu. Postanowiłem zadać zestaw anonimowych pytań kilku firmom/projektom. Wyniki nie były zbyt pocieszające. Na pytanie „czy rozmawiasz z klientami o bezpieczeństwie”, zaledwie 8,3% ankietowanych odpowiedziało twierdząco. Pozostali (91,7%!) w ogóle nie rozmawia lub robią to tylko wtedy, gdy klient zainicjuje temat. Idąc dalej, okazuje się, że w skali miesiąca specjaliści spędzają od 12 do 23 godzin na rozmowach z klientami. Czy ciężko w takiej ilości spotkań zmieścić temat bezpieczeństwa, nawet ograniczając go do small talka?

Czy rozmawiasz z klientami

O BEZPIECZEŃSTWIE





Na drugie zapytanie, o świadomość zagrożeń w wytwarzanym projekcie, 66,7% ankietowanych odpowiedziało twierdząco, ale nadal pozostaje około 1/3 ankietowanych, którzy nie mają wiedzy na temat potencjalnych zagrożeń.

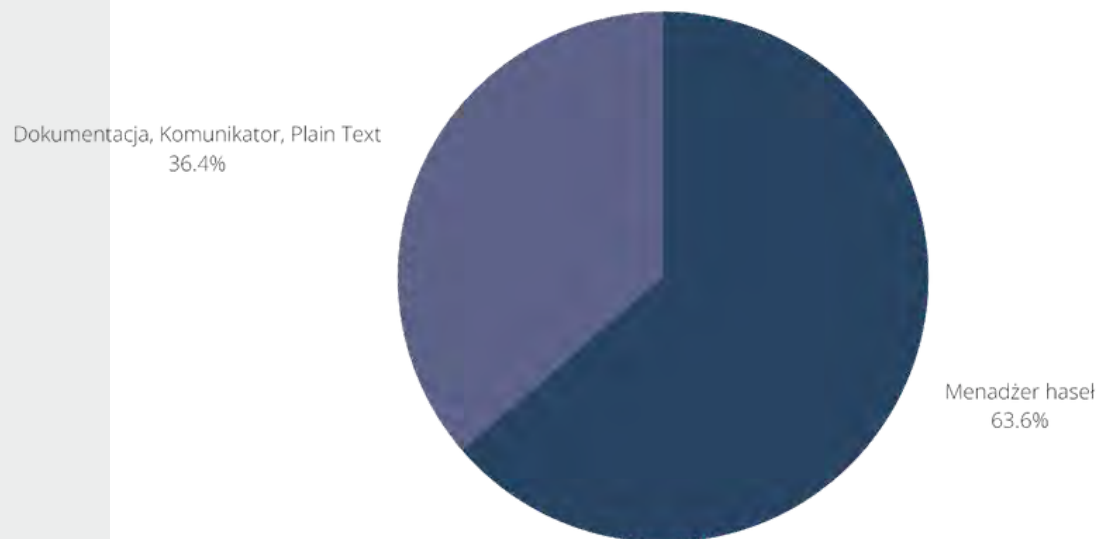
Kolejne zagadnienia były nieco bardziej techniczne. Okazuje się bowiem, że tylko w 1/3 ankietowanych projektów (z różnych firm technologicznych), użytko-

wnik końcowy może na koncie uruchomić 2FA.

Zaledwie w 25% projektów jest jakieś logowanie ruchu (w celu wykrycia nadużyć), ale praktycznie nikt tego nie weryfikuje. 63,6% ankietowanych przechowuje swoje hasła i licencje w menadżerze haseł, co jest bardzo dobrym wyborem. Nie cieszy jednak, że aż 36,4% korzysta z dokumentacji i komunikatorów (plain text).

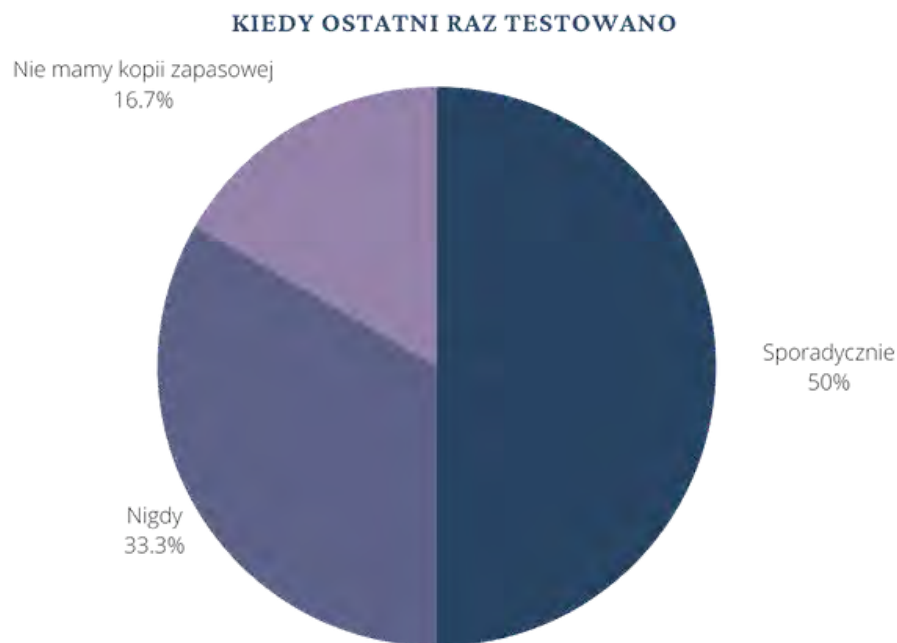
## Hasła, licencje i tokeny

### JAK JE PRZECHOWUJECIE



Z ciekawszych odpowiedzi, warto wspomnieć, że 83,3% ankietowanych robi kopię zapasową, a zaledwie połowa sporadycznie testuje jej przywracanie. Mając tego typu dane, można podejść do analizy problemu i rozebrania go na czynniki pierwsze.

## Przywracanie kopii zapasowej



### Problem 1: Klient nie chce bezpieczeństwa

Może się to wydawać dziwne i nietypowe, ale klienci nie zawsze chcą być bezpieczni. A może, po prostu, nie chcą przeznaczać na to budżetu (zazwyczaj do pierwszego incydentu). W każdym razie, chcąc zapewnić bezpieczeństwo w projekcie, musieliśmy się zmierzyć z tym problemem.



## **Problem 2: Ograniczony budżet**

Nawet jeżeli klient chciałby być bezpieczny, czasami nie jest w stanie za to zapłacić. Z różnych powodów, w które teraz nie będziemy wchodzić. Pełne testy penetracyjne czy oceny podatności są czasochłonne, a co za tym idzie, również kosztowne. I nierzadko się zdarza, że w kwocie projektu, w ogóle nie uwzględniono kosztów bezpieczeństwa.

## **Problem 3: Dużo projektów, deficyt bezpieczników**

Deficyt tematów bezpieczeństwa może wystąpić w momencie, gdy w firmie realizowanych jest wiele produktów. Przejście pełnych testów penetracyjnych w dziesięciu projektach, gdy mamy ograniczoną liczbę specjalistów jest albo nierealne, albo czasowo liczone w miesiącach (lub latach). Co więcej, w takim przypadku projekty mogą różnić się między sobą technologicznie, a świadomość specjalistów związanych z procesem wytwórczym może być naprawdę zróżnicowana – od wysokiej po totalną nieznajomość aspektów bezpieczeństwa.

## **FUNKcjONALNOŚĆ PONAD BEZPIECZEŃSTWO**

Analizując te wszystkie problemy oraz wyniki ankiet, można zauważyć jeszcze jedną kwestię – domyślnie

projekty nie są pisane bezpiecznie.

