03/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Kobiety w IT. Siła przebranżowienia i zarobki

Technologia rozpoznawania twarzy zdominuje te branże

Branża AV. Nowe wyzwania po 24 lutego

Niewielki budżet na cyberbezpieczeństwo wyeliminuje zagrożenia

Cyfryzacja ochrony zdrowia to wyzwanie

SPIS TREŚCI

SZANOWNI PAŃSTWO,

Czy jest szansa na trwałą zmianę wizerunku typowej firmy IT, kojarzonej z zespołami męskimi? Czy kobiety mogą odmienić branżę?

Jak zmieniają się realia w zakresie walki z cyberprzestępcami w obliczu narastających zagrożeń?

Jakie są wymogi prawne w zakresie cookies na stronie WWW?

Jak bezpiecznie cyfryzować ochronę zdrowia i z jakimi wyzwaniami się to wiąże?

Na te oraz wiele więcej pytań znajdziesz odpowiedź w naszym najnowszym numerze magazynu.

Wiedzą dzielą się doświadczeni praktycy, specjaliści w swojej branży. W tym miejscu zachęcam wszystkich, którzy chcą przekazać szerokiemu gronu informacje z zakresu szeroko pojętego bezpieczeństwa w firmie, do dołączenia do elitarnego grona ekspertów "Security Magazine".

Zapraszam do lektury i współpracy.

Rafał Stępniewski


ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA
SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy
SECURITY MAGAZINE
ZAPISZ SIĘ
NEWSLETTER
YOUR EMAIL HERE
SUBSCRIBE

INFORMACYJNE BEZPIECZEŃSTWO PRZEDSIĘBIORSTWA PRZY OGRANICZONYM BUDŻECIE

Oleksandr Chyzhykov
Intellias

Jeśli zastanawiałeś się nad wzmocnieniem bezpieczeństwa informacyjnego w swojej firmie, prawdopodobnie spotkałeś się ze stwierdzeniem, że wymaga to znacznych inwestycji. Rzeczywiście, oprogramowanie, infrastruktura i zespół specjalistów potrzebują finansowania, czasem - dużego. Ale co, jeśli pieniądze i ludzie nie wystarczą?

INWENTARYZACJA, OCENA I SKUPIENIE SIĘ NA TYM, CO WAŻNE

Przy ograniczonym budżecie nie rób wszystkiego na raz. Efektywniej jest skoncentrować się bardziej na ochronie najbardziej ważnych aktywów, takich jak dane osobowe, hasła, klucze, bazy danych, serwery, konta i tak dalej. Zrób inwentaryzację aktywów i przejdź do oceny ryzyka.

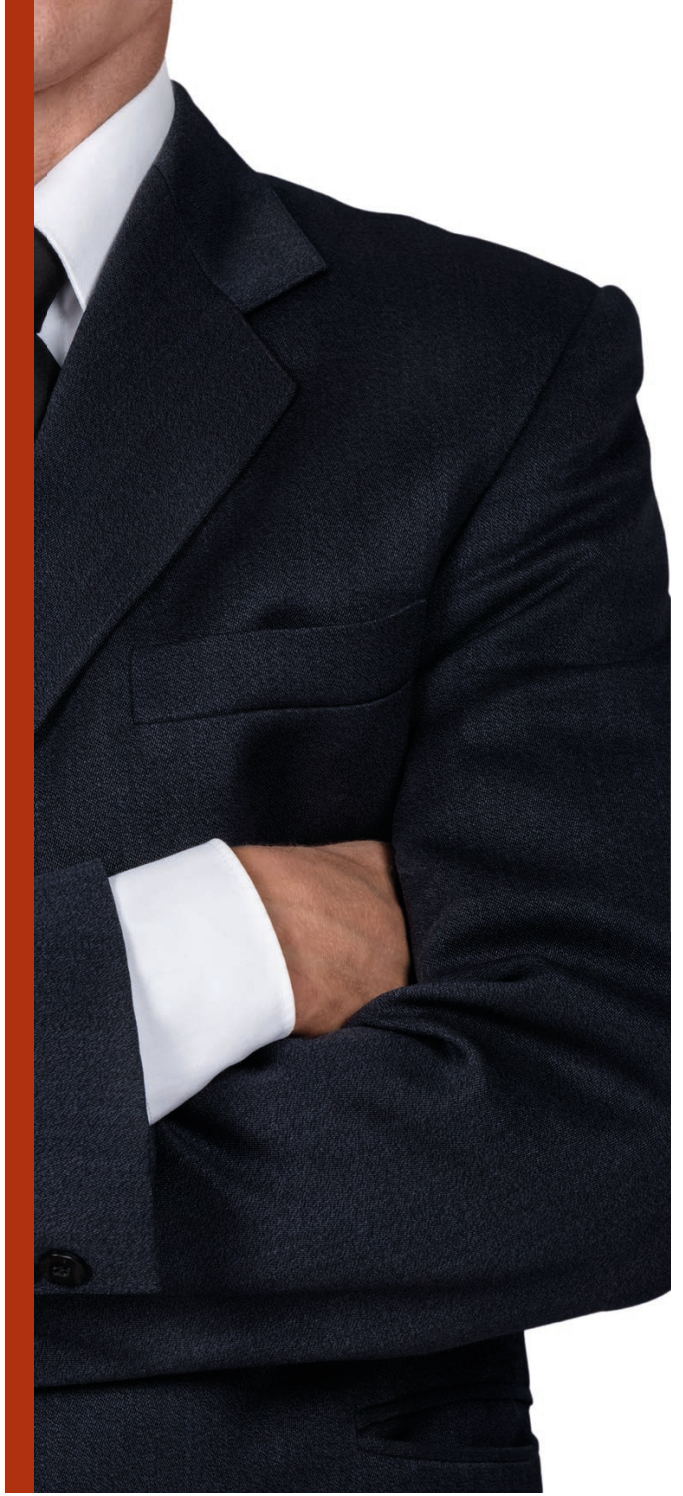
Podczas oceny ryzyka ważne jest, aby dokładnie zidentyfikować wrażliwości, zagrożenia i możliwe wektory ataku. Przykład:

- Utrata danych osobowych - RYZYKO.
- Kradzież laptopa specjalisty - ZAGROŻENIE.
- Kradzież miała miejsce na terenie firmy - WEKTOR.
- Laptop ma nieograniczony dostęp i brak szyfrowania dysku - WRAŻLIWOŚĆ.
- Następnie przejdź do PLANU postępowania z ryzykiem.

PLAN POSTĘPOWANIA Z RYZYKIEM

Priorytetem w twoim planie powinny być te ryzyka, które będą miały największy wpływ i prawdopodobieństwo. Nie zapomnij o wartości aktywów. Do obliczenia ryzyka można użyć następującego wzoru:

Kwota ryzyka = prawdopodobieństwo + wpływ * wartość aktywów.



Plan postępowania z ryzykiem powinien składać się z co najmniej trzech elementów:

ŚRODKI ORGANIZACYJNE

Zakaz lub ograniczenia na poziomie organizacyjnym, takie jak zakaz pracy z danymi osobowymi na urządzeniu prywatnym.

ŚRODKI TECHNICZNE

Ograniczenia techniczne, takie jak szyfrowanie dysku z danymi osobistymi, umożliwienie uwierzytelniania dwuskładnikowego i tak dalej.

ŚRODKI BEZPIECZEŃSTWA

Kontrola nad bezpieczeństwem informacji, monitorowanie zdarzeń związanych z bezpieczeństwem, incydentów, zarządzanie lukami w zabezpieczeniach i zmianami, zgodność itp.

W celu wzmocnienia bezpieczeństwa informacji przy ograniczonym budżecie zwróć także uwagę na następujące zalecenia:

1. Dobrze znane praktyki. Nie musisz wymyślać koła na nowo, aby wybudować wszystkie rodzaje bezpieczeństwa informacji. Korzystaj ze znanych i sprawdzonych praktyk, takich jak ISO 27001, ISO 27002 i NIST 800-53. Nie komplikuj polityk, standardów i wymagań - zrób je jasnymi i przejrzystymi, aby ułatwić wdrożenie. Każda komplikacja może stworzyć dodatkowe ryzyko, na przykład specjaliści nie rozumieją wymagań i po prostu je ignorują.

2 **Konta i uprawnienia.** Realizuj scentralizowany system zarządzania kontami i uprawnieniami (Identity and Access management). Jeśli Twój system będzie w stanie realizować SSO z Twoimi systemami i aplikacjami innych firm, uwierzytelnianie dwuskładnikowe i Role or Attribute based access model, będziesz w stanie zamknąć większość „standardowych" ryzyków przy minimalnym budżecie. Jeśli pracujesz z Office 365, użyj Azure AD do zarządzania kontami i szeregiem innych usług, które przydadzą się w zarządzaniu ryzykiem. Google G Suite ma również podobne usługi.

3 **Wendorzy i dostawcy.** Zawsze pytaj swoich wendorów i dostawców o dodatkowe opcje lub usługi w zakresie bezpieczeństwa informacji. Często możesz nawet nie wiedzieć, że masz już pod ręką narzędzia zabezpieczające, za które nie musisz płacić. Na przykład wendorzy mogą zapewnić usługi ochrony antywirusowej, monitorowania i zgłaszania incydentów.

4 **Macierz dostępu.** Stwórz macierz dostępu, aby zrozumieć funkcje i obowiązki swojego zespołu. W tym celu wystarczy zwykła tabela, w której wpiszesz stanowiska specjalistów i jakie dostępy powinni mieć.

Następnie za pomocą Identity and Access management stwórz niezbędne role i przydziel je specjalistom. Wraz z usprawnieniem procesów ta macierz będzie się uzupełniać, a Ty będziesz kontrolować dostęp całego zespołu.

5 **Centralizacja**. Korzystaj ze scentralizowanych rozwiązań do zarządzania zdarzeniami technicznymi i nie rób tego ręcznie. Dzięki temu zaoszczędzisz dużo czasu i zredukujesz tzw. „prostój". Ponadto centralizacja pozwoli Ci szybko reagować na incydenty i redukować wpływ szybkich zmian.

6 **Kopie zapasowe.** Zorganizuj regularny proces tworzenia kopii zapasowych i przetestuj odzyskiwanie krytycznych danych. Nie warto robić kopii zapasowej wszystkiego. Zamiast tego zidentyfikuj krytyczne aktywy i skopiuj je. To zmniejszy budżet.

7 **Szukaj wrażliwości technicznych.** Zorganizuj regularny proces wyszukiwania wrażliwości technicznych w sieci, systemach operacyjnych i aplikacjach za pomocą narzędzi budżetowych, takich jak OpenVAS, Wazuh, Burp Suite, Software from Kali Linux. Korzystanie z tych narzędzi pozwoli zaoszczędzić i pokryć większość zagrożeń związanych z identyfikacją wrażliwości technicznych.

8 **Logging and Monitoring.** Zorganizuj proces Logging and Monitoring zdarzeń związanych z bezpieczeństwem z krytycznych systemów, aplikacji i serwerów za pomocą narzędzi budżetowych, takich jak ELK, Wazuh.

Narzędzia te zapewniają szeroką gamę narzędzi nie tylko do zbierania zdarzeń związanych z bezpieczeństwem, ale także pozwalają budować analitykę, aby reagować na incydenty i identyfikować zagrożenia z wyprzedzeniem.

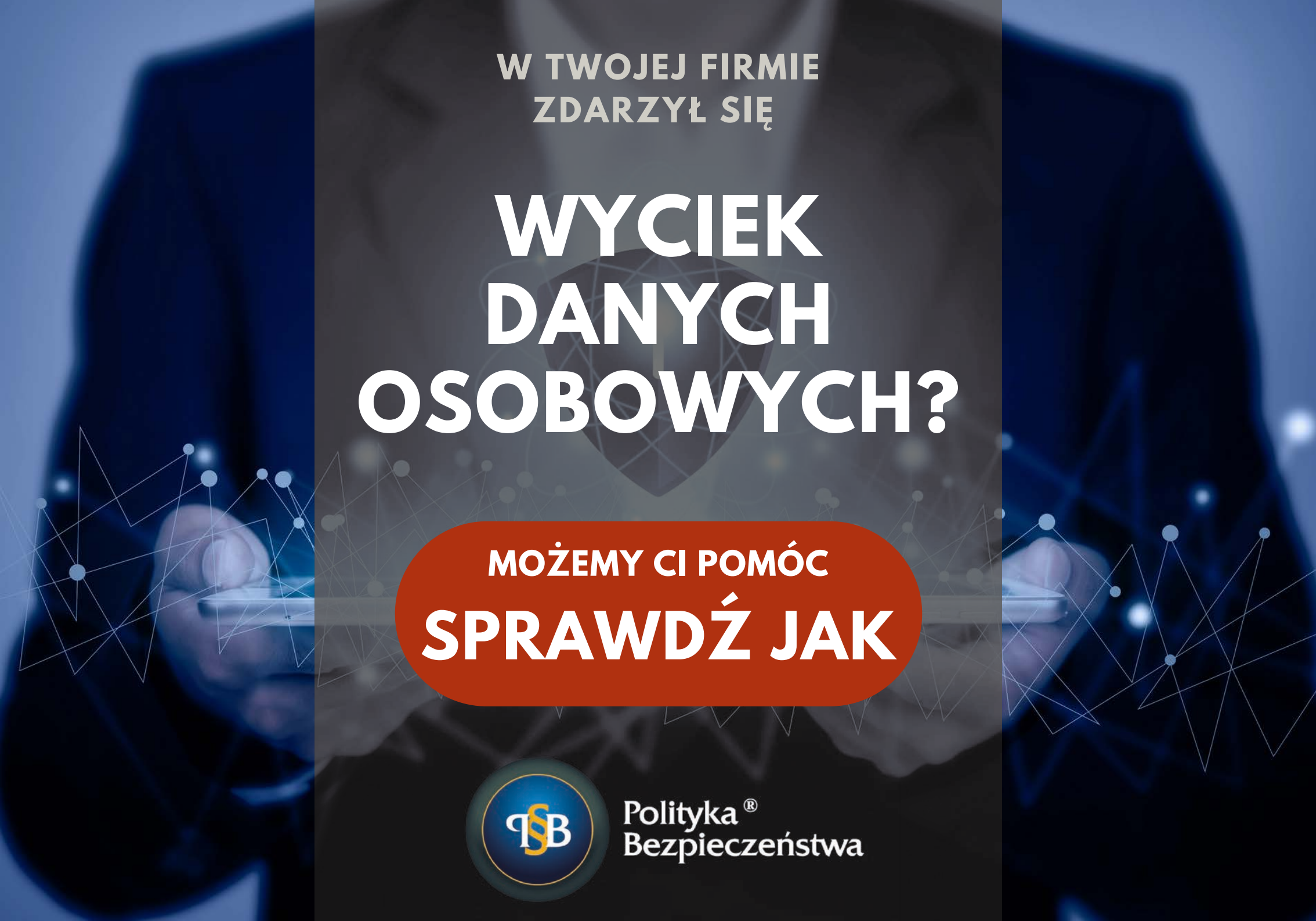
8 **Antywirus.** Jeśli nie masz środków na zakup scentralizowanego systemu antywirusowego, skorzystaj z wbudowanego antywirusa w systemie Windows OS (Defender)

9 **Szyfrowanie dysku.** Aby zaoszczędzić pieniądze, możesz zrezygnować ze scentralizowanego systemu szyfrowania dysków. Zamiast tego użyj native szyfrowania Bitlocker w OS Windows, FileVault na MacOS i bezpłatnego Fscrypt lub Lux w systemie Unix

10 **Poziomy reagowania.** Podziel proces reagowania na incydenty na poziomie (Tiers). Zwyczajny IT Support Specialist będzie mógł pracować z incydentami bezpieczeństwa na pierwszej linii - na przykład analizować wiadomości o incydentach. Na innych poziomach konieczne będzie zaangażowanie zespołu ds. bezpieczeństwa informacji. Dzięki temu będziesz mógł reagować na incydenty całodobowo i podłączyć bardziej kompetentnych i wysoko opłacanych pracowników tylko wtedy, gdy jest to konieczne.

11 **Automatyzacja.** Maksymalnie zautomatyzuj procesy bezpieczeństwa informacji. Dzięki temu ominiesz zarówno czynnik ludzki, jak i zaoszczędzisz czas zespołu ds. bezpieczeństwa informacji.

Mając takiej celowej oceny i planu zarządzania ryzykiem, będziesz w stanie zbudować system bezpieczeństwa, który będzie potrzebował tylko procesów, systemów i ludzi. Po uporaniu się z krytycznymi ryzykami, opracowuj te, które są mniej priorytetowe. W ten sposób będziesz w stanie konsekwentnie radzić sobie ze wszystkimi zagrożeniami, równomiernie rozdzielając budżet i wysiłki.
Nie zapomnij również rozpocząć proces regularnego przeglądu aktywów, identyfikacji nowych wrażliwości i zagrożeń oraz ponownej oceny ryzyka. Powinieneś również regularnie oceniać już wdrożony plan, aby upewnić się, że został wybrany prawidłowo. Do oceny ryzyka zalecam stosowanie następujących metodologii i frameworków - ISO 27005, ISO 27001, IRAM2, NIST SP800-30, OCTAVE.


