



04/2022

# SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

## **Pułapki** **gotowych rozwiązań IT**

**Korzyści kontrolowanych**  
**ataków hakerskich**

**Nie dbasz o cyberbezpieczeństwo?**  
**B2G nie będzie z Tobą współpracować**

**Zagrożenia związane**  
**z nielojalnością pracowników**

**Które startupy pomogą Ci**  
**zwiększyć bezpieczeństwo w Twojej firmie?**

# SPIS TREŚCI

Jak technologia pomaga agrobiznesowi i chroni przed cyberatakami?	4
Które startupy pomogą Ci zwiększyć bezpieczeństwo w Twojej firmie?	12
Dane medyków także trzeba chronić	18
Korzyści kontrolowanych ataków hakerskich	25
Nie dbasz o cyberbezpieczeństwo? B2G nie będzie z Tobą współpracować	32
Jak sprawdzić czy Twoja strona www jest bezpieczna?	39
Pułapki gotowych rozwiązań IT	45
Zagrożenia związane z nielojalnością pracowników	56
Biznesowe social media pod ostrzałem hakerów. Jak unikać wycieków?	68
Bezpieczeństwo danych w wiadomościach e-mail	85
Ekspertcy wydania i partnerzy	90

## SZANOWNI PAŃSTWO,

Coraz częściej współpracą z naszą redakcją zainteresowani są specjaliści zagraniczni. Bardzo nas to cieszy, bo dla naszych Czytelników to niezwykła, wręcz unikatowa szansa na doświadczenie, jak poza Polską podchodzi się do tematyki szeroko rozumianego bezpieczeństwa w firmach. Czy na przykład stosujemy te same narzędzia do ochrony danych, czy podobnie rozumiemy ten temat i czy ma dla nas takie samo znaczenie, a nawet czego możemy się nauczyć na bazie doświadczeń ekspertów od bezpieczeństwa z zagranicy.

Prawdopodobnie z najprężniej rozwijającą się branżą security mamy do czynienia za naszą wschodnią granicą. Ukraina nadal walczy, nie tylko militarnie. Każdy dzień to walka o przetrwanie również firm, które napędzają gospodarkę. Jak sobie radzą? Jaką naukę mają dla nas? Zachęcamy naszych wschodnich przyjaciół do współpracy, a tym, którzy już ją rozpoczęli - dziękujemy za zaufanie.

Zapraszam do lektury.

*Rafał Slepniowski*





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

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



**ZAPISZ SIĘ**

**NEWSLETTER**



YOUR EMAIL HERE

**SUBSCRIBE**



# NASIONA, MULCZ I CYBEROBRONA: JAK TECHNOLO- GIA POMAGA AGROBIZNESOWI I CHRONI PRZED CYBERATAKAMI



Dmytro Lennyi  
Intellias



Cyfryzację można nazwać trzecią rewolucją w agrobiznesie. Technologia pomaga rolnikom zdalnie monitorować, analizować i prognozować plony, efektywnie wykorzystywać wodę, mulcz i pestycydy i nie tylko. Jednak wraz z korzyściami płynącymi z cyfryzacji, agrobiznes napotyka również zagrożenia cybernetyczne. A dzisiaj cyberbezpieczeństwo jest stałym i niezbędnym atrybutem jakości w agrobiznesie.



Dziś agrobiznes stoi u progu trzeciej rewolucji. Pierwsza rozpoczęła się wraz z wprowadzeniem zmechanizowanej pracy, kiedy konie zostały zastąpione traktorami. Drugą rewolucją był rozwój bioinżynierii. Korzystając z modyfikacji genetycznej lub konwencjonalnej selekcji, naukowcy byli w stanie uzyskać produkty hybrydowe, które rosną w nietypowych warunkach. Cyfryzację można nazwać trzecią rewolucją w agrobiznesie.

## **AGROBIZNES I CYBER- BEZPIECZEŃSTWO: DLACZEGO TO MA ZNACZENIE?**

Rolnicy to w większości ludzie konserwatywni. Są przyzwyczajeni do korzystania z warunkowego Excela i niechętnie przechodzą na nowe technologie. Pandemia koronawirusa była silnym impulsem do cyfryzacji agrobiznesu.

**NA RYNKU ISTNIEJĄ OBECNIE ROZWIĄZANIA CYFROWE, KTÓRE MOGĄ CZĘŚCIOWO LUB CAŁKOWICIE ZASTĄPIĆ KSIĘGOWYCH I ROLNIKÓW LUB UMOŻLIWIĆ IM EFEKTYWNE ZDALNE WYKONYWANIE OBOWIĄZKÓW.**

Technologia pomaga rolnikom zdalnie monitorować, analizować i prognozować plony, efektywnie wykorzystywać wodę, mulcz i pestycydy i nie tylko. Jednak wraz z korzyściami płynącymi z cyfryzacji, agrobiznes napotyka również zagrożenia cybernetyczne. A dzisiaj cyberbezpieczeństwo jest stałym i niezbędnym atrybutem jakości w agrobiznesie.

W tym czasie rolnicy musieli zająć się dwoma powiązаныmi ze sobą kwestiami: zmniejszeniem kosztów produkcji i wprowadzeniem narzędzi do pracy zdalnej. W obu przypadkach rozwiązaniem była technologia cyfrowa. W końcu na rynku istnieją obecnie rozwiązania cyfrowe, które mogą częściowo lub całkowicie zastąpić księgowych i rolników lub umożliwić im efektywne zdalne wy-





konywanie obowiązków. W ten sposób rolnicy mogli obniżyć koszty i zoptymalizować zasoby. W dzisiejszych czasach coraz więcej przedsiębiorstw rolnych zaczyna wykorzystywać cyfrowe systemy i aplikacje w swojej codziennej pracy.

Jedną z największych zalet technologii jest efektywne gospodarowanie zasobami. Na przykład rolnictwo jest największym na świecie użytkownikiem słodkiej wody. Według raportu McKinsey, w 2030 roku zapotrzebowanie na słodką wodę przekroczy dostępne zasoby o 40%. Jednak przy pomocy technologii rolnictwo może obliczyć optymalne wykorzystanie wody, co jest niezwykle ważne nie tylko z punktu widzenia oszczędności, ale także zachowania ekosystemów słodkowodnych.

Ponadto technologia pomaga w optymalnym wykorzystaniu pestycydów, zbliżając rolnictwo do koncepcji „precyzyjnego biznesu”. Na przykład rolnik traktuje swoją ziemię chemią, a za godzinę zaczyna się ulewa, która spłukuje je do wód gruntowych lub rzeki. Można tego uniknąć, stosując technologię i analizę. Można dokładnie obliczyć, kiedy, gdzie i w jakiej ilości stosować pestycydy, aby były jak najbardziej skuteczne



i powodowały jak najmniejsze szkody w środowisku. Eksperci szacują, że optymalizacja zasobów i wykorzystanie „inteligentnych” technologii, takich jak sztuczna inteligencja lub powiązane czujniki, może zwiększyć rentowność globalnego przemysłu rolnego o 500 miliardów dolarów do 2030 roku.

Cyfrowe systemy zarządzania dla agrobiznesu to rodzaj super dashboardu z dużą ilością ważnych danych. Oto dane z satelitów, stacji meteorologicznych i sprzętu rolniczego, takiego jak najnowsze kombajny John Deer, które są w pełni zintegrowane z aplikacją. Te zagregowane informacje sprawiają, że agrobiznes jest skuteczny. Jednocześnie utrata tych informacji to duże ryzyko dla firm.

Kradzież danych osobowych to jedno z najczęstszych cyberprzestępstw. Każdego dnia firmy tracą około 4 mln plików danych osobowych. Na przykład w maju 2020 r. osoby atakujące zaatakowały Harvest Sherwood Food Distributors i ukradły 2600 plików z analizą finansową, danymi dostawców i klientów, żądając okupu w kryptowalucie. Takie cyberataki mają poważne konsekwencje dla agrobiznesu, gdyż dla rolnictwa ważna jest pewna dziedziczność i chronologia historyczna danych.

To dzięki wstępnym informacjom o osobliwościach przechowywania lub sadzenia niektórych roślin powstają najlepsze praktyki ich przyszłej uprawy. Ponadto osoby atakujące mogą sprzedawać dane osobowe, ukrywając je jako informacje „wewnętrzne”. Może to spowodować duże wahania na giełdzie, a także doprowadzić do znacznych strat finansowych, a nawet bankructwa poszkodowanej firmy. Tym samym ochrona systemów cyfrowego agrobiznesu jest priorytetem dla każdego nowoczesnego rolnika czy agroholdingu.



## **CZYNNIK LUDZKI JEST GŁÓWNYM ZAGROŻENIEM DLA CYFROWEGO AGROBIZNESU**

W Intellias mamy zespół ds. cyberbezpieczeństwa. Zajmuje się budowaniem systemów zintegrowanych, gdy bezpieczeństwo jest kluczowe dla klienta. Jednym z naszych projektów dla Agri-Tech było stworzenie systemu IoT dla pionowej farmy.

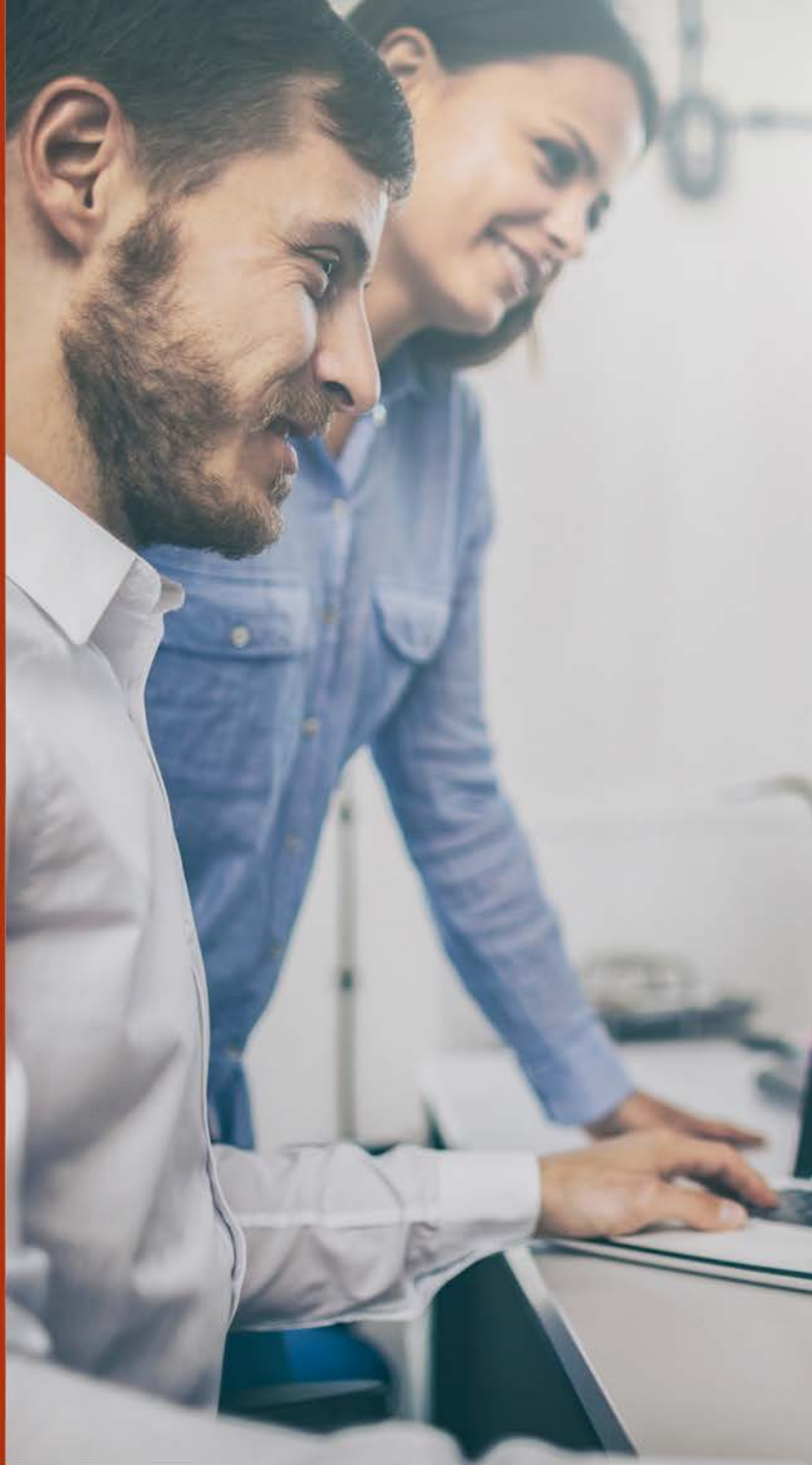
Zazwyczaj systemy IoT muszą być wystarczająco otwarte, aby obsługiwać wymaganą liczbę czujników, które stale przesyłają dane o stanie upraw. System IoT może być w 100% zautomatyzowany i w pełni kontrolować proces, od ogrodnictwa, podlewania, nawożenia i zbioru, po ważenie i pakowanie. Ale taka otwartość czyni go podatnym na cyberataki.

Po pracy nad frameworkiem IoT, Dział Bezpieczeństwa Intellias zaczął testować go pod kątem wytrzymałości. Proces ten obejmuje testy penetracyjne, testy fuzzingu i nie tylko. Jednym z najważniejszych aspektów weryfikacji systemu jest celowe przeciążanie. W końcu większość błędów pojawia się, gdy system jest przeciążony.

Dodatkowo zagrożeniem dla systemu są niebezpieczne moduły open source. Na przykład w NPM (Node Package Manager) istniał niezwykle prosty i popularny moduł, z którego korzystało wiele firm. W pewnym momencie twórca tego modułu usunął go, a systemy, w których został zintegrowany, stały się niesprawne.







Jednak największym zagrożeniem dla systemu jest czynnik ludzki, ponieważ to właśnie dzieje się z około 80% cyberprzestępczości. Tak, atakujący mogą ukraść słabe hasło lub klucze, które były niewłaściwie przechowywane w publicznym repozytorium. Dlatego stworzenie niezawodnego systemu, który uwzględni wszystkie powyższe podatności i jest główną cechą produktu wysokiej jakości.

## **JAK ZBUDOWAĆ BEZPIECZNY SYSTEM**

Bezpieczeństwo systemu oznacza jego poufność, integralność, niezawodność, autentyczność i rozliczalność. Te zasady bezpieczeństwa określamy na samym początku rozwoju systemu. Jednocześnie wdrażamy GitOps, aby zapewnić przestrzeganie tych zasad.

GitOps to zestaw praktyk, który pozwala śledzić wszystkie zmiany w systemie i odmawia dostępu do publicznego środowiska produktu każdemu poza Git.

Proces jest następujący. Żądasz pewnych zmian w systemie, GitOps je zbiera, następnie te zmiany przechodzą serię kontroli, po czym zebrane i przetestowane żądanie jest wysyłane do ciągłej integracji (CI, Continuous Integration). I dopiero po pełnej weryfikacji żądanie jest aktualizowane na środowisku produkcyjnym. Uniemożliwia to osobom z zewnątrz – nawet twórcom projektów – interweniowanie i dokonywanie nieautoryzowanych zmian w systemie.

Uwierzytelnianie dwuskładnikowe to kolejny poziom bezpieczeństwa. Dzięki niemu chronimy w szczególności konta DevOps, które wypuszczają produkty cyfrowe i mają dostęp do środowiska produkcyjnego. Korzystamy również z różnorodnych narzędzi, które wykonują statyczną lub dynamiczną analizę kodu. Ich głównym celem jest identyfikacja potencjalnych zagrożeń, takich jak błędy programistów, które zagrażają systemowi.

Ponadto zawsze używamy kluczy, które zostały wygenerowane w bezpieczny sposób i które są przechowywane w bezpiecznych repozytoriach. Oznacza to, że tylko maszyna wirtualna ma dostęp do klucza, do którego programiści nie mają dostępu. Innymi słowy, programiści nie mogą, jak poprzednio, wejść do magazynu kluczy pod przykrywką maszyny wirtualnej.

Przecież w praktykach GitOps maszyna wirtualna generuje klucze dla siebie, tylko ona ma do nich dostęp i dzięki tym kluczom może uzyskać dostęp do bazy danych i dokonywać zmian.

Generalnie system jest tak zbudowany, że mimo złożonego procesu wprowadzania zmian, dodatkowo sprawdzamy każdą zmianę, czyniąc proces jeszcze bardziej złożonym. Gdyby cyberprzestępcy w jakiś sposób dostali się do tego systemu, musieliby przepisać 20% całej aplikacji i poświęcić pół roku na wprowadzanie zmian. Musieliby najpierw dobrze zrozumieć system, następnie napisać go od nowa, a następnie sprawić, by środowisko produkcyjne zaakceptowało ich żądania i zmieniło infrastrukturę. A to jest prawie nierealne.

Zatem tworzenie bezpiecznego systemu dla agrobiznesu zaczyna się od zakorzenienia zasad bezpieczeństwa w infrastrukturze. Następnie do produktu dodawane są praktyki CI/CD oraz weryfikacja kodu. Wszystko to kończy się wdrożeniem mechanizmów bezpieczeństwa w rozwoju. I oczywiście po tym ponownie sprawdzamy, czy wszystkie nasze narzędzia bezpieczeństwa działają. W efekcie mamy system, który może zwiększyć efektywność agrobiznesu i przeciwdziałać cyberatakam.



W TWOJEJ FIRMIE  
ZDARZYŁ SIĘ

# WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC  
**SPRAWDŹ JAK**



Polityka®  
Bezpieczeństwa

# KTÓRE STARTUPY POMOGĄ CI ZWIĘKSZYĆ BEZPIECZEŃ- STWO W TWOJEJ FIRMIE?



Redakcja  
SECURITY MAGAZINE



**Bezpieczeństwo to jedna z kluczowych kwestii w każdej firmie. Przedsiębiorstwa są narażone na ataki hakerskie, wycieki danych z dokumentacji, a nawet fizyczne uszkodzenia sprzętu. Na polskim rynku funkcjonują jednak liczne startupy, które adresują problemy bezpieczeństwa – zarówno cyfrowego, jak i fizycznego. Dowiedz się, jak ich usługi mogą wpłynąć na Twoją firmę.**



## **DOXYCHAIN ZADBA O TWOJE DOKUMENTY**

Wywodzący się z Warszawy DoxyChain to dzieło m.in. Gabriela Dymowskiego – foundera wyróżnionego w rankingu Forbes 25 under 25. Startup wyspecjalizował się w kwestii zarządzania dokumentacją i optymalizacją wszystkich procesów z nią związanych. Nazwa zapewne przywodzi Ci na myśl blockchain (sieć/łańcuch bloków) i słusznie, bo spółka faktycznie z niego korzysta. Jednak wbrew pozorom nie ma nic wspólnego z kryptowalutami czy tokenami NFT.

Blockchain od dawna wykorzystuje się do dokumentacji, potwierdzania transakcji i wielu innych. Jest to technologia, która magazynuje dane w formie jednokierunkowych zapisów określanych właśnie jako bloki (stąd „blockchain”). Dane zawarte w blockchainie są następnie kodowane przez algorytmy kryptograficzne, a cała sieć działa w sposób zdecentralizowany. Jako tako nikt nie jest właścicielem łańcucha bloków, a oszustwo jest tutaj prawie niemożliwe, bowiem każda kolejna transakcja czy zmiana są zapisywane i możliwe do odczytania przez autoryzowanych użytkowników. Praktycznie nie da się usunąć danych zapisanych w blockchainie czy ich podrobić.