Możemy przyjrzeć się, w jaki sposób programiści uczą się swojego fachu – niezależnie czy na własną rękę, czy korzystając ze szkoleń, dość rzadko pojawiają się tam elementy bezpieczeństwa. Programistów szkoli się pisać kod funkcjonalny, wydajny, ale niekoniecznie domyślnie bezpieczny. Umiejętności w zabezpieczaniu swoich produktów wynosi się z doświadczenia komercyjnego, a i to tylko wówczas, gdy jest zapotrzebowanie na to bezpieczeństwo lub „ktoś wyżej” o to prosi. Ale to nie zdarza się w każdym miejscu i w każdym projekcie. Wniosek?

Świadomość bezpieczeństwa zależy od nas – bezpieczników, ale również programistów. Dopóki o tym nie rozmawiamy i nie analizujemy, dopóty często nie wdramy bezpiecznych mechanizmów i sprawdzonych rozwiązań.

## **JEDNO SPOTKANIE – UNIWERSALNE ROZWIĄZANIE**

Postanowiliśmy więc wyjść z tego założenia – skoro trzeba zacząć od budowania świadomości, a niekoniecznie od skomplikowanych oraz trudnych testów penetracyjnych (na które w opisywanym przypadku nie ma czasu, budżetu



tu i brakuje specjalistów), postanowiliśmy realizować jedno spotkanie, które trwa od 60 do 120 minut.

Podczas sesji rozmawiamy o bezpieczeństwie, zadajemy otwarte pytania i sprawdzamy stan bezpieczeństwa danego produktu, czego wynikiem jest wysyłany do zespołu raport z rekomendacjami. Oczywiście, aby było to wartościowe, spotkanie nie może być traktowane jak formalny audyt, który trzeba zaliczyć. Same pytania również powinny być sensowne – i tu pojawiają się gotowe rozwiązania, z których można czerpać garściami. Mowa między innymi o listach OWASP (Application Security Verification Standard, Top 10 Privacy Risks), CIS Benchmark, NIST SP 800-53, ISO 27001. W zależności, co chcemy zweryfikować – aplikacje mobilne, webowe, infrastrukturę, prywatność w organizacji, aspekty GDPR lub cokolwiek innego – przygotowujemy specjalną listę kilkudziesięciu trafnych pytań.

## KONKLUZJE POPARTE DOŚWIADCZENIEM

Po przeprowadzeniu takich audytów, udało się zauważyć kilka istotnych elementów. Budowanie świadomości rozpoczyna się od wspólnych dyskusji, dlatego też warto ograniczyć wszelkie pytania zamknięte oraz odpowiedzi „tak/nie”. Jeżeli zespół nam w pełni nie ufa, tego typu odpowiedzi mogą być furtką, by szybko uciec ze spotkania, odpowiadając tylko „tak, mamy”. Jest to o tyle istotne, że na zebraniu ograniczamy się do rozmowy – audytu, a nie konkretnych działań i czasochłonnych testów. Warto iść w stronę dyskusji.



Zespół projektowy lubi rozmawiać i szuka pomocy. Tematy bezpieczeństwa są przeważnie interesujące, a programiści naprawdę je lubią. Potrzebny jest tylko zapalnik w postaci inicjatywy – w tym przypadku - spotkania połączonego z debatą.

Bezpieczeństwo powinno rozpocząć się od podstaw. Zauważyłem to już kilka lat temu. Gdy ktoś wspomina o zagrożeniach, od razu przychodzą na myśl skomplikowane testy, czasochłonne penetra-

cje i inne tego typu tematy.

Podczas gdy przeważnie brakuje fundamentów – walidacji rejestracji czy logowania wskazujące na istnienie adresu w bazie, polityka haseł wymuszająca tonę znaków specjalnych, brak podstawowych nagłówek bezpieczeństwa i inne braki, które udowadniają, że często wystarczy zejście do fundamentów, nim ruszymy na pojedynek między Red a Blue Teamem.

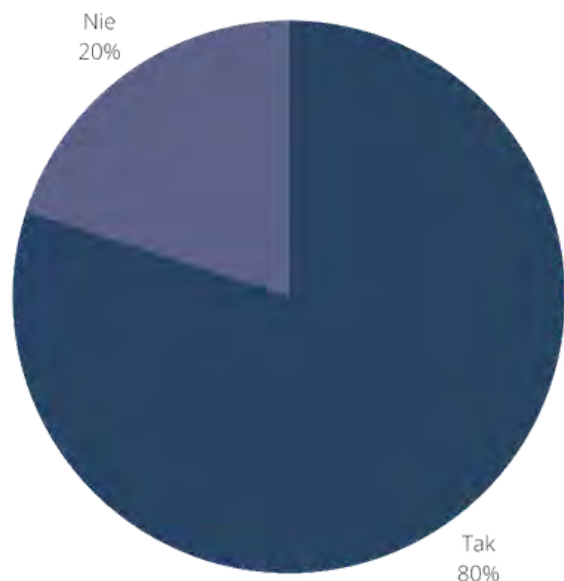


## CZY TAKIE SPOTKANIE DAJE WARTOŚĆ?

Podsumowując, mówimy tu o zaledwie jednym spotkaniu, które trwa 60-120 minut, a po nim tworzony jest raport z rekomendacjami. Nie jest to bardzo czasochłonne, a co za tym idzie, nie jest aż tak kosztowne. Oczywiście, ktoś koszt spotkania (i wdrożenia rekomendacji) musi ponieść – może to być klient, może to być firma, która oprogramowanie wytwarza – jako standard jakości.

Tytuł „Cyberbezpieczeństwo bez budżetu” jest, oczywiście, delikatnie naciągany, bo pewnymi środkami musimy dysponować. I byłem tego świadom w momencie pisania artykułu. Ale nie mówimy tu o wielotysięcznych kosztach związanych z czasochłonnymi testami penetracyjnymi. Czy spotkanie dało wartość? Sprawdźmy wyniki ankiety. Okazuje się, że 80% ankietowanych (którzy taki audyt przeszli) odpowiedziało twierdząco.

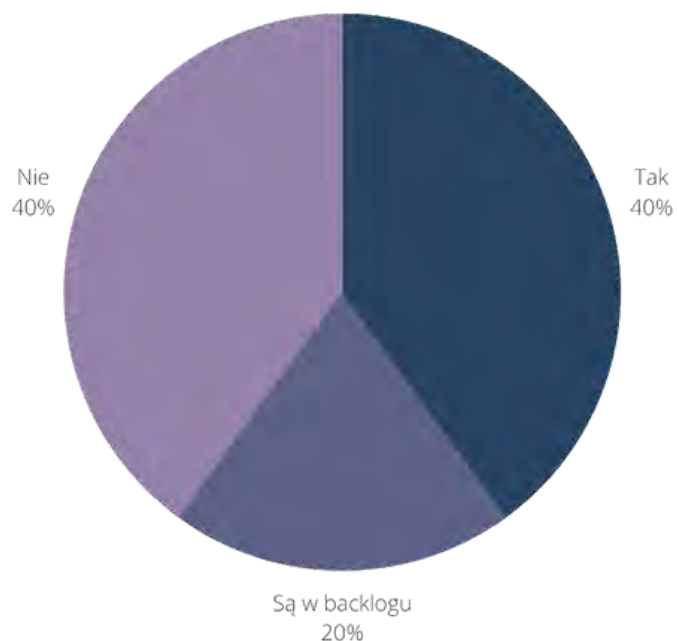
### Czy uważasz audyty za wartościowe?





Jeszcze bardziej cieszy fakt, że aż 60% zaudytowanych projektów już wdrożyło lub za moment wdroży zaproponowane rekomendacje. To tylko pokazuje, że wystarczył delikatny zapalnik, by wznieść produkt na wyższy poziom bezpieczeństwa, zacząć testować (oraz tworzyć) kopie zapasowe, rozmawiać z klientami o zagrożeniach, wdrożyć Zero Trust oraz wiele funkcjonalnych aspektów podnoszących poziom bezpieczeństwa.

## Czy wdrożono rekomendacje?



## KONKLUZJE

W jaki sposób podejdziesz do spotkania, jakie pytania zadasz, ile ich będzie i w jaki sposób wdrożysz to do procesu w swojej organizacji, zależy już tylko od Ciebie.