W TWOJEJ FIRMIE
ZDARZYŁ SIĘ
WYCIEK
DANYCH
OSOBOWYCH?
MOŻEMY CI POMÓC
SPRAWDŹ JAK
Polityka ®
Bezpieczeństwa

KOBIETY W IT. SIŁA PRZEBRANŻOWIENIA I ZAROBKI

Anna Żbikowska
No Fluff Jobs

Kobiety świadomie zmieniają swoją karierę na IT, mają duże możliwości rozwoju i awansu, a świat technologii wybierają nie tylko ze względu na atrakcyjne zarobki, ale również szczerą pasję do IT. Tak wynika z raportu dotyczącego kobiet w IT, którego wyniki rozprawiają się z największymi stereotypami o specjalistkach w branży tech.

PRACA W IT TO NIE TYLKO PROGRAMOWANIE

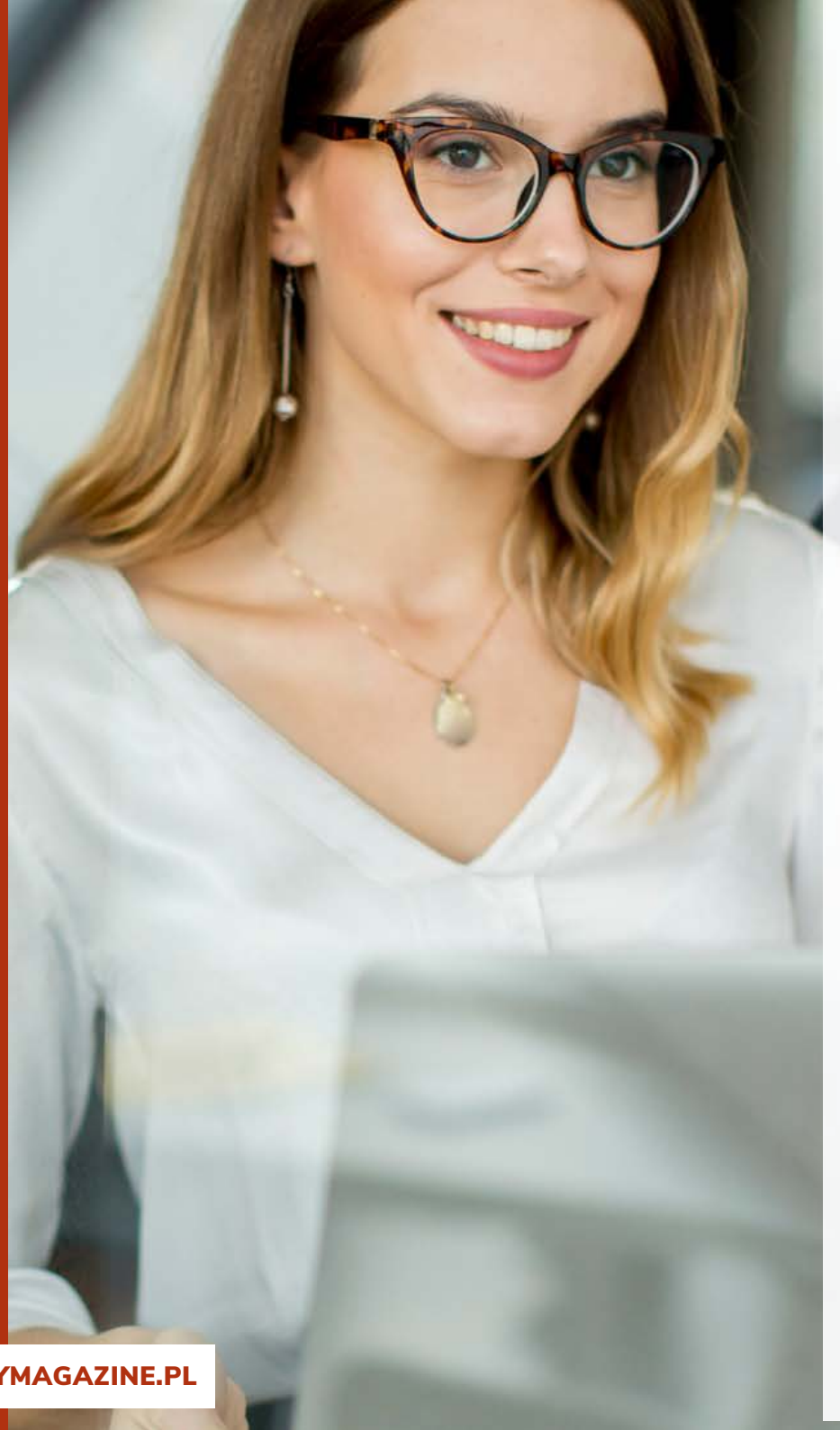
Jak czytamy we wspomnianym raporcie „Kobiety w IT 2022", 46% respondentek piastuje stanowiska niezwiązane bezpośrednio z programowaniem. Największy odsetek deklaruje pracę jako testerki (18,6%) oraz project managerki (16%). Jeśli chodzi o specjalizacje wymagające znajomości kodu, uczestniczki badania najczęściej zajmują się Backendem (15%), Frontendem (12%) oraz Fullstackiem (5,4%).

O wymarzoną specjalizację spytano także kandydatki, czyli osoby, które dopiero przymierzają się do rozpoczęcia kariery w IT. Co trzecia aspiruje do roli **UX/UI Designerki,** a co piąta wskazała **Testing.** Następnie kandydatki wybierały kolejno:

- **Frontend,**
- **Project Management,**
- **Design**
- **oraz Business Analysis.**

Warto wspomnieć, że w ostatnim czasie w branży wzrosło znaczenie ról niewymagających kodowania.

Ten trend ma swoje odzwierciedlenie w zarobkach i liczbie ofert pracy. Z wewnętrznych danych No Fluff Jobs wynika, że w I kwartale 2022 roku mediana górnych widełek wynagrodzenia dla kategorii Project Management wyniosła 20 tys. netto + VAT na umowie B2B.



To ważny wynik, bo przez lata pułap 20 tys. był „zarezerwowany" jedynie dla programistów czy programistek. To także dobry znak dla wszystkich juniorów i juniorek, bo choć firmy wciąż jeszcze nie odmroziły w pełni rekrutacji na początkujące stanowiska, próg wejścia dla ról nieprogramistycznych pozostaje niższy niż w przypadku tych, na których znajomość kodu jest niezbędna.

HISTORIA MONIKI PIĄTKOWSKIEJ, JUNIOR IT PROJECT MANAGERKI W NO FLUFF JOBS

Moja przygoda z IT rozpoczęła się od tego, że w szkole średniej pracowałam jako copywriterka w agencji interaktywnej. Każdego dnia obserwowałam, jak koledzy z pracy tworzą strony internetowe i bardzo mi się to spodobało. Wtedy wyznaczyłam sobie cel, że w ciągu roku nauczę się kodowania i stworzę kilka stron oraz sklepów internetowych. Wiedzę zdobywałam częściowo w pracy, częściowo samodzielnie. W taki sposób zostałam Webmasterką. W międzyczasie stwierdziłam, że spróbuję czegoś innego i poszłam na studia ekonomiczne, wyjechałam do Stanów na 4 miesiące i zajmowałam się tam marketingiem. Po roku doszłam do wniosku, że to nie jest to, co chcę robić w życiu, i zmieniłam kierunek na informatykę.

Zaczęłam się bardziej rozwijać w IT, zmieniłam stanowisko na Wordpress Developerkę i zdobywałam doświadczenie w 2 firmach. Nadszedł moment, w którym zrozumiałam, że nie do końca chcę zajmować się tylko kodem, bez praktycznie żadnego kontaktu z innymi ludźmi. Wtedy zainteresowałam się stanowiskiem IT Project Managera, zaczęłam studiować drugi kierunek (zarządzanie w IT) i szukać pracy w tym zawodzie. I tak właśnie znalazłam się w No Fluff Jobs jako Junior IT Project Managerka.

SIŁA PRZEBRANŻOWIENIA

Jak podaje najnowszy raport „Kobiety na politechnikach", kobiety stanowiły 35% wśród studentów publicznych uczelni technicznych. W przypadku kierunków informatycznych odsetek ten wyniósł 16%. Szacuje się natomiast, że kobiety liczą około 30% wśród wszystkich specjalistów IT w Polsce. Bardzo możliwe, że w najbliższych latach wynik ten poszybuje w górę. Zapotrzebowanie na wykwalifikowane zespoły IT rośnie, a luka kadrowa stale się powiększa. Co więcej, na rynku można zauważyć coraz więcej inicjatyw czy programów mentoringowych mających na celu włączenie kobiet do społeczności IT i pomoc w rozwinięciu kariery.

- Dlaczego w IT jest wciąż tak mało kobiet? Niestety w społeczeństwie nadal silnie funkcjonują stereotypy, według których m.in. kierunki ścisłe i techniczne są domeną mężczyzn, a kobietom świat technologii na pewno nie wyda się interesujący. Takie krzywdzące poglądy sprawiają, że kobiety odkrywają pasję do IT znacznie później i nie zawsze mają warunki i możliwości, by wejść na ścieżkę przebranżowienia. Co więcej, często panuje błędne przekonanie, że w IT pogodzenie życia zawodowego z prywatnym jest niemożliwe. Tymczasem to branża, która oferuje bardzo elastyczne warunki pracy – tłumaczy **Magdalena Gawłowska-Bujok, współzałożycielka i COO w No Fluff Jobs.**

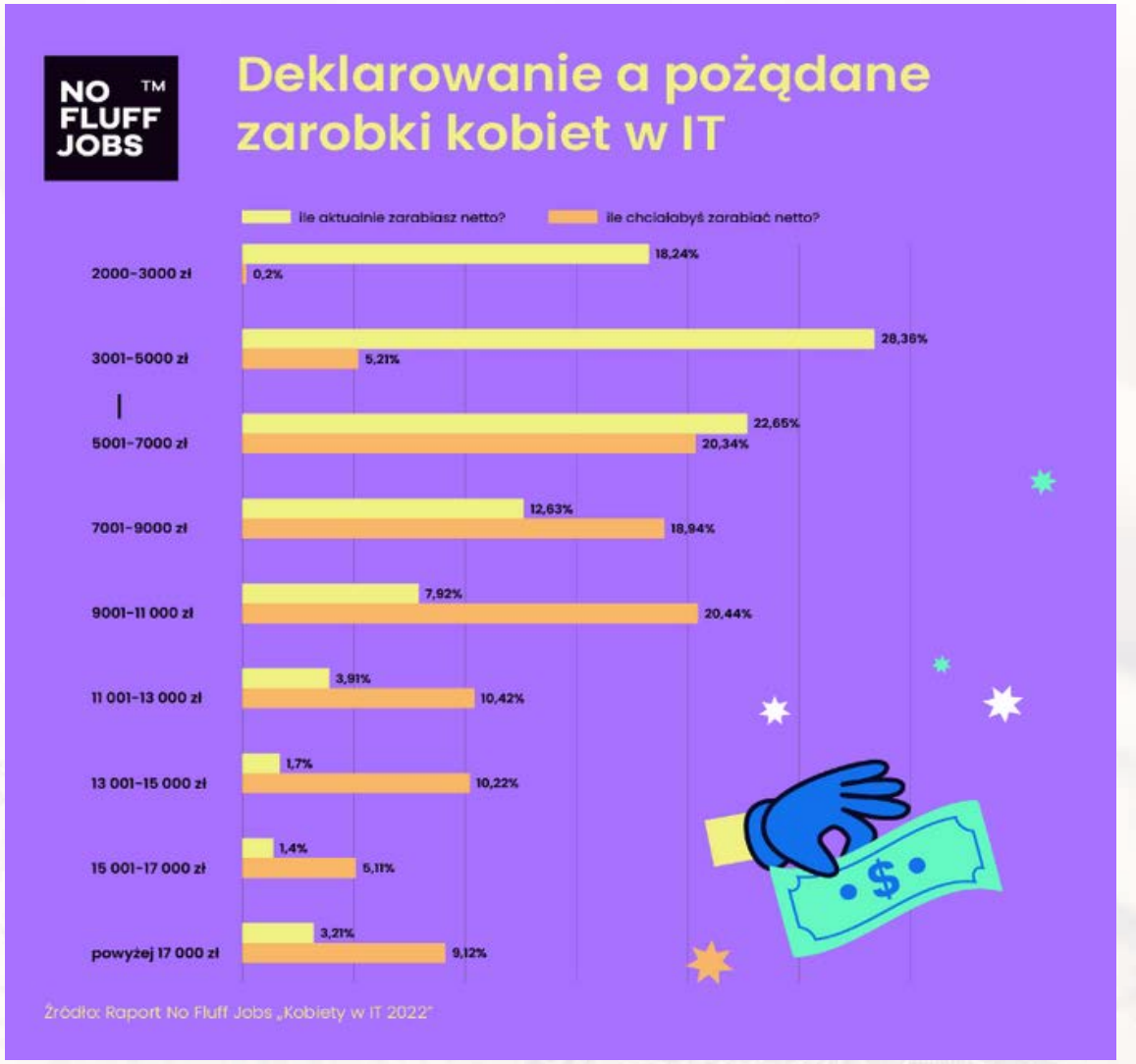
Z danych No Fluff Jobs wynika, że aż 55% respondentek przeszło niestandardową ścieżkę, w tym: 23,8% podjęło pracę w IT po studiach nietechnicznych, 15,2% po kursach/szkoleniach, bootcampach, a 16,2% po procesie samodzielnej nauki. Takie wyniki jednoznacznie naprowadzają na trop przebranżowienia. Pamiętajmy, aby nie lekceważyć doświadczenia zdobytego w poprzednich miejscach pracy, nawet jeśli wcześniejsza branża nie ma nic wspólnego z IT.

Mowa zwłaszcza o kompetencjach miękkich, które w przypadku stanowisk juniorskich bywają przepustką do zdobycia pracy w IT. Szczególnie istotne są m.in. umiejętności komunikacji, pracy w zespole, zarządzania projektem, przyjmowania/odbierania feedbacku czy szybkiego przystosowania się do nowej sytuacji.

ILE ZARABIAJĄ KOBIETY W IT?

Zarobki ponad połowy (51%) specjalistek IT oscylują w granicy 3001–7000 netto, chociaż co piąta uczestniczka badania wyraziła wyższe oczekiwania. Pamiętajmy jednak, że na wynagrodzenie wpływa wiele czynników m.in. poziom doświadczenia, specjalizacja, lokalizacja czy też typ umowy.

PAMIĘTAJMY, ABY NIE LEKCEWAŻYĆ DOŚWIADCZENIA ZDOBYTEGO W POPRZEDNICH MIEJSCACH PRACY, NAWET JEŚLI WCZEŚNIEJSZA BRANŻA NIE MA NIC WSPÓLNEGO Z IT.



CZY SPECJALISTKI IT CZUJĄ SIĘ SPEŁNIONE W PRACY?

Jak najbardziej. Okazuje się, że aż 71% badanych kobiet odczuwa spełnienie w pracy, a 68% z czystym sumieniem poleca obecnego pracodawcę. Dodatkowo aż 68% specjalistek deklaruje, że w 2021 roku ich wynagrodzenie wzrosło.

Kiedy kobiety zaczynają rozglądać się za nowym pracodawcą? Najczęściej myślą o zmianie firmy, gdy brakuje im możliwości rozwoju (74,7%), oczekują wyższego wynagrodzenia (54,9%) lub awansu (16,7%).

– Dane z najnowszego raportu No Fluff Jobs „Kobiety w IT 2022" cieszą i powinny dodać odwagi wszystkim kandydatkom, które wciąż zastanawiają się, czy warto obrać tę drogę zawodową. Aż 55 proc. badanych specjalistek IT podjęło pracę w IT po procesie przebranżowienia, a ponad 70 proc. czuje spełnienie u obecnego pracodawcy. Kobiety wybierają IT m.in. z uwagi na duże możliwości rozwoju, ciekawe projekty i wyzwania, a prawie połowa naszych respondentek wyznała, że świat technologii jest dla nich ciekawy – dodaje **Magdalena Gawłowska-Bujok:** – Choć czeka nas jeszcze wiele pracy w kwestii zapewnienia kobietom równości szans i płac, wyraźnie widać, że branża IT oferuje im coraz więcej możliwości rozwoju wymarzonej kariery i spełnienia zawodowego.