Technologię tę wykorzystują zachodnioeuropejskie spółki do zawierania transakcji. Również Europejski Bank Inwestycyjny wyemitował w blockchainie Ethereum obligacje o wartości 100 mln euro. Platforma DoxyChain pozwala na tworzenie cyfrowej dokumentacji, która będzie zabezpieczona przed podrabianiem, nieautoryzowaną modyfikacją, czy po prostu zniszczeniem.

Z powodu zastosowanej technologii dokumenty mogą być jedynie aktualizowane w formie przyrostowej. Tj. pojawiania się nowych punktów, paragrafów itp. A co więcej – każda ze stron danej umowy, jest informowana o wszelkich zmianach i może je monitorować.

DoxyChain chwali się, że takie rozwiązanie pozwala na zawarcie 1250 transakcji na sekundę, o 78% skraca czas realizacji biznesowych, a także pozwala stworzyć smart kontrakty, zabezpieczać e-podpisy i wiele więcej. Z usług startupu korzystają już m.in. amerykańska korporacja technologiczna Oracle, duża krakowska kancelaria prawna Jacka Bajorka, a nawet firmy z obszaru beauty.



## **TRAPTECH POMOŻE CI ZASTAWIĆ PUŁAPKĘ NA HAKERA**

Problemy cyberbezpieczeństwa adresuje z kolei startup TrapTech. Startup z siedzibą w Stalowowolskiej Strefie Gospodarczej został założony przez Piotra Madeja, który zarówno sprzedawał produkty IT, jak i pracował jako pentester. W swojej karierze współpracował m.in. z Bankiem ING, czy wykrywał błędy w cyberzabezpieczeniach Microsoftu, czy Oracle.

Startup TrapTech to – jak twierdzi jego twórca – „cyfrowe pole minowe”, czy też system pułapek i wabików na hakerów. Rozwiązanie to określa się jako Honeypot (dosłownie garnek miodu). Dzięki temu TrapTech haker decydując się na atak, podąża za fałszywym tropem, który wydaje mu się łatwy i cenny. W rzeczywistości jednak penetruje obszar, który jest pozbawiony istotnych danych czy zasobów. To daje firmie dodatkowy czas na obronę, a także szansę na wykrycie hakera.

Co więcej – TrapTech umożliwia skonfigurowanie powiadomień, kiedy haker połknie haczyk. Dzięki temu informację o cyberataku możesz dostać nawet za pomocą SMS-a. Startup ponadto umożliwia tworzenie własnych pułapek na podstawie udostępnionego standardu. A także dąży do stworzenia społeczności specjalistów ds. cyberbezpieczeństwa, którzy tworzyliby własne wersje Honeypot sprzedawane w wewnętrznym marketplace.



## **NIGRIV – SPRAWDŹ, KTÓRY PRACOWNIK TO NAJSŁABSZE OGNIWO ZABEZPIECZEŃ**

Choć hollywoodzkie filmy czy gry komputerowe typu AAA, sugerują, że haker to niezwykle zdolny programista, który za pomocą smartfona złamie wszelkie zabezpieczenia – w rzeczywistości jest inaczej. Hakerzy w zasadzie najczęściej dopuszczają się ataków socjotechnicznych. Cyberprzestępcy doskonale wiedzą, jak manipulować ludźmi i wyłudzić od nich potrzebne dane czy informacje. Ba, nawet zmusić ich do zainstalowania szkodliwego oprogramowania.

W raporcie firmy Proofpoint pt. The Human Factor 2022 czynnik ludzki jest wskazywany jako jedna z najczęstszych przyczyn udanych cyberataków. Przykładowo 50% zagrożeń związanych z cyberprzestępczością dotyczy się kadry kierowniczej i menedżerów.

**Z raportu „Cisco Annual Cybersecurity Report” dowiadujemy się, że 22% firm utraciło klientów w wyniku cyberataku, 29% straciło przychody, a kolejne 23% wskazało, że przez hakerów ich szanse na rozwój się zmniejszyły.**







Zachariasz Kuczkowski i Łukasz Leśniewski zauważyli problem tzw. czynnika ludzkiego w cyberbezpieczeństwie i postanowili temu zaradzić. Tak w Warszawie powstał startup Nigriv, który za pomocą symulacji cyberataków pomaga zidentyfikować najsłabsze ogniwa wśród pracowników, a następnie ich edukuje. Co ważne – Nigriv działa zarówno na rynku B2B, jak i B2G, wspierając firmy prywatne i podmioty publiczne.

Cały pomysł na rozwiązanie zrodził się w ramach hackathonu, aż w końcu wyewoluował do startupu. Nigriv symuluje głównie ataki phishingowe i wykorzystuje do tego własne, stale rozwijane oprogramowanie.

### **ICSEC ZAPEWNI CI STAŁY MONITORING SIECI**

Wywodzący się z Poznania ICsec S.A. to startup, który dba o bezpieczeństwo infrastruktury przemysłowej. W spółkę zainwestował m.in. PGNiG Ventures, a ich głównymi klientami są firmy energetyczne, przemysłowe, transportowe czy górnicze. ICsec działa w obszarze bezpieczeństwa IoT (internet rzeczy), monitorowania sieci OT, detekcji anomalii w ruchu sieciowym, a nawet szkoleń i edukacji w zakresie bezpieczeństwa.

Ich główny produkt – SCADVANCE XP całodobowo monitoruje sieci OT, co pozwala na wykrywanie zagrożeń i anomalii wewnątrz organizacji. Ta technologia to samouczący się moduł sztucznej inteligencji, dostarczający audyty w czasie rzeczywistym. Dzięki temu od razu wykryjesz złośliwe oprogramowanie, awarie czy inne problemy związane z siecią energetyczną, czy automatyką przemysłową. A także będziesz mógł w łatwy sposób zarządzać incydentami. SCADVANCE XP wdrożyła m.in. PKP Energetyka.



## **ZABEZPIECZ SWOJE MATERIAŁY WIDEO Z VESTIGIT**

Firmy, które tworzą sporo contentu wideo (np. platformy VOD czy SVOD albo agencje kreatywne, czy spółki zajmujące się pay-per-view) z pewnością zaciekawili wrocławski startup Vestigit. Spółka pozwala na dokładniejsze zabezpieczenie treści wideo. Flagowym produktem Vestigit jest nakładanie unikalnych znaków wodnych na wideo online, co ma zapobiegać jego nieautoryzowanej dystrybucji. Osadzenie watermarku opiera się o tzw. kodowanie A/B i pozwala na szybkie wykrycie rozprowadzania transmisji czy filmiku dalej. A także powiązania tej nieautoryzowanej dystrybucji z konkretnym użytkownikiem.

Za powstanie startupu odpowiada grupa naukowców z Politechniki Wrocławskiej, która od dawna zajmuje się kryptografią sieci neuronowych. W spółkę zaangażowani są także wieloletni handlowcy wyspecjalizowani w transmisjach OTT i IPTV.

Startup pozyskał niedawno 2 mln zł na rozwój m.in. od funduszu RKKVC. Vestigit rozwija także swoje usługi w zakresie cyberbezpieczeństwa, aby zminimalizować ryzyko ataków hakerskich. Oprócz tego spółka adresuje swoje usługi także dla influencerów, którzy tworzą content wideo np. na TikToku czy YouTube i narażeni są na retransmisję, czy redystrybucję swoich materiałów.

Polskich, jak i zagranicznych startupów zwiększających bezpieczeństwo firm jest naprawdę sporo. I to zarówno kwestie dot. cyberbezpieczeństwa, jak i bardziej fizycznych aspektów. Chociażby awarii sprzętu czy infrastruktury przemysłowej. Na każdym etapie rozwoju swojej firmy warto dbać o bezpieczeństwo, tak swoje, swoich pracowników, jak i klientów. W końcu niedotrzymanie standardów może się wiązać nie tylko ze stratami finansowymi, ale też wizerunkowymi czy nawet sankcjami prawnymi i administracyjnymi.



# DANE MEDYKÓW TAKŻE TRZEBA CHRONIĆ



Konrad Dyda  
Med&Lex-Klinka  
Wsparcia Personelu  
i Jednostek  
Ochrony Zdrowia



**Podmioty lecznicze muszą prawidłowo przetwarzać nie tylko dane osobowe pacjentów, ale również pracujących dla nich medyków. Niedopełnienie tych obowiązków również stanowi naruszenie RODO. Niestety, rzadko kiedy pamięta się o prawach medyków w ogóle, a tym samym w szczególności o prawidłowej ochronie ich danych osobowych.**



Bez personelu – dobrze przygotowanego do wykonywania swoich obowiązków oraz odpowiednio wynagradzanego – niemożliwe jest stworzenie efektywnego systemu ochrony zdrowia. To z kolei stawia przed decydentami oraz podmiotami leczniczymi – zresztą także w sektorze prywatnym – spore wyzwania. I nie chodzi tutaj tylko o zaplecze organizacyjne oraz finansowe. Niezwykle istotnym – choć niestety często pomijanym – elementem budowy systemu ochrony zdrowia jest prawidłowe zabezpieczenie praw medyków. Także w sferze ochrony ich danych osobowych.

## PROBLEMY Z OCHRONĄ DANYCH W PLACÓWKACH MEDYCZNYCH

Najwyższa Izba Kontroli w listopadzie 2019 roku opublikowała raport dotyczący praktyki ochrony danych osobowych w podmiotach leczniczych. Głównym celem kontroli była odpowiedź na pytanie, czy podmioty te prawidłowo wdrożyły przepisy RODO. Niestety, tezy postawione przez NIK były niepokojące. Kontrolerzy wskazali na takie problemy, jak:

- 1 brak rozwiązań gwarantujących pacjentom zachowanie prywatności w procesie rejestracji (w ponad 1/3 kontrolowanych podmiotów)
- 2 umieszczanie na opaskach identyfikacyjnych pacjentów ich danych osobowych (w 46% skontrolowanych szpitali)
- 3 przechowywanie dokumentacji w niezamykanych szafkach (9 na 24 szpitali).

Wykryto także przypadki przyznawania pielęgniarcom w systemie HIS dostępu do danych pacjentów z poradni i oddziałów, w których one nie świadczyły pracy; nieodbierania byłym pracownikom szpitala możliwości dostępu do danych pacjentów, czy udzielenie takiego dostępu pracownikom niemedycznym (np. salowym i sanitariuszom).

NIK przeprowadziła swoją kontrolę w 24. szpitalach z sześciu województw. Stąd trudno w prosty sposób uogólniać jej wyniki – tym bardziej, że od przeprowadzenia działań kontrolnych i publikacji raportu minęło już trochę czasu, a doświadczenie pokazuje, że poziom ochrony danych osobowych w placówkach leczniczych systematycznie się podnosi.

Nie zmienia to faktu, że sformułowane wówczas rekomendacje nadal pozostają aktualne.

**Chodzi tu zwłaszcza o zalecenia skierowanie do kierowników podmiotów leczniczych, tj. m.in.:**

- konieczność analizowania ryzyka dotyczącego ochrony danych;
- przeprowadzanie regularnych szkoleń osób uczestniczących w procesach przetwarzania informacji;
- nadawanie pracownikom uprawnień w systemach operacyjnych komputerów oraz systemach HIS w stopniu adekwatnym do realizowanych przez nich zadań;
- przekazywanie firmom świadczącym usługi serwisowe jedynie danych osobowych niezbędnych do usunięcia usterek oprogramowania.

Oczywiście wprowadzenie systemowych rozwiązań dotyczących ochrony danych osobowych zawsze należy do kierownika podmiotu leczniczego, ewentualnie przy współpracy organów założycielskich bądź właścicieli. Jednak w praktyce standardy ochrony danych w placówkach leczniczych zależą także od zachowań pacjentów. W końcu rzadko kiedy podmiot leczniczy ma takie warunki lokalowe, aby zapewnić pełną intymność pacjentom „przy okienku”.

Od bardzo prostej sprawy – zachowania przez pozostałych oczekujących odpowiedniej odległości czy wystrzeganie się „podśluchiwania” – w dużej mierze zależy to, czy dane osobowe pacjenta dotyczące jego stanu zdrowia, a więc znajdujące się pod szczególną ochroną, rzeczywiście nie staną się dostępne dla osób postronnych. Choć – co oczywiste – za zachowania innych pacjentów nie odpowiada administrator danych, chyba że był w stanie im zapobiec, a celowo tego nie zrobił, ignorując tym samym swoje obowiązki wynikające z RODO.





## **KTO MYŚLI O MEDYKACH?**

Rzeczywiście w kontekście zasad ochrony danych osobowych w placówkach ochrony zdrowia – zarówno prywatnych, jak i publicznych – temat prawidłowego przetwarzania danych osobowych medyków jest rzadko poruszany. Oczywiście można by wskazać wiele przyczyn takiego stanu rzeczy, jednak do najważniejszych osobiście zaliczam swego rodzaju ignorancję praw medyków w ogóle. Skoro mało kto interesuje się zakresem praw medyków, ich treścią oraz zasadami korzystania, to właściwie niczym dziwnym jest, że w tym kontekście nie porusza się także zagadnień związanych z RODO. Tymczasem jest to błędna perspektywa.

**JEDNOSTKI OCHRONY ZDROWIA MAJĄ  
SŁUŻYĆ PRZED E WSZYSTKIM  
PACJENTOM, JEDNAK NIE SĄ ONE  
W STANIE PRAWIDŁOWO WYPEŁNIAĆ  
SWOICH OBOWIĄZKÓW, JEŻELI NIE  
PRACUJE DLA NICH ODPOWIEDNI  
PERSONEL. TRUDNO ZAŚ WYMAGAĆ OD  
NIEGO EFEKTYWNEJ PRACY, SKORO  
LEKCEWAŻY SIĘ JEGO PRAWA.**

Ochrona danych osobowych medyków w miejscu pracy ma także jeden, istotny aspekt. Otóż zawsze trzeba pamiętać, że pracownicy medyczni przed podjęciem zatrudnienia muszą legitymować się ściśle określonymi badaniami. Samo przeprowadzenie badań z zakresu medycyny pracy przed podjęciem zatrudnienia nie jest niczym nadzwyczajnym, ale w przypadku placówek medycznych ich zakres jest dużo szerszy i obejmuje chociażby badanie w kierunku nosicielstwa wirusa HIV. Informacje te – podobnie, jak inne dane osobowe odnoszące się do stanu zdrowia – muszą być chronione w sposób szczególny.

## WSZYSTKO ZALEŻY OD FORMY ZATRUDNIENIA

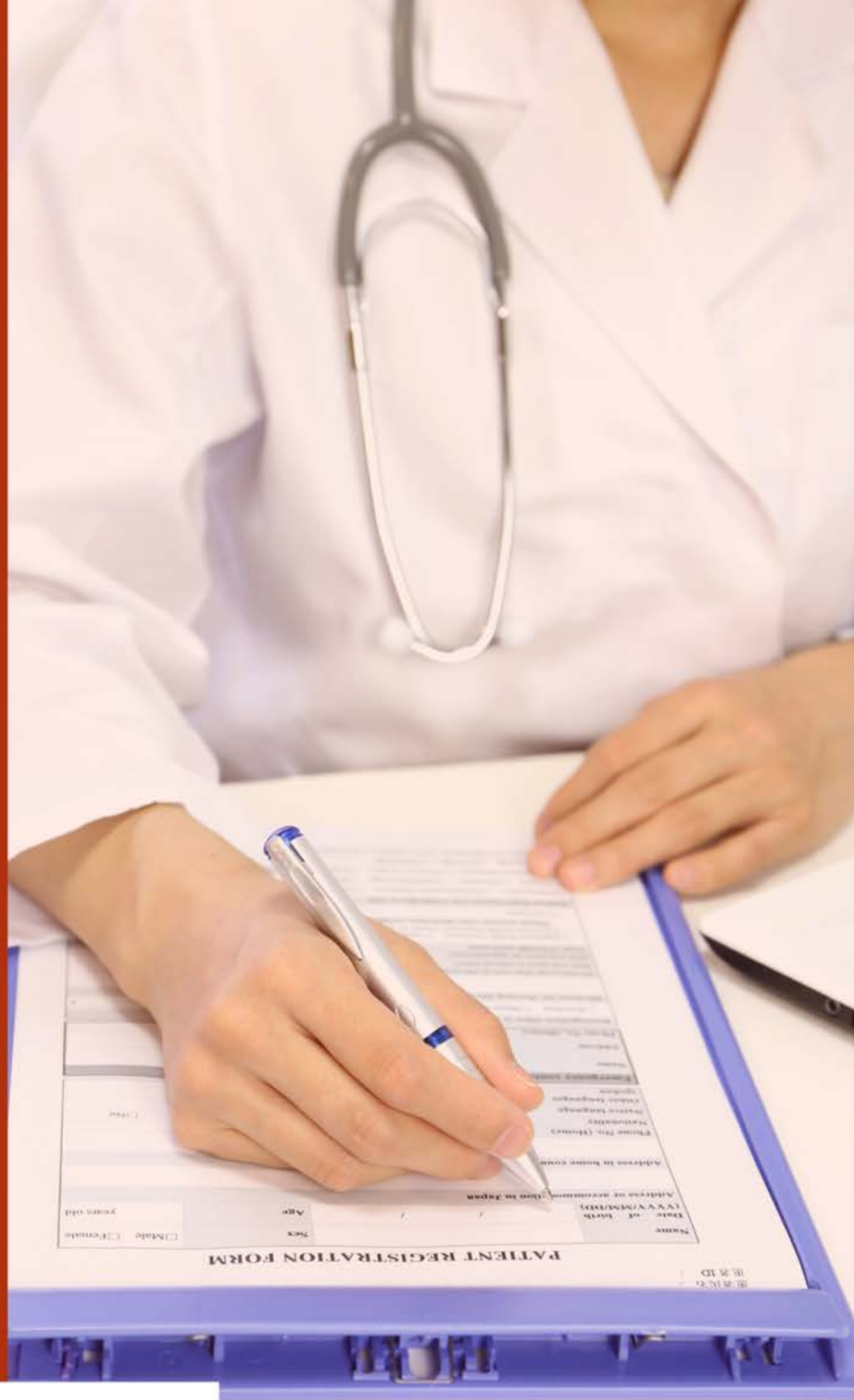
Z praktycznego punktu widzenia zasady ochrony danych osobowych medyków zależą od tego, czy wykonują oni swoje obowiązki w ramach stosunku pracy (bez względu na to, jak nazwano ich umowę – w końcu „śmieciovka” też może zostać uznana za umowę o pracę) czy też w ramach „samozatrudnienia”.

W pierwszym ze wskazanych tu przypadków to na pracodawcy medyka spoczywa obowiązek zapewnienia prawidłowej ochrony danych, które ten przetwarza w związku z zatrudnieniem pracownika medycznego. Wówczas obowiązują tu analogiczne zasady, jak w przypadku wszystkich innych pracowników – stąd ich dane osobowe mogą być przetwarzane przez pracodawcę tylko w takim zakresie, jaki jest niezbędny do osiągnięcia celu przetwarzania.

Więcej problemów pojawia się wtedy, gdy medyk realizuje swoje zadania na rzecz podmiotu leczniczego w ramach prowadzonej przez siebie jednoosobowej działalności gospodarczej. Teoretycznie wówczas sam dla siebie będąc „pracodawcą” – samodzielnie odpowiada za prawidłowe zabezpieczenie swoich danych osobowych.