Ja chciałem w tym artykule udowodnić, że wystarczy jedna sesja, by uruchomić zapalnik i zaangażować programistów w aspekty bezpieczeństwa.

Zauważ, że bezpiecznik jest tu potrzebny tylko na czas spotkania – a jeżeli dobrze to rozgrasz, być może uda Ci się wdrożyć taki proces, który nie będzie wymagał bezpiecznika lub będzie on potrzebny tylko do przeanalizowania krótkiego raportu. Czy warto spróbować zainwestować w taki pomysł? Zdecydowanie tak.



Rzetelny®  
Regulamin

# DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP  
DO NOWYCH PRZEPISÓW

**SPRAWDZAM OFERTĘ**





SECURITYMAGAZINE.PL

# CYFROWY „SEJF” NA DANE, ZAPOBIEGANIE ATAKOM I LOGOWANIE BEZ HASEŁ



Redakcja  
SECURITY MAGAZINE



#SECURITY  
#STARTUP

**Startupy dostarczają coraz więcej rozwiązań z zakresu cyberbezpieczeństwa. W tym zestawieniu poznasz spółki, dzięki którym będziesz zabezpieczać swoje dane, zapobiegać cyberatakam, a nawet logować się bez użycia haseł. Sprawdź, jak te startupy mogą Ci pomóc.**

## LOGPASS, CZYLI LOGOWANIE SIĘ BEZ HASEŁ

Warszawski startup Logpass sp. z o.o. wierzy, że przyszłość to passwordless. Prawda jest taka, że hakerzy coraz łatwiej łamią nawet najbardziej skomplikowane hasła. Najnowsza karta graficzna – GeForce RTX 4090 łamie 8-znakowe szyfry już w 48 minut! Przetestował to Sam Croley – badacz ds. cyberbezpieczeństwa.

Oznacza to, że rekomendowana przez większość serwisów długość haseł jest niezwykle prosta do złamania. Jednak już RTX 3090 – poprzednik – łamał szyfry „zaledwie” 2,5 razy wolniej. To znaczy, że haker w ciągu ośmiu godzin roboczych przy RTX 4090 może złamać w zasadzie osiem haseł. W przypadku karty starszej generacji złamałby ich 3.

Co zatem robić? Bardziej skomplikowane hasła to jeden ze sposobów. Jednak jak je wszystkie zapamiętać? Z pomocą przychodzą menedżery haseł, ale i one mogą zostać złamane przez cyberprzestępców, a nasze dane dostępne przejęte.

Logpass ma inny pomysł – wykorzystując rejestr publiczny, pozwala się logować bardzo szybko.

I to zarówno Tobie, jak i Twoim klientom.

Platforma zbiera dane Twoich klientów, anonimizuje je i umożliwia im logowanie się bez podawania haseł. Ba, Logpass weryfikuje też wiek użytkownika oraz uaktualnia ich dane poprzez zbieranie zgód.

Co więcej – wszystkie dane są przetwarzane zgodnie z RODO, a one same przechowywane są na urządzeniu użytkownika. Wszystko jest anonimowo, bezpiecznie i szybko. Z usług Logpassa korzystają już zresztą m.in. Deal Done czy Itelix Software sp. z o.o.

## BITFOLD – PRYWATNY „SEJF” NA TWOJE DANE

Kolejnym interesującym startupem jest Bitfold R&D sp. z o.o. Choć to spółka założona i prowadzona przez Polaków, to siedzibę ma w Szwajcarii. Startup opiera swoje rozwiązania o blockchain, czyli blok łańcuchów.

Technologię znaną głównie z kryptowalut i tokenów NFT, ale mającą także zastosowania w cyfryzacji dokumentacji, inteligentnych kontraktach itp.



Bitfold tłumaczy swoje rozwiązanie jako innowacyjny portfel sprzętowy dla kluczy prywatnych i w innych zastosowaniach asymetrycznej kryptografii. Tłumacząc na prostszy język – startup tworzy fizyczne urządzenia, które pozwalają na przechowywanie i zabezpieczanie wirtualnych aktywów. Np. kryptowalut, ale też danych czy cyfrowej tożsamości.

Startup stworzył technologię opatentowaną w całej Europie oraz Stanach Zjednoczonych. Do jej przygotowania pozyskał grant NCBiR w kwocie ponad 21 mln zł, a także ponad 12,5 mln zł od inwestorów prywatnych.

Spółka jest dość tajemnicza i nie zdradza wszystkich swoich możliwości czy projektów. Mimo to transparentnie pokazuje, jak wykorzystuje swoje finansowanie. Cyfrowy sejf pozwala na przechowywanie wirtualnych danych oraz aktywów, co pozwala na ich faktyczne, praktycznie fizyczne posiadanie.

## **CYBER QUANT – CYBERBEZPIECZEŃSTWO DLA TWOJEJ FIRMY**

Warszawski Cyber Quant to dość standardowa spółka z obszaru cyberbezpieczeństwa. Startup zajmuje się przede wszystkim OSINT-em, analizą bezpieczeństwa i doradztwem. Spółka pomaga w identyfikacji słabych punktów w Twojej firmie, dokonując audytu.



Startup testuje też Twoją obecną ochronę przed cyberprzestępcami, podejmując się tzw. etycznego hakingu, a także opracowuje strategię cyberbezpieczeństwa. To jednak nie koniec, bo spółka oferuje też ochronę kluczowych osób w firmie – oczywiście od strony cyberzagrożeń.

Ponadto startup udostępnia raporty bezpieczeństwa OSINT dla nowych pracowników w firmie i przeprowadza szkolenia z zakresu cyberbezpieczeństwa. Ponadto Cyber Quant zajmuje się monitoringiem darkwebu w poszukiwaniu informacji o Twojej firmie, wyciekach itp. W startupie pracuje ośmiu doświadczonych ekspertów, a sama spółka została założona przez Pawła Poleńskiego, który

ma ponad 10-letnie doświadczenie w prowadzeniu spółek IT.

Cyber Quant wierzy, że w ciągu najbliższych 5 lat większość ludzi będzie posiadać dedykowaną aplikację, tj. cyberstrażnika, który ochroni go przed zagrożeniami ze strony cyberprzestępców. I to właśnie namiastkę takiego cyberstrażnika oferuje warszawski startup.

To tylko niektóre ze startupów oferujących rozwiązania z zakresu cyberbezpieczeństwa. Jak widzisz – adresują one różne kwestie oraz sprawdzają się w odmiennych obszarach. Warto o cyberbezpieczeństwie myśleć w sposób holistyczny i zabezpieczać się z każdej możliwej strony.



# -20%

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PL



## NOWOROCZNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

**WAŻNY DO**  
**28.02.2023**



KONTAKT I SZCZEGÓŁY: REDAKCJA@SECURITYMAGAZINE.PL



# NOWA ERA BEZPIECZEŃSTWA W UE. NOWE PRAWO I OBOWIĄZKI FIRM

---



Piotr Nowak

**Zwiększenie ogólnego poziomu cyberbezpieczeństwa w Unii Europejskiej to jeden z priorytetów obecnych czasów. Jednak bez właściwych środków prawnych nie byłoby to możliwe. Dlatego 16 stycznia 2023 roku w życie weszła w życie dyrektywa NIS2, która przebudowała ramy europejskiego porządku infrastruktury krytycznej i cyfrowej. Fabryki, elektrownie, wodociągi, a także banki czy szpitale czekają spore zmiany.**



## **NETWORK AND INFORMATION SECURITY**

Unijne przepisy dotyczące cyberbezpieczeństwa wprowadzone w 2016 r. zostały zaktualizowane dyrektywą NIS2, która weszła w życie w tym roku. Dyrektywa ma na celu zwiększenie poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej poprzez wprowadzenie wymogów dotyczących ochrony przed cyberatakami i innymi zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych w obecnych czasach.