Bitdefender

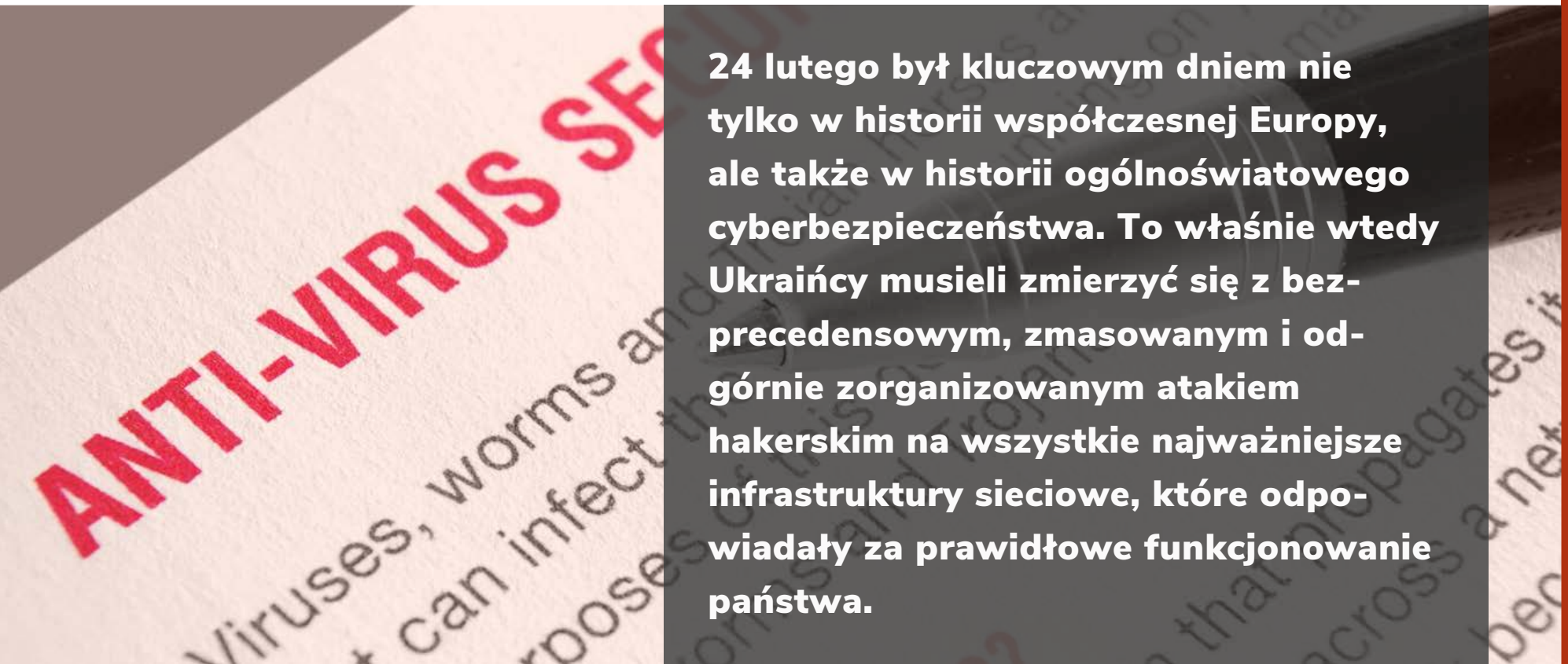
BUILT FOR RESILIENCE

Oferta skierowana do firm

Zmień swoje rozwiązanie antywirusowe i zyskaj dodatkowe 12 miesięcy gratis!

NOWE WYZWANIA W BRANŻY AV PO 24 LUTEGO

Piotr Rozmiarek
Marken Oficjalny dystrybutor Bitdefender w Polsce



24 lutego był kluczowym dniem nie tylko w historii współczesnej Europy, ale także w historii ogólnoświatowego cyberbezpieczeństwa. To właśnie wtedy Ukraińcy musieli zmierzyć się z bezprecedensowym, zmasowanym i odgórnie zorganizowanym atakiem hakerskim na wszystkie najważniejsze infrastruktury sieciowe, które odpowiadały za prawidłowe funkcjonowanie państwa.

SŁOWEM WSTĘPU

Podczas tego konfliktu mogliśmy zaobser-wować także zupełnie nowe zjawiska związane z szeroko pojętym cyberbezpieczeństwem, które zmuszają nas do wzbogacenia naszej branżowej nomenklatury o terminy takie, jak: cyberwojna, czy cyberarmia. Musimy pamiętać także o tym, że jako kraj bezpośrednio sąsiadujący zarówno z Ukrainą, jak i z Rosją, my także jesteśmy w tej chwili szczególnie podatni na ataki.

Dlatego postaram się przedstawić, najpopular-niejsze metody ataków hakerskich wykorzysty-wane podczas bieżącej wojny, cyberzagrożenia czyhające na nasz kraj oraz to, w jaki sposób możemy się przed nimi obronić.

24 LUTEGO ZOSTAŁA ODNOTOWANA REKORDOWA LICZBA ATAKÓW NA UKRAIŃSKĄ INFRASTRUKTURĘ SIECIOWĄ.

I CYBERWOJNA ŚWIATOWA?

Działania hakerów, które zostały podjęte pod-czas wojny w Ukrainie, w zasadzie są bardzo podobne do tych standardowych, obserwo-wanych przez nas w poprzednich latach.

Różnicę stanowią:

- skala,
- sposób zorganizowania
- stopień kompatybilności ataków cyberne-tycznych oraz tych czysto militarnych.

24 lutego została odnotowana rekordowa licz-ba ataków na ukraińską infrastrukturę sieciową. Producent oprogramowania Bitdfender zaob-serwował, że najczęstszą formą działań o zna-mionach cyberprzestępstwa były **ataki DDOS**, z którymi musiały się zmagać poszczególne mini-sterstwa, strony rządowe, centra strategiczne, ośrodki wojskowe, banki, firmy, media i insty-tucje związane z dostępem do Internetu. Ich celem było uniemożliwienie działania wszelkich usług sieciowych związanych z najważniejszy-mi ośrodkami w kraju i ich całkowity paraliż, co ostatecznie miało doprowadzić do utraty płyn-ności finansowej oraz zakłóceń w komunikacji pomiędzy powyższymi podmiotami.

Takie działania, jeśli są odpowiednio skoordynowane z atakami militarnymi, mogą być kluczowym elementem w wojnie.
Warto zauważyć, że Rosjanie z sukcesem wykorzystali już tę taktykę w 2014 roku, podczas aneksji Krymu. Wtedy, w przeciwieństwie do obecnego konfliktu, Ukraina była całkowicie nieprzygotowana do takiej formy ataku, co znacząco przyczyniło się do stosunkowo łatwej utraty tego terytorium.

Drugą formą ataku było wykorzystanie nowego rodzaju **złośliwego oprogramowania typu malware o nazwie HermeticWiper**, które po zainfekowaniu systemu całkowicie niszczyło wszystkie jego dane. Takie działania miały na celu paraliż nie tylko ośrodków administracyjnych i wojskowych, lecz także wielu gałęzi przemysłu, sektorów energetycznych i komunalnych. Agresorzy chcieli w ten sposób długotrwale spowolnić gospodarkę Ukrainy oraz przerwać łańcuch dostaw podstawowych produktów pierwszej potrzeby.

Trzecim aspektem wojny cybernetycznej są **działania dezinformacyjne.** Obie strony próbują pokazać się z jak najlepszej strony oraz zastraszyć rywala.

Rosjanie wykorzystują do tego armię botów, które zalewają fora i media społecznościowe propagandowymi komentarzami. Ukraińcy skupiają się na przekazie sugerującym ich wyższość nad agresorem i ośmieszeniu jego armii. Warto zauważyć, że takie działania mają coraz większy wpływ na realne pole bitwy, ponieważ wpływają na opinię publiczną w innych krajach i przyczyniają się na przykład do decyzji o dostarczeniu pomocy humanitarnej i broni.

Bieżąca wojna w Ukrainie jest dowodem na to, że cyberprzestrzeń stała się bardzo ważną przestrzenią w życiu ludzi i w prawidłowym funkcjonowaniu państwa. Podczas działań wojennych jest wykorzystywana tak samo, jak ląd, woda i powietrze. A co możemy powiedzieć o nowoczesnej cyberarmii?

Specjaliści do spraw cyberbezpieczeństwa do niedawna sceptycznie podchodzili do terminów takich jak „cyberwojna" i „cyberarmia". Swoje zdanie argumentowali tym, że zorganizowane grupy przestępcze działające w sieci ukrywają swoją tożsamość i ich schemat ataków przypomina bardziej terroryzm niż prowadzenie skoordynowanej operacji militarnej.

Najnowsze doniesienia na temat działań w cyberprzestrzeni wskazują na to, że te tezy są już nieaktualne, ponieważ w obecnym konflikcie naprzeciw siebie stanęły de facto dwie armie hakerów. Jedna związana z Rosją, Koreą Północną i Chinami. Druga, która zrzesza grono zwolenników Ukrainy z całego świata. Nie możemy mówić tutaj o oddolnej inicjatywie haktywistów, ponieważ ich cele są jasne i czytelne, a działania doskonale skoordynowane.

CYBERPRZESTRZEŃ STAŁA SIĘ BARDZO WAŻNĄ PRZESTRZENIĄ W ŻYCIU LUDZI I W PRAWIDŁOWYM FUNKCJONOWANIU PAŃSTWA.

W nowej formie wojny cybernetycznej możemy odnaleźć szerokie spektrum standardowych działań wojennych takich, jak:

OTWARTY ATAK

(na przykład na serwery i strony rządowe),

WOJNA NA WYNISZCZENIE

(ataki malware i ransomware)

SZPIEGOSTWO

(kradzież danych)

WOJNA PARTYZANCKA

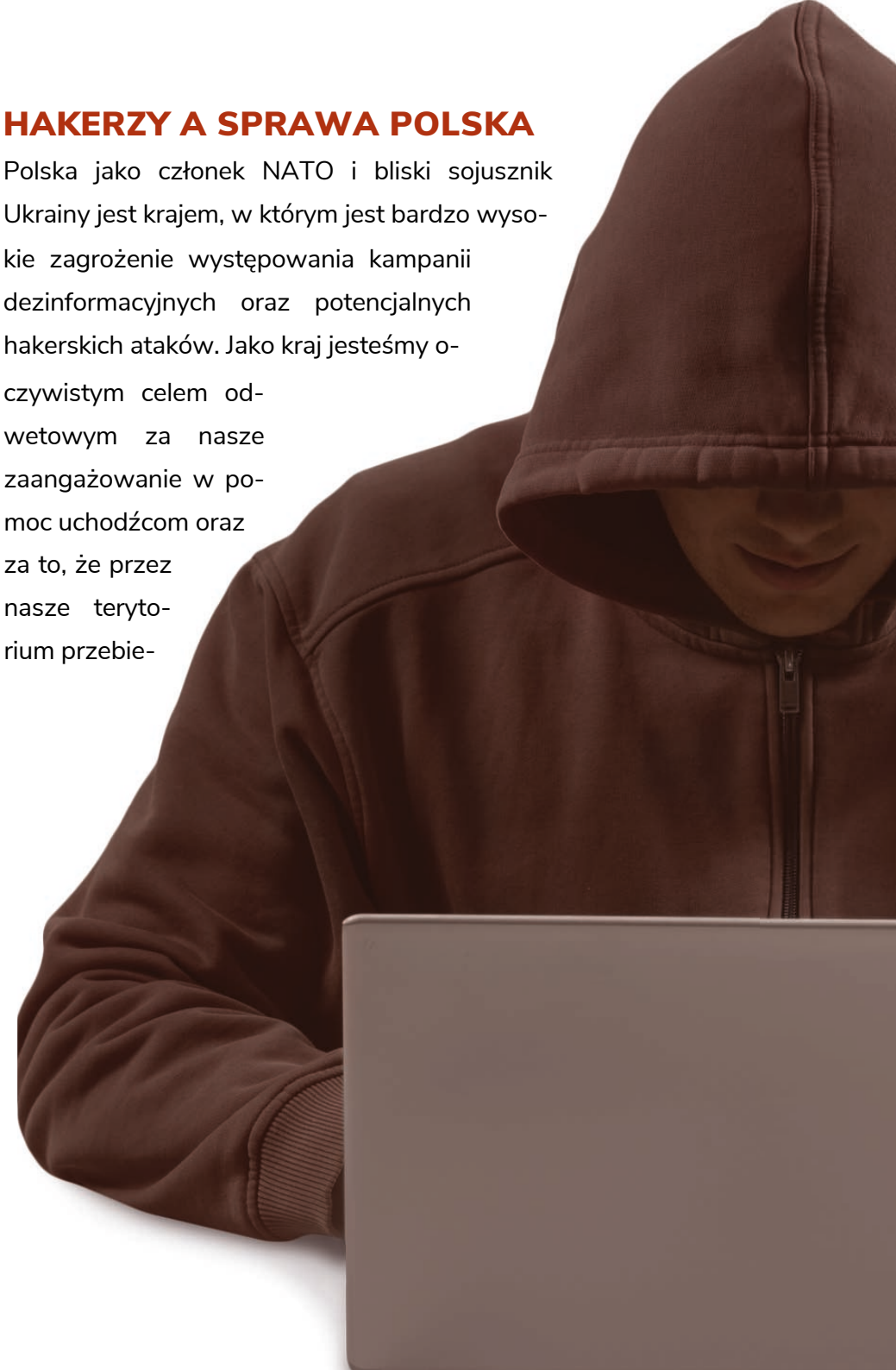
(zakłócanie komunikacji wojskowej)

WOJNA INFORMACYJNA

Konflikt w Ukrainie doskonale uwidocznił to, że cyberprzestępstwa mogą zostać wykorzystane jako broń, która może zagrażać egzystencji całego narodu. Co doskonale pokazuje, jak ważne jest zachowanie cyberbezpieczeństwa w aktualnych czasach. A co możemy powiedzieć na temat zagrożeń skierowanych bezpośrednio przeciwko nam?

HAKERZY A SPRAWA POLSKA

Polska jako członek NATO i bliski sojusznik Ukrainy jest krajem, w którym jest bardzo wysokie zagrożenie występowania kampanii dezinformacyjnych oraz potencjalnych hakerskich ataków. Jako kraj jesteśmy oczywistym celem odwetowym za nasze zaangażowanie w pomoc uchodźcom oraz za to, że przez nasze terytorium przebie-



ga tranzyt broni i pomocy humanitarnej z Zachodu. Co więcej, nasz kraj został zaatakowany już przed rozpoczęciem bezpośrednich działań wojennych w Ukrainie.

Kampanię dezinformacyjną mogliśmy zaobserwować już w listopadzie 2021 roku podczas rosyjsko-białoruskiej operacji „Śluza", która polegała na destabilizacji Unii Europejskiej oraz Polski. W tym celu posłużono się uchodźcami i za pomocą kampanii dezinformacyjnych próbowano podzielić nasze społeczeństwo i „obrzydzić" obraz uchodźców. Krótko po 24 lutego nasz kraj został ponownie zaatakowany w ten sam sposób. Grupy hakerskie związane z Rosją przeprowadziły akcję, podczas której sugerowali, że uchodźcami z Ukrainy, którzy przybyli do Przemyśla są głównie agresywni mieszkańcy Afryki i Bliskiego Wschodu, co było, oczywiście, nieprawdą. A skąd wiemy, że nie była to inicjatywa samych mieszkańców Przemyśla? **Po zweryfikowaniu adresów IP osób, które aktywnie uczestniczyły w kampanii, okazało się, że były one zarejestrowane na całym świecie. Co ciekawe, statystycznie najbardziej zaniepokojony sytuacją na dworcu w Przemyślu był mieszkaniec Indii.**

Poza akcjami dezinformacyjnymi producent oprogramowania Bitdefender od rozpoczęcia wojny odnotował znaczący wzrost kampanii phishingowych oraz prób ataków za pomocą oprogramowania malware i ransomware. Dzięki współpracy z amerykańską firmą MITRE, która specjalizuje się w rozpoznawaniu nowych typów ataków i ich analizie, Bitdefender, bezustannie aktualizuje swoją bazę danych i na bieżąco monitoruje bezpieczeństwo w sieci firm korzystających z oprogramowania Bit-defender GravityZone. Dzięki temu możemy zagwarantować bezpieczeństwo na najwyższym możliwym poziomie.

Obecna sytuacja na świecie wskazuje, że zadbanie o cyberbezpieczeństwo swojej firmy jeszcze nigdy nie było tak ważne, jak dziś. Dlatego w kolejnej części tego artykułu przeanalizujemy, w jaki sposób przygotować się na cyberatak i jakie funkcje powinno zawierać oprogramowanie antywirusowe w firmie, która może być celem wyrafinowanego ataku.

W JAKI SPOSÓB BRONIĆ SIĘ PRZED NAJNOWSZYMI CYBERZAGROŻENIAMI?

Kluczowym elementem skutecznej ochrony przed wszelkimi zagrożeniami sieciowymi jest zrozumienie powagi sytuacji oraz tego, że każda firma i każdy użytkownik sieci może stać się celem zorganizowanego ataku.

W końcu nie bez przyczyny od 4 marca w Polsce obowiązuje trzeci stopień zagrożenia, czyli CHARLIE-CRP.

Drugim krokiem powinna być **dogłębna analiza struktury sieciowej** swojej firmy oraz procedur związanych z potencjalną utratą lub kradzieżą danych.

Następnym etapem powinien być **wybór odpowiedniego oprogramowania dostosowanego do rzeczywistych potrzeb firmy.** Jakie więc funkcje powinno zawierać oprogramowanie dla średnich i dużych firm oraz ośrodków administracyjnych.

Program antywirusowy używany w takich firmach musi posiadać kilka kluczowych modułów bezpieczeństwa. Pierwszym jest **skuteczna ochrona przed phishingiem i spamem.** Ta funkcja pozwala zdecydowanie ograniczyć możliwość zainfekowania systemu przez błąd ludzki, ponieważ pracownik najprawdopodobniej nigdy nie zobaczy potencjalnie niebezpiecznych wiadomości.