Dlatego warto podkreślić, że wówczas gdy medyka-przedsiębiorcę łączy z podmiotem leczniczym umowa o świadczenie usług, a w ramach jej wykonywania medyk przekazuje swoje dane osobowe, również muszą być one prawidłowo przetwarzane przez ten podmiot. W przeciwnym przypadku powinien on liczyć się z surową odpowiedzialnością.



**/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**



# KORZYŚCI KONTROLOWANYCH ATAKÓW HAKERSKICH

---



Patryk Bogdan  
Grandmetric

Jeszcze do niedawna zagrożenia cyberbezpieczeństwa spędzały sen z powiek niemal wyłącznie właścicielom wielkich korporacji. Wraz ze zmieniającą się rzeczywistością przedsiębiorstw - rosnącą popularnością pracy zdalnej, internetowym aplikacjom i rozwiązaniom chmurowym, a przede wszystkim zależnością ich funkcjonowania od wielowymiarowej łączności z siecią - czasy te bezpowrotnie minęły.





## AUTOMATYZACJA ATAKÓW HAKERSKICH

W dobie automatyzacji wielu procesów, które dotąd były mozolnie wykonywane ręcznie, swoje działania automatyzują również przestępcy działający w świecie wirtualnym. Są w stanie jednocześnie atakować setki, jeśli nie tysiące firm w tym samym czasie. Ze względu na mniej restrykcyjne polityki bezpieczeństwa, skromniejsze nakłady finansowe i niższy poziom świadomości ryzyka, szczególnie małe i średnie przedsiębiorstwa są dla nich atrakcyjnym targetem.

**Wg raportu "Cost of Cybercrime" firmy Accenture, 43% cyberataków jest wymierzona w małe biznesy, ale tylko 14% z nich jest przygotowanych do tego, by skutecznie się przed nimi obronić.**

To właśnie nieduże firmy mają sporo do stracenia, szczególnie, jeśli przechowują patenty, dane osobowe chronione prawnie czy opierają się na produkcji, której zatrzymanie i ponowne uruchomienie wiąże się z kosztami rzędu setek tysięcy złotych. Należy pamiętać, że prócz okupu dla którego działają hakerzy, w sytuacji cyberataku firmy ponoszą również inne koszty, takie jak straty wizerunkowe czy utrata zaufania klientów i partnerów biznesowych.

**Badanie przeprowadzone przez Cisco wykazało, że 40% małych firm, które padły ofiarą cyberataku musiało mierzyć się z przestojem trwającym ponad 8 godzin, co stanowiło dużą część poniesionych kosztów.**





## **PRZYCZYNY BŁĘDÓW BEZPIECZEŃSTWA**

W przeciwieństwie do konsekwencji przyczyny błędów bezpieczeństwa bywają trywialne.

**Przyjrzyjmy się najczęstszym z nich:**

**NIEAKTUALNE OPROGRAMOWANIE LUB JEGO KOMPONENTY**

**NIETYCZĄCE PROCEDURY BEZPIECZEŃSTWA**

**LUKI W OPROGRAMOWANIU ALBO W SPRZĘCIE**

**NIEWŁAŚCIWA KONFIGURACJA**

**NIEDOCIĄGNIĘCIA TECHNICZNE**

**NIEOSTROŻNOŚĆ UŻYTKOWNIKÓW**





## JAK PRZYGOTOWAĆ SIĘ NA POTENCJALNY CYBERATAK?

Przede wszystkim nie dać się zaskoczyć i zadbać o to, by firmowa infrastruktura informatyczna była bezpieczna. Podstawowym narzędziem służącym do sprawdzenia stanu cyberbezpieczeństwa jest przeprowadzenie testu penetracyjnego, nazywanego w skrócie pentestem.

Test penetracyjny to atak hakerski przeprowadzany w sposób kontrolowany, na zlecenie właściciela infrastruktury teleinformatycznej, sieci, strony internetowej czy aplikacji. Służy do wykrycia błędów, które zagrażają bezpieczeństwu badanego systemu.

Pentester wciela się w tej sytuacji w hakera, który działa „w białych rękawiczkach”. Jego zadaniem jest wykrycie luk systemu, wskazanie miejsc wrażliwych na potencjalny atak i zaproponowanie rozwiązań, które wyeliminują zagrożenie.

Pentesty powinny być przeprowadzane w sposób systematyczny i mogą mieć różny zakres, najczęściej też stanowią część szerszego audytu cyberbezpieczeństwa systemów i infrastruktury IT. Ich głównym celem jest zbadanie, na ile dana sieć jest odporna na włamanie i jaka jest skuteczność zastosowanych zabezpieczeń.

Niezbędną częścią każdego testu jest raport, opisujący zidentyfikowane problemy. Jego bardzo ważną częścią są rekomendacje, które mają na celu ich skuteczne wyeliminowanie.



**Testy bezpieczeństwa dzielą się na trzy typy na podstawie ilości wiedzy na temat badanego systemu, jaka jest udostępniana pentesterom przez klienta:**

- 1** testy white box - pełna wiedza pentesterów, mających do dyspozycji dokumentację projektu infrastruktury, informacje dotyczące konfiguracji urządzeń w sieci czy kod źródłowy strony
- 2** testy black box - minimalna wiedza pentesterów – najlepiej odzwierciedlają rzeczywisty cyberatak i wymagają dużego nakładu pracy ze strony testerów, a ich wiedza może ograniczać się tylko do adresu strony czy nazwy firmy, której zabezpieczenia testują.
- 3** testy gray box - częściowa wiedza pentesterów, hybryda obu wyżej wymienionych metod.

Wybierając firmę, której zlecimy przeprowadzenie testów naszej infrastruktury, warto zwrócić uwagę na to, jakie metody wykorzystuje. Ważne, by testy penetracyjne były wykonywane nie tylko w sposób automatyczny z użyciem oprogramowania, ale przede wszystkim ręcznie, w sposób dostosowany do konkretnego przypadku.

Należy pamiętać o tym, że kluczowy wpływ na sukces pentestu ma doświadczenie, kreatywność, wiedza i wytrwałość pentestera, który go przeprowadza. To rola wymagająca szerokiego zakresu kompetencji nie tylko technicznych, potwierdzonych certyfikatami, ale też komunikacyjnych czy z zakresu zarządzania.

**JAK PROGNOZUJE STEVE MORGAN, REDAKTOR NA-CZELNY CYBERCRIME MAGAZINE, W 2025 ROKU GLOBALNE CYBERPRZESTĘPSTWA BĘDĄ WYMAGAŁY NAPRAWY STRAT RZĘDU 10,5 TRYLIONA DOLARÓW (!). WARTO ZADBAĆ, BY NIE DZIAŁO SIĘ TO KOSZTEM MAJĄTKU NASZEGO I NASZEJ FIRMY.**

## TESTY PENETRACYJNE – FAQ

### 1. Jakie są fazy testu penetracyjnego?

- Rekonesans – kluczowy etap, polegający na zebraniu jak największej ilości danych niezbędnych do przeprowadzenia testu
- Skanowanie – sprawdzanie istniejących mechanizmów zabezpieczeń
- Eksploatacja – próba złamania zabezpieczeń systemu, czyli usługi bądź aplikacji
- Eskalacja – rozszerzenie uprawnień i dalsze kroki w sieci lub systemie
- Raport – zawiera szczegółowy opis metod zastosowanych w symulacji cyberataku, wykrytych błędów i podatności oraz rekomendacje działań, które mają na celu ich eliminację.

### 2. Jakie korzyści wynikają z wykonania testów penetracyjnych?

- Weryfikacja skuteczności zabezpieczeń systemu
- Zbadanie podatności systemu na potencjalny cyberatak
- Uzyskanie rekomendacji dotyczących poprawy bezpieczeństwa systemu
- Uniknięcie ogromnych kosztów związanych z zakłóceniem działania systemu w przedsiębiorstwie.

### 3. Jak często należy przeprowadzać pentesty?

Najlepszym rozwiązaniem jest przeprowadzanie testów penetracyjnych cyklicznie, przynajmniej raz do roku, a także w przypadku wprowadzania zmian w systemach. Po fazie pentestów warto również wykonać re-test, czyli weryfikację wprowadzonych zmian (sprawdzenie, czy zostały poprawnie zaimplementowane i nie doprowadziły do powstania nowych luk bezpieczeństwa).

### 4. Jak długo trwa test penetracyjny?

Pentest, w zależności od rodzaju, wielkości i poziomu skomplikowania badanej struktury może trwać od kilku dni do kilku tygodni.



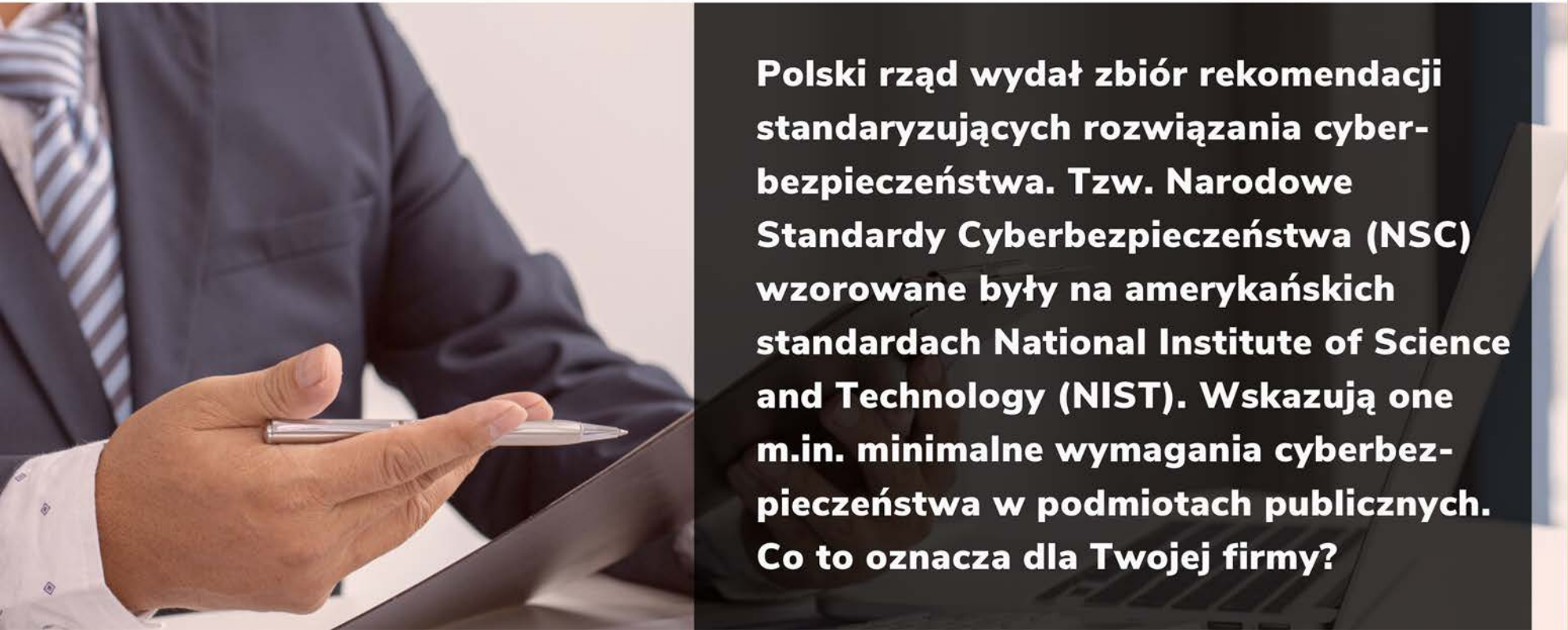


**Możesz naprawdę odpocząć wiedząc, że Twój biznes jest z nami bezpieczny.**

# NIE DBASZ O CYBERBEZPIECZEŃSTWO? B2G NIE BĘDZIE Z TOBĄ WSPÓŁPRACOWAĆ



Redakcja  
SECURITY MAGAZINE



**Polski rząd wydał zbiór rekomendacji standaryzujących rozwiązania cyberbezpieczeństwa. Tzw. Narodowe Standardy Cyberbezpieczeństwa (NSC) wzorowane były na amerykańskich standardach National Institute of Science and Technology (NIST). Wskazują one m.in. minimalne wymagania cyberbezpieczeństwa w podmiotach publicznych. Co to oznacza dla Twojej firmy?**



## CZYM SĄ NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA?

Polska administracja zaczyna podchodzić coraz poważniej do spraw cyberbezpieczeństwa. I nie ma się co dziwić, bo jesteśmy coraz bardziej narażeni na ataki hakerów. Z danych policji wynika, że w 2020 r. doszło do ok. 55 tys. cyberprzestępstw, czyli o ponad połowę więcej niż cztery lata wcześniej. Lwią część z tych odnotowanych stanowią ataki typu ransomware – czyli w – skrócie zablokowanie dostępu do plików i żądanie za nie okupu. Popularne są również phishing i oszustwa internetowe.

Niestety, jednocześnie wykrywalność cyberprzestępstw wcale nie rośnie, a wręcz spada. Szkopuł leży w tym, że polska policja ciągle ma problem z właściwą klasyfikacją ataków hakerskich. A dodatkowo, jak wspominał Adam Heartle w rozmowie z Rzeczpospolitą – niektórzy obywatele zwyczajnie nie zgłaszają cyberprzestępstw organom ścigania. Prawdopodobnie zatem wspomniane 55 tys. i tak jest znacznie zaniżoną liczbą.

Żeby choć częściowo przeciwdziałać temu problemowi polska administracja postanowiła stworzyć Narodowe Standardy Cyberbezpieczeństwa. Zbiór tych rekomendacji wzorowany był zresztą na swoim amerykańskim odpowiedniku. Jest to część strategii cyberbezpieczeństwa Polski na lata 2019–2024. Znajdziemy w nich m.in. standardy kategoryzacji bezpieczeństwa czy minimalne wymagania dot. bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych.

**NIEZALEŻNIE OD TEGO, CZY  
PROWADZISZ FIRMĘ, CZY NIE,  
WAŻNE, BYŚ WIEDZIAŁ, CO ROBI  
TWÓJ KRAJ W CELU OCHRONY  
TWOICH, JAKI INSTYTUCJO-  
NALNYCH DANYCH.**

Kwestia ta może być o tyle istotniejsza, jeśli kierujesz usługi do tzw. rynku B2G (Business to Government, tj. samorządy, agencje rządowe itp.) – tym bardziej że organizacje państwowe mogą nie chcieć z Tobą współpracować, jeśli nie dbasz o zasady cyfrowego bezpieczeństwa.



## **MINIMALNE WYMAGANIA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH**

**Dokument dot. minimalnych wymagań cyberbezpieczeństwa wskazuje aż 20 obszarów, które organizacje powinny wdrożyć. I trzeba przyznać, że są one bardzo sensowne. Punkty obejmują:**

- Kontrolę dostępu – ograniczenie dostępu do systemu informatycznego tylko dla autoryzowanych użytkowników;
- Uświadamianie i szkolenia – informowanie o cyberzagrożeniach, dyrektywach, standardach itd. Szkolenie personelu z zakresu cyberbezpieczeństwa;
- Audyt i rozliczalność – tworzenie i ochrona rejestrów audytów systemów informatycznych w celu ich monitorowania. Możliwość powiązywania działań z konkretnymi użytkownikami systemu informatycznego, aby mogli być pociągnięci do odpowiedzialności w przypadku ew. naruszeń;
- Ocenę, autoryzację i monitorowanie – testowanie swoich cyberzabezpieczeń i ich stałe ulepszanie;
- Zarządzanie konfiguracją – utrzymywanie podstawowej konfiguracji i wykazów organizacyjnych systemów informatycznych, a także prowadzenie dokumentacji;
- Planowanie awaryjne i ciągłość działania – tworzenie kopii zapasowych, zabezpieczenia przed awariami, przygotowywanie planów reakcji na wypadek problemów technicznych;
- Identyfikację i uwierzytelnienie – identyfikowanie użytkowników systemu informatycznego, weryfikowanie ich tożsamości i uwierzytelnianie;
- Reagowanie na incydenty – przygotowanie planu operacyjnego na wypadek incydentów, a także wykrywanie i zapobieganie nim;
- Utrzymanie i wsparcie – zabezpieczanie sprzętu i okresowy audyt działania systemu informatycznego;



- Ochronę nośników danych – zezwolenie na dostęp do nośników danych tylko upoważnionym użytkownikom. Zabezpieczanie nośników – niezależnie od tego, czy są one cyfrowe, czy analogowe, a także ich właściwa utylizacja;
- Ochronę fizyczną i środowiskową – ograniczenie fizycznego dostępu do systemów informatycznych nieupoważnionym użytkownikom. Wlicza się w to sprzęt, a także instalacje i infrastrukturę systemów (np. serwery);
- Planowanie – dokumentowanie, wdrażanie i aktualizowanie planów dot. cyberbezpieczeństwa;
- Programy zarządzania – chronienie programów zarządzania przed nieupoważnionymi użytkownikami;
- Bezpieczeństwo osobowe – zapewnienie ochrony informacji i danych, a także systemów informatycznych. Dbanie o kompetencje pracowników na stanowiskach dot. systemów informatycznych, a także stosowne sankcje za nieprzestrzeganie przez personel zasad i procedur;
- Przejrzystość przetwarzania danych osobowych – jasne polityki i procedury dot. przejrzystości danych osobowych, programów bezpieczeństwa oraz ochrony prywatności;
- Ocenę ryzyka – okresowe ocenianie ryzyka dot. cyberzagrożeń;
- Nabywanie systemu i usług – korzystanie z oprogramowania podnoszącego standardy cyberbezpieczeństwa. Weryfikowanie zew. dostawców, czy stosują adekwatne środki bezpieczeństwa w celu ochrony informacji, aplikacji lub usług zleconych przez organizację;
- Ochronę systemów i sieci telekomunikacyjnych – monitorowanie, chronienie i kontrolowanie komunikacji organizacyjnej, tj. np. przekazywania lub odbierania informacji;
- Integralność systemu i informacji – identyfikowanie, zgłaszanie i korygowanie błędów systemów informatycznych. Zapewnianie ochrony przed złośliwym oprogramowaniem;
- Zarządzanie ryzykiem w łańcuchu dostaw – strategia zarządzania ryzykiem uwzględniająca koszty, harmonogramy, wyniki i kwestie dot. łańcucha dostaw w organizacji. Organizacje powinny opracować polityki i procedury dot. zarządzania ryzykiem oraz wdrożyć odpowiednie programy bezpieczeństwa.





## **6 NA 10 CYBERATAKÓW UDAJE SIĘ ZE WZGLĘDU NA CZYNNIK LUDZKI**

W całym tym dokumencie na szczególną uwagę zasługują dwie rzeczy. Pierwszą z nich jest szkolenie personelu i podnoszenie jego kompetencji. Praktycznie w każdym raporcie dotyczącym się kwestii cyberzagrożeń czynnik ludzki wskazywany jest jako główny powód naruszenia bezpieczeństwa w firmie. Tak pokazuje, chociażby badanie „Barometr cyberbezpieczeństwa”, gdzie czynnik ludzki (63%) wskazano jako największe wyzwanie dla firm w zapewnieniu oczekiwanego poziomu zabezpieczeń.