Dyrektywa NIS2 wymaga, aby kraje członkowskie UE wprowadziły odpowiednie przepisy i procedury w celu zapewnienia bezpieczeństwa swoich sieci i systemów informatycznych, a także aby zapewnić współpracę między państwami członkowskimi w zakresie ochrony przed cyberzagrożeniami.

Zmodernizowane zostały istniejące ramy prawne, aby nadążyć za zwiększoną cyfryzacją i ewoluującym krajobrazem zagrożeń dla cyberbezpieczeństwa. Rozszerzając zakres przepisów dotyczących cyberbezpieczeństwa na nowe sektory i podmioty, przyczynia się do

dalszej poprawy odporności i zdolności reagowania na incydenty podmiotów publicznych i oraz prywatnych, właściwych organów i całej UE.

**Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii przewiduje środki prawne mające na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa przez zapewnienie:**

- gotowości państw członkowskich, wymagając od nich odpowiedniego wyposażenia.
- współpracy między wszystkimi państwami członkowskimi poprzez ustanowienie grupy współpracy wspierającej i ułatwiającej współpracę strategiczną i wymianę informacji między państwami członkowskimi,
- kultury bezpieczeństwa we wszystkich sektorach, które są niezbędne dla gospodarki i społeczeństwa i które w dużym stopniu opierają się na technologiach informacyjno-komunikacyjnych, takich jak energia, transport, woda, bankowość, infrastruktura rynku finansowego, opieka zdrowotna i infrastruktura cyfrowa.



“Przedsiębiorstwa wskazane przez państwa członkowskie jako operatorzy usług kluczowych w powyższych sektorach będą musiały podjąć odpowiednie środki bezpieczeństwa i powiadomić właściwe organy krajowe o poważnych incydentach. Kluczowi dostawcy usług cyfrowych, takich jak wyszukiwarki, usługi przetwarzania w chmurze i internetowe platformy handlowe, będą musieli przestrzegać wymogów w zakresie bezpieczeństwa i powiadamiania na mocy dyrektywy” - przekazała Komisja Europejska.

## WSPÓŁCZESNE ZAGROŻENIA

Ostatnie dwa lata, a w szczególności 2022, pokazały, jak wiele zagrożeń jest zagrożeń dla bezpieczeństwa zbiorowego. - Stoimy w obliczu nowego sposobu prowadzenia wojny. Powtarzające się ataki o podobnym charakterze na wrażliwe cele infrastruktury krytycznej stały się częścią naszej rzeczywistości. Stawka jest wysoka. Od tego, czy będziemy w stanie odpowiedzieć cyberprzestępcom, zależeć będzie, w jakiej Europie przyjdzie nam żyć: niestabilnej, targanej kryzysami, czy potrafiącej ochronić swoją infrastrukturę i obywateli - powiedział Krzysztof Wójtowicz z ICsec, licencjonowanego dostawcy usług z zakresu cyberbezpieczeństwa dla przemysłu.

**Obowiązujące dotychczas reguły prawne okazały się nieskuteczne wobec nowych niebezpieczeństw. Dyrektywa ma zabezpieczyć czułe punkty wspólnoty na wypadek zagrożeń porządku publicznego takich jak:**

- ataki terrorystyczne,
- sabotaże
- czy cyberataki.

Powołana zostanie Europejska Sieć Organizacji Łącznikowych ds. Cyberkryzysów (EU-CyCLONE), która ma odpowiadać za wsparcie koordynacji zarządza-





nia incydentami i dużymi kryzysami cybernetycznymi.

Kraje członkowskie mają też zapewnić funkcjonowanie odpowiednich organów związanych z zapewnieniem cyberbezpieczeństwa (w tym m.in. wyznaczyć pojedyncze punkty kontaktu i właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego – CSIRT).

Obowiązkiem każdego państwa wspólnoty będzie też opracowanie własnej strategii cyberbezpieczeństwa (w ramach której powinny zostać opracowane odpowiednie polityki, m.in. w zakresie rozwoju i promowania kompetencji dotyczących cyberbezpieczeństwa). Państwa mają być zobowiązane do przeznaczania większych środków na wzmocnienie swoich zabezpieczeń.

## **CO ZMIENIA DYREKTYWA?**

Dyrektywa ma ułatwić zarządzanie ryzykiem, dlatego wprowadza dwie jasne kategorie podmiotów: kluczowe i ważne.

**Zostaną one objęte szczególnymi środkami nadzoru i egzekwowania przepisów w oparciu o cztery założenia:**

- skuteczność,
- proporcjonalność,
- odstraszanie,
- dostosowanie do indywidualnego przypadku.

Różnica między podmiotami ważnymi i kluczowymi wyraża się

w stosowaniu środków nadzoru.

W przypadku podmiotów ważnych audyty są przeprowadzane po naruszeniach, nie są one też objęte kontrolami wyrywkowymi.

NIS 2 oznacza powszechną mobilizację oraz współodpowiedzialność. Dyrektywa rozszerza definicje sektorów i rodzajów podmiotów krytycznych objętych regulacjami na polu cyberbezpieczeństwa.

**Od 16 stycznia dyrektywa obejmie swym parasołem 11 sektorów:**

- energetyka,
- transport,
- bankowość,
- infrastruktura rynku finansowego,
- ochrona zdrowia,
- wodociągi,
- spółki wodno-kanalizacyjne,
- infrastruktura cyfrowa,
- administracja publiczna,
- przestrzeń kosmiczna
- produkcja żywności.





Firmy z tych obszarów zostały zobligowane do regularnego przedstawiania dowodów na prowadzenie realnej polityki cyberbezpieczeństwa, oceny ryzyka, a także przeprowadzania audytów bezpieczeństwa, powiadamiania władz o wszelkich nieprawidłowościach oraz podejmowania działań w celu przeciwdziałania zagrożeniom.

Firmy, które rozpoczną proces modernizacji swoich systemów bezpieczeństwa mogą liczyć na wsparcie finansowe.

## **DRAKOŃSKIE KARY ZA ZANIEDBANIA**

Organizacje, które nie dostosują się do prawa, czekają poważne konsekwencje. Za nieprzestrzeganie przepisów grozi grzywna do 2 procent globalnych obrotów. W pierwszej kolejności firmy zostaną wezwane do usunięcia uchybień lub zapewnienie zgodności, a w przypadku braku pożądanych działań mogą stracić certyfikaty czy zezwolenia na świadczenie usług, lub nawet na całość działalności gospodarczej. Kary przewidziane są też dla dyrektorów generalnych i przedstawicieli prawnych spółek. Mogą oni zostać zawieszeni.

- Twórcom nowych reguł zależało na tym, by były one skuteczne i egzekwowalne. Największa odpowiedzialność spoczywa na operatorach infrastruktury krytycznej. Obiekty takie, jak elektrownie, stacje uzdatniania wody czy rafinerie w coraz większym stopniu polegają na technologii niewymagającej udziału człowieka. Podłączone do sieci, komunikujące się między sobą urządzenia nie tylko ułatwiają zarządzanie dostawami i zwiększają wydajność, ale stanowią też punkt krytyczny całego systemu. Skuteczny atak na ten obszar mógłby uruchomić katastroficzny scenariusz dla gospodarki i społeczeństwa. Dlatego ich odpowiedzialnie zabezpieczenie stanowi dziś główne wyzwanie dla zarządców spółek - wytłumaczył ekspert z ICsec.

## **WDROŻENIE W POLSCE**

Na początku stycznia w wykazie prac legislacyjnych i programowych Rady Ministrów pojawiła się kolejna wersja projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Znalazły się w niej zapisy dotyczące współpracy operatorów przy tworzeniu strategii bezpieczeństwa, zgłaszania incydentów, zasad przyznawania certyfikatów.