Drugim niezbędnym modułem jest **ochrona przed złośliwym oprogramowaniem typu ransomware**. Jeśli pierwszy moduł nie powstrzyma ataku, to system sieciowy firmy powinien być dodatkowo chroniony funkcjami, które ochronią sieć przed zaszyfrowaniem lub przynajmniej zminimalizuje jego skutki. Oprogramowanie Bitdefender GravityZone zawiera trzy skorelowane ze sobą moduły: Hyperdetect, Sandbox Analizer oraz Szczepionkę Ransomware. Hyperdetect natychmiastowo umieszcza podejrzany plik w kwarantannie i sprawdza, w jaki sposób wpływa na system. Sandbox Analizer umożliwia wysłanie próbki podejrzanego pliku na poligon na serwerach producenta oraz zapewnia dogłębną analizę wyników testów. Szczepionka Ransomware to moduł, który chroni sieć w razie zainfekowania oprogramowaniem szyfrującym. Funkcja ta umożliwia odtworzenie kopii zapasowej najważniejszych zasobów systemu.

Co ciekawe, do walki z fake newsami mają zostać powołane zaufane podmioty działające w interesie publicznym w celu przeciwdziałania dezinformacji rozpowszechnianej za pośrednictwem internetowych serwisów społecznościowych.

Jego funkcjonalność umożliwia wykrywanie zaawansowanych ataków na wiele punktów końcowych i infrastrukturach hybrydowych. To narzędzie jest szczególnie pomocne dla zespołów reagowania na incydenty, ponieważ umożliwia wizualizację historii i postępów ataków na mapie struktur sieciowych. Dzięki temu pomaga w ustaleniu najsłabszych ogniw w infrastrukturze firmy.

Najbliższe lata będą bardzo trudne dla wszystkich pracowników związanych z cyberbezpieczeństwem i ochroną zasobów sieciowych. Możemy być pewni tego, że nasze serwery i strony internetowe będą wciąż atakowane przez nieprzyjaźnie nastawione podmioty. Działania cyberwojenne z pewnością nie ustaną nawet po ogłoszeniu pokoju między zwaśnionymi stronami konfliktu.

Dlatego musimy pamiętać o tym, że najważniejszym narzędziem służącym do obrony zasobów sieciowych jest skuteczne oprogramowanie antywirusowe.

/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

SECURITYMAGAZINE.PL

TRANSFER DANYCH POZA UE A REŻIM PRZEPISÓW RODO

Katarzyna Szepelak
Izba Gospodarki Elektronicznej

Standardowe klauzule ochrony danych osobowych jako odpowiednie zabezpieczenie pozwalające na transfer danych do państw trzecich przez przedsiębiorców z branży e-commerce.

Od 25 maja 2018 roku polscy przedsiębiorcy z branży e-commerce, przesyłający dane osobowe poza obszar EOG (Europejski Obszar Gospodarczy - strefa wolnego handlu i wspólny rynek, obejmująca państwa Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu (EFTA), z wyjątkiem Szwajcarii. Opiera się on na: swobodzie przepływu ludzi, kapitału, towarów i usług), mają obowiązek zapewnić ich ochronę na tym samym poziomie, jaki gwarantuje Rozporządzenie RODO. W związku z tym, że handel elektroniczny często łączy się z transgranicznymi, elektronicznymi transferami danych, warto zwrócić uwagę na wygodne narzędzie, gwarantujące zgodność tego typu transferów z prawem unijnym, jakim są standardowe klauzule umowne.

W uproszczeniu można powiedzieć, że standardowe klauzule umowne, które zostały określone szczegółowo w decyzji wykonawczej Komisji UE nr 2021/914, mają za zadanie ułatwić transfer danych do państw spoza EOG.

TRANSFER DANYCH POZA UE

Przedsiębiorcy zajmujący się handlem transgranicznym muszą liczyć się z tym, że ich aktywność w zakresie przetwarzania danych osobowych nadal poddana jest reżimowi prze-pisów RODO. Z tego powodu przedsiębiorcy, którzy prze-kazują dane osobowe, np. spółkom ze swojej grupy kapitałowej lub swoim pracownikom umiejscowionym poza EOG, powinni

PRZEKAZUJĄC DANE OSOBOWE Z UNII DO PAŃSTW TRZECICH, NALEŻY PAMIĘTAĆ O KONIECZNOŚCI ZACHOWANIA STOPNIA OCHRONY DANYCH NA TAKIM SAMYM POZIOMIE JAK W UE.

zwrócić uwagę na zasady rządzące tym procesem. Przekazując dane osobowe z Unii do państw trzecich, należy pamiętać o konieczności zachowania stopnia ochrony danych na takim samym poziomie jak w UE.

Warto zwrócić od razu uwagę, że przekazanie danych osobowych poza EOG nie wymagające uzyskania specjalnego zezwolenia i spełnienia dodatkowych przesłanek możliwe jest, gdy Komisja Europejska stwierdzi, że w danym państwie lub w danej organizacji zapewniono odpowiedni stopień ich ochrony.

Do tej pory Komisja za państwa trzecie zapewniające odpowiedni stopień ochrony uznała: **Andorę, Argentynę, Kanadę (podmioty komercyjne), Wyspy Owcze, Baliwat Guernsey, Izrael, Wyspę Man, Japonię, Okręg Jersey, Nową Zelandię, Republikę Korei, Szwajcarię, Wielką Brytanię oraz Urugwaj.**

Jeśli państwo, bądź terytorium spoza EOG, do których przesyłane mają być dane osobowe, nie znajdują się na powyższej liście, należy zapewnić w takiej sytuacji inne „odpowiednie zabezpieczenia” zgodne z wymogami RODO.

Takimi zabezpieczeniami mogą być między innymi standardowe klauzule ochrony danych przyjęte przez Komisję, które są narzędziem pomocnym w przypadku przekazywania danych poza EOG.

STANDARDOWE KLAUZULE UMOWNE

Standardowe klauzule umowne mogą być stosowane w przypadku:

1. przekazywania danych osobowych przez administratora innemu administratorowi znajdującemu się poza EOG
2. przekazywania danych osobowych przez administratora podmiotowi przetwarzającemu znajdującemu się poza EOG
3. przekazywania danych osobowych przez podmiot przetwarzający innemu podmiotowi przetwarzającemu znajdującemu się poza EOG
4. przekazywania danych osobowych przez podmiot przetwarzający administratorowi znajdującemu się poza EOG.

Co do zasady, same standardowe klauzule nie mogą być zmieniane, jednak dopuszczalne jest umieszczanie klauzul o szerszym zakresie – lub zawieranie w umowie szerszych zabezpieczeń.

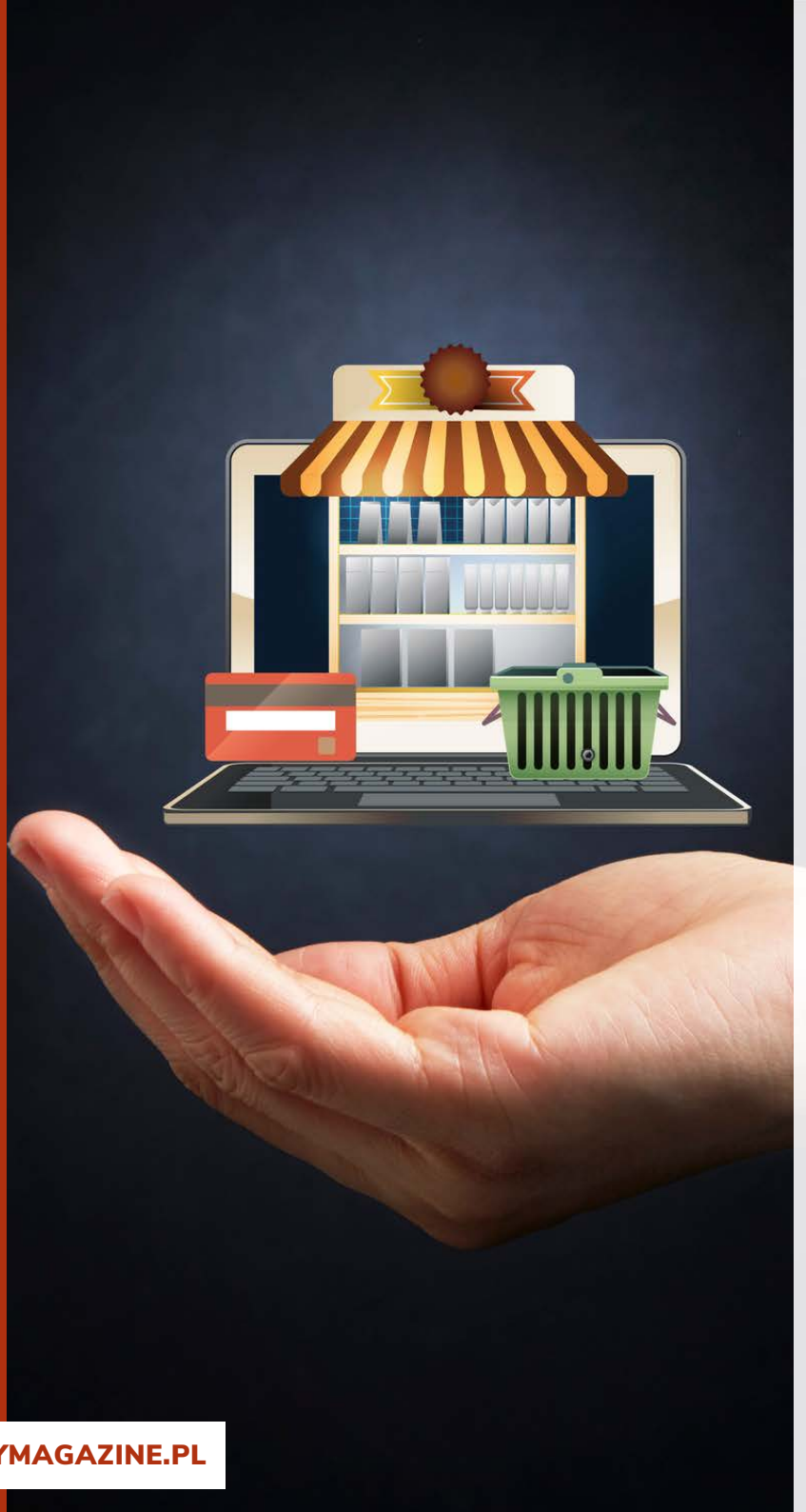
Przyjęcie standardowych klauzul umownych wydawało się znacznym udogodnieniem. Jednak od samego początku zdarzały się głosy przedstawicieli branży, wyrażające niepewność co do znaczenia klauzul i bezpieczeństwa posługiwania się nimi w celu wypełnienia obowiązków wynikających z RODO.

Ecommerce Europe – organizacja reprezentująca przedsiębiorców z sektora handlu elektronicznego - w komentarzu do projektu decyzji poprosiła Komisję o potwierdzenie, że nowa decyzja wykonawcza gwarantuje, że standardowe klauzule umowne są wystarczającym instrumentem zapewniającym zgodność przekazywania danych osobowych do krajów trzecich z RODO.

Jak wskazała **Ecommerce Europe**, niezwykle ważne jest, aby osoby trudniące się handlem elektronicznym mogły polegać na klauzulach zatwierdzonych przez Komisję Europejską, bez ponoszenia ryzyka, że organy ochrony danych będą próbowały nakładać na nich dodatkowe wymagania. Tworzyłoby to bowiem sytuacje prowadzące do niepewności prawnej oraz chaosu informacyjnego.

Aby tego uniknąć, Ecommerce Europe zasugerowała, aby Komisja oficjalnie potwierdziła m. in., że klauzule mogą być stosowane do przekazywania danych do dowolnego podmiotu odbierającego dane w dowolnym państwie trzecim, a przedsiębiorcy nie muszą polegać na żadnych dodatkowych klauzulach umownych.

Niestety, z opublikowanej niedawno interpretacji Europejskiego Urzędu Ochrony Danych Osobowych jasno wynika, że samo poleganie na instrumencie standardowych klauzul umownych będzie niewystarczające dla zapewnienia odpowiedniego poziomu ochrony danych osobowych. EUODO podkreślił, że, jeśli transfer danych nie jest dokonywany do terytorium lub państwa objętego decyzją Komisji stwierdzającą odpowiedni poziom ochrony, należy sprawdzić w każdym indywidualnym przypadku, czy prawo lub praktyka tego państwa trzeciego nie podważa zabezpieczeń zawartych w stan-



dardowych klauzulach umownych. Jeśli w trakcie takiej oceny okaże się, że użycie standardowych klauzul umownych jest niewystarczające dla zapewnienia odpowiedniego poziomu ochrony, należy zastosować dodatkowe środki, np. zabezpieczenia techniczne.

Przyjęcie przez Komisję Europejską nowego zestawu standardowych klauzul umownych, mających na celu zapewnienie zgodności z prawem transferu danych poza EOG, z pewnością stanowi krok w dobrą stronę. Klauzule zdają się być bowiem narzędziem wygodnym i dostosowanym do różnych konfiguracji przetwarzania danych osobowych, szczególnie jeśli chodzi o ułatwienie przedsiębiorcom z branży e-commerce operowania danymi osobowymi w relacjach transgranicznych. Niestety rozwiązania zaproponowane przez Komisję, nie uchronią przedsiębiorców z branży e-commerce przed obowiązkiem indywidualnego badania ryzyka naruszenia poziomu ochrony gwarantowanego przez RODO w państwach trzecich.

OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

SECURITYMAGAZINE.PL

JAK ROSYJSCY HAKERZY ATAKUJĄ ZACHODNIE FIRMY? ANALIZA

Redakcja
SECURITY MAGAZINE

Rosja od początku wojny w Ukrainie pada celem ataków hakerskich. Na reżim Putina czy zachodnie firmy, które prowadzą bądź prowadziły swoją działalność w Rosji – kładzie się cień Anonymous. Nie oznacza to jednak, że nie dochodzi do żadnych odwetów. Rosyjscy hakerzy też atakują firmy. Czy Twoja także padnie ich ofiarą i jaka jest skuteczność cyberprzestępców ze wschodu?

ROSJA A HAKERZY I PROGRAMIŚCI

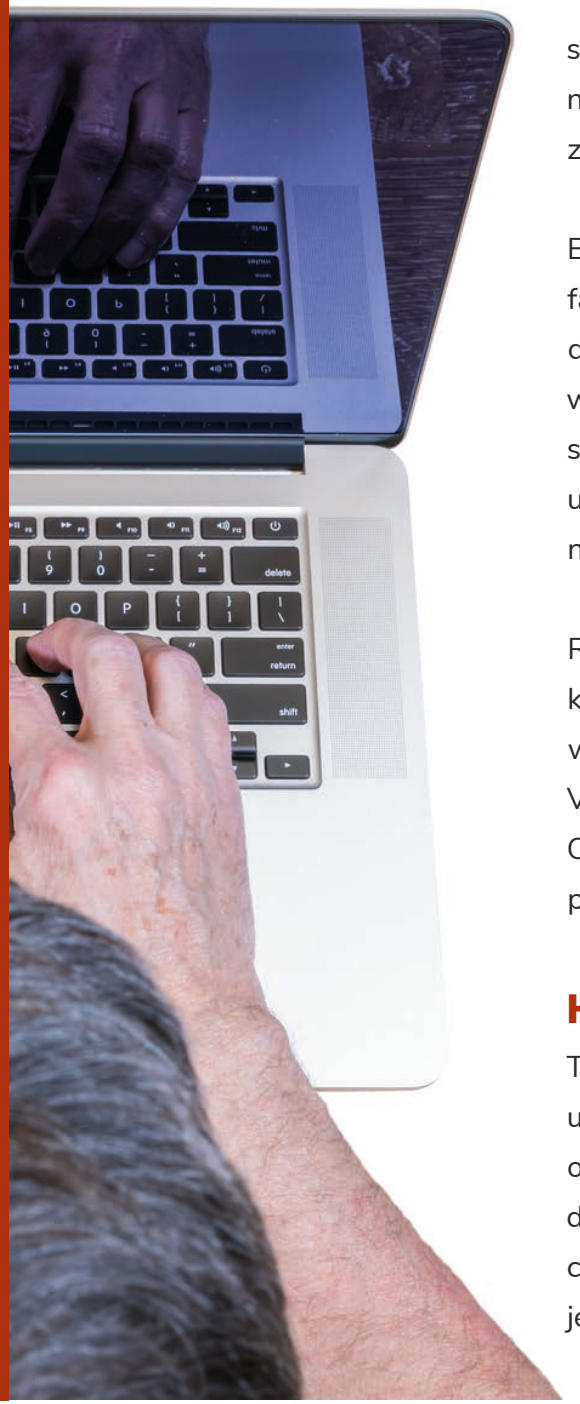
Eksperci ds. cyberbezpieczeństwa z Uniwer-ooysytetu w Cambridge przeanalizowali w IV kwartale 2021 r. ruchy ataków hakerskich na świecie. Z ich badań wynikało, że te 10 lat temu najwięcej cyberprzestępstw pochodziło z Chin (41%), Stanów Zjednoczonych (10%), Turcji (4,7%) i Rosji (4,3%). Federacja Rosyjska często w badaniach, artykułach i wypowiedziach ekspertów wskazywana jest jako ojczyzna hakerów, ale również wybitnych programistów czy informatyków.