Zatem szkolenie personelu jest niezwykle ważne, ponieważ to od niego zależy cyberbezpieczeństwo Twojej firmy. Problem jednak w tym, że polskie organizacje (nie tylko te rządowe) w zasadzie w ogóle nie są dojrzałe cyfrowo. W indeksie gospodarki cyfrowej i społeczeństwa cyfrowego Polska znalazła się na 24. miejscu w UE pod względem cyfryzacji i jest to jeden z najgorszych wyników w tym rankingu.



A niestety, rozwój cyfryzacji polskich firm jest bardzo słaby. Według raportu COVID-19 Business Pulse Survey – Polska ponad 50% organizacji uważa, że nie potrzebuje dalszej cyfryzacji. Ponadto w 2020 r. aż 49% firm nie przeszkoliło swoich pracowników. Dlaczego? Najczęściej (63%) dlatego, że uważają kompetencje swoich pracowników za wystarczające. Co niestety jest bzdurą, bo według badań umiejętności cyfrowe polskich pracowników są poniżej średniej europejskiej.

## **KLIENCI B2G NIE BĘDĄ Z TOBĄ WSPÓŁPRACOWAĆ, JEŻELI NIE DBASZ O CYBERBEZPIECZEŃSTWO**

W przypadku firm, którzy kierują swoje usługi do

rynku B2G Narodowe Standardy Cyberbezpieczeństwa mogą mieć kluczowe znaczenie.

Dlaczego? Ponieważ w dokumencie jasno określono, że organizacje powinny dbać o to, aby ich zew. dostawcy wdrażali odpowiednie standardy dot. cyberbezpieczeństwa.

Wszelkie aplikacje, produkty czy usługi dla rynku B2G muszą być transparentne i chronione przed złośliwym oprogramowaniem. Nie spełnienie tych standardów oznacza wycofanie się z rynku B2G czy B2B2G. Jeśli Twoja firma nie adresuje problemów dotyczących cyberbezpieczeństwa, to możesz być pewien, że praktycznie nie wygra żadnego przetargu z podmiotem publicznym.



A te – wbrew pozorom – dla firm technologicznych potrafią być dość sporym rynkiem. Przykładowo według raportu „Polskie Startupy 2021” rynek B2G to grupa docelowa 31% wszystkich startupów w naszym kraju. Z kolei organizacje pozarządowe (NGO) i pożytku publicznego (B2B2G) stanowią 11%. Łącznie zatem dla sektora publicznego produkty sprzedaje (lub wykonuje zlecenia) 42% polskich startupów.

Jeśli Twoja organizacja znajduje się wśród tych spółek – z pewnością powinieneś zapoznać się z całym zbiorem Narodowych Standardów Cyberbezpieczeństwa i odpowiednio przygotować swoją organizację.





# JAK SPRAWDZIĆ CZY TWOJA STRONA WWW JEST BEZPIECZNA?

---



Joanna Gizgier  
by Fehu

**Internet jest genialnym narzędziem do promocji marki, budowania wizerunku. Świetnie wspiera sprzedaż, można dzięki niemu poznawać nowe osoby i kontaktować się z bliskimi. Niestety Internet, ma też wiele negatywnych stron. Będąc właścicielem strony internetowej, narażeni jesteśmy na wiele problemów. Warto zdać sobie sprawę, że wirusy, boty i ataki hakerskie nie dotyczą tylko dużych firm, ale również MŚP.**

Nie jest ważne czy prowadzisz sklep z akcesoriami kosmetycznymi, czy stronę z usługami szkoleniowymi. Kradzież danych klientów, danych Twojego konta bankowego czy zaatakowanie jej dedykowanym wirusem lub botami ma ogromny wpływ na banowanie Twojej strony przez wyszukiwarki. Utrata wiarygodności marki, jest jednym z najgorszych scenariuszy jakie chce przeżyć właściciel firmy online.

## KILKA DANYCH

Najwięcej procesów cyberbezpieczeństwa jest realizowanych w firmach, które posiadają wyodrębniony do realizacji tych zadań zespół zewnętrzny lub wewnętrzny. Według raportu KPMG, w 2022 tylko 14 % firm jest chroniona przed cyberzagrożeniami, 7% firm bierze pod uwagę i kwantyfikuje ryzyko wynikające z wykorzystania technologii cyfrowych przy podejmowaniu decyzji strategicznych i/lub operacyjnych. 8 % firm ma znajomość procedur reagowania na incydenty cyberbezpieczeństwa przez pracowników lub firmy zewnętrzne do tego zatrudnione 2% firm planuje zwiększyć wydatki na cyberbezpieczeństwo w ciągu następnych 12 miesięcy.

Te dane nie są optymistyczne, nadal wiele firm nie zdaje sobie sprawy z konsekwencji, jakie mogą wynikać z braku odpowiednich zabezpieczeń.

## CO MOŻE CI GROZIĆ?

Oszuści wykorzystują ludzkie słabości. Wiedzą kiedy i gdzie można szybko i łatwo kogoś oszukać. Problemów jest cała masa. Najczęściej grozi nam utrata pieniędzy z konta bankowego, utrata konta w mediach społecznościowych czy utrata strony www.

### Najpopularniejsze przestępstwa w sieci:

**PHISHING** jest obecnie jedną z najpopularniejszych metod. Przestępca podszywa się pod inną osobę lub instytucję. Często namawia użytkownika w wiadomości e-mail czy przez komunikator do odwiedzenia określonej strony internetowej, kliknięcia w nietypowy link. Nieświadomie wtedy udostępnimy poufne dane na przykład do konta bankowego czy hasła do stron.

**SCAM** to oszustwo, które polega na wzbudzeniu zaufania, tak aby zmusić kogoś do na przykład powierzenia danych osobowych.





## JAK ZADBAĆ O BEZPIECZEŃSTWO WWW?

### ODPOWIEDNI HOSTING

Przy wyborze serwera uwagę zwrócić należy na działanie jego procesorów, ile mamy pamięci na dostępie swobodnym. Kluczowe to, jest zwłaszcza, kiedy mamy zaimplementować duże sklepy internetowe, portale, czy platformy streamingowe. Czy jest dostępny pełen panel administracyjny, oraz zgodność i aktualizacje MySQL - system zarządzania relacyjnymi bazami danych oraz aktualna wersja PHP. Zbyt często firmy popełniają błędy przy wyborze serwera, przez dobry marketing nośników hostingowych, lub skuszeni reklamą wybieramy tani host, bez chociażby sprawnie reagującego supportu na problemy. Pamiętaj również, że ten sam serwer będzie obsługiwał Twoją pocztę, newsletter i wiele innych automatyzacji, więc warto zacząć od poprawnego wyboru.

### ZACZNIJMY OD AUTOINSTALACJI CMS-ów

Pamiętajmy, że wdrożenie CMS-a przez autoinstalator, nie służy stronie w ogóle. Instalujemy masę przestarzałych wtyczek, kompletnie nie dobranych do potrzeb strony, zabiera nam możliwość zarządzania ścieżką instalacji, ma powtarzalne klucze i sole, takie same prefixy tabel i bardzo przewidywalną nazwę samej bazy danych.

Wiele elementów, które się powtarzają, a powinny być unikatowe oraz narzucają ustawienia. I co gorsza jest wtedy brak możliwości zmian, co z kolei zabiera nam możliwość porządnego zabezpieczenia strony przed niechcianymi wizytami. Zatem, jeżeli jesteś dopiero przed założeniem swojej firmy, nigdy nie korzystaj z tego typu rozwiązań, a jeżeli już posiadasz w taki sposób zainstalowaną, jak najszybciej należy to zmienić.

## TRANSPORT LAYER SECURITY

Kolejnym krokiem bezpieczeństwa jest certyfikat SSL, protokół zabezpieczający stronę, który zapewnia poufność transferu danych. Kiedy nie zadamy o taki certyfikat na naszej stronie czy sklepie, jesteśmy traktowani jako strona niebezpieczna, drastycznie tracimy zaufanie użytkowników oraz pozycję w Google, którą będziemy musieli odbudować ponownie, po jego instalacji. Warto również dobrać odpowiedni certyfikat do serwera czy usług, aby cały jego pakiet zabezpieczał przed wyciekami danych Twoich i klientów.

## SMTP

Autoryzacja protokołu poczty to ważny element bezpieczeństwa. Zaniedbania w tym zakresie odpowiadają za swobodne uzyskanie dostępu do Twojego e-maila. Można całkowicie przewidzieć jakie konsekwencje poniesiemy, kiedy te dane zostaną skradzione i np. ktoś potwierdzi zmianę naszych haseł bankowych lub haseł do połączenia płatności w naszym sklepie.

## reCAPTCHA

Ogromny wpływ na stronę www mają ataki botów na domenę, spamowe komentarze czy blokowanie serwera.

Bardzo dobrym rozwiązaniem jest najnowszy reCAPTCHA v3. To API, które rozróżnia zachowania człowieka od robota na stronie www bez interakcji użytkownika oraz już bez konieczności zaznaczania puzzli na obrazku np. zaznacz wszystkie mosty. Chroni Twoje formularze kontaktowe, dyskusje i komentarze, blogi i różnego rodzaju portale oraz WHOIS czyli ogólnodostępną bazę danych o domenach internetowych oraz ich właścicielach.

## AKTUALIZACJE

Ważnym elementem jest aktualizacja baz danych, systemów CMS oraz wszystkich segmentów automatyzacji i dodatkowych. Zaniedbanie tego zakresu na stronach powoduje niesamowitą ilość dziur, które umożliwiają hakowanie i wirusowanie stron.

## KONIECZNIE O TYM PAMIĘTAJ

### Twórz kopie zapasowe

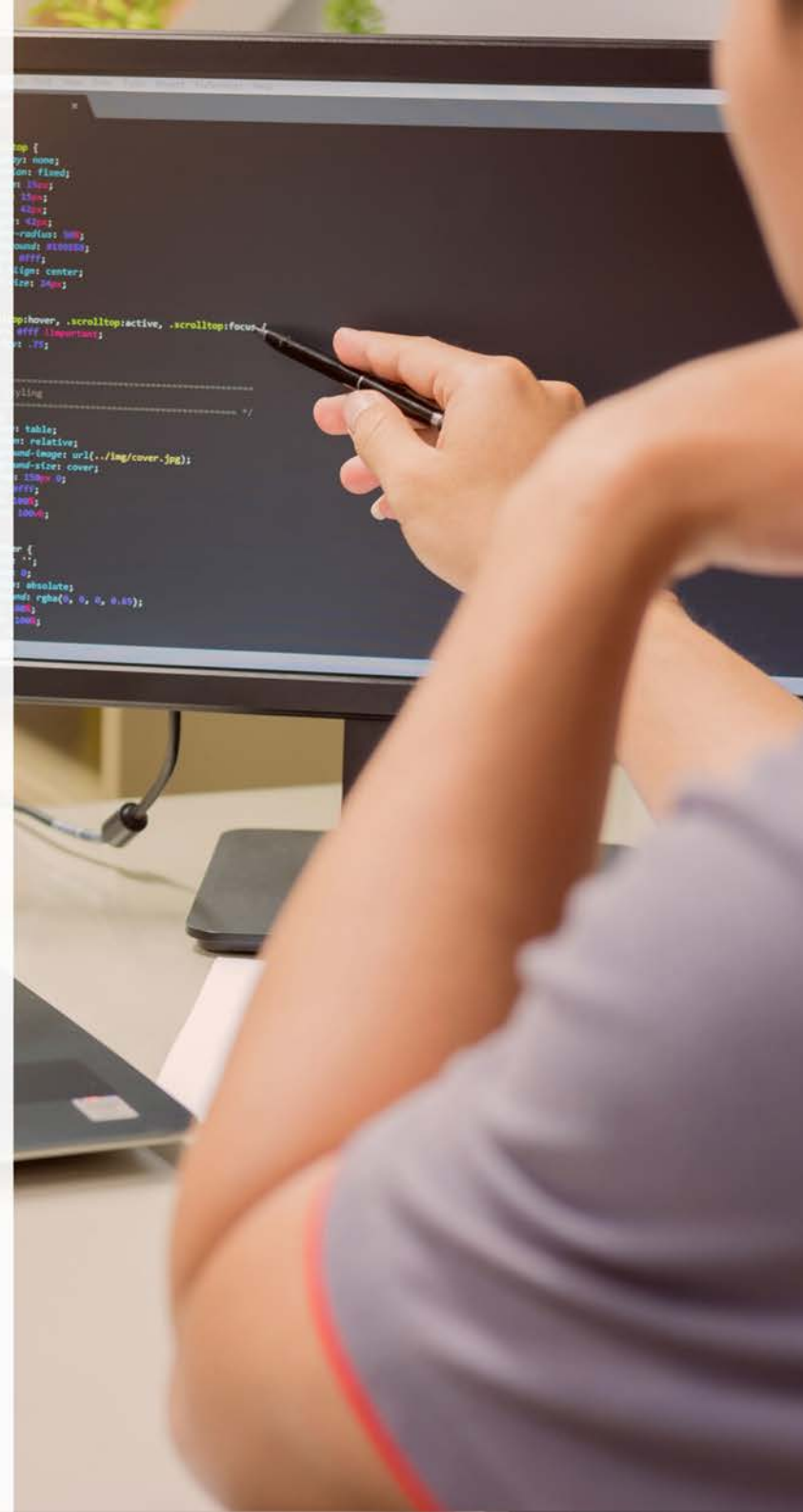
Regularność w tworzeniu kopii baz danych zapewni nam odtworzenie w każdym momencie strukturę strony i jej baz, dzięki temu możemy odizolować część uszkodzoną na danym etapie i przywrócić jej kopie.



## Usuwać i czyścić

Duży wpływ na bezpieczeństwo mają zbędne wtyczki, brak ich prawidłowych ustawień czy instalowanie, ich bez konfigurowania, pobieranie wtyczek niepotrzebnych z autoinstalatora. Instalowanie wtyczek zaczerpniętych z jakiegoś artykułu, które nie są dostosowane odpowiednio do naszego serwera, produktu czy strony. Powielanie ich do jednego polecenia, czyli zlecanie kilku wtyczkom tego samego zadania i zmuszania ich do walki między sobą „pod spodem”. Tworzą kolejne luki w kodach na stronach dzięki czemu ułatwiamy dostęp do hakowania. Brak czyszczenia czyszczenia strony po takich lukach może narobić ogrom szkód.

Pamiętajmy, że lepiej zapobiegać niż zalecać i tworzyć problemy, które będą wymagały głębszych analiz i kosztów, poprzez wymuszanie dokładnego audytu strony. Wiąże się to z przeglądaniem jej kodów, lokalizowania błędów i wirusów, oraz czyszczenia jej kodu, co w następstwie doprowadzi do lokalizowania takiej dziury w kodach, która doprowadzi do wejścia wirusa czy hakera i usuwanie jej w kodzie.





# sygnisoft

## **Bądź o krok przed innymi.**

W Sygnisoft sprawnie projektujemy, tworzymy  
i wdrażamy Twój pomysł.

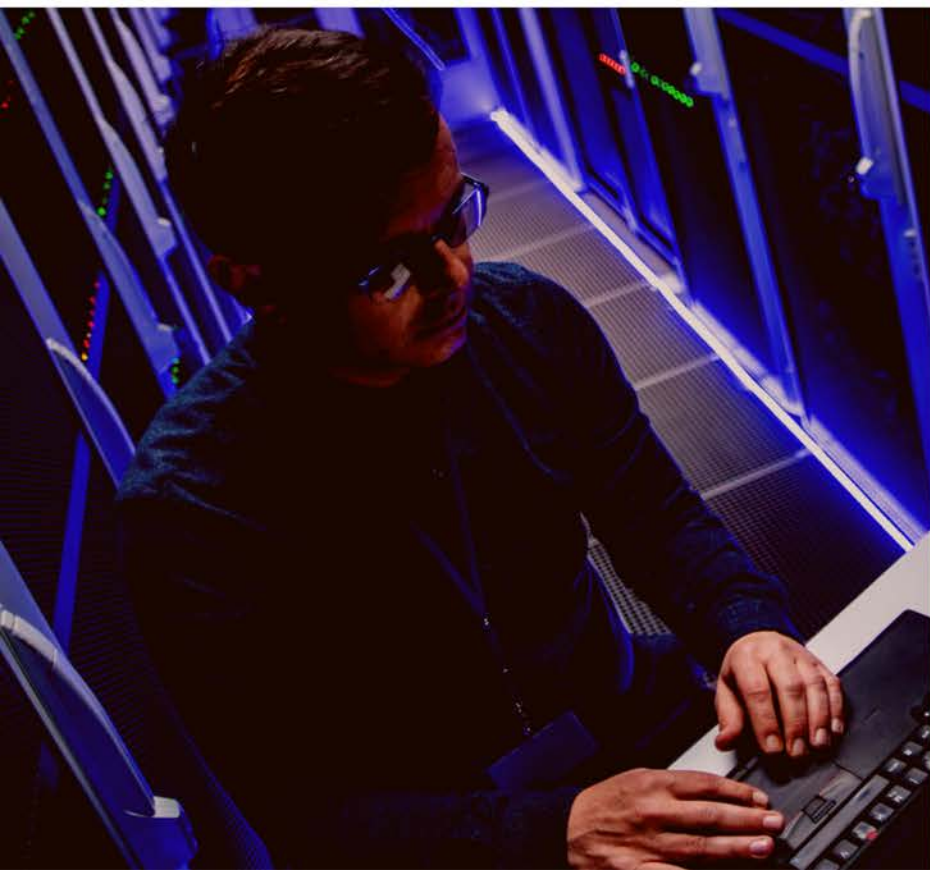


# PUŁAPKI GOTOWYCH ROZWIĄZAŃ IT

---



Dorota Dyś  
Sygnisoft S.A.



**Bez wątpliwości marzeniem każdego przedsiębiorcy jest rozwój własnego biznesu, w końcu rozwój to większe perspektywy, możliwości, dochody. Już sama obserwacja jak nasz pomysł kiełkuje, rozwija się, a potem rozrasta, gromadząc wokół coraz większą liczbę klientów, jest źródłem satysfakcji - ciężka praca opłacała się i zaczyna przynosić owoce.**

Bez wątpliwości marzeniem każdego przedsiębiorcy jest rozwój własnego biznesu, w końcu rozwój to większe perspektywy, możliwości, dochody. Już sama obserwacja jak nasz pomysł kiełkuje, rozwija się, a potem rozrasta, gromadząc wokół coraz większą liczbę klientów, jest źródłem satysfakcji - ciężka praca opłacała się i zaczyna przynosić owoce.

W strategii działania każdej firmy jest szereg aspektów, które należy uwzględnić: zasoby, marketing, zapewnienie konkurencyjności, stałe analizy rynku i wiele innych... Rozwój przynosi ze sobą ciągłe zmiany i popycha do dalszego rozwoju - rynek przecież nie stoi w miejscu, klienci wymagają, a konkurencja nigdy nie śpi. W tym całym pościgu za klientem często zapomina się o jednym z ważniejszych obszarów, jakim jest informatyzacja przedsiębiorstwa.

Kiedy dotychczasowe metody przestają być wystarczające, a procedury i systemy, które jeszcze nie tak dawno spełniały nasze oczekiwania, zamiast pomagać w codziennej pracy, zaczynają ją spowalniać lub utrudniać, pojawia się pytanie: co dalej?

Każdego dnia odbywamy w Sygnisoft co najmniej kilka rozmów, które oscylują wokół tego z pozoru prostego pytania: co dalej? Jak rozwijać swoją firmę, kiedy przeszkodą stają się jej własne procedury i niewystarczające możliwości dotychczasowych rozwiązań informatycznych?