Projekt wprowadza też niezwykle istotną w kontekście wykonania postanowień dyrektywy kategorię Operatora Strategicznej Sieci Bezpieczeństwa. Będzie to jednoosobowa spółka Skarbu Państwa, przedsiębiorca telekomunikacyjny, który posiada infrastrukturę telekomunikacyjną niezbędną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Musi posiadać środki techniczne i organizacyjne, zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej czy świadectwo bezpieczeństwa przemysłowego pierwszego stopnia.

Na implementację będziemy musieli jeszcze poczekać. Zanim projekt zostanie skierowany do Sejmu, musi się nim zająć Komitet Stały Rady Ministrów.

## WYZWANIE, ALE TEŻ SZANSA

Obowiązki wynikające z dyrektywy mogą okazać się dla wielu polskich organizacji szansą na wejście na wyższy poziom zaawansowania technologicznego. Podmioty krytyczne będą miały obowiązek ochrony infrastruktury niezbędnej do utrzymania usług kluczowych, jednak ślad za nowymi powinnościami pojawią się pieniądze na inwestycje. Operatorzy będą mogli liczyć na wsparcie finansowe ze strony państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. Takie wsparcie nie będzie traktowane jako niedozwolona pomoc publiczna.

**To ważna wiadomość dla podmiotów, które w dotychczasowych regulacjach dotyczących cyberbezpieczeństwa nie były traktowane jako wymagające najwyższej uwagi. NIS 2 zakłada rozszerzenie zakresu podmiotów uznawanych za „kluczowe” w porównaniu do katalogu podmiotów mogących stanowić operatorów usług kluczowych na gruncie dyrektywy NIS.**



Jako podmioty kluczowe z perspektywy zapewnienia cyberbezpieczeństwa, oprócz podmiotów z sektora energetycznego, transportowego, bankowego, finansowego, czy zdrowotnego, uznano m.in.: dostawców usług przetwarzania w chmurze obliczeniowej (cloud computing service providers) – należących wcześniej do „niższej” kategorii dostawców usług cyfrowych, dostawców usług centrów danych (data centre service providers) – nowej kategorii usług, obejmującej w szczególności usługi scentralizowanego przechowywania, przetwarzania i transportu danych łącznie z zapewnieniem wszelkich niezbędnych do tego celu narzędzi (np. obiektów i infrastruktury) oraz środków (np. dostaw energii), a także dostawców usług CDN (content delivery network providers) – nowej kategorii usług, polegających na udostępnianiu sieci serwerów w celu zapewnienia możliwości dalszego udostępniania użytkownikom treści internetowych.

Poza tym z nowymi obowiązkami będą musieli się zmierzyć dostawcy usług zaufania, dostawcy publicznych sieci łączności elektronicznej oraz usług łączności elektronicznej.

Wśród podmiotów kluczowych wskazano również operatorów infrastruktury naziemnej, wspierających świadczenie usług kosmicznych – to obecnie można traktować w kategoriach ciekawostki, jednak dobrze pokazuje spójne i przyszłościowe podejście Unii Europejskiej do kwestii cyberbezpieczeństwa.

W TWOJEJ FIRMIE  
ZDARZYŁ SIĘ

# WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC  
**SPRAWDŹ JAK**



Polityka<sup>®</sup>  
Bezpieczeństwa



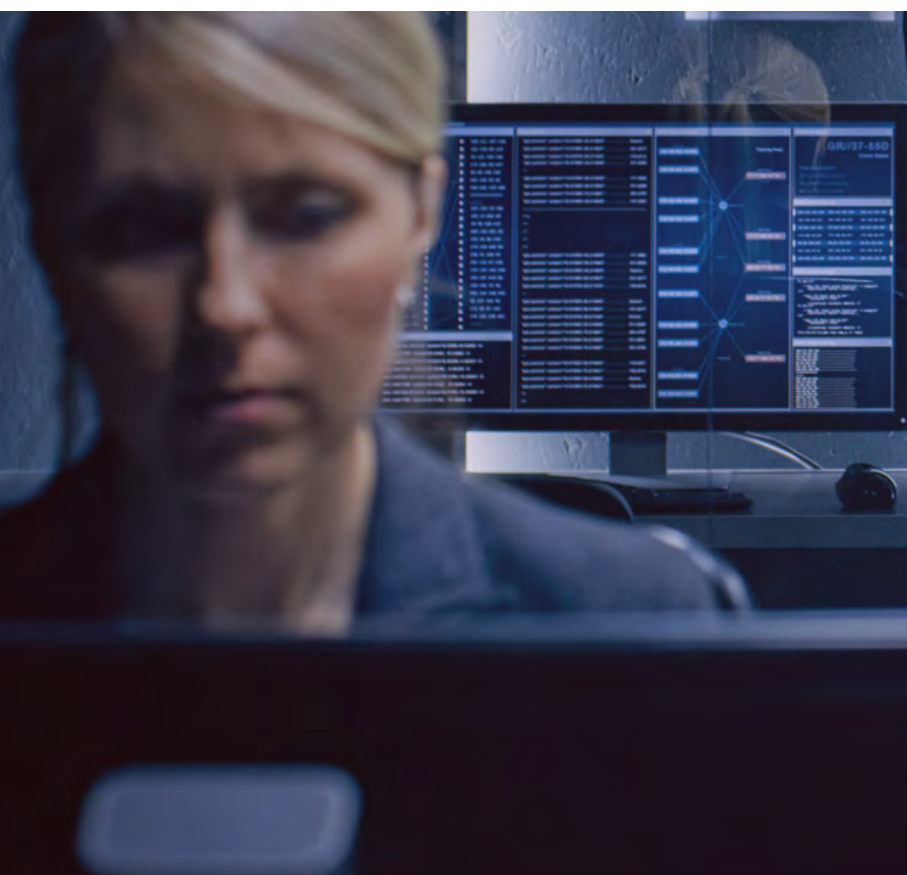


# ZAROBKI W SEKTORACH SECURITY & AI

---



Tomasz Wija  
No Fluff Jobs



**Specjaliści i specjalistki zajmujący się Security oraz AI mogą liczyć na jedno z najwyższych zarobków w branży. Według raportu „Rynek pracy IT w 2022 roku” opublikowanego przez No Fluff Jobs wynika, że AI znalazło się na trzecim miejscu, a Security na czwartym pod względem oferowanego wynagrodzenia w ubiegłym roku.**

## POTRZEBY REKRUTACYJNE

No Fluff Jobs podsumował miniony rok. W ubiegłym roku na portalu odnotowano o 8 procent więcej ogłoszeń o pracę niż rok wcześniej. Specjaliści mówią o luce branżowej na poziomie 150 tys. osób, a zarobki w branży IT sukcesywnie idą w górę.

Mediany oferowanych wynagrodzeń w branży IT w ogłoszeniach na poziomie senior w 2022 roku oscylowały w przedziale od 18 do 25 tys. złotych netto, a na poziomie mid od 14 do 20,2 tys. złotych netto. Natomiast juniorzy mogli zarobić od 6 do 9,5 tys. złotych netto.

– Potrzeby rekrutacyjne firm w Polsce i w całym regionie Europy Środkowo-Wschodniej są wysokie. Nawet w czasie doniesień z Zachodu o zwolnieniach lub wstrzymaniu nowych zatrudnień sytuacja w naszej części kontynentu niewiele się zmienia. Pracodawcy(-czynie) wciąż potrzebują wykwalifikowanych specjalistów(-tek) IT, luka kadrowa powiększa się wraz z kolejnym rokiem – komentuje Tomasz Bujok, CEO No Fluff Jobs.

W 2022 roku na No Fluff Jobs opublikowanych

zostało o 8 proc. więcej ogłoszeń niż rok wcześniej. Trzy najpopularniejsze kategorie związane z programowaniem (Backend, Frontend i Fullstack) tak naprawdę stanowią około połowę wszystkich ogłoszeń o pracę na rynku IT. Ale na stanowiska związane z Security czy AI również poszukiwani są pracownicy i to ze stawkami niewiele niższymi.