Niejednokrotnie zestawia się ją właśnie z Chinami jako miejsce, z którego pochodzi najwięcej ataków hakerskich na świecie. I choć demografia ta nieco się zmienia (przykładowo w 2021 r. Rosja, jeśli chodzi o źródło ataków DDoS znalazła się na 7. miejscu, a wyprzedziły ją takie kraje jak Indonezja, Malezja, Indie czy Brazylia), to coś w tym jest.

Wielu znamienitych programistów czy informatyków na całym świecie wywodzi swoje korzenie właśnie z Rosji. Przykładowo **Vitalik Buterin** – jeden z ojców kryptowaluty i blockchaina Ethereum jest właśnie Rosjaninem (choć w wieku 6 lat wyjechał z rodzicami do Kanady.

Notabene jego ojciec – Dmitry Buterin – również jest programistą). Współzałożyciel Google – **Sergey Brin** – również urodził się w Rosji. **Pavel i Nikolai Durov** – twórcy **VKontakte.ru** (VK) i **Telegrama,** to także Rosjanie. **Yevgeny Kaspersky** – ojciec antywirusa Kaspersky – Rosjanin. **Vadim Gerasimov i Alexey Pajintov, twórcy Tetrisa** – Rosjanie. **Ilya Segalovich**, założyciel i pierwszy programista **Yandex** – Rosjanin. **Andrey Andreev**, twórca **Badoo** – Rosjanin. I moglibyśmy tak wymieniać jeszcze bardzo długo.

Skąd tyle znamienitych ojców licznych aplikacji, programów, gier, a nawet kryptowalut i wyszukiwarek wywodzących się z Rosji? Choć dla niektórych może brzmieć to absurdalnie, to w Związku Radzieckim nauka zajmowała dość ważną pozycję. Rosjanie (i inne narody znajdujące się pod butem ZSRR), wierzyli, że za pomocą nauki uda im się prześcignąć zachód, a nawet zaprowadzić prawdziwy komunizm ze



snu Marksa (polecam zapoznać się z projektem OGAS). Kiedy zatem zaczęto rozwijać nauki komputerowe i informatykę – zaczęło przybywać rosyjskich programistów zainteresowanych tworzeniem innowacyjnych rozwiązań.

Bo gdy spojrzymy na daty urodzenia poszczególnych programistów i ich życiorysy, to faktycznie większość z nich urodziła się (i przynajmniej częściowo), kształciła czy dorastała w Związku Radzieckim. Wyjątkiem jest tutaj Vitalik Buterin, który urodził się w 1994 r., lecz częściowo odziedziczył tę sowiecką myśl i szkołę informatyczną po swoim ojcu. Jednak rozpad ZSRR spowodował, że żelazna kurtyna opadła, a wielu uzdolnionych i wykształconych programistów, postanowiło rozwijać swoje projekty na zachodzie.

Rosyjski system okazał się dla nich wyjątkowo nieprzyjazny. Oligarchia, czy rząd, które gdy tylko ktoś się rozwijał, kładły łapy na czyjś biznes, nie są dogodnymi warunkami do pracy. Taki los spotkał m.in. braci Durov, których wręcz okradziono z VK, a gigant social media zostawał coraz mocniej uzależniany od rosyjskich władz. Obecnie 57,3% udziałów w VK posiada Gazprombank i SOGAZ – spółki oczywiście podporządkowane reżimowi Putina.

HAKERZY W ROSJI TO DZIECI STRACONYCH SZANS?

Tak nieprzyjazna rzeczywistość do prowadzenia biznesu spowodowała drenaż umysłów – uzdolnieni programiści czy eksperci od cyberbezpieczeństwa zwyczajnie odpłynęli na zachód. Ewentualnie sami stali się oligarchami współpracującymi z rządem jak Yevgeny Kaspersky. Ci, którym się nie poszczęściło zwyczajnie „przeszli na ciemną stronę mocy". Hakerstwo to stosunkowo dobry zarobek – zwłaszcza kiedy jest się uzdolnionym.

Jak rosyjscy hakerzy atakują zachodnie firmy?

Według BBC News aż 74% przychodów z oprogramowania ransomware (wirus, który blokuje dostęp do danych czy komputera i żąda okupu za przywrócenie wszystkiego do normalnego stanu) trafia do hakerów powiązanych z Rosją. Kraj ten ma być też domem dla licznych grup cyberprzestępczych m.in. tajemniczego tzw. Evil Corp, którą od dawna zlikwidować próbuje amerykańska administracja. Jednym z jej liderów mają być Rosjanie Igor Olegovich Turashev i Maksim Yakubets, których stara się wytropić FBI. Rzecz jasna Władimir Putin zaprzecza, jakoby jego państwo miało być schronieniem dla hakerów.

Evil Corp miało ukraść ponad 100 mln dolarów z 40 różnych państw za pomocą szkodliwego oprogramowania imitującego bankowość internetową, a także za pomocą phishingu. FBI zdecydowało się nawet wyznaczyć 5 mln dolarów nagrody za jakiekolwiek informacje nt. grupy. Evil Corp to jednak niechlubny crème de la crème cyberprzestępczości w Rosji. Hakerów jest znacznie więcej i atakują nie tylko zwykłych konsumentów, ale również firmy.

Mocno we znaki – zwłaszcza amerykańskim firmom – daje się grupa Nobelium. Ci hakerzy powiązani mają być z rosyjskimi Służbami Wywiadu Zagranicznego.

W 2020 r. zaatakowali m.in. firmę IT SolarWinds oraz infrastrukturę amerykańskiego rządu. W 2021 r. z kolei dopuścili się cyberataków na Microsoft. Według amerykańskiego bigtechu Nobelium dopuściło się 23 tys. ataków na sam tylko Microsoft. Dokonano także prób włamania się do 140 sprzedawców oprogramowania i firm technologicznych. Nobelium w swoich atakach stosuje głównie phishing.

ROSYJSCY HAKERZY KRADNĄ TECHNOLOGIE

Cyberataki Rosjan miały jednak miejsce na długo przed latami 2020–2021. W 2014 roku New York Times opublikowało raport firmy badawczej CrowdStrike, według którego ataki rosyjskich hakerów dotknęły ponad 1000 podmiotów w 84 krajach. Grupę, która stała za cyberatakami zeszłej dekady nazwano „Energetycznym Niedźwiedziem". Hakerzy infekowali głównie systemy firm, które dostarczały rozwiązania technologiczne z zakresu przemysłu 4.0 i spółek energetycznych.

Celem cyberataków było pozyskanie poufnych informacji, ale także kradzieży technologii. Wówczas wielu ekspertów ds. cyberbezpieczeństwa spekulowało, że Energetyczny Niedźwiedź był powiązany z rosyjskimi spec-służbami lub w ogóle był ich częścią. Hakerzy wykorzystywali metody phishingowe, a także podsyłali szkodliwe oprogramowania imitujące instalację sterowników. Cyberprzestępcy włamywali się również do BIOS-ów, co utrudniało ich wykrycie czy cofnięcie zmian.

Jednak niektórzy spekulowali, że za tymi atakami nie stali Rosjanie, a... Chińczycy.

Co prawda w kodzie szkodliwych oprogramowań znajdowano znaki pisane cyrylicą, lecz część ekspertów podkreśla, że chińscy hakerzy niekiedy pozostawiają fałszywe tropy prowadzące właśnie do Rosji, żeby oddalić od siebie podejrzenia.

ROSYJSCY HAKERZY ZMUSILI RAFINERIĘ ROPY DO ZAMKNIĘCIA ZAKŁADU

Według amerykańskiej administracji w latach 2012–2017 Rosjanie dopuścili się licznych cyberataków na amerykańskie firmy i spółki państwowe. Jednak ich macki sięgają znacznie dalej. Rosyjscy hakerzy nie atakują bowiem tylko państw zachodu. W 2017 r. przekonała się o tym Arabia Saudyjska.

Spółka Petro Rabigh, która zajmuje się m.in. rafinacją ropy naftowej – została wówczas zaatakowana przez hakerów, których wiążę się z rosyjskimi służbami GRU. Chodzi tutaj o tzw. grupę Sandworm. Cyberprzestępcy za pomocą złośliwego oprogramowania Triton wywołali w saudyjskim zakładzie eksplozję, co uwolniło toksyczne związki chemiczne. Rafineria musiała zostać zamknięta.

Z kolei w 2015 r. rosyjscy hakerzy zaatakowali trzy różne ukraińskie sieci energetyczne i odłączyli ponad 60 podstacji w całym kraju. Spowodowało to przerwy w dostawie prądu dla od 80 tys. do nawet 225 tys. osób w środku zimy. Oba te incydenty przez Roberta Lee – byłego hakera i współ-założyciela firmy ds. cyberbezpieczeństwa Dragos – zostały okrzyknięte pierwszym cyberatakiem przeprowadzonym w celu zabijania ludzi.

W 2021 roku Rosjanie zaatakowali także amerykański system rurociągów Colonial Pipeline, który odpowiada za transport 45% dostaw oleju napędowego, benzyny i paliwa do silników odrzutowych we wschodniej części USA. Za pomocą oprogramowania ransomware grupa niepowiązana z rosyjskim rządem zablokowała system komputerowy Colonial Pipeline i wstrzymała dostawy surowców. Spółka obsługująca rurociąg przyznała później, że za-płaciła cyberprzestępcom okup w wysokości 4,4 mln dolarów w bitcoinach, aby przywrócić system.

Kilka tygodni później grupa REvil (którą rzekomo na prośbę Stanów Zjednoczonych rozmontowało w Rosji FSB) zaatakowała największego przetwórcę wołowiny na świecie – JBS. Hakerzy zablokowali systemy informatyczne w wielu za-kładach w Ameryce Północnej i Australii, na-leżące do spółki, a także wykradli jej dane. JBS przyznało, że wpłaciło hakerom aż 11 mln do-larów okupu. Choć cyberprzestępczy początkowo żądali 22,5 mln dola-rów.

ROSYJSCY HAKERZY ATAKUJĄ POLSKĘ

Oczywiście, Polska również jest na celowniku rosyjskich grup cyberprzestępczych i spec-służb. Jednak głównie ofiarami w Polsce pada nasza administracja i rząd, a niekoniecznie firmy. W niebezpieczeństwie są również zwykli konsumenci.

W końcu w zeszłym roku wielu cyberprzes-tępców i oszustów podawało się m.in. za pracowników banków i w ten sposób próbowali wyłudzać pieniądze od ludzi. Spora część z tych oszustów mówiła z dość charakterystycznym wschodnioeuropejskim akcentem czy też bu-dowała zdania w charakterystyczny dla języka rosyjskiego sposób.

16 maja 2022 rosyjska grupa KILLNET wypowiedziała cyberwojnę 10 państwom, w tym Polsce.

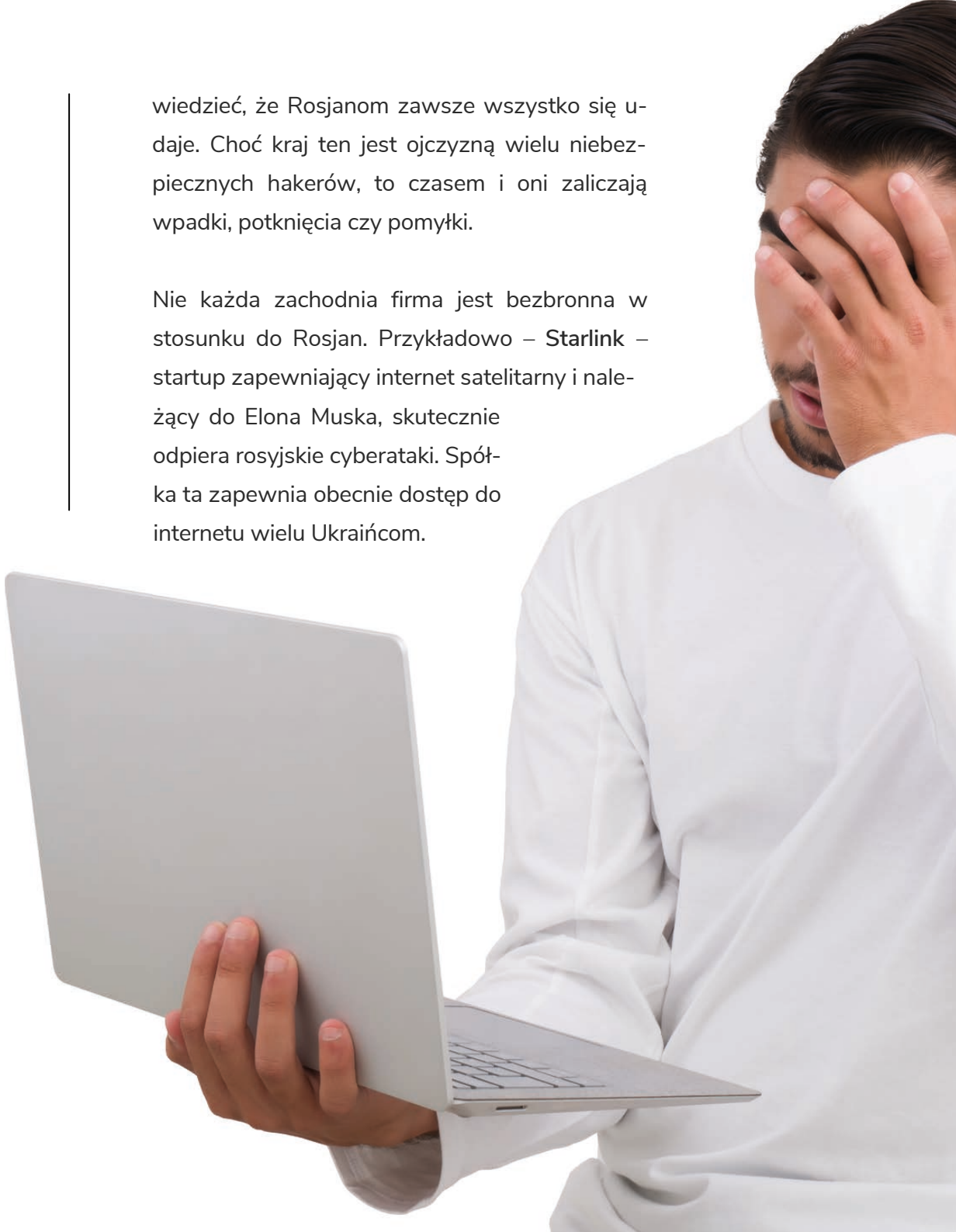
Ofiarą rosyjskich hakerów padł m.in. generał Waldemar Skrzypczak – obecnie będącego w rezerwie. Rosjanie wykradli jego pocztę i materiały z analizy możliwego przebiegu inwazji Rosji na nasz kraj. Obecnie to właśnie Wojsko Polskie jest na celowniku rosyjskich hakerów i cyberprzestępców.

Co więcej, 16 maja serwis informacyjny NEXTA podał, że rosyjska grupa KILLNET wypowie-działa cyberwojnę 10 państwom. To hakerzy powiązani stricte z rosyjskim rządem. KILLNET chce przypuścić cyberataki na Polskę, ale też Stany Zjednoczone, Niemcy, Włochy, Wielką Brytanię, Ukrainę, Łotwę, Litwę, Estonię i Rumunię. KILLNET zaatakował już stronę włoskiej policji. **Grupa jednak już od dawna groziła różnym rządom europejskich państw.**

WPADKI ROSYJSKICH HAKERÓW

Choć w tekście podkreślam światłość rosyjskich programistów, wskazuję udane ataki i wyłu-dzenia ze strony cyberprzestępców czy piszę o wyjątkowo groźnych grupach, to nie można powiedzieć, że Rosjanom zawsze wszystko się udaje. Choć kraj ten jest ojczyzną wielu niebezpiecznych hakerów, to czasem i oni zaliczają wpadki, potknięcia czy pomyłki.

Nie każda zachodnia firma jest bezbronna w stosunku do Rosjan. Przykładowo – **Starlink** – startup zapewniający internet satelitarny i należący do Elona Muska, skutecznie odpiera rosyjskie cyberataki. Spółka ta zapewnia obecnie dostęp do internetu wielu Ukraińcom.



W zasadzie odkąd tylko sprzęt ten trafił w ręce Ukraińców – rosyjscy hakerzy starali się zakłócić jego działanie.

Satelity Starlink były jednak na cyberataki przygotowane i uruchomiły system obronny, który blokował próby włamania i zagłuszania łączności. Za skuteczność cyber-bezpieczeństwa startup pochwalił nawet rzecznik prasowy Pentagonu, który stwierdził, że spółka jest fantastycznie przygotowana do obrony przed hakerami. Pentagon wskazał wręcz, że amerykańska armia powinna jak najszybciej wdrożyć podobne rozwiązania.