## **ROZWIĄZANIE DEDYKOWANE. CZYM JEST I JAK PRACOWAĆ Z TYM POJĘCIEM?**

Ilość dostępnych na rynku narzędzi, rozwiązań i gotowych produktów informatycznych jest ogromna i dla osoby, która na co dzień nie jest związana z IT, może być zwyczajnie przytłaczająca lub powodować dezorientację. Szczególnie, kiedy zapotrzebowanie funkcjonalne obejmuje kilka niezależnych działów, a każdemu z nich chcemy pomóc, aby zapewnić płynność operacyjną firmy. W przypadku rozwijających się firm z sektora małych i średnich przedsiębiorstw, w pewnym momencie przed osobami zarządzającymi staje decyzja: czy wybrać gotowy produkt, czy postawić na rozwiązanie dedykowane.





W tym miejscu niezbędnym wydaje się krótkie wyjaśnienie, czym w ogóle jest to tajemnicze rozwiązanie dedykowane. Rozwiązanie dedykowane to takie, które tworzone jest od początku do końca zgodnie z zapotrzebowaniem klienta, a sam klient bierze aktywny udział w całym procesie wytwórczym - od momentu analiz funkcjonalnych, aż po testy akceptacyjne wypracowanych rozwiązań. Oczywiście nie musi być tak, że całość funkcjonalności jest realizowana od zera przez wykonawcę.

Jeśli jest jakieś gotowe rozwiązanie, które służyć może jako uzupełnienie funkcjonalności to najczęściej zapada decyzja o integracji (np. płatności, kurierzy, chatboty itp.), jednak większość procesów w budowanym systemie lub aplikacji jest realizowana na podstawie wcześniej wypracowanej specyfikacji funkcjonalnej, która stanowi podstawę do budowy systemu informatycznego, aplikacji webowej czy aplikacji mobilnej.

Praca nad dedykowanym rozwiązaniem jest trochę jak szycie garnituru na miarę. W pierwszej kolejności pobiera się wymiary, a w naszym przypadku realizuje się analizę potrzeb, która najczęściej ma formę warsztatów prowadzonych z klientem.



Wynikiem takiej analizy powinien być dokument, w którym możliwie jak najbardziej szczegółowo zostaną opisane kluczowe procesy oraz wszystkie funkcjonalności, które mają zostać zawarte w tworzonym rozwiązaniu. Dopiero mając taki dokument możliwe jest rzetelne podejście do wyceny i w dalszej kolejności - prac deweloperskich nad systemem lub aplikacją.

## ROZWIĄZANIE DEDYKOWANE A GOTOWE ROZWIĄZANIA

Z perspektywy klienta po wykonaniu wstępnej analizy rynku i dostępnych możliwości, zwykle okazuje się, że pozornie dopasowane do potrzeb rozwiązanie gotowe jest dużo tańsze niż rozwiązanie dedykowane. Nie bez powodu użyte zostało sformułowanie pozornie dopasowane, ale do tego pozwolę sobie wrócić w dalszej części. Teraz skupmy się na cenie.

Rozwiązanie gotowe często wydaje się tańsze od rozwiązań dedykowanych, chociaż w praktyce może okazać się, że koszty są porównywalne. Dlaczego nie widać tego na początku? Skupmy się na kilku kluczowych problemach:

### ZROZUMIENIE PROCESU WYCENY ROZWIĄZANIA DEDYKOWANEGO

patrząc na zapytania ofertowe, które trafiają do Sygnisoft, na 10 (a może nawet więcej) zapytań tylko 1 posiada gotowy draft lub chociaż zdefiniowany zakres funkcjonalności, co znacznie utrudnia przygotowanie rzetelnej oceny kosztów projektu, przez co pierwsza wycena może okazać się szeroko rozstawionymi widełkami, które w porównaniu z ceną rozwiązania gotowego mogą klienta przytłoczyć. Warto również zauważyć, że większość software house'ów na początku podaje wycenę wyższą, uwzględniając margines błędu, wynikający z braku lub niewystarczającej ilości informacji od klienta. Bardzo często zdarza się również, że klient wysyłając zapytanie o wycenę rozwiązania dedykowanego nie precyzuje swoich wymagań, oczekując, że zrobi to za niego potencjalny wykonawca.





Z tego powodu okazać się może, że przedstawiona wycena będzie nieadekwatna do rzeczywistych potrzeb biznesu klienta z uwagi na np. zbyt szerokie podejście do funkcji systemu. W końcu, to klient najlepiej zna potrzeby swojego biznesu, więc chcąc otrzymać rzetelną wycenę warto na początek zdefiniować oczekiwania względem przyszłego rozwiązania informatycznego.

### UKRYTE KOSZTY GOTOWYCH PRODUKTÓW

większość rozwiązań gotowych poza ceną wyjściową, która ładnie wygląda na stronie lub w folderze ofertowym, wiąże się z szeregiem opłat dodatkowych, o których klient dowiaduje się dopiero później, np. opłata licencyjna

aktualizacyjna, za moduły dodatkowe, za dostęp do API i inne, które finalnie mogą zbudować całkiem sporą sumę stałych kosztów płatnych cyklicznie. W tym miejscu warto również zaznaczyć, że większość producentów gotowych rozwiązań w pewnym momencie rezygnuje ze świadczenia usług wsparcia dla użytkowników. Przykładem mogą być znane powszechnie systemy ERP (Enterprise Resources Planning), które budują sieci partnerów, świadczących usługi wsparcia i utrzymania systemu. Należy więc wziąć pod uwagę koszty wsparcia, świadczonego przez zewnętrznego usługodawcę przy konfiguracji, awariach czy aktualizacjach systemu.



## BRAK LUB BARDZO OGRANICZONE MOŻLIWOŚCI ADAPTACYJNE

Jedną z większych wad rozwiązań gotowych jest to, że zakres funkcji, które udostępniają jest ograniczony, a możliwości adaptacyjne najczęściej mocno ograniczone - o ile w ogóle jakieś są. Tutaj możemy wrócić do wspomnianego wcześniej pozornego dopasowania - chociaż przeglądając funkcje produktu może wydawać się, że jest to właśnie to, czego oczekujemy i potrzebujemy, szybko okazuje się, że owszem system ma gotowy proces, jednak jest on zupełnie niezgodny z tym jak działa firma, lub mamy do wyboru kilka gotowych szablonów, żaden jednak nie spełnia naszych wymagań. Klient nie dość, że płaci za produkt, to musi dodatkowo zdecydować się na szereg ustępstw lub dokonać modyfikacji działania swojej organizacji do systemu - a tak być nie powinno.

**TO SYSTEM MA BYĆ DOPASOWANY  
DO POTRZEB FIRMY, A NIE FIRMA DO  
SYSTEMU - TO JAK Z GARNITUREM:  
ON MA PASOWAĆ NA CZŁOWIEKA,  
A NIE CZŁOWIEK DO NIEGO.**

W efekcie klient, aby uzyskać produkt końcowy o funkcjonalności zgodnej z jego rzeczywistym zapotrzebowaniem, często jest zmuszony do wyboru kilku rozwiązań gotowych i próby połączenia ich funkcjonalności na własną rękę, co często nie jest takie łatwe, jak może się początkowo wydawać. W innym przypadku brakujące funkcje można zbudować korzystając z usług firm trzecich, co wiąże się z kolejnymi kosztami i daje efekt produktu częściowo dedykowanego w cenie takiej samej, o ile nie wyższej niż system dedykowany, stworzony od A do Z dla nas.



## JEDNA DECYZJA, KTÓRA MOŻE KOSZTOWAĆ DUŻO W PRZYSZŁOŚCI

Decyzja o wyborze rozwiązania, które będzie odpowiednie dla firmy nigdy nie jest prosta. Często przychodzą do nas klienci, którzy są już zwyczajnie bezsilni i nie wiedzą, jakie rozwiązanie informatyczne pomoże im w dalszym rozwoju biznesu - i nie oszukujmy się, nie muszą tego wiedzieć, bo nie to jest zakresem ich specjalizacji.

Równie często są to klienci doświadczeni już wcześniej obietnicami, które nie zostały spełnione lub, co gorsza, mający za sobą decyzję zakupową gotowych produktów, które miały stworzyć wspólnie coś większego, jednak okazało się, że nie działa to tak, jak powinno albo nie działa wcale.

Nie od dziś wiadomo, że tańsze zwykle nie idzie w parze z lepsze, a większość ludzi zwyczajnie nie lubi, kiedy ich pieniądze idą w przysłowiowe błoto. W przypadku wyboru oprogramowania jedna decyzja zakupowa, która nie została dokładnie przeanalizowana, może wiązać się z ogromnymi kosztami wtórnymi.

W celu lepszego zobrazowania problemu posłużę się krótkim case study jednej z firm, z którymi ostatnio prowadziliśmy rozmowy.

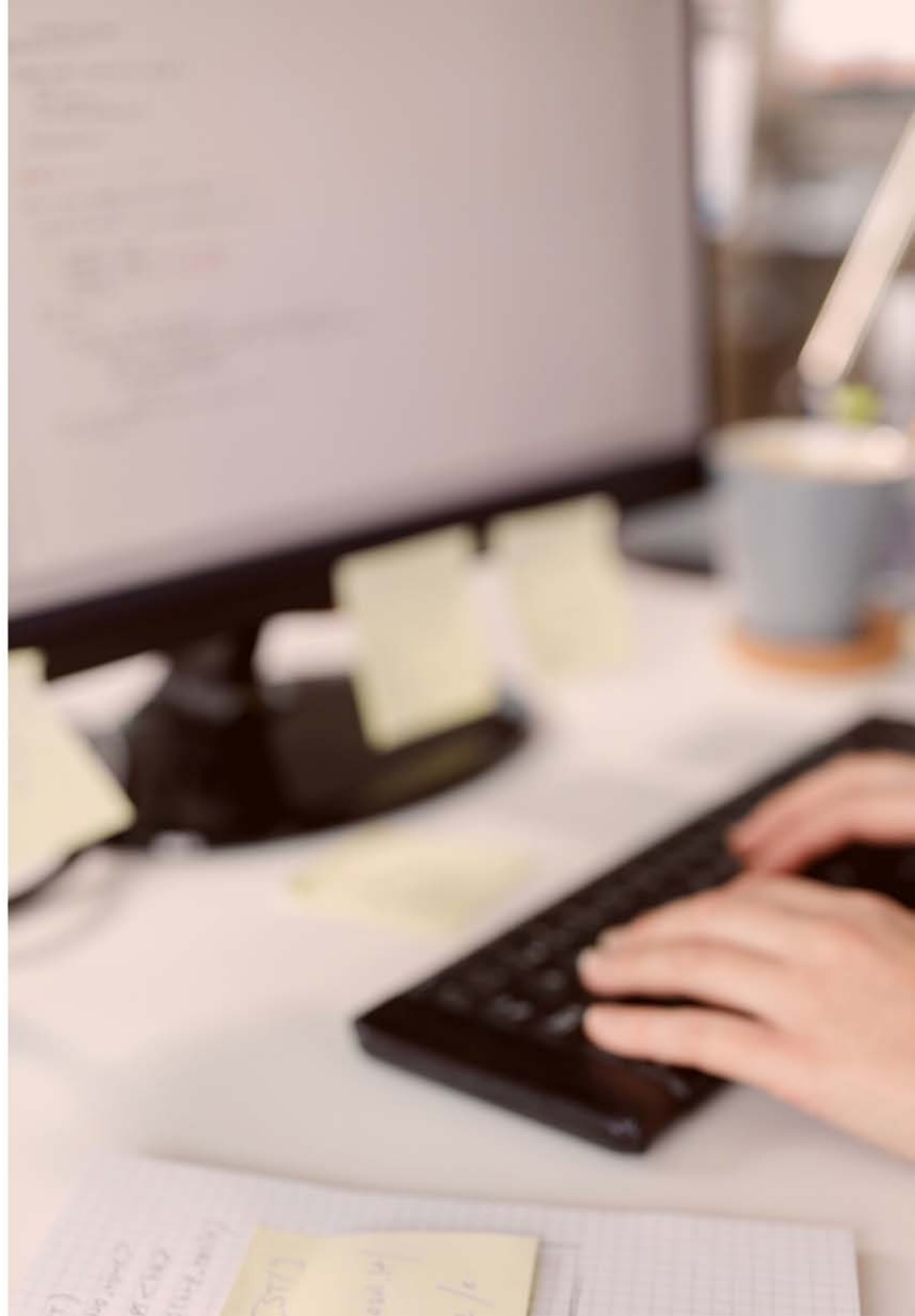
Jakiś czas temu przyszedł do nas klient, który poprosił o pomoc w konfiguracji i integracji dwóch rozwiązań gotowych, na których zakup firma się zdecydowała. Firma po latach działalności i pracy na rozwiązaniach, które już dawno przestały zaspokajać potrzeby procesowe, zdecydowała się na krok w stronę zakupu systemu informatycznego, który pomoże w optymalizacji procesów, szybszej obsłudze klientów i połączeniu pracy kilku działów w jednym narzędziu. Po analizie rynku decyzja została podjęta, a w firmie wdrożone dwa rozwiązania gotowe: system klasy ERP oraz sklep internetowy. Oba systemy zakupione zostały pod wpływem obietnic o łatwości integracji ich ze sobą.

Jak szybko się okazało integracja systemów okazała się nie być wcale łatwym procesem, zasoby wewnętrzne firmy nie wystarczyły, żeby samodzielnie skonfigurować i uruchomić nowe narzędzia, a firma zmuszona była do sięgnięcia po pomoc trzeciej organizacji, która miała prze-

prowadzić integrację zakupionych produktów. Czas wdrożenia się przedłużał, integracja została wykonana, a klient został zapewniony, że wszystko będzie działać jak należy. Co ciekawe, firma została jedynie poinformowana o prawidłowym przebiegu integracji, która nie miała pokrycia w żadnym dokumencie lub chociaż manualu, w jaki sposób obsługiwać oba systemy, aby proces przebiegał płynnie i umożliwiał pracę.

W efekcie okazało się, że klient nie wie, jak pracować na obu systemach, konfiguracja nadal nie była wykonana, a systemy nie działały. Po podjęciu kolejnych prób konfiguracyjnych przy użyciu zasobów własnych, klient postanowił jeszcze raz poszukać pomocy z zewnątrz.

Spójrzmy przez chwilę na orientacyjne koszty, jakimi był obciążony klient. Nie licząc opłat startowych za zakupione produkty, zanim otrzymaliśmy zapytanie klient już był po nieudanej próbie integracji, za którą zapłacił oraz płacił na bieżąco opłaty związane z utrzymaniem (licencje, środowiska, moduły integracyjne), chociaż systemy nie były używane. Do tego można doliczyć wewnętrzne koszty związane z próbami samodzielnej konfiguracji, analiz, ponownego po-







nowego poszukiwania wykonawcy, który będzie w stanie pomóc i doprowadzić systemy to stanu, w którym możliwa będzie praca przy ich użyciu.

Klient przyszedł do nas już mocno zniechęcony z naszkicowanym procesem: w jaki sposób chce, żeby to wszystko razem zadziało. I tylko tym. Nie było dokumentacji poprzednich wykonawców, wiedzy na temat przebiegu integracji oraz tego, czy i w jaki sposób zostało przygotowane mapowanie danych, które umożliwiłoby przepływ informacji pomiędzy zakupionymi systemami. Po wstępnych rozmowach okazało się, że wykonana integracja jest niekompletna i nawet przy naszych najlepszych chęciach udzielenia pomocy nie umożliwi w zastanej formie płynności realizacji procesu sprzedażowego, który od początku był zaplanowany przez klienta.

Ogólny wniosek był jeden: podsumowując koszty niezbędne do zapewnienia działania systemów w sposób, który obsłużyłby pełny proces klienta, zdecydowanie bardziej opłacalne byłoby stworzenie systemu dedykowanego, który na początku wydawał się rozwiązaniem droższym.

## INTEGRACJE SYSTEMÓW - JAK TO UGRYŹĆ?

Jeżeli w firmie zapada decyzja o zakupie rozwiązań gotowych warto pamiętać o dokładnej weryfikacji możliwości integracyjnych wybieranych systemów i analizie udostępnianego API pod kątem całości procesu, jaki ma zostać obsłużony. Dobrze jest już na etapie rozeznania rynku skorzystać z pomocy wykonawcy, który ma doświadczenie w integracji różnych rozwiązań i będzie w stanie przeprowadzić analizę oraz chociażby wstępne mapowanie zależności i przepływów danych między systemami. Same takie analizy są procesem kosztownym, jednak mogą zapobiec decyzji zakupowej, która przyniesie za sobą dużo wyższe straty finansowe i transakcyjne niż mogło się z początku wydawać.



W drugiej kolejności należy wziąć pod uwagę szacunki czasochłonności przeprowadzenia integracji systemów. Przy systemach ERP sam proces integracyjny potrafi zająć bardzo dużo czasu (od kilku tygodni nawet do kilku miesięcy), szczególnie biorąc pod uwagę obsłużenie całości procesu biznesowego. Już na etapie poszukiwania rozwiązania dobrze jest mieć sprecyzowane oczekiwania i potrzeby oraz przemyślany cały proces z uwzględnieniem różnych aktorów, biorących w nim udział, a także możliwych scenariuszy skrajnych. Takie podejście pomoże w identyfikacji możliwych ograniczeń i problemów, jakie mogą wystąpić podczas planowanej integracji.

I w końcu - warto wziąć pod uwagę to, czy nie lepiej zdecydować się na system dedykowany, który zrealizowany zostanie od początku do końca pod potrzeby organizacji i procesy w niej zachodzące. Szczególnie, że może okazać się, iż nie będzie on przy tym rozwiązaniem znacznie odbiegającym finansowo od całości kosztów związanych z oprogramowaniem gotowym.

### **PRZEWAGI ROZWIĄZANIA DEDYKOWANEGO**

Chociaż stworzenie systemu dedykowanego (w krótkim okresie) może wydawać się droższym przedsięwzięciem, podsumowując wszystkie koszty, jakie musi ponieść klient chcąc zapewnić płynne i optymalne działanie kilku rozwiązań gotowych, może okazać się, że finalna cena będzie mocno zbliżona, a niekiedy nawet wyższa niż rozwiązania autorskiego.

Przede wszystkim, rozwiązanie dedykowane pozwala na zbudowanie przewagi konkurencyjnej. Dzięki indywidualnemu podejściu do obsługiwanego w systemie procesu, całość zostaje stworzona zgodnie z wytycznymi. Inaczej jest w przypadku rozwiązania gotowego, którego funkcjonalności są takie same dla nas, jak i dla konkurencji.





Niewątpliwą zaletą systemów budowanych od podstaw na zlecenie klienta jest ich elastyczność i możliwości adaptacyjne. Z uwagi na to, że systemy takie z reguły buduje się etapowo, podczas całego procesu wytwórczego istnieje możliwość dostosowywania i bieżącej optymalizacji zaplanowanych funkcjonalności pod potrzeby biznesu oraz zmieniających się warunków. Dodatkowo, systemy dedykowane są zdecydowanie bardziej otwarte na dalszy rozwój, co pozostawia klientowi przestrzeń dla wdrażania nowych pomysłów i inicjatyw już po zakończeniu wdrożenia funkcjonalności wyjściowej.