## WYNAGRODZENIA DO GÓRY

Mediany oferowanych wynagrodzeń w ogłoszeniach na poziomie senior w 2022 roku wzrosły o 19 procent w stosunku do 2021 roku zarówno w medianie dolnych, jak i górnych widełek. Mediany oferowanych wynagrodzeń w ogłoszeniach na poziomie mid w 2022 roku wzrosły o 17 proc. w stosunku do 2021 roku w medianie dolnych i 12 proc. w medianie górnych widełek.

Mediany oferowanych wynagrodzeń w ogłoszeniach na poziomie junior w 2022 roku oscylowały wzrosły o 8 procent.

Najwyższe zarobki przy B2B niezmiennie odnotowano w kategoriach: DevOps (19-26,9 tys. złotych +VAT), Big Data (19,6-26,7 tys. zł

Najwyższe zarobki przy umowie o pracę odnotowano w kategoriach między innymi AI i Security (14-20 tys. złotych brutto).

– Z roku na rok w topie najlepiej opłacanych kategorii są Big Data, DevOps, Security oraz AI. Zwłaszcza w tym ostatnim obszarze możemy zaobserwować ogromny postęp zarówno w liczbie nowopowstających rozwiązań AI (np. Chat-GPT, Lensa), jak i w pojawiających się stanowiskach. To nowy, gorący trend na całym świecie, a specjaliści(-tki) od sztucznej inteligencji, machine learningu i NLP są teraz rozchwytywani(-e) na rynku pracy. To oznacza też, że rosną nie tylko liczba ogłoszeń we wspomnianych kategoriach, lecz przede wszystkim stawki, jakie dziś trzeba zapłacić, by pozyskać topowych(-e) specjalistów(-tki) z tych dziedzin – skomentował Tomasz Bujok, CEO No Fluff Jobs.

– W 2022 roku w większości technologii w przypadku umów B2B zauważalne było, że bardziej wzrosły mediany górnych widełek niż dolnych. To oznacza nie tylko, że stawki wzrosły ogółem, lecz także, że częściej szukano osób o wyższym poziomie doświadczenia oraz pracodawcy(-czynie) byli skłonni płacić coraz większe kwoty za najlepsze talenty. Ten trend jeszcze będzie się nasilał przy zwiększonym zapotrzebowaniu na doświadczonych osoby – dodała Magdalena Gawłowska-Bujok, COO No Fluff Jobs.





## SECURITY ORAZ AI

Na jedne z najwyższych zarobków w branży mogą liczyć specjaliści i specjalistki zajmujący się Security oraz AI. Według raportu „Rynek pracy IT w 2022 roku” opublikowanego przez No Fluff Jobs wynika, że AI znalazło się na trzecim miejscu, a Security – na czwartym pod względem oferowanego wynagrodzenia w ubiegłym roku.

Udział procentowy ogłoszeń w kategorii AI wzrósł o 19% w ciągu roku, a w kategorii Security – 14%.

## TECHNOLOGIA ZAGROŻENIEM DLA JUNIORÓW?

Systemy sztucznej inteligencji jak ChatGPT oraz inne podobne narzędzia są rozwijane od wielu lat. Na ten moment, pomimo szerokiego udostępnienia tego narzędzia, uważamy, że juniorzy i juniorki w sektorze IT nie powinni czuć się zagrożeni.

Potencjalne zastępstwo stanowisk pracy przez modele językowe w pierwszej kolejności może mieć miejsce w branżach poza IT, szczególnie w rolach opartych na tworzeniu treści. Według danych z raportu No Fluff Jobs „Rynek pracy IT w 2022” udział ogłoszeń o pracy dla początkujących w branży oscylował na poziomie blisko 20% (12 punktów procentowych więcej niż rok wcześniej). Na razie jest za wcześnie, by wyrokować, czy ten pozytywny trend się utrzyma w 2023 roku, gdyż aktualna sytuacja makroekonomiczna krótkoterminowo może mieć większy wpływ na obniżenie zapotrzebowania na takie stanowiska.

Paradoksalnie rozwój tak zaawansowanych technologii, jak sztuczna inteligencja czy uczenie maszynowe, może mieć pozytywny wpływ na rynek pracy IT. Co prawda, w pierwszej kolejności firmy najczęściej szukają doświadczonych osób, natomiast w obliczu istniejącej luki kadrowej organizacje powinny inwestować także w rozwój juniorów(-ek), którzy przecież

z czasem awansują na wyższe stanowiska.

Natomiast masowe zastąpienie programistów(-ek) przez narzędzia automatycznego generowania tekstu AI np. do pisania kodu, na chwilę obecną wydaje się melodią przyszłości.







**/GDPSYSTEM.EU**

# ZGODA NA COOKIES

Czy Twoja strona WWW spełnia wymogi prawne i daje  
możliwość elastycznego zarządzania cookies osobom,  
które ją odwiedzają?

**SPRAWDŹ**

**SPEŁNIJ  
WYMOGI  
PRAWNE**



# PIĘĆ TRENDÓW W CYBERSECURITY W 2023



Redakcja  
SECURITY MAGAZINE

we współpracy z



**Cyberprzestępcy wciąż wymyślają nowe taktyki oraz techniki ataków. Aby skutecznie reagować, konieczne jest określenie, co naprawdę ma znaczenie, i skoncentrowanie się na ochronie najbardziej krytycznych zasobów.**

**W tym wydaniu już po raz ostatni przyglądamy się, co, według naszych ekspertów, może mieć w tym roku znaczenie i na czym należałoby się skupić w temacie cyberbezpieczeństwa.**

W grudniowym i styczniowym wydaniu szczegółowo wraz z naszymi ekspertami przyglądaliśmy się, jakie w tym roku branżę cybersecurity czekać wyzwania, jakie będą priorytety oraz na co, w kontekście cyberprzestępstw, będą musiały zwrócić uwagę działy bezpieczeństwa w firmach i administracji.

## PIĘĆ TRENDÓW WEDŁUG BARRACUDA NETWORKS

Tym razem to eksperci Barracuda Networks, firmy dostarczającej rozwiązania z obszaru bezpieczeństwa IT, przeanalizowali zachowania cyberprzestępców w 2022 roku i wytypowali zagrożenia, z którymi z największym prawdopodobieństwem będą mierzyć się organizacje w 2023 roku.

Jak wskazali, rok 2022 rok pokazał, że cyberzagrożenia nie mają granic, a świat jest na nie bardzo podatny. Obserwacja i analiza tego, co się wydarzyło, pozwoli organizacjom lepiej przygotować się do tego, co przyniesie przyszłość.

- W 2023 roku wszystkie organizacje – niezależnie od wielkości i w jakim sektorze działają – muszą być gotowe na cyberataki. Powierzchnia ataku wciąż się rozszerza, bo przedsiębiorstwa i instytucje dodają do swojej infrastruktury coraz więcej urządzeń, korzystają z ciągle rosnącej liczby usług w chmurze, kontynuują też pracę zdalną. To wszystko sprawia, że firmy muszą ponownie przemysleć kwestie bezpieczeństwa. Przez lata podstawowym



celem bezpieczeństwa było utrzymywanie złośliwego oprogramowania i napastników z dala od naszej sieci. Teraz musimy również przygotować się na sytuację, w której cyberprzestępca do niej przeniknie, i wiedzieć, jak wtedy zareagujemy – powiedział Mateusz Ossowski, CEE Channel Manager w Barracuda Networks.

Firma wskazała pięć prognozowanych trendów w zakresie cyberzagrożeń, na które organizacje muszą być gotowe w 2023 roku.

## **Coraz więcej podatności zero-day**

W 2022 roku zarejestrowano 21 000 nowych podatności. Wiele z nich zostało sklasyfikowanych jako "krytyczne", wiele było aktywnie wykorzystywanych przez atakujących. Organizacje muszą mieć zespół gotowy do łatania oprogramowania i usuwania błędów tak szybko, jak to możliwe.