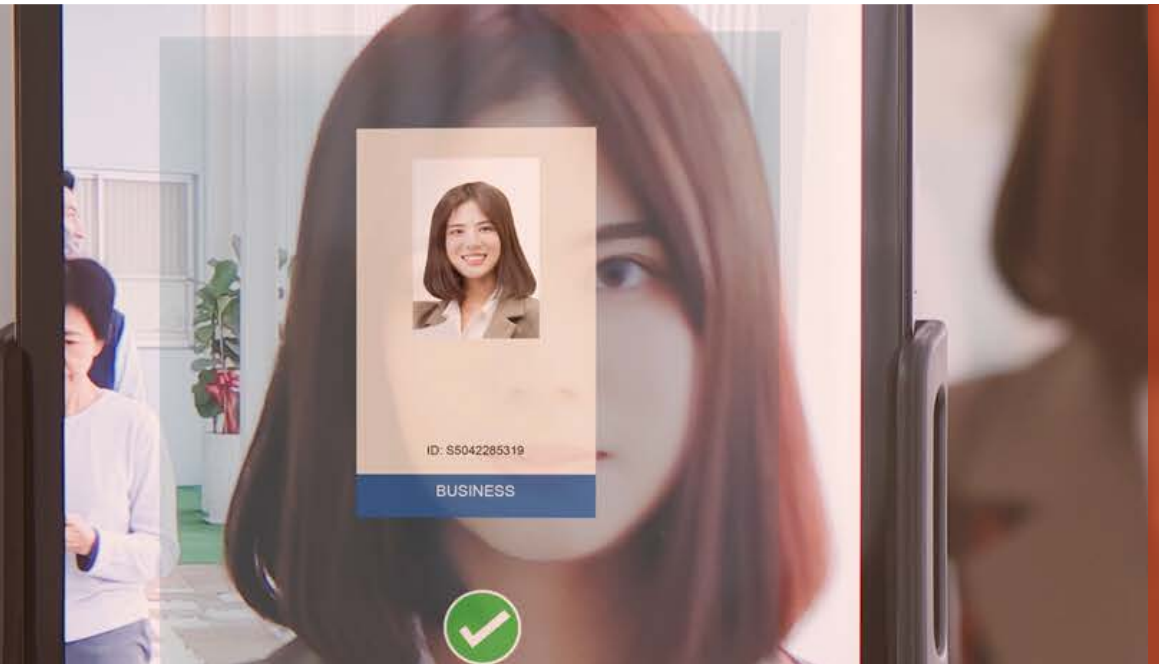
Jakiś czas temu grupa rosyjskich hakerów pochwaliła się także, że udało im się przejąć oficjalną stronę Anonymous – organizacji, która od początku wojny stoi po stronie Ukrainy. Problem jednak w tym, że... Anonymous nie ma żadnej oficjalnej strony. Wpadka ta nie umknęła uwadze wspomnianej grupy, która od razu skomentowała ją na swoim twitterowym profilu.

Na początku kwietnia wspomniana organizacja rosyjskich hakerów KILLNET sama padła ofiarą cyberataku. Grupy haktywistów z DoomSec i BlueHornet rozpracowały zarówno KILLNET, jak i FancyBear, ujawniając dane ich kluczowych hakerów, a nawet imiona i nazwiska najbliższych, adresy czy konta w mediach społecznościowych.

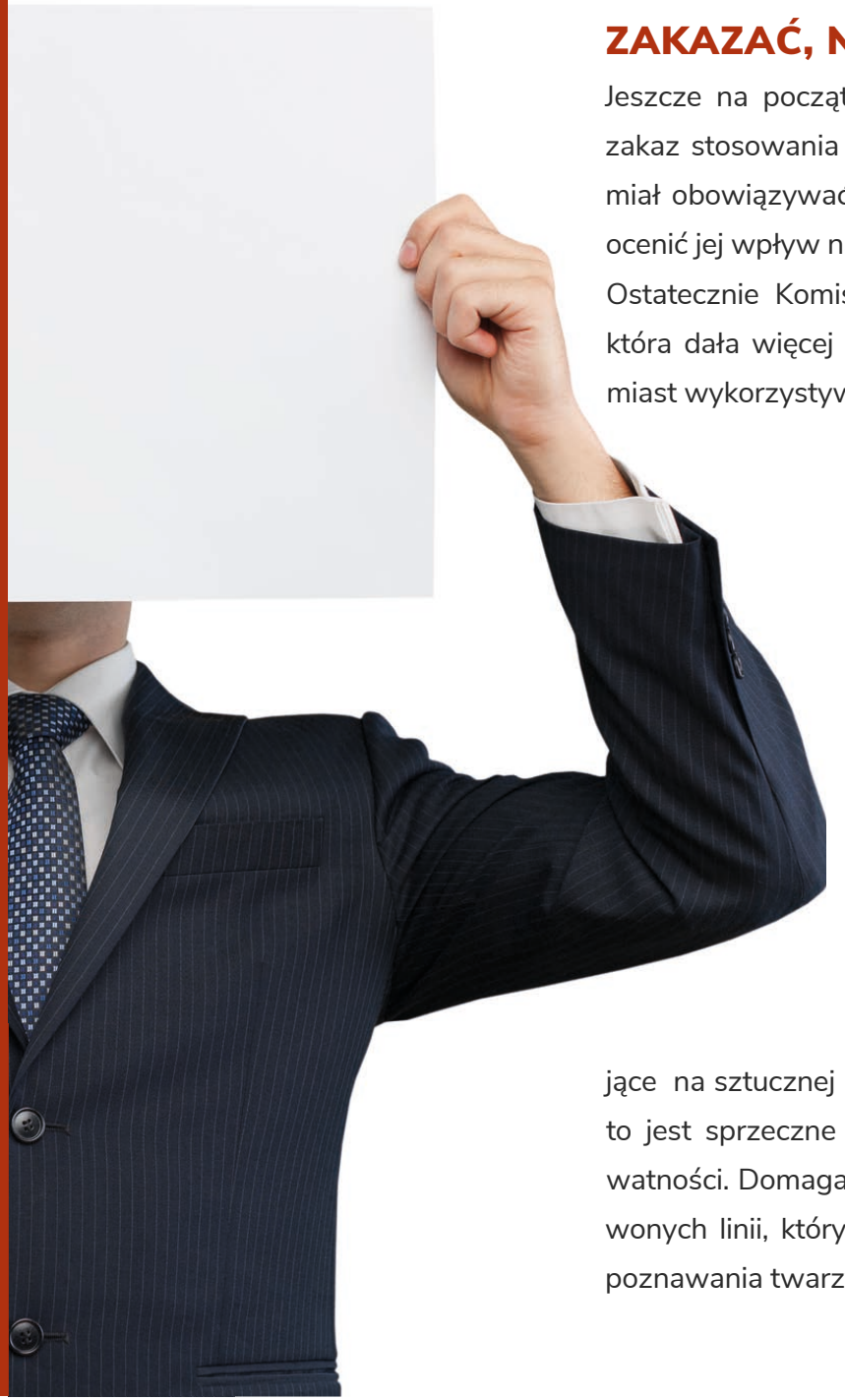
Bez wątpliwości rosyjscy hakerzy są groźni. Jednak po „jasnej stronie mocy” stoją liczne zastępy pentesterów, ekspertów ds. cyberbezpieczeństwa i haktywistów chroniących konsumentów, internautów, firmy, a także państwowe administracje. Cyberprzestępczość z roku na rok staje się coraz poważniejszym tematem. Dlatego Twoja firma powinna być odpowiednio zabezpieczona i przygotowana do cyberataków – i to nie tylko tych rosyjskich. Powinieneś obawiać się każdego cyberprzestępcy, bo jak widzisz – ofiarami mogą paść nawet największe spółki na świecie i to w każdej możliwej branży.

TECHNOLOGIA ROZPOZNAWANIA TWARZY ZDOMINUJE WŁAŚNIE TE BRANŻE

Redakcja
SECURITY MAGAZINE



Rozwój technologii rozpoznawania twarzy był kwestią czasu. Dlaczego Unia Europejska chciała jej zakazać? jakie ryzyko niesie za sobą “face recognition”? Które branże zdominuje? Jakie daje im szanse na rozwój?



ZAKAZAĆ, NIE ZAKAZAĆ?

Jeszcze na początku 2020 roku Komisja Europejska brała pod uwagę tymczasowy zakaz stosowania technologii rozpoznawania twarzy w miejscach publicznych. Zakaz miał obowiązywać do czasu, gdy Unia Europejska będzie mogła w sposób właściwy ocenić jej wpływ na ochronę prywatności.

Ostatecznie Komisja opublikowała **„Białą księgę w sprawie sztucznej inteligencji”**, która dała więcej możliwości technologii rozpoznawania twarzy. Zakazane jest natomiast wykorzystywanie jej do zdalnej identyfikacji biometrycznej.

Nie mówiąc już o tym, że europejskie organy nadzorujące prywatność wezwały do wprowadzenia zakazu używania rozpoznawania twarzy w przestrzeni publicznej ze względu na "niezwykle wysokie" ryzyko dla prywatności. Europejska Ochrona Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) rekomendują, by zakazać wykorzystywania sztucznej inteligencji na potrzeby "ustalania emocji" oraz wszelkiego rodzaju scoringu społeczności (metoda oceny wiarygodności podmiotu).

- *Technologia rozpoznawania twarzy powinna być zabroniona w Europie ze względu na „głęboką i niedemokratyczną ingerencję” w życie prywatne* – powiedział Europejski Inspektor Ochrony Danych, dodał że zaawansowane systemy do rozpoznawania twarzy bazujące na sztucznej inteligencji skanują twarz każdego, kto znajdzie się na linii kamery. A to jest sprzeczne z podstawowymi prawami człowieka dotyczącymi prawa do prywatności. Domaga się tym samym sprecyzowania przepisów i ustanowienia tzw. czerwonych linii, których nie można byłoby przekroczyć przy korzystaniu z systemu rozpoznawania twarzy.

Na tę decyzję miał zapewne wpływ sposób wykorzystania tej technologii przez Chiny. Natomiast nieco inne stanowisko przedstawiła Komisja Europejska. Z projektu nowych regulacji dotyczących wykorzystania technologii sztucznej inteligencji wynika, że **Bruksela nie chce całkowicie blokować rozwoju AI.**

- Nie zamierzamy zakazywać samej technologii, ale uregulować jej wykorzystanie - zapewnił komisarz UE ds. rynku wewnętrznego Thierry Breton.

Zastosowanie technologii podzielono więc na cztery kategorie ryzyka:

1. **Technologie o minimalnym ryzyku**, które nie zagrażają prawom ani bezpieczeństwu ludzi albo ryzyko jest minimalne, dlatego nie wymagane są dodatkowe obostrzenia, np. filtry wyłapujące spam w poczcie elektronicznej.

2. **Technologie o ograniczonym ryzyku**. Przykładem są tu chatboty, które komunikują się z internautą i proponują pomoc lub odpowiadają na pytania.

3. **Technologie o wysokim ryzyku,** które mają negatywny wpływ na bezpieczeństwo ludzi i mogą naruszać ich prawa podstawowe. Stosowane są m.in. w medycynie, w diagnostyce i sądownictwie, gdzie oceniają wiarygodność dowodów.

4. **Technologie o niedopuszczalnym ryzyku dla ludzi**, które w szkodliwy sposób manipulują zachowaniem, opiniami i decyz-jami. Ta kategoria w Unii Europejskiej będzie bezwzględnie za-kazana, choć np. w Chinach jest stosowana.

Rozpoznawanie twarzy zostało zakwalifikowane do technologii trzeciej - wysokiego ryzyka. Wykorzystywanie ich w miejscach publicznych będzie na terenie Unii Europejskiej zakazane, choć będzie wyjątek. Z tej technologii będzie można korzystać podczas walki z przestępczością, czy to w czasie zagrożenia atakiem terrorystycznym, czy przy poszukiwaniach osób zaginionych, szczególnie dzieci. O tym, czy będzie będzie można zastosować rozpoznawanie twarzy, będzie decydował sąd albo organy ścigania. Oczywiście wykorzystanie tego rodzaju AI będzie ograniczone w czasie, miejscu i dotyczyć będzie przestępstw zagrożonych karą minimum 5 lat pozbawienia wolności.

TWARZ JAK ODCISK PALCA

O tej technologii mówi się od lat, jednak jej szerokie zastosowanie zaczęło przybierać na sile w kontekście szalejącej pandemii. I mówi się nie tylko w Polsce, ale na całym świecie. Początkowo służyła wojsku, ale szybko zauważono, że służyć może również innym dziedzinom.

Jak działa system rozpoznawania twarzy? Bazą jest nakładanie na twarz człowieka “siatki punktów”, która odpowiada poszczególnemu rozstawowi oczu, kształtowi nosa, konturu warg i kształtom podbródka i uszu. Algorytm rozpoznaje, czy twarz przed kamerą lub ze zdjęcia zgadza się z tą, która wcześniej została zapisana na tej siatce. Pozytywna weryfikacja uzyskana jest wówczas, gdy urządzenie widzi zgodność. Najnowocześniejsze systemy mogą znaleźć w tłumie twarz osoby, która jest, na przykład, poszukiwana i to w przypadku, gdy częściowo zakryta jest czapką, chustą lub innym wierzchnim okryciem. Technologia ta jest bardzo dokładna i wykorzystywana na szeroką skalę w prawie każdej dziedzinie życia. To powoduje słuszne pytania o bezpieczeństwo takich rozwiązań, o których już niejednokrotnie mówił EIOD.

Czy instytucje właściwie chronią dane, czy wizerunek klientów nie będzie kiedyś udostępniony publicznie? Wątpliwości budzi też brak prywatności, choć to gwarantuje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Według niego osoby trzecie nie mają prawa wykorzystywać wizerunku bez wiedzy i zgody samych zainteresowanych.

Firmy działające na terenie Unii Europejskiej będą musiały dostosować się do nowych przepisów. Jeśli tego nie zrobią, grożą im ogromne kary od 20 mln euro do nawet 4 procent rocznych obrotów. Nadzór nad nowymi przepisami miałyby sprawować wyznaczone przez państwa członkowskie krajowe organy nadzoru rynku. A samego ich wdrożenia pilnować miałaby Europejska Rada ds. Sztucznej Inteligencji.

Ciekawe statystyki związane z rynkiem AI zaprezentowała firma Global Market Insights. Szacuje ona, że nakłady na sztuczną inteligencję w handlu detalicznym do 2024 roku wyniosą 8 miliardów dolarów.

W samym 2022 roku detaliści wydadzą ponad 7,5 mld dolarów na technologie wykorzystujące SI.

BRANŻE, KTÓRE MOGĄ OPIERAĆ DZIAŁALNOŚĆ NA "FACE RECOGNITION"

Zastosowań rozpoznawania twarzy jest co najmniej kilka, w szczególności w trzech kategoriach:

- **monitoring i bezpieczeństwo**
- **medycyna**
- **marketing.**

Musimy jednak założyć, że w miarę, jak technologia będzie ulepszana, a jej mankamenty będą eliminowane, znajdzie zastosowanie również w innych sektorach rynku.

SZACUJE SIĘ, ŻE NAKŁADY NA SZTUCZNĄ INTELIGENCJĘ W HANDLU DETALICZNYM DO 2024 ROKU WYNIOSĄ 8 MILIARDÓW DOLARÓW.

MONITORING ORAZ BEZPIECZEŃSTWO

W porównaniu z metodami biometrycznymi (skan siatkówki oka czy odcisk palca) rozpoznawanie twarzy jest o wiele szybsze i nieangażujące osoby, która jest sprawdzana, choć oczywiście nie jest tak dokładne.

Trzeba mieć jednak na uwadze, by ten rodzaj monitoringu i identyfikacji nie posłużyły do inwigilowania obywateli i łamania praw człowieka. Świat przygląda się obecnie Chinom, w których na daną chwilę funkcjonuje już prawie 3 miliardy kamer przemysłowych. Technologia używana jest przez pekińskich policjantów. Specjalne okulary skanują twarze przechodniów i rejestracje przejeżdżających samochodów. W szkołach monitoruje się emocje uczniów, ich zachowania, każdy krok obserwowany jest przez kamery.

MEDYCYNA

Face recognition pozwala monitorować zdrowie, a nawet dać obraz przebytych chorób.