Kolejnym ważnym aspektem jest dedykowany pod dany projekt zespół, który jest z klientem od samego początku (etap analiz i planingu funkcjonalnego) po testy końcowe systemu, a często nawet później, kiedy system jest już w fazie utrzymania. Taki model daje bezpieczeństwo i gwarancję, że osoby realizujące projekt będą znały jego historię i aktywnie uczestniczyły w całym procesie, zapewniając kompleksową obsługę klienta oraz bieżące wsparcie merytoryczno-techniczne.

Podsumowując, jeśli firma stoi przed wyborem rozwiązania, które w najlepszy sposób wspomogą jej dalszy rozwój, warto rozważyć wszystkie możliwe opcje. A także... zastanowić się: czy zadowalający będzie pospolity garnitur, który leży jako-tako, czy lepiej postawić na taki szyty na miarę, który idealnie dopasuje się do naszych preferencji.

# ZAGROŻENIA ZWIĄZANE Z NIELOJALNOŚCIĄ PRACOWNIKÓW

---



Dawid Mrowiec  
B-secure

**Niełojalne zachowania pracowników stanowią jeden z najistotniejszych obszarów zarządzania bezpieczeństwem przedsiębiorstwa. Generują one olbrzymie koszty (mieralne i niemieralne), trudno je zidentyfikować, a tym bardziej ciężko z nimi walczyć. Jakie są najczęściej występujące zagrożenia związane z pracowniczymi nadużyciami? Ile nas kosztują i których branż dotyczą najczęściej?**



Szeroko rozumiane nadużycia popełniane przez członków organizacji stanowią jedno z największych wyzwań w zakresie zarządzania ryzykiem w organizacji. Innymi słowy, jest to jeden z najistotniejszych tematów z obszaru zarządzania bezpieczeństwem.

Z badań na temat nadużyć prowadzonych przede wszystkim przez duże firmy audytorskie takie, jak PwC wynika, że odsetek nadużyć oscyluje w granicach około 50 procent. Szacowane ich koszty zazwyczaj są bardzo wysokie i zależą m.in. od pozycji sprawcy w hierarchii, zajmowanego stanowiska, charakteru nadużycia, czy czasu jego trwania.

## PRACOWNIK NIELOJALNY. PO CZYM GO POZNASZ?

Pracownik lojalny działa przede wszystkim w interesie pracodawcy i firmy. Działania te utożsamia także z własnym interesem. W swojej aktywności powstrzymuje się od zachowań, które w jakiś sposób mogłyby być sprzeczne z interesem jego firmy. Stara się także uniknąć szeroko rozumianego konfliktu interesów.

Pracownik niełojalny z kolei działa przede wszystkim w interesie własnym, sprzecznym z interesami pracodawcy i firmy. Niejednokrotnie działa także w interesie konkurencji, czy innych podmiotów, których dążenia są sprzeczne z interesem zatrudniającej go organizacji.

Pracownik lojalny będzie chronił materialne i niematerialne zasoby firmy. Pracownik niełojalny nie interesuje się ochroną zasobów firmy. Lojalny pracownik reaguje na niebezpieczeństwa grożące zasobom organizacji, nie wykorzystuje ich też do celów prywatnych bez zgody pracodawcy.

Z kolei pracownik nielojalny nie interesuje się tego typu rzeczami, a więc: ignoruje zagrożenia zasobów firmy, nadużywa i wykorzystuje powierzone mu zasoby niezgodnie z ich przeznaczeniem. Często też wykorzystuje zasoby organizacji do realizacji własnych interesów niezwiązanych bezpośrednio z dobrem firmy.

Pracownik lojalny podejmuje osobistą odpowiedzialność za wykonywaną pracę i pełnione w ramach organizacji funkcje. Z kolei pracownik nielojalny nie czuje się odpowiedzialny za wykonywaną pracę i pełnione funkcje. Lojalny pracownik będzie zwracał uwagę na problemy organizacji i w jakiś sposób dążył do ich rozwiązania. Będzie także sygnalizował problemy i nieprawidłowości występujących w miejscu pracy: czy to kierownictwu, współpracownikom czy właścicielom. Z kolei nielojalny pracownik nie interesuje się problemami firmy. Nie będzie sygnalizował zaobserwowanych nieprawidłowości, ewentualnie będzie przekazywał te informacje osobom niepowołanym (np. przedstawicielom konkurencji). Wreszcie pracownik lojalny troszczy się o sukces firmy.

Swoimi działaniami stara się przyczynić do jej rozwoju. Utożsamia także sukces firmy ze swoim własnym. Z kolei nielojalny pracownik na pewno nie będzie zainteresowany sukcesem swojej firmy. I co istotne, w najmniejszym stopniu nie będzie wiązał sukcesu firmy ze swoim własnym.

**Jak więc widać, w pewien sposób lojalność i nielojalność to dwa przeciwstawne bieguny. Każdy z pracowników może zostać umiejscowiony na tym wymiarze: czy to bliżej ideału lojalności czy nielojalności. Warto o tym pamiętać.**

Warto także mieć na uwadze, że pracownik powinien być oceniany sytuacyjnie. To znaczy, na przykład nie zawsze informowanie podmiotów spoza firmy będzie działaniem, które powinniśmy uznać ewidentnie za przejaw nielojalności pracowniczej.

## JAK ROZUMIEĆ NIELOJALNOŚĆ PRACOWNICZĄ?

Problematyka nielojalności pracowniczej jest różnie rozumiana w literaturze naukowej, ale też



różnie ujmowana w praktyce doradczej, audytorskiej itd.

**Pojęciami istotnie związanymi z nielojalnością pracowniczą są bez wątpienia zachowania nieetyczne, a więc zachowania, które kolidują z powszechnie przyjmowanymi zasadami etyki, czy z normami etycznymi przyjętymi w samej organizacji.**

Częstym hasłem używanym szczególnie przez media, ale także w wielu opracowaniach o charakterze eksperckim są po prostu nadużycia. W przedsiębiorstwie jest to dość szeroka kategoria. Oczywiście nie dotyczy tylko nielojalnych zachowań pracowników, ale może dotyczyć także np. władz przedsiębiorstwa.

Inne pojęcie związane z nielojalnością to patologie w firmie. Jest to pojęcie bardzo szerokie. Jeszcze innym określeniem nielojalnych zachowań, przynajmniej częściowo związanych z omawianym problemem, są dewiacje w miejscu pracy, które również, podobnie jak patologie, można traktować dość szeroko.

Mówiąc o nielojalności pracowniczej jako problemie zarządzania bezpieczeństwem mamy na myśli przede wszystkim zagrożenia związane z zachowaniami pracowników, które naruszają relację lojalności łączącą ich z firmą (organizacją), i które w konsekwencji generują ryzyko.

## **GŁÓWNE ZAGROŻENIA ZWIĄZANE Z NIEUDOLNOŚCIĄ PRACOWNIKÓW**

Pierwszym z nich jest kradzież składników majątkowych przedsiębiorstwa.



Przykładami może być kradzież paliwa, narzędzi, czy zapasów produkcyjnych. Podobną kategorię do kradzieży stanowią przywłaszczenia i sprzeniewierzenia składników majątkowych przedsiębiorstwa. Polegają one z jednej strony na nadużyciu swojego stanowiska do przywłaszczenia np. części materiałów z magazynu, czy też sprzeniewierzenia np. pieniędzy, odzieży roboczej czy telefonu służbowego.

Innym bardzo często występującym i szczególnie niebezpiecznym zagrożeniem są oszustwa. Istotą oszustwa jest wykorzystanie błędu bądź celowe wprowadzenie w błąd. Dzięki temu sprawca uzyskuje jakieś korzyści. Zwykle są to korzyści majątkowe. Przykładem oszustwa może być posłużenie się nieprawdziwymi dokumentami w celu zafałszowania stanu faktycznego magazynu, czy zafałszowanie pomiarów ilości lub wagi towarów w celu spieniężenia nadwyżek.

Kolejna kategoria zagrożeń to sabotaż oraz zachowania kontrproduktywne. Pojęcie to oznacza działanie na szkodę lub zaniechanie działania, które ma na celu wywołanie strat, ale także **bezczytność** w sytuacjach, gdy od pracownika wymagane jest działanie (np. pracownik obserwuje jakąś awarię i nie podejmuje żadnych działań w celu zapobieżenia jej skutkom).

Innym przejawem tego typu działań jest marnotrawstwo zasobów. Przykład tego zagrożenia to sytuacja, w której pracownik celowo uszkadza maszynę, wywołuje skażenie niedopuszczalną substancją, czy niszczy partię wytwarzanego produktu.

Kolejna bardzo ciekawa kategoria zagrożeń to szpiegostwo gospodarcze, a także kradzież informacji i wiedzy. Przykładami takich zagrożeń jest kopiowanie dokumentacji dotyczącej np. nowego produktu i sprzedaż jej konkurencji, czy wynoszenie informacji na temat zabezpieczeń w celu przekazania ich grupie przestępczej, która planuje zaatakować firmę.



Zagrożeniem, które spędza sen z powiek przede wszystkim menedżerom, to **nadużycie zaufania** (karalna niegospodarność). Polega ono, najprościej mówiąc, na **nadużyciu przez sprawcę uprawnień lub niedopełnienia obowiązków** w wyniku czego organizacji ponosi znaczna szkodę majątkową. Przykładem tego zagrożenia będzie sytuacja, w której menedżer mimo podejrzeń akceptuje umowę opracowaną przez swojego podwładnego, która finalnie powoduje wysokie straty finansowe po stronie spółki.

Innym bardzo powszechnym zagrożeniem jest **kradzież czasu pracy**: polega ona na częstym przeznaczeniu czasu pracy na czynności niezwiązane z pracą. Chciałbym zaznaczyć, że nie chodzi tu o to, że jeśli ktoś w pracy zrobi sobie pięciominutową przerwę na przeglądanie Facebooka, to od razu jest złodziejem czasu pracy. Chodzi tutaj o bardzo częste podejmowanie tego typu czynności, co jest oszukiwaniem swojego pracodawcy, który - jakby na to nie patrzeć - jednak płaci nam za to, że określoną ilość czasu poświęcamy pracy na jego rzecz. Przykładami kradzieży czasu pracy będzie: znaczne przeciąganie przerw, częste wy-

chodzenie z pracy przed czasem, czy też długotrwałe przeglądanie Internetu w celach niezwiązanych z pracą.

Dobrze znanym z mediów typem zagrożenia jest **korupcja gospodarcza**, która w kontekście pracowniczej nielojalności przejawia się głównie w postaci **przekupstwa**. A przykładem tego zagrożenia będzie sytuacja, gdy menedżer odpowiadający za marketing przejmuje od konkurencyjnej firmy łapówkę jako ekwiwalent obniżenia swojej sprawności menedżerskiej na czas wprowadzenia na rynek nowej serii produktów zatrudniającej go firmy.





Kolejne niebezpieczeństwo z omawianej grupy to fałszowanie dokumentacji dotyczącej działalności gospodarczej. Ryzyko to może przejawiać się w niszczeniu, przerabianiu, usuwaniu lub podrabianiu dokumentów.

Inna kategoria zagrożeń, trudna do jednoznacznego uchwycenia, aczkolwiek bez wątpienia będąca znakiem naszych czasów, to cyber-nadużycia. Tego typu zagrożenia wiążą się z wykorzystaniem komputera i sieci internetowej do szkodliwej dla firmy działalności. Przykładem cyber-nadużycia może być złamanie wewnętrznych zabezpieczeń w celu ułatwienia ataku hakerskiego z zewnątrz, bądź wykorzystanie znajomości zabezpieczeń komputera do kradzieży pieniędzy firmy.

**Wszystkie wspomniane wyżej typy nadużyć mogą łączyć się ze sobą, np. korupcja może się wiązać z fałszowaniem dokumentacji firmowej.**

## **BRANŻE SZCZEGÓLNIE ZAGROŻONE NIELOJALNOŚCIĄ PRACOWNICZĄ**

Jeśli już wiemy, co może zagrażać firmom w związku z niełojalnością pracowniczą, dobrze byłoby wiedzieć, które firmy w tym kontekście są najbardziej eksponowane na ryzyko.

Odwołajmy się do badania Association of Certified Fraud Examiners (ACFE), która publikuje bardzo rzetelny i sporządzony na dużej grupie raport dotyczący nadużyć w przedsiębiorstwach. Wyniki tych badań wskazują, że najbardziej zagrożone i poszkodowane organizacje to małe firmy zatrudniające poniżej 100 osób.



W drugiej kolejności zagrożone są przedsiębiorstwa, które zatrudniają od 1000 do 10000 pracowników. Względnie najbezpieczniejsze wydają się firmy największe, czyli powyżej 10000 pracowników oraz między 100 a 1000 osób. Trzeba jednak pamiętać, że średnia strat w przypadku największych firm wynosi zdecydowanie najwięcej.

**Jeśli chodzi o najbardziej zagrożone branże (obszary działalności), są to:**

- bank i sektor finansowy,
- sprzedaż i obsługa klienta,
- transport i logistyka,
- przemysł wytwórczy,
- komunikacja i łączność,
- przemysł lotniczy i obronny,
- sektor ubezpieczeń,
- sektor energetyczny,
- rozrywka i media,
- sektor budownictwa,
- sektor technologiczny,
- przemysł samochodowy,
- opieka zdrowotna,
- edukacja,
- przemysł chemiczny,
- profesjonalne usługi.



## KOSZTY NIEŁOJALNOŚCI PRACOWNIKA

Większość badań stara się uchwycić koszty pracowniczej niełojalności. Trzeba jednak zdawać sobie sprawę, że koszty tego zjawiska są trudne do oszacowania. Zasadniczo można podzielić je na koszty mierzalne i niemierzalne.

### Mierzalne koszty niełojalności pracowniczej obejmują:

- stratę środków pieniężnych,
- stratę środków trwałych,
- stratę zapasów.

### Jeśli chodzi o koszty niemierzalne, to niełojalność pracownicza wpływa na:

- morale pracowników,
- reputację przedsiębiorstwa,
- relacje biznesowe,
- relacje z organami regulacyjnymi czy nadzorczymi,
- kulturę organizacyjną,
- proces produkcji,
- w przypadku spółek akcyjnych także na cenę akcji oraz na samych udziałowców.

Dodatkowo niełojalne zachowania pracowników mogą zniechęcać do firmy klientów oraz potencjalnych przyszłych pracowników (to z kolei rodzi m.in. ryzyko niedoborów kadrowych).

Koszty niemierzalne, mimo że trudniejsze do uchwycenia w przemawiających do wyobraźni liczbach, mogą być dla firm znacznie bardziej krytyczne, gdyż uderzają w zasoby organizacji, które na ogół bardzo trudno odtworzyć, a także zakłócają funkcjonalność procesów, które decydują o tym, czy firma będzie w stanie realizować swoje cele.





Nielojalność nie tylko niszczy organizację od wewnątrz ze wszystkimi tego konsekwencjami, ale także niszczy ją z zewnątrz uderzając w reputację oraz wizerunek przedsiębiorstwa, co pociąga za sobą spadek liczby i jakości zasobów relacyjnych, które są kluczowe dla sukcesu w świecie sieciowej gospodarki.

Wszystko to sprawia, że problem nielojalności pracowniczej jest bardzo poważny i kosztowny dla wszystkich organizacji, niezależnie od tego czy są małe czy duże. Znaczenie tego problemu dla bezpieczeństwa przedsiębiorstwa rośnie drastycznie w okresie kryzysu gospodarczego, który niewątpliwie sprzyja nasileniu zjawiska nadużyć.

Musimy sobie też otwarcie powiedzieć, że nielojalność pracowników to niejako temat tabu. Jest bardzo mało badań naukowych poruszających ten temat, ze względu na trudności w badaniu tego zjawiska. Wynika to z tego, że nie tylko sami sprawcy z oczywistych względów chcą ukryć swoje niegodziwe działania, ale często ukrywają je także same pokrzywdzone organizacje, widząc w ich ujawnianiu źródło dodatkowych problemów.

## JAK SOBIE RADZIĆ Z NIELOJALNOŚCIĄ PRACOWNICZĄ?

Musimy pamiętać, że różne zagrożenia wymagają innego podejścia. Inaczej przeciwdziała się szpiegostwu gospodarczemu, inaczej ogranicza się problem kradzieży czasu pracy. Trzeba jednak pamiętać, że przedsiębiorstwa narażone są na większość, jeśli nie na wszystkie z wymienionych typów zagrożeń. Dlatego najlepszym sposobem jest systematyczne, całościowe podejście do problemu pracowniczej niełojalności.

Moim zdaniem, istnieje kilka kluczowych obszarów, które wspólnie pomagają sobie radzić skutecznie z tym problemem. Są nimi:

### **REKRUTACJA I DEREKRUTACJA PRACOWNIKÓW**

właściwy dobór, ale również przemyślane praktyki w zakresie zwalniania pracowników;

### **WSPIERANIE LOJALNOŚCI PRACOWNIKÓW**

wielokierunkowe działania podejmowane przez organizację, mające na celu pielęgnowanie lojalności i pożądanych postaw zatrudnionych osób;

### **KONTROLA LOJALNOŚCI ORAZ WYKRYWANIE ZACHOWAŃ NIELOJALNYCH**

pomiar i ocena poziomu lojalności, a także wykorzystanie zróżnicowanych sposobów identyfikacji zachowań niełojalnych;

### **WYJAŚNIANIE ZIDENTYFIKOWANYCH NADUŻYĆ**

pracowniczych (postępowania wyjaśniające) i karanie ich sprawców.

Co istotne, działanie tylko w jednym ze wskazanych kierunków to zdecydowanie za mało. Dlatego tak kluczowe jest holistyczne i systematyczne podejście.





# OBSŁUGA PRAWNA E-COMMERCE



# BIZNESOWE SOCIAL MEDIA POD OSTRZAŁEM HAKERÓW. JAK UNIKAĆ WYCIEKÓW?



Redakcja  
SECURITY MAGAZINE

**70% Polaków ma aktywne konta na portalach społecznościowych. Takie liczby są łasym kąskiem dla hakerów. W 2021 roku z tych kanałów wyciekło ponad miliard (!) danych w skali całego świata. Ostatnio obserwujemy wzmożone ataki na typowo biznesowe serwisy, tam gdzie rozwijane są relacje biznesowe, gdzie toczą się rozmowy współpracowników, partnerów, gdzie przekazywane są często dane poufne czy wrażliwe. Jak chronić dane przed wyciekami na Facebooku, LinkedIn czy Twitterze?**







## BEZPIECZNY MAIL - PODSTAWĄ BEZPIECZEŃSTWA W SOCIAL MEDIA

Jednym wyciekiem można narazić na szwank reputację całej firmy i jej wizerunek budowany latami. Wielu przedsiębiorców nadal nie rozumie, jak ważna jest ochrona danych, które znajdują się na naszym profilu (konto prywatne lub firmowe), w naszej korespondencji (wiadomości prywatne, czaty, pokoje) czy zarchiwizowanych live'ach, webinarach, wideokonferencjach, filmach, zdjęciach, screenshottach. Nie wspominając o danych pozyskanych z menedżera reklam (w tym dane karty kredytowej).

Dostęp do naszych kont, czy to prywatnych czy firmowych opiera się na mailu, za pomocą którego rejestrowaliśmy je. Dlatego kluczowe jest, by oprócz samych kont używać bezpiecznego adresu mailowego. Sprawdzenie, czy padł on "ofiara" wycieku lub wycieków jest banalnie proste. Można do tego użyć narzędzia stworzonego przez Troy'a Hunt'a, dyrektora regionalnego Microsoftu - "Have I been pwned".