## **Kradzież danych uwierzytelniających**

Przejmowanie kont nadal jest jednym z głównych celów atakujących i najważniejszym ryzykiem dla organizacji. Skradzione poświadczenia otwierają drzwi do zdalnego dostępu do

sieci organizacji, poczty elektronicznej czy korporacyjnych aplikacji internetowych przechowujących dane klientów. Cyberprzestępcy wykorzystują phishing, smishing i inne taktyki socjotechniczne, by nakłonić pracowników do otwarcia niebezpiecznych załączników lub podania danych uwierzytelniających do kont i systemów. Techniki podszywania się stale ewoluują, a wraz z postępującym zmęczeniem wieloskładnikowym uwierzytelnianiem (MFA) – odnoszą coraz większy sukces.

## **MFA nie jest odpowiedzią na wszystkie problemy**

Rok 2022 był rokiem, który pokazał, że MFA nie jest odpowiedzią na wszystkie problemy związane z bezpieczeństwem. Rosła łatwość ataków wykorzystujących zmęczenie uwierzytelnianiem dwu- i wieloskładnikowym. Dlatego w 2023 roku można spodziewać się wprowadzenia technologii bezhasłowej oraz technologii klucza bezpieczeństwa FIDO U2F (Universal 2nd Factor).

## **Ransomware nadal groźne**

Rok 2022 był pierwszym, w którym zaobserwowano ukierunkowane ataki ransomware na





osoby fizyczne w oparciu o ich osobiste profile w mediach społecznościowych. Wszystko wskazuje na to, że w 2023 roku przedsiębiorstwa i instytucje nadal będą mierzyć się z tego rodzaju atakami. Model biznesowy Ransomware as a Service bardzo się rozwinął w ostatnich latach. Dziś przestępcy mogą kupić w darknecie licencje na wykorzystanie gotowego oprogramowania do szyfrowania danych i żądania okupu. Co więcej – producenci tego typu malware'u oferują także pełne wsparcie.

2022 rok przyniósł też zwiększone wykorzystanie oprogramowania wiperware. W 2023 r. wiperware pochodzący z Rosji prawdopodobnie rozprzestrzeni się na inne kraje w związku z utrzymującymi się napięciami geopolitycznymi.

## **Ataki na łańcuchy dostaw**

2022 był rokiem ataków na łańcuchy dostaw, które są dziś coraz bardziej złożone i zintegrowane. Atakujący szukają najsłabszego ogniwa w takim łańcuchu i atakują je, by dostać się do sieci ich dostawców lub klientów.

- Na koniec dnia to i tak pracownik otwiera załącznik, który nie jest tym, czym się wydaje. Kluczowe jest więc dziś nieustające szkolenie pracowników. Liczba zagrożeń rośnie, krajobraz cyberbezpieczeństwa wciąż się zmienia. Nie wystarczy inwestować w technologie. Du-

zo uwagi trzeba poświęcić też tym, którzy z tej technologii na co dzień korzystają – podsumowuje Mateusz Ossowski z Barracuda Networks.

## TRENDY 2023 WEDŁUG SECFENCE

Jeszcze kilka lat temu mówiono, że jeśli cyberprzestępczość byłaby państwem, to znalazłaby się na 13. miejscu w rankingu gospodarek mierzonych wskaźnikiem produktu krajowego brutto. Statystyki z 2021 r. wskazują, że w zaledwie kilka lat cyberprzestępczość wzbiła się w rankingu o 10 miejsc do góry i obecnie jest na 3 miejscu, zaraz po ekonomiach USA i Chin.

### To nasza bitwa

Cyberbezpieczeństwo wcale nie jest bitwą między cyberprzestępcami a ekspertami ds. bezpieczeństwa. Faktycznie, czasami zagrożenia pochodzą od wrogich państw lub przebiegłych i obeznaných z technologią intruzów, ale w rzeczywistości najczęściej problemy wynikają ze źle zabezpieczonych sieci i aplikacji.

Na ataki narażają firmy ich nieostrożni pracownicy, którzy korzystają z niezabezpieczonych

urządzeń, np. podczas pracy z domu. Często też intruzi dostają się do zasobów organizacji, stosując podstęp i wykorzystując roztargnienie, zmęczenie użytkowników. Tak było niedawno w przypadku Ubera, który padł ofiarą tzw. bombardowania MFA (MFA Prompt Bombing lub MFA Fatigue), ponieważ stosował – jak się okazuje – słabe uwierzytelnianie polegające na powiadomieniach push.

### Konieczność na 2023

W tym roku temat ochrony i zabezpieczenia użytkowników i aplikacji silnym, wieloskładnikowym uwierzytelnianiem będzie więc nie tylko trendem, a koniecznością. Wszystkie organizacje bowiem, którym zależy na najwyższym poziomie bezpieczeństwa, muszą nie tylko mieć włączone MFA na każdej aplikacji, ale przede wszystkim powinny zrezygnować z półśrodków i zastąpić je metodami dużo doskonalszymi i dającymi prawdziwą ochronę przed phishingiem i bombardowaniem MFA.

Mowa tu o uwierzytelnianiu opartym na standardzie FIDO2, czyli metodzie uwierzytelniania z wykorzystaniem nowoczesnej odmiany biometrii twarzy lub kciuka lub fizycznych kluczy

kryptograficznych FIDO2/U2F.

Implementacja dobrych i skutecznych metod uwierzytelniania na szeroką skalę powinna utrudnić „pracę” intruzom, którzy czerpią dziś ogromne zyski z kradzieży tożsamości w sieci.

## PIĘĆ TRENDÓW WEDŁUG NETWRIX

Amerykańska firma Netwrix, tworząca oprogramowania dotyczące ochrony wrażliwych danych, wykrywania ataków, reagowania na nie, również podzieliła się swoimi spostrzeżeniami dotyczącymi trendów w cyberbezpieczeństwie, które będą miały wpływ na organizacje w 2023 roku.

Dirk Schrader, wiceprezes ds. badań nad bezpieczeństwem i Michael Paye, wiceprezes ds. badań oraz rozwoju, opierając się na globalnym doświadczeniu Netwrix, w tym technologii, finansów, produkcji, administracji i opieki zdrowotnej dokonali analizy, dochodząc do wniosku, że cyberprzestęp-

czość to biznes: profesjonalni napastnicy będą coraz częściej atakować użytkowników i łańcuchy dostaw w celu infiltracji organizacji. Oto pięć konkretnych trendów na rok 2023 według Netwrix.

### **Biznes cyberprzestępczości ulegnie dalszej profesjonalizacji**

Powrót odmian złośliwego oprogramowania, takich jak Emotet, Conti i Trickbot, wskazuje na ekspansję cyberprzestępczości najemnej. W szczególności rozwój ransomware-as-a-service umożliwia przestępcom nieposiadającym większych umiejętności technicznych zarabianie pieniędzy poprzez wymuszanie okupu za klucze do odszyfrowania lub sprzedaż skradzionych danych w darknecie lub konkurentom ofiary.

W związku z tym organizacje powinny spodziewać się wzrostu liczby kampanii phishingowych. Kluczowe strategie obronne obejmują terminowe instalowanie poprawek i aktualizowanie oprogramowania, a także blokowanie dostępu do sieci za po-

# CYBERSECURITY



mocą rozwiązań do uwierzytelniania wieloskładnikowego (MFA) i zarządzania dostępem uprzywilejowanym (PAM).

## **Ataki na łańcuch dostaw**

Nowoczesne organizacje opierają się na złożonych łańcuchach dostaw, w tym małych i średnich przedsiębiorstwach (SMB) oraz dostawców usług zarządzanych (MSP).

Przeciwnicy będą w coraz większym stopniu atakować tych dostawców, a nie większe przedsiębiorstwa, wiedząc, że zapewniają oni ścieżkę do wielu partnerów i klientów. Aby zaradzić temu zagrożeniu, organizacje różnej wielkości podczas przeprowadzania oceny ryzyka, muszą wziąć pod uwagę luki w zabezpieczeniach wszelkiego oprogramowania lub oprogramowania układowego innych firm.