Technologia pomaga w przynajmniej czterech aspektach związanych ze zdrowiem człowieka:

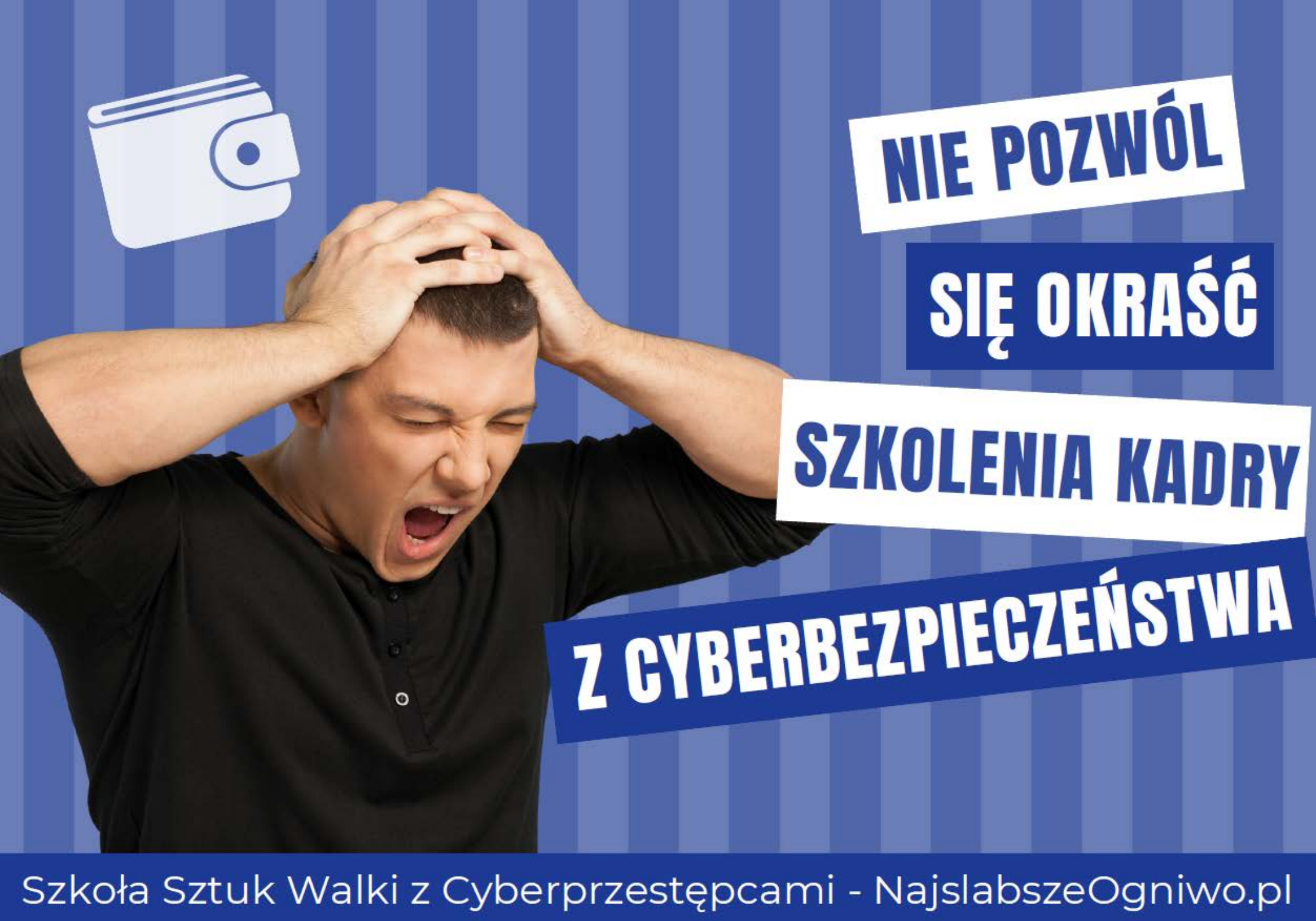
- **Wykrywa** choroby, których symptomy widoczne są w zmianach rysów twarzy (np. zespół DiGeorge'a czy udar)
- **Wspiera** leczenie bólu i monitoruje jego natężenie
- **Śledzi** stosowanie leków, które pacjent powinien zażywać
- **Pomaga** seniorom, niepełnosprawnym czy osobom z wadami wymowy w komunikacji.

SPRZEDAŻ I MARKETING

Wydaje się, że rozpoznawanie twarzy to idealne rozwiązanie dla takich działań marketingowych, które opierają się na personalizacji i rozumieniu potrzeb konsumentów. Dla sprzedawców nie byłoby lepszego rozwiązania, jak możliwość błyskawicznego dopasowana do jego cech (płci, wieku, rasy, historii zakupów czy nawet emocji) towaru lub usługi. To jest jeden aspekt. Kolejnym jest ułatwienie płacenia klientom za zakupiony towar czy wykonaną usługę. Tak dzieje się np. w Alipay (należący do Alibaby) czy Amazon GO. Technologia coraz powszechniej stosowana jest również do logowania za pomocą twarzy do niektórych serwisów i usług (np. bank Nat West, czy Apple - do odblokowania telefonu).

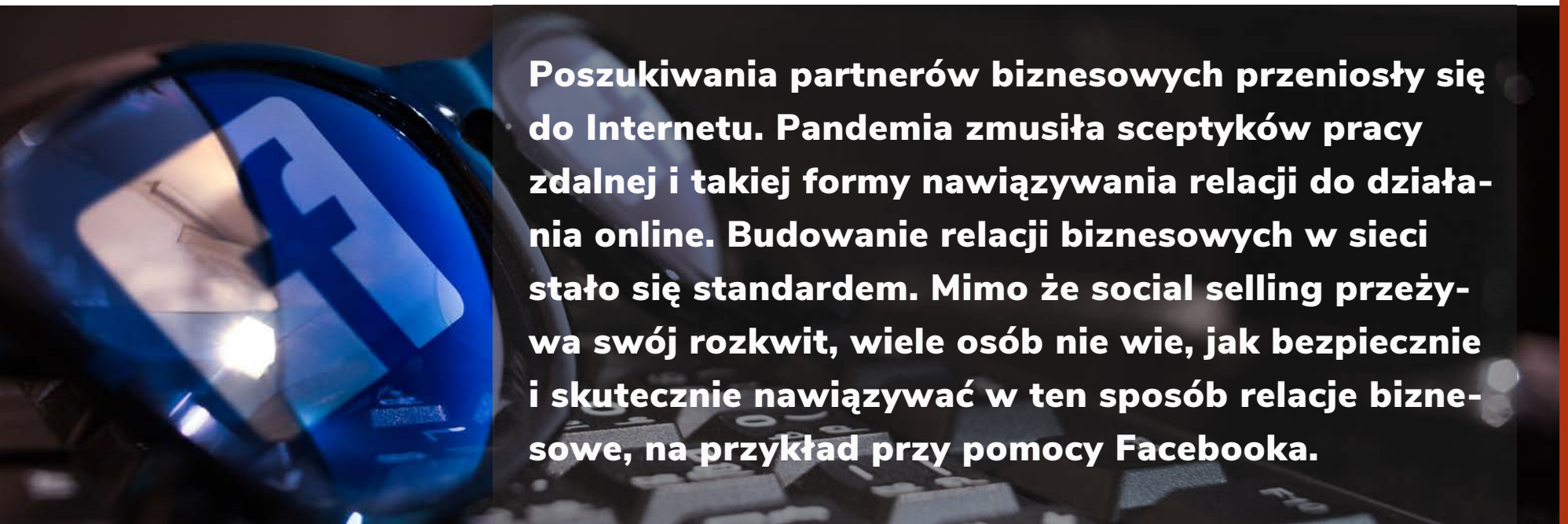
EUROPEJSKIE WYTYCZNE DOTYCZĄCE ROZPOZNAWANIA TWARZY

- Wśród zaleceń skierowanych do ustawodawców i decydentów wskazano kwestie zgodności z prawem, niezbędnego zaangażowanie organów nadzorczych, certyfikacji oraz konieczności podnoszenia świadomości - przekazał **Urząd Ochrony Danych Osobowych**, dodając: - W dokumencie wskazano też zalecenia dla branż takich jak twórcy, producenci i dostawcy usług IT, tak by w tej dziedzinie również zadbano o przestrzeganie ochrony danych osobowych w kontekście m.in. jakości przetwarzanych danych i algorytmów, niezawodności wykorzystanych narzędzi, a także świadomości i rozliczalności. Dokument zawiera także wskazówki w odniesieniu do praw osób, których dane dotyczą. Zalecenia dla podmiotów wykorzystujących technologię rozpoznawania twarzy obejmują m.in. kwestie zgodności przetwarzania danych z prawem i ich jakości, a także bezpieczeństwa oraz rozliczalności i dotyczą zarówno sektora publicznego, jaki prywatnego.


NIE POZWÓL
SIĘ OKRAŚĆ
SZKOLENIA KADRY
Z CYBERBEZPIECZEŃSTWA
Szkoła Sztuk Walki z Cyberprzestępcami - NajslabszeOgniwo.pl

RELACJE BIZNESOWE ZA POŚREDNICTWEM SOCIAL MEDIA. JAK JE WERYFIKOWAĆ?

Anna Petynia-Kawa
Agencja Kreatywna AjPi Media



Poszukiwania partnerów biznesowych przeniosły się do Internetu. Pandemia zmusiła sceptyków pracy zdalnej i takiej formy nawiązywania relacji do działania online. Budowanie relacji biznesowych w sieci stało się standardem. Mimo że social selling przeżywa swój rozkwit, wiele osób nie wie, jak bezpiecznie i skutecznie nawiązywać w ten sposób relacje biznesowe, na przykład przy pomocy Facebooka.

SOCIAL SELLING

Social selling polega na budowaniu relacji oraz zaufania w mediach społecznościowych. By działanie było skuteczne bardzo istotne jest doskonałe poznanie oraz świadomość, na jakiej grupie docelowej klientów/partnerów biznesowych nam zależy. Jej znajomość pozwoli nam odpowiednio spersonalizować przekaz oraz poszukać odpowiednich kanałów dotarcia do jej przedstawicieli.

Facebook mimo upływu lat wciąż jest doskonałym miejscem dotarcia do konkretnych osób. Co istotne, daje możliwość nawiązania relacji biznesowych z partnerami dosłownie z całego świata.

W tym kontekście niezwykle istotnym aspek-tem jest odpowiednie zbudowanie swojego wizerunku, tak by był po pierwsze autentyczny, a po drugie wzbudzał zaufanie. Nie od dzisiaj bowiem wiadomo, że Internet sprzyja osobom, które są oszustami i nie mają czystych intencji. Dlatego istotnym aspektem jest dbanie o codzienne bezpieczeństwo budowania relacji biznesowych online.

JAK ZBUDOWAĆ SWOJE KONTO NA FACEBOOKU, ABY BUDZIŁO ZAUFANIE?

Przede wszystkim zacznij od profesjonalnego zdjęcia profilowego. Avatar wiele powie na temat posiadacza konta w mediach społecznościowych. Jeśli chcesz, by Facebook był dla Ciebie źródłem kontaktów biznesowych zrób sobie profesjonalną sesję zdjęciową. W ten sposób zyskasz zaufanie już na samym początku budowania relacji.

Weryfikując potencjalnych kontrahentów zwróć uwagę na to, czy mają zdjęcie profilowe, dodaną historię zatrudnienia. Jeśli sprawdzasz stronę firmową na Facebooku, istotne jest jej odpowiednie przygotowanie. Pamiętaj o publikowaniu materiałów graficznych, które będą zawierały logo oraz rzetelne informacje na temat produktów/usług, które świadczysz. To nie tylko buduje wizerunek, ale i zaufanie do marki.

DBANIE O CODZIENNE BEZPIECZEŃSTWO BUDOWNIA RELACJI BIZNESOWYCH TO PODSTAWA.

ZADBAJ O BEZPIECZEŃSTWO TWOJEGO KONTA NA FACEBOOKU

Ważnym elementem codziennego korzystania z mediów społecznościowych jest odpowiednie zabezpieczenie własnego konta. **Dwuetapowe logowanie** (tzw. uwierzytelnianie dwuskładnikowe) to prosty i skuteczny sposób na uniknięcie wykradnięcia konta. Dzięki temu unikniemy przykrych konsekwencji kradzieży konta lub włamania.

To szczególnie istotne, jeśli za pośrednictwem naszego profilu realizujemy **płatne kampanie reklamowe Facebook Ads.** Wiąże się z tym bowiem podpięcie karty kredytowej lub przelew pieniędzy na konto prepaid. Włamywacze często wykorzystują również naszą bazę znajomych oraz zbudowane przez nas zaufanie np. do wyłudzania pieniędzy przez Blika.
Uruchomienie dwuetapowego logowania wymaga od nas wejścia w **„Ustawienia i prywatność”**, następnie wybrania „Bezpieczeństwo i logowanie”, tutaj wybieramy uwierzytelnianie za pomocą telefonu komórkowego. Następnie dodajemy nasz numer telefonu i zapisujemy dane. Od tego czasu w momencie logowania do platformy będziemy otrzymywać SMS lub powiadomienie z prośbą o potwierdzenie działania. Dzięki temu każde logowanie z nieznanego sprzętu będzie poprzedzone potwierdzeniem go w aplikacji lub poprzez wprowadzenia kodu, który otrzymasz drogą SMS-ową.

W tym samym miejscu możesz również kontrolować logowania do portalu. Dzięki temu w razie podejrzanej aktywności naszego profilu (np. znalezieniu logowania z innego miasta czy kraju) możemy szybko i skutecznie zareagować. Wystarczy wybrać opcję **wylogowania się**

ze wszystkich urządzeń i zmienić hasło. Warto pamiętać o tworzeniu haseł które będą silne, składać się z liter, cyfr i znaków specjalnych. Zabezpieczenie powinno mieć minimum 6 znaków.

SKUTECZNE BUDOWANIE RELACJI NA FACEBOOKU

Wciąż pokutuje błędne przekonanie, że relacje na Facebooku (podobnie na LinkedIN) buduje się poprzez wysyłanie wiadomości prywatnych przy pomocy Messengera. Nic bardziej mylnego. Obecnie skuteczny social selling to nie tylko zawieranie sieciowych znajomości, gdzie kładziemy nacisk na to, by zakończyła się ona sprzedażą usługi. To stałe budowanie wizerunku oraz komunikacja z odbiorcami, ciągle budowany personal branding.

Wiele osób błędnie kojarzy social selling z cold mailingiem i spamowaniem w wiadomościach prywatnych na Facebooku. Już w pierwszej wiadomości usiłuje w nachalny sposób sprzedawać usługi/produkty. W ten sposób można bardzo skutecznie zniechęcić do siebie potencjalnego kontrahenta.

Warto budować relacje, pokazywać wartość i pomagać w wypadku problemów.

JAK WERYFIKOWAĆ OSOBY, Z KTÓRYMI NAWIĄZUJESZ RELACJE?

Najprostszym sposobem jest po prostu wejście na profil osoby, z którą chcesz nawiązać relację biznesową. Popatrz na niego krytycznym okiem i koniecznie sprawdź, **jakie informacje są na niej publikowane.** Zwróć uwagę na zdjęcie profilowe, imię i nazwisko osoby, autentyczność publikowanych treści. Sprawdź, czy ma listę znajomych, ile jest na niej osób.

W dobie fake newsów alarmowa lampka powinna zapalić się w momencie, kiedy **czytasz wpisy w których są dziwne sformułowania i mało spotykane błędy językowe.** Często w treś-ci wplecione są również tematy o silnym nacechowaniu emocjonalnym, podejmujące tematy polityczne. To sposób manipulacji faktami. Takie informacje są chętnie udostępniane i czasami stają się viralem. Często wprowadzane są do Internetu przez osoby celowo siejące dezinformację.

Jeśli jest to przedsiębiorca prowadzący firmę, warto zweryfikować jej dane w ogólnodostępnej bazie CEIDG (jednoosobowe działalności gospodarcze) lub KRS (różnego rodzaju spółki). Bardzo ważne jest również zweryfikowanie opinii na temat jego biznesu (można to zrobić na Facebooku lub Google).

Media społecznościowe to miejsce, w którym można nawiązywać satysfakcjonujące relacje biznesowe. Wystarczy trzymać się kilku prostych zasad, pamiętać o bezpieczeństwie i zasadzie ograniczonego zaufania - nim zaprosisz do współpracy potencjalnego partnera, klienta bądź pracownika, zweryfikuj jego tożsamość. Nie zapominaj przy tym, że on najpewniej zrobi to samo w stosunku do Ciebie i Twojej firmy.

ajPi MEDIA

+ 48 731 638 957
biuro@ajpimedia.pl
www.ajpimedia.pl

W ofercie AjPi Media znajdziesz:

- strony/sklepy internetowe
- reklama Google Ads i Facebook Ads
- media społecznościowe
- copywiting
- projekty graficzne
- doradztwo reklamowe
- szkolenia z zakresu reklamy i marketingu

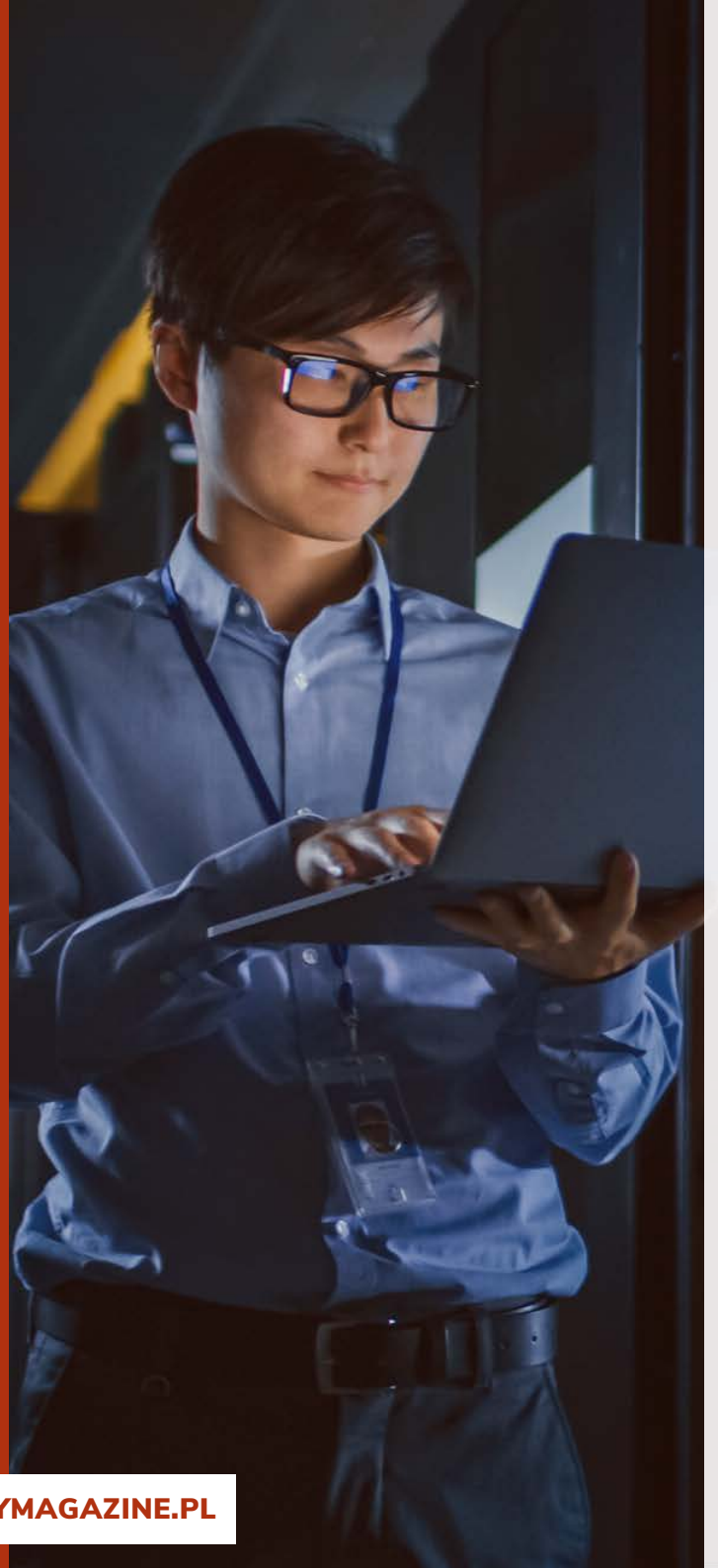
SECURITYMAGAZINE.PL

NAWET NIEWIELKI BUDŻET NA CYBERBEZPIE-CZEŃSTWO WYELIMINUJE POWAŻNE ZAGROŻENIA

Jakub Staśkiewicz
OpenSecurity.pl

Czy zapewnienie bezpieczeństwa firmowej infrastrukturze wymaga dużych nakładów finansowych? Odpowiadając krótko, tak. Jednak zagłębiając się w temat można powiedzieć „to zależy”. Możliwe jest bowiem takie wydatkowanie środków, by przy minimalnych nakładach wyeliminować najpoważniejsze zagrożenia.