Jest to darmowy portal pozwalający na sprawdzenie, czy używane przez nas adresy mailowe są nadal bezpieczne. Jego historia sięga 2013 roku i jest to data masowego wycieku danych w firmie Adobe. To właśnie rozpowszechnienie naruszeń danych w połączeniu z analizą ataku Adobe doprowadziło Troya Hunta, australijskiego eksperta ds. bezpieczeństwa cybernetycznego, blogera i mówcę, do stworzenia **HIBP**. Jak może nam pomóc to narzędzie? To skarbnica wiedzy o naruszeniach danych osobowych, które są już publiczne. Będąc na stronie, należy wpisać adres e-mail, który chcemy sprawdzić.

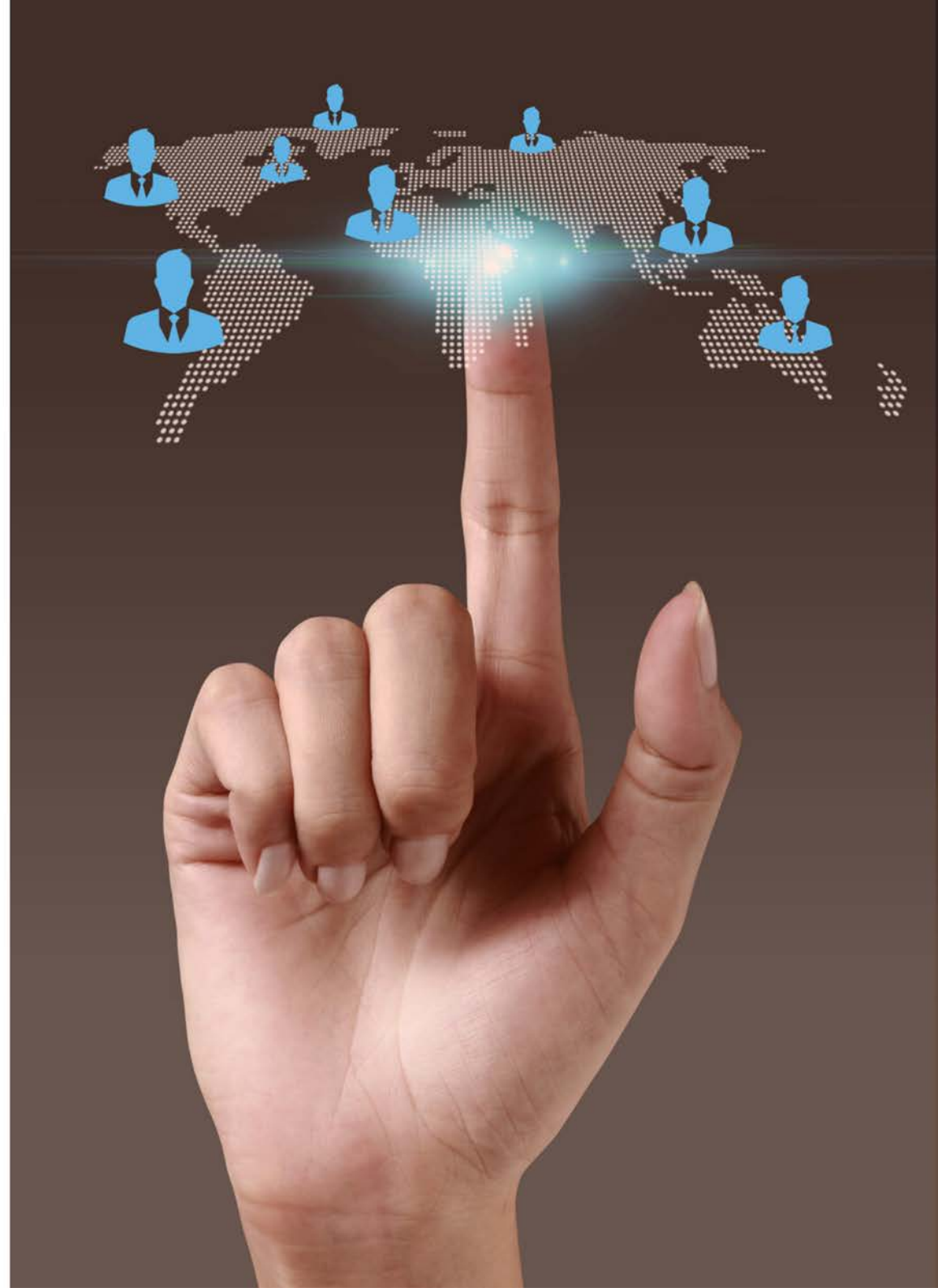


Po tym natychmiast uzyskamy informację, czy audytowany przez nas adres znalazł się na czerwonej liście, tzn. czy został powiązany z wyciekiem danych. To nie wszystko, bo dowiemy się, z jakim konkretnie wyciekiem ofiarą padł nasz adres e-mail, kiedy miał miejsce oraz jakie dane zostały ujawnione (np hasło, login czy lokalizacja). Z kolei, jeśli sprawdzany adres mailowy nie wyciekł, informacje o tym, że jest bezpieczny wyświetlą się w kolorze zielonym.

Możliwe jest także sprawdzenie, czy używane hasło jest wystarczająco bezpieczne, czy nie jest ono dostępne publicznie po wycieku czy kradzieży danych. Po wpisaniu go do wyszukiwarki otrzymamy stosowny komunikat. Osobiście jednak radzimy nie testować haseł, które nas jeszcze nie zawiodły - ze względu właśnie na ich bezpieczeństwo. Nigdy nie mamy pewności, które inne programy pracują w tle.

Wróćmy do social mediów. Dla biznesu w Polsce pod względem budowania relacji biznesowych kluczowe są obecnie trzy serwisy społecznościowe:

- **LinkedIn**
- **Facebook (Messenger, WhatsApp)**
- **Twitter.**





Dlaczego LinkedIn? Z założenia to serwis o charakterze biznesowym. Daje możliwość dzielenia się ekspercką wiedzą i nawiązywania nowych kontaktów. To również narzędzie dla rekruterów, ale także dla marketerów w szczególności B2B. Jest idealnym miejscem budowania wizerunku brandu, a pracowników firm może wykreować jako ekspertów. To także miejsce, gdzie stosunkowo prosto jest zdobyć leady sprzedażowe, a to ze względu na społeczność, którą tworzą w znacznej większości osoby decyzyjne w firmach.

Dlaczego Facebook, Messenger i WhatsApp? Meta ma w swoich rękach potężne narzędzie, jakim jest Messenger. To za jego pośrednictwem nawiązywane są relacje biznesowe, to tego narzędzia używa się zarówno do zewnętrznych, jak wewnętrznych spotkań online. Są biznesy, które nie mając własnej strony internetowej korzystają z tego medium w ten sposób, że podpinają domenę z nazwą firmy pod fanpage. Profil na Facebooku daje możliwość nie tylko szybkiego kontaktu marki z klientem, ale również z partnerami biznesowymi, współpracownikami czy pracownikami firmy. Z myślą o biznesie Facebook wprowadził menedżera firmy.

Jest on podstawowym miejscem, w którym można zarządzać całą swoją aktywnością marketingową i reklamową w serwisie. Powstał z myślą o firmach, by nie tylko tworzyć reklamy, zarządzać zasobami, ale pozwala też na dostęp do tych zasobów członkom zespołu czy partnerom zewnętrznym.

Dlaczego Twitter? Kojarzony głównie z polityką i publicystyką, jednak niesłusznie. Bo biznes również znajduje tam swoje miejsce. To idealny serwis społecznościowy dla tych marek, które po pierwsze prowadzą zaangażowany społecznie marketing, a po drugie, którym zależy na relacjach z sektorem public. Tak samo, jak na LinkedIn, możemy kontaktować się z osobami decyzyjnymi, ale również publicznymi, influencerami, samorządowcami. Wszyscy ci mogą stać się Twoimi potencjalnymi partnerami biznesowymi.

**SOCIAL MEDIA DAJĄ  
MOŻLIWOŚĆ DZIELENIA SIĘ  
EKSPERCKĄ WIEDZĄ  
I NAWIĄZYWANIA NOWYCH  
KONTAKTÓW BIZNESOWYCH.**



Social media dają ogrom możliwości, są dziś nieodłącznym elementem budowania wizerunku i relacji biznesowych. Mają jednak również swoją czarną stronę. Jak i strony internetowe, tak i social media stają się ofiarami ataków hakerskich, które w konsekwencji wyrządzają ogromne szkody nie tylko serwisowi jako takiemu, ale również milionom jego użytkowników, w tym, oczywiście firmom.

## POWODY HACKINGU

W przeciągu ostatnich 10 lat media społecznościowe urosły czterokrotnie. W 2010 roku z social mediów korzystało 970 mln ludzi, dziś co drugi człowiek na świecie z nich korzysta - to prawie 4,5 miliarda ludzi. To potężna baza zgromadzonych w jednym miejscu danych, która kusi hakerów z różnych powodów.

### Są to najczęściej:

- chęć zarobku (szantażowanie ofiary czy sprzedaż danych albo włam na konto bankowe),
- zemsta,
- chęć zniszczenia wizerunku marki, firmy, człowieka,
- zabawa,
- testowanie na ofierze różnych sposobów hackingu.



Bez względu na to, jaki powód ma haker, skutki dla ofiary mogą być dramatyczne.

**W przypadku social mediów możemy mówić o trzech najważniejszych powodach:**

1. chęć sprzedaży danych osobowych ich użytkowników,
2. udowodnienie, jak wiele luk bezpieczeństwa ma dany portal,
3. utrata reputacji niektórych osób przez upublicznienie danych na ich temat (tu flagowym przykładem jest wyciek danych (w tym numer telefonu) z Facebooka samego twórcy portalu, Marka Zuckerberga.

Przyjrzyjmy się, o których wyciekach było głośno w ciągu ostatniego roku.

## **NAJWIĘKSZE WYCIEKI DANYCH Z FACEBOOKA**

Publiczne dyskusje na temat bezpieczeństwa i ochrony prywatności nie tylko na Facebooku, ale wszystkich social media rozpoczęły się po aferze z Cambridge Analytica w 2018 roku. Firma ta gromadziła i analizowała dane 50 mln amerykańskich użytkowników Facebooka.

Baza danych pomogła trafić do właściwych wyborców, a tym samym - uważa się - że kierowane do nich spersonalizowane przekazy polityczne wpłynęły na wygraną Donalda Trumpa w wyborach 2016 roku.

Facebook był nawet oskarżany o bierność w tym temacie.

Dopiero wówczas wprowadzone tam zostały nowe ustawienia prywatności, które dawały osobom korzystającym z platformy większą kontrolę nad udostępnionymi informacjami. Jednak... do kradzieży danych osobowych nadal dochodzi.

O pierwszym w 2021 roku rozmawiano w kwietniu. Ofiarą padło wówczas 533 milionów(!) kont użytkow-





ników, w tym sam założyciel Facebooka, Mark Zuckerberg. Upublicznione zostały dane z 2,6 mln kont Polaków.

Największy do tej pory atak hakerski na Facebooka miał miejsce jesienią 2021 roku. Pod koniec września użytkownik znanego forum hakerskiego napisał ogłoszenie, w którym twierdził, że jest w posiadaniu danych osobowych ponad 1,5 miliarda(!!) użytkowników Facebooka. Dane były wystawione na sprzedaż na platformie forum. Jeden z potencjalnych nabywców twierdził, że otrzymał za 5000 USD dane miliona kont użytkowników tego serwisu.

## **JAK CHRONIĆ DANE PRZED WYCIEKAMI NA FACEBOOKU?**

Twoje dane to nie tylko imię i nazwisko. To Twój adres mailowy, numer telefonu, historia rozmów na Messengerze, tym zawodowych również, Twoje zdjęcia, treści postów. Jeśli używasz Messengera czy WhatsAppa do rozmów z klientami, współpracownikami, pracownikami, partnerami biznesowymi, warto sprawdzić czy już nie padłeś ofiarą wycieku danych. Można to zrobić za pośrednictwem wspomnianej już strony [haveibeenpwned.com](https://haveibeenpwned.com). Nie musisz się logować, wystarczy, że w okno znajdujące się na wprost Twojego wzroku wpiszesz adres, na który zarejestrowałeś swoje konto. Co ważne, strona ta sprawdzi nie tylko, czy dane wyciekły z Facebooka, ale z każdego innego źródła. Po wpisaniu adresu dostaniesz szczegółowe informacje, czy jest on bezpieczny czy został już zhakowany.



Natomiast jak chronić dane przed przyszłymi atakami? Aby zapobiec włamaniu na konta, wykorzystaniu ich w niewłaściwy sposób lub posłużeniu się nimi bez zgody użytkownika, należy poświęcić trochę czasu na przeprowadzenie kontroli bezpieczeństwa, by sprawdzić, czy obecne ustawienia zabezpieczeń są właściwe.

Można ją wykonać w zakładce "Privacy, Safety and Securit" na Facebooku poprzez kliknięcie w "Rozpocznij kontrolę zabezpieczeń". Przejdziemy przez weryfikację tożsamości a dzięki kontroli zabezpieczeń można otrzymywać powiadomienia, gdy ktoś spróbuje zalogować się do konta z nieznanego komputera lub urządzenia mobilnego, dowiedzieć się, jak chronić hasło i włączyć uwierzytelnianie dwuskładnikowe – opcjonalną funkcję zwiększającą bezpieczeństwo.

**Uwierzytelnianie dwuskładnikowe to najłatwiejszy i bardzo skuteczny sposób ochrony. To dodatkowa, oprócz hasła przy logowaniu, metoda zabezpieczająca, którą można samemu wybrać:**

**FIZYCZNY KLUCZ** - urządzenie przypominające swoim wyglądem pamięć zewnętrzną i tak też się z niego korzysta. Urządzenie to jest wpinane w port USB komputera. Zanim zakupimy taki klucz zabezpieczeń, należy upewnić się, że jest on obsługiwany przez przeglądarkę i urządzenie, za pomocą których logujemy się do konta.

**WIADOMOŚCI SMS Z KODAMI** które będziemy otrzymywać za każdym razem, kiedy logujemy się na konto.

**APLIKACJE UWIERZYTELNIAJĄCE** - zewnętrzna aplikacja uwierzytelniająca typu Google Authenticator lub LastPass, która generuje kody logowania ułatwiające potwierdzenie tożsamości podczas pierwszego logowania na nowym urządzeniu.

Początkiem 2022 roku Meta wprowadziła opcję mającą na celu dodatkową ochronę jego użytkowników. To Facebook Protect uruchomiony ponad pół roku temu. Serwis sam sprawdza, który użytkownik należy do "grupy ryzyka" i wymusza na nim włączenie dodatkowych zabezpieczeń pod rygorem blokady konta.

Wszystko z myślą o jego bezpieczeństwie, dlatego prędzej czy później warto te dodatkowe zabezpieczenia uruchomić. Facebook Protect to głównie wymuszenie uwierzytelniania dwuetapowego i dodatkowego skanowania konta w celu ewentualnego wykrycia nieprawidłowości.

Nie do wszystkich trafi powiadomienie o przymusie włączenia tej dodatkowej funkcji zabezpieczającej.

**Jeśli prowadzisz konto lub konta, które obserwuje masa odbiorców, Facebook może uznać, że objęcie ich dodatkową ochroną jest konieczne. Wówczas dostaniesz powiadomienie, że musisz włączyć tę opcję. W przypadku, gdy tego nie zrobisz, Twoje konto prywatne zostanie zablokowane, a co za tym idzie, stracisz dostęp do kont firmowych.**

Tak konieczność ochrony tłumaczy Facebook: "Twoje konto może być potencjalnie odwiedzane przez znacznie większą liczbę osób niż w przypadku przeciętnego użytkownika Facebooka. Hakerzy często atakują konta o dużej liczbie obserwujących, zawierające ważne strony lub istotne dla społeczności. Aby ułatwić ochronę przed tymi ukierunkowanymi atakami, wymagamy włączenia tego zaawansowanego programu zabezpieczeń."

Jak włączyć tę funkcję? Facebook sam się o to upomni. Kiedy na ekranie podczas logowania się do serwisu, pojawi Ci się informacja o "Facebook Protect", nie cofaj się, nie wyłączaj tego okna. Uruchomienie Facebook Protect zajmuje kilkanaście sekund.







Jeśli natomiast wycofasz się, powiadomienie możesz za jakiś czas otrzymać ponownie. Facebook poinformuje Cię, do kiedy masz czas i co stanie się, jeśli odmówisz.

## **LUKI W APLIKACJI LINKEDIN?**

W tamtym roku mówiło się o dwóch atakach na LinkedIn. Pierwszy z nich miał prawdopodobnie miejsce kilka dni po kwietniowym ataku na Facebooka. Prawdopodobnie, ponieważ nie ma pewności czy informacja o incydencie była równoznaczna z terminem samego ataku - czy przeprowadzono go dużo wcześniej.

Ofiarami padło 500 mln użytkowników, a ich dane miały być wystawione na sprzedaż, z czego 2 mln rekordów zostało opublikowanych publicznie na znak wiarygodności danych posiadanych przez sprzedającego. Dotyczyły one identyfikatorów LinkedIn, pełnych nazw profili, adresów e-mail, numerów telefonów, płci, linków do innych kont w social mediach, tytułów zawodowych i informacji o miejscach pracy. Tego typu informacje hakerzy mogą wykorzystać nie tylko do sprzedaży, ale także do ataków phishingowych, spamowych czy wymuszania hasła.

W lipcu dowiedzieliśmy się o kolejnym ataku na ten sam portal, tym razem naruszenie mogło dotyczyć aż 92% użytkowników tego serwisu, w tym 4,2 mln Polaków. Najprawdopodobniej wyciek to konsekwencja ataku na interfejs programowania aplikacji.

Tutaj również baza danych, pochodzących z lat 2020-2021 - była wystawiona na sprzedaż i zawierała następujące informacje: adresy e-mail, imiona i nazwiska, adresy, dane o geolokalizacji, adresy URL profili użytkowników w serwisie LinkedIn, doświadczenia osobiste i zawodowe, płeć, informacje o kontach w innych mediach społecznościowych. Nie ma tu haseł dostępu.

- Badamy zestaw rzekomych danych LinkedIn, które zostały wystawione na sprzedaż. Chcemy wyraźnie zaznaczyć, że nie było to naruszenie danych i żadne prywatne dane członków LinkedIn nie zostały ujawnione. Nasze wstępne dochodzenie wykazało, że rzeczywiście dane te zostały pozyskane z LinkedIn i innych różnych stron internetowych, ale obejmują te same dane, które trafiły do sieci w wyniku naruszenia, o którym informowaliśmy wcześniej w kwietniu tego roku - napisał w oficjalnym oświadczeniu LinkedIn.

Później przekazana została informacja, że do "wycieku" de facto nie doszło, a jedynie ktoś

zebrał publicznie dostępne informacje i dalej je udostępnił. Emocje wzbudził fakt, że mimo iż dane są publiczne, to wykorzystano je do dalszego rozpowszechniania bez wiedzy użytkowników.