## **Braki kadrowe zwiększą rolę partnerów dystrybucyjnych**

Zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa znacznie przewyższa podaż. Ten niedobór talentów w zakresie cyberbezpieczeństwa zwiększy ryzyko dla firm, ponieważ ataki stają się jeszcze bardziej wyrafinowane.

Aby sprostać temu wyzwaniu, organizacje będą w większym stopniu polegać na swoich zaufanych partnerach w zakresie bezpieczeństwa, takich jak partnerzy dystrybucyjni, integratorzy systemów, MSP i MSSP.



## Czynnik ludzki

Użytkownicy od dawna są najsłabszym ogniwem w bezpieczeństwie IT, skłonni do otwierania zainfekowanych załączników wiadomości e-mail, klikania złośliwych łączy i innych ryzykownych zachowań. Obecnie szybki postęp w inżynierii społecznej i łatwa w użyciu technologia głębokiego fałszowania umożliwiają atakującym oszukać większą liczbę użytkowników, aby dali się nabrać na ich schematy.

W związku z tym kompleksowy audyt aktywności użytkowników stanie się jeszcze ważniejszy, jeśli chodzi o wykrywanie nieprawidłowych zachowań na czas i zapobieganie poważnym incydentom. Ponadto wdrożenie podejścia opartego na zerowych uprawnieniach (ZSP) pomoże organizacjom zapobiegać nadużyciom ich najpotężniejszych kont, zarówno w sposób niezamierzony przez ich właścicieli, jak też przez przeciwników, którzy je skompromitują.

## Konsolidacja dostawców będzie nadal nabierać tempa

Aby zwalczać cyberprzestępczość, organizacje nieustannie inwestują w bezpieczeństwo IT. Ale więcej narzędzi nie zawsze oznacza lepsze bezpieczeństwo — punktowe rozwiązania różnych dostawców działają oddzielnie, oferują nakładające się lub sprzeczne funkcje i wymagają od organizacji pracy z wieloma zespołami wsparcia.

Aby zminimalizować luki w zabezpieczeniach spowodowane tą złożonością, organizacje starają się teraz zbudować architekturę bezpieczeństwa z wybraną, mniejszą grupą zaufanych dostawców, która oferuje dodatkową korzyść w postaci obniżonych kosztów dzięki cenom lojalnościowym. To z kolei prowadzi do szybszego zwrotu z inwestycji (ROI), co ma coraz większe znaczenie w obecnym klimacie gospodarczym.



## **BARTOSZ BAZIŃSKI**

współzałożyciel i COO  
SentiOne



## **MARCIN ZAGÓRSKI**

podkomisarz  
Centralne Biuro Zwalczania  
Cyberprzestępczości



## **KRIS DURSKI**

Founder i dyrektor ds. technologii  
Vault Security



## **PIOTR NOWAK**

dziennikarz technologiczny



Programista, przedsiębiorca, pasjonat wdrażania innowacyjnych technologii do świata biznesu. Od 2011 roku kieruje rozwojem narzędzia do monitoringu internetu i automatyzacji obsługi klienta - SentiOne.

Oficer Policji w stopniu podkomisarza. Odpowiada za kontakty z mediami i udzielanie odpowiedzi na zapytania prasowe. Aktualnie w Zespole Prasowym Centralnego Biura Zwalczania Cyberprzestępczości, od stycznia 2018 roku do lipca 2022 roku oficer prasowy Komendanta Powiatowego Policji w Mińsku Mazowieckim.

Starszy analityk oprogramowania, programista, menedżer z ponad 20-letnim doświadczeniem w developingu i marketingu oprogramowania. Opracował koncepcję spersonalizowanego bezpieczeństwa w celu ochrony zasobów cyfrowych i materialnych. Współtworzył kilka start-upów z branży medycznej, technologii informacyjnej i cyberbezpieczeństwa.

Dziennikarz zajmujący się tematyką technologiczną. Śledzi działania cyberprzestępców, analizuje rozwiązania zabezpieczające infrastrukturę krytyczną. Chmury obliczeniowe nie mają dla niego żadnych tajemnic. Publikuje m.in. w Rzeczpospolitej, Dzienniku Gazecie Prawnej i Logistyka24.



**ADAM GOLA**

Security Specialist  
The Software House



Od 2016 związany z szerokopojętą jakością, główny nacisk stawiając na cyberbezpieczeństwo. Oprócz wykonywania Vulnerability Assessment i dbania o bezpieczeństwo organizacji, aktywnie udziela się na największych konferencjach w Polsce, tworzy kursy i szkolenia oraz dzieli się wiedzą w social mediach.

**PAWEŁ KACZMARZYK**

Prezes Zarządu  
Serwis komputerowy Kaleron



Prezes i technik w serwisie komputerowym Kaleron sp. z o. o. Specjalizuje się w odzyskiwaniu danych i naprawach elektronicznych urządzeń komputerowych, a także prowadzi szkolenia w tym zakresie.

**TOMASZ WIJA**

Chief Growth Officer  
No Fluff Jobs



Przez 13 lat pracował w Chatham Financial, największej na świecie firmie doradczej zajmującej się ryzykiem finansowym. Obecnie wspiera prorozwojowe inicjatywy No Fluff Jobs w Polsce i za granicą. Uwielbia wszelkie aktywności związane z górami.

**TOMASZ KOWALSKI**

CEO i współzałożyciel  
Secfense



CEO i współzałożyciel firmy z branży cybersecurity Secfense. Posiada ponad 20-letnie doświadczenie w sprzedaży technologii IT, brał udział w setkach wdrożeń sprzętu i oprogramowania w dużych i średnich firmach z sektora finansowego, telekomunikacyjnego, przemysłowego i wojskowego.

## ROCKET SCIENCE COMMUNICATIONS

AGENCJA PUBLIC RELATIONS  
M.IN. DLA IT I TECHNOLOGII



## PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW  
Z DZIENNIKARZAMI



## POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY  
O BEZPIECZEŃSTWIE FIRM



## RZETELNY REGULAMIN

BLOG POŚWIĘCONY  
POLSKIEMU E-COMMERCE



Polityka<sup>®</sup>  
Bezpieczeństwa



Rzetelny<sup>®</sup>  
Regulamin

# ZOBACZ WYDANIA

Wydanie 1/2022

**POBIERZ**



Wydanie 2/2022

**POBIERZ**



Wydanie 3/2022

**POBIERZ**



Wydanie 4/2022

**POBIERZ**



Wydanie 5/2022

**POBIERZ**



Wydanie 6/2022

**POBIERZ**



Wydanie 7/2022

**POBIERZ**



Wydanie 8/2022

**POBIERZ**



Wydanie 9/2022

**POBIERZ**



Wydanie 1(10)/2023

**POBIERZ**





**Wydawca:****Rzetelna Grupa sp. z o.o.**

al. Jana Pawła II 61 lok. 212  
01-031 Warszawa

KRS 284065

NIP: 524-261-19-51

REGON: 141022624

Kapitał zakładowy: 50.000 zł

Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy  
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

**Redaktor Naczelny: Rafał Stępniewski**

Redakcja: Monika Świetlińska, Damian Jemioło, Anna Petynia-Kawa  
Projekt, skład i korekta: Monika Świetlińska

**Wszelkie prawa zastrzeżone.**

**Współpraca i kontakt: [redakcja@securitymagazine.pl](mailto:redakcja@securitymagazine.pl)**

Publikacja w całości jak i każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia Rzetelna Grupa sp. z o.o. z siedzibą w Warszawie. Wszelkie znaki towarowe, nazwy własne, logotypy oraz znaki graficzne i inne treści są chronione prawem autorskim.

Redakcja ma prawo do korekty i edycji nadesłanych materiałów celem dostosowania ich do wymagań pisma.





[SECURITYMAGAZINE.PL](http://SECURITYMAGAZINE.PL)