## LINKEDIN - NAJWIĘCEJ ATA-KÓW PHISHINGOWYCH

Raport Check Point Research "Q1 Brand Phishing Report" zaprezentował zestawienie marek, pod które w pierwszych trzech miesiącach tego roku hakerzy najczęściej się podszywali, by wyłudzić od użytkowników dane osobowe i dane uwierzytelniające płatności. Chyba nikt nie spodziewał się, że niechlubne pierwsze miejsce należało będzie do... LinkedIn. Po raz pierwszy w na czele rankingu znalazł się portal dla ludzi biznesu co wydawałoby się niemal niemożliwe. Portal uchodził za względnie bezpieczne miejsce, tymczasem w ciągu pierwszych trzech miesięcy tego roku był wykorzystywany w ponad połowie wszystkich ataków phishingowych.

Podobnie wypowiada się ESET zajmujący się tworzeniem oprogramowania antywirusowego.



Według jego badań w ostatnich miesiącach gwałtownie wzrosła liczba ataków wykorzystujących markę LinkedIn, a model działania cyberprzestępców nieustannie ewoluuje. Oprogramowanie ESET wykrywa najnowsze zagrożenie pod nazwą trojan Win32/Agent.AEGY.

Niektórzy oszuści mogą odnieść sukces, wykorzystując proste sztuczki, jak np. proszenie o podanie danych w zamian za pozornie uczciwą rozmowę o pracę w „atrakcyjnej” firmie. Inni bywają bardziej wyrafinowani w swoich działaniach. Dlatego w trakcie naszych poszukiwań powinniśmy być ostrożni wobec ofert, które otrzymujemy, nawet jeśli pozornie wydają się pochodzić z zaufanego serwisu, jakim jest LinkedIn.

## **JAK SIĘ CHRONIĆ PRZED ATAKAMI NA LINKEDIN?**

W zakładce "Preferencje konta" - "Logowanie i bezpieczeństwo" mamy do wyboru ustawienia dostępu do naszego konta. Tam decydujemy, jaki adres mailowy oraz numer telefonu są wykorzystywane m.in. do logowania - możemy je zmieniać, tak samo jak hasło. W zakładce tej widnieją informacje między innymi o tym, na ilu i jakich urządzeniach aktualnie korzystamy z LinkedIn. Możemy je edytować lub wylogować się z jednej lub wszystkich sesji jednocześnie. Portal w zakładce "Dostęp do konta" wskazuje nam też urządzenia, które pamiętają hasło do konta - możemy nimi dowolnie zarządzać.





Jak w innych portalach, jest też możliwość dwustopniowej weryfikacji. Po włączeniu tej funkcji zostaniemy wylogowani wszędzie tam, gdzie jesteśmy obecnie zalogowani. Wszystkie zapamiętane urządzenia zostaną usunięte. Następnie wymagane będzie wpisanie kodu weryfikacyjnego przy pierwszym zalogowaniu się na nowym urządzeniu lub aplikacji mobilnej LinkedIn. Kod uzyskamy za pomocą aplikacji weryfikującej, takiej jak Microsoft Authenticator lub SMS-a.

## **TWITTER NA RAZIE WOLNY OD ATAKÓW. MIMO TO ZACHOWAJ CZUJNOŚĆ**

W 2021 roku, do tej pory nie odnotowano wycieków danych osobowych na samym Twitterze. Ostatnie, o jakich słyszeliśmy, miały miejsce w 2019 roku (wówczas udostępniono publicznie dane 19 milionów użytkowników) i w 2020 - mówiło się wtedy o największym ataku hakerskim na Twittera od początku jego istnienia. Hakerzy włamali się na konta znanych osób oraz dużych firm, aby wyłudzać bitcoiny.

Zaatakowane zostały konta wysoko postawionych osób, w tym Jeffa Bezosa, CEO Amazona, Billa Gatesa, a także Elona Muska. Ofiarami ataku stały się też duże firmy, w tym Apple i Uber, a także profile firm specjalizujących się w kryptowalucie. Atak polegał na przejęciu oficjalnego konta znanej osoby lub firmy i udostępniania postów w ich imieniu. We wpisie zamieszczona była prośba o przestanie symbolicznej sumy pieniędzy w zamian za odesłanie większej.

Od tamtego czasu Twitter nie poinformował o atakach hakerskich. To jednak nie zwalnia nas od czujności również i w tym serwisie.

### **JAK CHRONIĆ SVOJE DANE NA TWITTERZE?**

Portal ma dużo mniej filtrów oraz barier w stosunku do innych sieci społecznościowych. Wiele treści na Twitterze zawiera skrócone linki, które nie wiemy, gdzie tak naprawdę mogą prowadzić.



Czasami pochodzą one z niebezpiecznych miejsc, takich jak fałszywe formularze wyłudające poufne dane lub zawierające wirusy, które są następnie pobierane przez naszą przeglądarkę. Klikanie w nieznane linki jest jedną z głównych przyczyn infekcji złośliwym oprogramowaniem za pośrednictwem portali społecznościowych, dlatego należy zachować ostrożność wobec wszelkich linków.

Najprostszym sposobem na sprawdzenie, co kryje się pod skróconym linkiem jest skorzystanie z rozszerzenia do przeglądarki, które zweryfikuje skrócony link. Do najpopularniejszych należą: unshorten.me (przeglądarka Chrome) i unshorten.link (przeglądarka Firefox) lub z każdej wyszukiwarki unshorten.it

Jak uniemożliwić innym osobom zmianę hasła do własnego konta na Twitterze? Jeśli ktoś włamie się do naszego konta, w pierwszej kolejności zapewne zmieni hasło. Aby temu zapobiec, należy skonfigurować konto na Twitterze tak, aby żądało podania dodatkowych informacji, np. numeru telefonu lub adresu e-mail, gdy ktoś, w tym sam właściciel konta, będzie próbował zmienić hasło. Aby uniemożliwić cyberprzestępcom zmianę hasła, w sekcji Konto należy przejść do pozycji Bezpieczeństwo i zaznaczyć pole "Ochrona resetowania hasła".

**UWAGA! TO USTAWIENIE MOŻE OKAZAĆ SIĘ  
BEZUŻYTECZNE, JEŚLI POWIĄZANY Z TYM KONTEM NUMER  
TELEFONU LUB ADRES E-MAIL WYCIEKŁ JUŻ DO  
PRZESTRZENI ONLINE.**

Zalecane jest też usunięcie nieznanych aplikacji z konta na Twitterze i nie dzielenie się swoim kontem z innymi osobami - a to częsta praktyka, kiedy ktoś zleca prowadzenie konta zatrudnionym czy zleconym specjalistom ds. social media.



## **CO GROZI ZA HANDEL SKRADZIONYMI DANYMI?**

- Oszuści handlują danymi personalnymi swoich ofiar oraz ich życiem online. Na tzw. czarnym rynku można znaleźć oferty sprzedaży poszczególnych dokumentów lub dostępu do konta wraz obserwującymi na portalu social media. Analizy jednej z popularnych polskich witryn ogłoszeniowych wynika, że koszt jednego skanu dokumentu lub wykonanego selfie z dowodem osobistym waha się w przedziale od kilkudziesięciu do kilkuset zł, a cena za zagraniczne konto bukmacherskie wynosi ponad tysiąc zł. Oszuści oferują zniżki hurtowe oraz rabaty - informuje portal chronpesel.pl

Dane mogą wydawać się atrakcyjne dla reklamodawców korzystających z różnych płatnych form promocji swoich działalności. A co mają wspólnego dane osobowe z reklamami, chociażby na Facebooku? Serwis umożliwia bardzo precyzyjne targetowanie kampanii na podstawie informacji o użytkownikach, np. dane demograficzne, zachowania, zainteresowania, polubienia, udostępnienia. Dzięki tym zebrany danym łatwiej jest dotrzeć z treściami do

wybranej grupy docelowej, a to generuje wyższą konwersję podczas prowadzenia kampanii.

**Kiedy doszło do wycieku danych z Facebooka w 2019 roku hakerzy próbowali zarobić na przejętych numerach telefonów. W styczniu próbowano je sprzedawać za około 78 zł za sztukę. W ramach "promocji" 10 tys. rekordów można było kupić za około 19,5 tys. zł.**

- Odpowiedzialność karna za nieuprawniony dostęp do zasobów strony internetowej, opisana jest w art. 267 Kodeksu Karnego i nie ma tu znaczenia cel, w jaki sprawca dokonał przełamania zabezpieczeń. Przestępstwo to zagrożone jest karą do 2 lat pozbawienia wolności. Kara jest wymierzana indywidualnie przez Sąd na podstawie zebranych w trakcie trwania postępowania przygotowawczego dowodów. Nie jest ustawowo określone zaostrzenie kary w zależności od pobudek, z jakich działał sprawca - dowiedzieliśmy się od podkom. Michała Gawła z Wydziału Prasowo-Informacyjnego Biura Komunikacji Społecznej Policji.



## Przestępstwa komputerowe według polskiego prawa dzielą się na:

- bezprawne uzyskanie informacji,
- utrudnianie zapoznania się z informacją,
- uszkodzanie albo niszczenie danych informatycznych,
- zakłócanie systemów komputerowych.

Art. 267 par. 1 i 2 k.k. mówią, że odpowiedzialności karnej w postaci grzywny, kary ograniczenia wolności albo kary pozbawienia wolności do lat dwóch podlega ten, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając informatyczne zabezpieczenie. Tej samej karze podlega ten, kto bez uprawnienia uzyskuje dostęp (do całości lub części) systemu informatycznego.

Jeśli ofiara doznała znacznej szkody majątkowej, sięgającej ponad 200 tys. zł, kara wynosić może aż do 5 lat pozbawienia wolności. W przypadku ataku na instytucje państwowe orzeka się maksymalnie 8 lat więzienia. Warto jednak wspomnieć o wyroku, który zapadł w USA. Hakera za ataki w cyberprzestrzeni skazano na 27 lat więzienia. Przyczynił się m.in. do obrotu cudzą tożsamością, sam z niej też korzystał.

- Podmiot, który zakupi bazę danych zawierającą dane osobowe w celu dalszego wykorzystania, może ponosić odpowiedzialność karną z art. 49. 1. Ustawy o ochronie danych osobowych, którego treść brzmi: „Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3” - przekazał nam podkom. Gawęł.





Ponadto podkom. Michał Gawęł sugeruje, by każdy fakt kradzieży danych osobowych zgłaszać do UODO, jednak z uwagi na globalny zasięg sieci Internet, większość firm gromadzących nasze dane osobowe znajduje się poza jurysdykcją polskich przepisów. Fakt nieuprawnionego przetwarzania danych osobowych może stwierdzić w trakcie kontroli UODO.



# BEZPIECZEŃSTWO DANYCH W WIADOMOŚCIACH E-MAIL

---



Rafał Stępniewski  
Rzetelna Grupa

**Na danych osobowych, które gromadzone są przez przedsiębiorców lub właścicieli firm, przeprowadzanych jest wiele operacji, a wśród nich, na przykład, przesyłanie ich w wiadomościach e-mail. Według ustawy o ochronie danych osobowych również taka operacja zalicza się do przetwarzania danych, a w konsekwencji — odpowiedniego ich zabezpieczenia.**



## ZABEZPIECZENIE DANYCH OSOBOWYCH W E-MAILACH

Każdy administrator danych osobowych ma obowiązek zadbać o to, aby powierzone mu informacje traktowane były z najwyższą poufnością — reguluje to ustawa o ochronie danych osobowych w artykule 36.:

**Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.**

Obowiązek ten należy spełnić zatem również w sytuacjach, kiedy informacje osobiste są one przekazywane innym firmom lub osobom (np. za pomocą poczty elektronicznej).

Co ważne jednak — ustawa nie wskazuje dokładnie, jakie środki należy wykorzystać w celu odpowiedniego zabezpieczenia przesyłanych pocztą elektroniczną danych. Wybór odpowiednich narzędzi i sposobów należy więc do jednego z obowiązków administratora danych osobowych.

## SPOSÓB SZYFROWANIA PRZESYŁANYCH DANYCH

Dla osób, które zastanawiają się nad najbardziej efektywnym sposobem zabezpieczania danych przekazywanych w wiadomościach e-mail, UODO przygotował zestaw wskazówek dla administratorów danych.

**W tekście autorzy zauważają, że w celu zapewnienia odpowiedniego poziomu bezpieczeństwa konieczne jest:**

- szyfrowanie przekazywanych informacji;
- zabezpieczenie komputerów (nadawcy jak i odbiorcy);
- zabezpieczenie serwerów pocztowych;
- ochrona kanałów komunikacyjnych.



Według UODO najlepszą i zarazem najbardziej skuteczną metodą na zabezpieczenie danych jest właśnie ich szyfrowanie. W takim przypadku nie ma bowiem konieczności stosowania innych środków ochrony infrastruktury w postaci kanałów używanych do komunikacji czy serwerów pocztowych.

Raz zaszyfrowana wiadomość trafia w takiej samej formie do odbiorcy i tylko uprawniona do tego osoba może je odczytać. W razie ewentualnego "przejęcia" danych ryzyko ich odczytania przez niepowołane osoby jest również minimalne, gdyż nie posiadają one odpowiednich metod, by je odszyfrować.

Do szyfrowania UODO poleca darmowy program 7-Zip, który potrafi w taki sposób zakodować dane, że ich odczytanie będzie możliwe tylko i wyłącznie w przypadku posiadania odpowiedniego klucza deszyfrującego. Plusem takiego rozwiązania jest fakt, że odbiorca nie musi też posiadać tego programu zainstalowanego na swoim komputerze, ponieważ system operacyjny potrafi sam takie pliki odczytywać — o ile posiadamy właściwe hasło.

Oczywiście, samo hasło powinno być przekazane odbiorcy innym (bezpiecznym) kanałem komunikacji, tak aby zminimalizować ryzyko jego przejęcia. Taka metoda szyfrowania jest stosunkowo łatwa do przeprowadzenia, jednak wymaga wdrożenia odpowiednich procedur zarówno po stronie nadawcy, jak i odbiorcy, a także ich konsekwentnego stosowania.

## **BEZPIECZNE KANAŁY KOMUNIKACJI I WERYFIKACJA NADAWCY**

Innym sposobem zabezpieczenia przesyłanych wiadomości jest też szyfrowanie całego kanału komunikacji. W tym przypadku nawet jeśli dojdzie do przejęcia zawartych w wiadomości danych, to nadal będą one niemożliwe do odczytania.

Problemem w tym przypadku jest natomiast konieczność używania tych samych serwerów pocztowych, które stosują podobne techniki szyfrowania. Taka metoda sprawdzi się szczególnie w przypadku przesyłania danych wrażliwych w obrębie jednej firmy, natomiast w przypadku wysyłki danych do zewnętrznego odbiorcy — już nie.

UODO w opisywanym dokumencie zwraca również uwagę na fakt, że w przypadku komunikacji drogą elektroniczną istnieje bardzo wysokie zagrożenie podszycia się pod inną osobę lub firmę. Odbiorca czytający wiadomość może widzieć w polu “Od” prawidłowy e-mail instytucji, jednak rzeczywisty (nieprawdziwy) adres pozostanie niewidoczny dla użytkownika.

**W tym przypadku zalecane jest szczególnie zastosowanie certyfikatu elektronicznego. Nie tylko potwierdza on tożsamość nadawcy, ale jednocześnie szyfruje samą wiadomość.**

## DOSTAWCA USŁUG E-MAIL

Zabezpieczenie danych przesyłanych pocztą elektroniczną lub kanałów komunikacji to jedna kwestia, natomiast znacznie ważniejsze jest wybranie takiego dostawcy usług e-mail, który zagwarantuje pełną poufność przesyłanych informacji.

Należy zwrócić uwagę na fakt, że w momencie przesyłania wrażliwych danych za pomocą poczty e-mail, są one jednocześnie powierzane firmie, która oferuje taką usługę. Oznacza to, że przedsiębiorstwo to może w każdej chwili (przypadkiem bądź umyślnie) przejąć te informacje — zwłaszcza, jeśli nie są one zaszyfrowane. Podczas podpisywania umowy o świadczenie usług poczty elektronicznej należy zatem zadbać o to, aby strony podpisały klauzule zachowania w tajemnicy danych, które są tą drogą przesyłane.





# ZOSTAŃ EKSPERTEM

# SECURITY MAGAZINE



**REDAKCJA@SECURITYMAGAZINE.PL**



**DMYTRO LENNYI**  
AgriTech practice leader  
Intellias



**KONRAD DYDA**  
Prezes Zarządu  
Med&Lex-Klinka Wsparcia Perso-  
nelu i Jednostek Ochrony Zdrowia



**PATRYK BOGDAN**  
Security Officer  
Grandmetric



**DOROTA DYS**  
Project Manager  
Sygnisoft S.A.



Ma ponad 10-letnie doświadczeniu w zakresie pracy z produktami. Wie, jak skutecznie opracowywać i wprowadzać rozwiązania rolnicze od pomysłu do rynku. Współpracuje ściśle z firmami rolniczymi i rolnikami, pomaga im zrozumieć najnowsze rozwiązania rynkowe i trendy technologiczne.

Prawnik i doktorant z zakresu prawa, właściciel polsko-włoskiej firmy Centrum Usług Prawnych i Biznesowych - Centro Servizi Legali e Commerciali, prezes zarządu w spółce Med&Lex - Klinka Wsparcia Personelu i Jednostek Ochrony Zdrowia oraz w Fundacji Praw Medyka.

Od ponad 10 lat wykonuje testy penetracyjne i szuka podatności w systemach i aplikacjach IT. Rozpoczął jako uczestnik programów bug bounty, dziś realizuje projekty pentesterskie i związane z audytami bezpieczeństwa jako Security Officer w Grandmetric.

Od 2015 roku zdobywa doświadczenie, realizując projekty dla branży IT. Współpracowała z renomowanymi software house'ami jako Project Manager realizując projekty dla MŚP. Specjalizuje się w projektach dla e-commerce, aplikacjach dedykowanych oraz integracjach systemów. Zwolenniczka pro-klienckiego podejścia do relacji biznesowych.



## JOANNA GIZGIER

CEO w marce  
by Fehu



Związana z branżą IT od ponad 11 lat. Zajmuje się projektowaniem i budowaniem stron internetowych oraz e-sklepów, tworzy layouty w WordPress. Dbą o działania SEO. Zajmuje się też identyfikacją wizualną marki. Jest autorką szkoleń: "Twoje miejsce w sieci" czy "Firmowe błędy w poruszaniu się online".

## RAFAŁ STĘPNIEWSKI

Prezes Zarządu  
Rzetelna Grupa Sp. z o.o.



Redaktor naczelny serwisu dziennikprawny.pl i Security Magazine. Z branżą e-commerce związany od ponad 15 lat. Manager z 20-letnim doświadczeniem w branżach IT&T i zarządzaniu. Autor wielu publikacji z zakresu prawa e-commerce oraz bezpieczeństwa.

## DAWID MROWIEC

Specjalista ds. bezpieczeństwa  
B-secure



Audytor, doradca i trener. Pomaga organizacjom i ludziom realizować ich cele w świecie pełnym ryzyka. W pracy bazuje na interdyscyplinarnej wiedzy łącząc doświadczenia zawodowe z wiedzą akademicką. Autor bloga B-secure i podcastu Bezpieczniej w biznesie.

## PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW  
Z DZIENNIKARZAMI



## POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY  
O BEZPIECZEŃSTWIE FIRM



## RZETELNY REGULAMIN

BLOG POŚWIĘCONY  
POLSKIEMU E-COMMERCE





# ZOBACZ WYDANIA

Wydanie 1/2022

**POBIERZ**



Wydanie 2/2022

**POBIERZ**



Wydanie 3/2022

**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

Projekt i skład: 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)