Nawet niewielki budżet na cyberbezpieczeństwo wyeliminuje poważne zagrożenia



Bezpieczeństwo kosztuje, ale musimy też zdawać sobie sprawę z faktu, iż niezależnie od wielkości budżetu przeznaczonego na jego zapewnienie nigdy nie osiągniemy celu w postaci 100% bezpieczeństwa.

Bezpieczeństwo, nie tylko to cybernetyczne, polega bowiem na minimalizowaniu ryzyka. Cała sztuka polega więc na tym, aby ograniczony budżet przeznaczyć do wyeliminowania tych ryzyk, które najprędzej mogą się zmaterializować i jednocześnie wyrządzić nam największe szkody.

Powoli rośnie świadomość niebezpieczeństw związanych ze stosowaniem nowoczesnych technologii i systemów. Świadomość ta wciąż jest jednak na tyle mała, że poziom bezpieczeństwa przeciętnej polskiej firmy pozostawia wiele do życzenia. Dopóki nie dotrze do wszystkich, że firewall i antywirus to za mało, by zadbać o bezpieczeństwo infrastruktury i procesów biznesowych, dopóty będzie dochodziło do incydentów, w których nastolatek z niewielką wiedzą techniczną jest w stanie narazić firmę na niebagatelne straty finansowe lub wizerunkowe.

SYSTEMY BEZPIECZEŃSTWA TO ZA MAŁO

Z drugiej jednak strony błędem jest myślenie, że kupno odpowiedniej ilości drogich i zaawansowanych systemów rozwiąże problemy z bezpieczeństwem. Zaawansowane systemy wymagają bowiem obsługi przez specjalistów, na których zatrudnienie często brakuje już środków.

Wydawać się może, że informatyk, którego mamy na etacie będzie w stanie obsłużyć zakupione rozwiązania. Niestety systemy te wymagają nie tylko zaawansowanej wiedzy specjalistycznej, ale dużej ilości czasu, który trzeba poświęcić na analizę gromadzonych w nich danych i obsługę generowanych przez nie alertów. W efekcie więc bardzo często dochodzi do poważnych incydentów bezpieczeństwa w firmach, które wydały niemałe pieniądze na zaawansowane technologie, ale nikt nie miał wiedzy i czasu by odpowiednio je wdrożyć i obsłużyć.

Ponadto istotnym jest zdanie sobie sprawy z faktu, iż nie wszystkie zagrożenia mają charakter techniczny i związane są z brakiem odpowiednich zabezpieczeń w postaci systemów obronnych. Bezpieczeństwo, to tak naprawdę nie kwestia budżetu, a świadomości zagrożeń, z którymi musimy się zmierzyć.

CYBERPRZESTĘPCA TO NIE GENIUSZ, A „BIZNESMEN”

Dzisiejsi cyberprzestępcy to nie romantyczni geniusze, a dobrze zorganizowani oszuści, których celem jest odniesienie jak największych korzyści jak najmniejszym nakładem czasu i środków. Zależy im zwyczajnie na maksymalizacji swoich zysków.

Łamanie zabezpieczeń technicznych, które wymaga wiedzy i czasu nie jest dla nich, wbrew pozorom, najprostszą drogą do zarobku. Stały się nią tzw. socjotechniki, czyli sposoby manipulacji i wprowadzania w błąd pracowników firmy w celu osiągnięcia określonego celu (np. wyłudzenia hasła lub poufnych danych). Przestępcy zawsze będą bowiem sięgali po tzw. „low hanging fruits”. Dlatego też zabezpieczenia techniczne mogą się okazać niewystarczające, a działania, które musimy podjąć w celu obrony wykraczają poza technologię i wymagają m.in. szkolenia pracowników korzystających z komputerów i Internetu.

SOCJOTECHNIKI JAKO ZAGROŻENIE

W socjotechnikach najistotniejszy jest szybki zysk i minimalne wykorzystanie środków potrzebnych do jego wygenerowania.

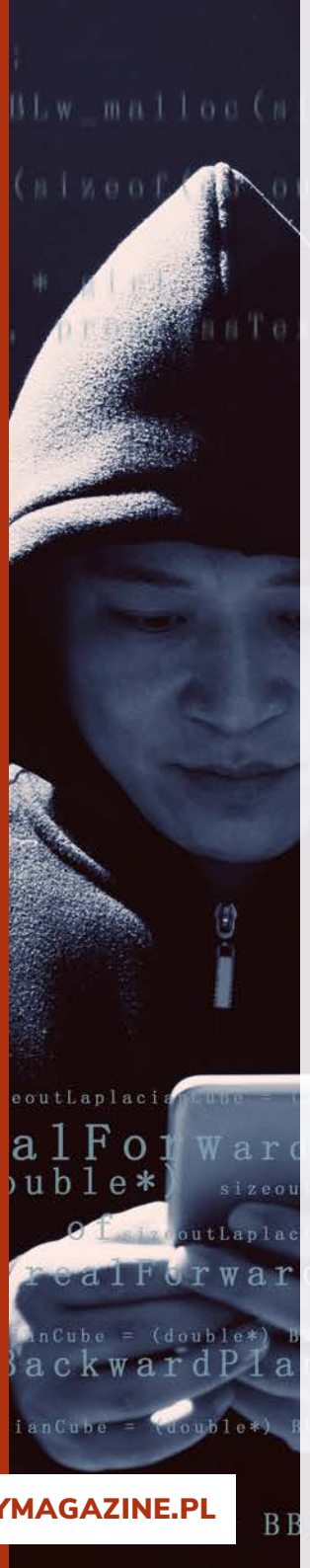
Nawet niewielki budżet na cyberbezpieczeństwo wyeliminuje poważne zagrożenia

Dlatego też e-mail i telefon zastępuje często przestępcom zaawansowane techniki ataków na infrastrukturę. Przestępca nie będzie sobie zawracał głowy poszukiwaniem podatności i łamaniem zabezpieczeń do systemu, skoro może w kilkanaście minut zdobyć hasło do niego. Albo jeszcze prościej, poprosić jego użytkownika o wykonanie określonego działania w systemie podając się telefonicznie np. za pracownika obsługi technicznej.

To właśnie szeregowi pracownicy firm określani są mianem „najsłabszego ogniwa" w łańcuchu zabezpieczeń. Niezależnie bowiem od ilości wdrożonych zabezpieczeń technicznych da się ich łatwo oszukać. I to właśnie w to najsłabsze ogniwo wycelowane są najczęściej działania zorganizowanych grup przestępczych. Warto więc o tym pamiętać decydując na jakie zabezpieczenia chcemy spożytkować nasz budżet.

Według opublikowanego właśnie raportu CERT.PL dotyczącego incydentów bezpieczeństwa odnotowanych w 2021 roku, 86,4% z nich stanowiły oszustwa komputerowe, z czego 76,57% próby phishingowe.

Nawet niewielki budżet na cyberbezpieczeństwo wyeliminuje poważne zagrożenia



VIII. Oszustwa komputerowe	25 472	86,40%
Nieuprawnione wykorzystanie zasobów	3	0,01%
Naruszenie praw autorskich	1	0,00%
Kradzież tożsamości, podszycie się	12	0,04%
Phishing	22 575	76,57%
Niesklasyfikowane	2 881	9,77%

Udział socjotechnik w zagrożeniach (źródło: raport CERT.PL za 2021 r.)

SZKOLENIA ZAMIAST TESTÓW SOCJOTECHNICZNYCH

Przyjęło się, że dobrym sposobem na sprawdzenie efektywności firmowych procedur bezpieczeństwa jest przeprowadzenie kontrolowanych testów socjotechnicznych. Jeśli jednak nigdy nie szkoliliśmy naszych pracowników i nie wdrożyliśmy odpowiednich procedur bezpieczeństwa testy takie będą jedynie marnowaniem budżetu na potwierdzenie czegoś, co można założyć w ciemno – znaczna część pracowników nie jest przygotowana na odparcie ataku socjotechnicznego.

Zamiast więc marnować czas i budżet do dowodzenie powyższego, lepiej jest przeznaczyć te środki od razu na odpowiednie szkolenia dla pracowników. Przeszkolenie jednej osoby z rozpoznawania ataków socjotechnicznych i odpowiedniego reagowania na nie to koszt rzędu od kilkudziesięciu do stu złotych. Przeznaczając zatem niewielkie środki na wzmocnienie „najsłabszego ogniwa" eliminujemy największe ryzyko i utrudniamy działanie przestępcom. Oszuści w większości przypadków pójdą po prostu tam, gdzie będzie im łatwiej działać.

WARSTWA TECHNICZNA

Gdy już zadbamy o odpowiednie przeszkolenie pracowników warto skupić się na

warstwie technicznej. Wspomniałem wcześniej o tym, że przestępcy zamiast bawić się w łamanie zabezpieczeń wolą skupić się na „najsłabszym ogniwie". Jednak tam, gdzie nie wymaga to zbędnego wysiłku chętnie skorzystają również z luk o charakterze technicznym. A tutaj znowu wybiorą te, które najłatwiej jest namierzyć i wy-korzystać. By oszczędzić sobie pracy robią to często z użyciem zautomatyzowanych botnetów, które potrafią znaleźć w Internecie dziurawy system i przejąć nad nim kontrolę.

Jak się przed takim zagrożeniem bronić? Zamiast nabywać nowe systemy bezpieczeństwa w pierwszej kolejności warto zadbać o pozbycie się tych, których posiadanie to proszenie się o kłopoty. Mowa tu o systemach, dla których producent nie prowadzi już wsparcia w postaci aktualizacji i łatek bezpieczeństwa. Według statystyk systemy takie jak np. Windows 7 są wciąż popularne wśród użytkowników, a posiadają wiele luk, które da się w prosty sposób wykorzystać do przełamania zabezpieczeń.

Popularność systemów Windows (źródło: statcounter.com)

To samo dotyczy wybranych usług w nowszych systemach, które jednak nie są aktualizowane. Nawet najnowsze oprogramowanie bez aktualizacji stanowi poważne zagrożenie. Tylko w ciągu ostatnich miesięcy w systemach z rodziny Windows znaleziono krytyczne luki w tak popularnych usługach, jak np. serwer wydruku czy zdalny pulpit. Każda z tych luk umożliwia zdalne przejęcie kontroli nad serwerem.

Wycofywanie przestarzałych systemów oraz aktualizacja stosowanego w firmie oprogramowania powinny zatem stanowić jeden z podstawowych procesów służących eliminacji zagrożeń. I wyjątkiem nie są tutaj niestety systemy bezpieczeństwa. Nawet najbardziej zaawansowane z nich zawierają często luki mogące to bezpieczeństwo naruszyć. Je również, i to w pierwszej kolejności, należy zatem aktualizować. W innym wypadku wydatki poniesione na zabezpieczenia okażą się bezcelowe.

NIEPOTRZEBNE USŁUGI

W punkcie poprzednim wspomnieliśmy o przestarzałych systemach, które w łatwy sposób mogą być przejęte przez intruzów. Często okazuje się, że systemy te dostępne są z poziomu Internetu bez konkretnej potrzeby biznesowej. Informatycy lub zewnętrzni dostawy uruchamiają w naszym środowisku usługi, które mają im ułatwić pracę zdalną, ale nie są niezbędne do działania firmy. Przykładem mogą być np. dostępne z poziomu Internetu kamery umożliwiające monitorowanie obiektów firmowych czy interfejsy administracyjne urządzeń takich jak firewalle.

Wyłączenie dostępu do nich, lub „schowanie" ich za firewallem z dostępem przez VPN to najprostszy sposób na zniknięcie z pola widzenia intruzów. Jest to kolejny przykład działania znacznie podnoszącego poziom bezpieczeństwa, a nie wymagającego wielkich nakładów finansowych.

PODSUMOWANIE

Warto podkreślić raz jeszcze, że istotniejsze od wielkości budżetu jest jego odpowiednie spożytkowanie. Posiadając nawet niewielkie środki na bezpieczeństwo jesteśmy w stanie wyeliminować najpoważniejsze zagrożenia minimalizując ryzyko stania się łatwym celem dla intruzów.

Szkolenia pracowników, aktualizacje systemów, brak zbędnych usług wystawianych do Internetu to dużo więcej niż może nam zapewnić niejeden cudowny w mniemaniu producenta i bardzo kosztowny system bezpieczeństwa.

CYFRYZACJA OCHRONY ZDROWIA TO WYZWANIE

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

Cyfryzacja usług zdrowotnych stwarza szanse na znaczącą poprawę ich jakości i dostępności. Jednak determinuje także szereg zagrożeń, zwłaszcza związanych z bezpieczeństwem przetwarzania wrażliwych danych o pacjentach. Jak im przeciwdziałać?

Od początku wybuchu pandemii nowego koronawirusa cyfryzacja usług medycznych przechodzi wręcz prawdziwą rewolucję. Wystarczy wspomnieć, że telewizyta stała się wręcz standardowym rozwiązaniem. I choć Ministerstwo Zdrowia oraz Narodowy Fundusz Zdrowia dbają o to, aby telewizyty nie były nadużywane, to obecnie właściwie nie sposób wyobrazić sobie bez nich funkcjonowania publicznego systemu ochrony zdrowia. Jednocześnie plany na przyszłość – w zakresie dalszej cyfryzacji usług zdrowotnych – są bardzo ambitne. Trudno mieć przy tym wątpliwości, że wykorzystywanie nowoczesnych technologii w procesie leczenia i opieki nad pacjentem to wręcz konieczność – wystarczy spojrzeć na pozytywne rezultaty stosowania takich rozwiązań w systemie prywatnym – jednak wiążę się z nią szereg zagrożeń. Zwłaszcza w obszarze cyberbezpieczeństwa. Jak ich unikać?

NIE TYLKO LECZENIE PRZEZ TELEFON

O skali wyzwań „cyfryzacyjnych" stojących przez publiczną ochroną zdrowia najlepiej świadczą plany zawarte w – przygotowanym przez Ministra Zdrowia – krajowym planie transformacji na lata 2022-2026. Szeroko pojęta cyfryzacja usług medycznych jest jednym z jego centralnych założeń.

Resort zdrowia planuje m.in. wdrożenie trzech centralnych usług cyfrowych, obejmujących narzędzie wspomagające analizę stanu zdrowia pacjenta, rozwój algorytmów sztucznej inteligencji oraz budowę centralnego repozytorium danych medycznych; cyfryzację dokumentacji medycznej i dalszy rozwój usług jej wymiany oraz wzmocnienie cyberbezpieczeństwa w ochronie zdrowia. W ślad za tym ma pójść zwiększenie cyfrowych kompetencji personelu medycznego – co z kolei stanowi kluczowe zagadnienie w perspektywie prawidłowego wykorzystania narzędzi z zakresu szeroko pojętej telemedycyny oraz bezpieczeństwa tego rodzaju usług.

W styczniu 2020 roku, kiedy obowiązkowym stało się wystawianie e-recept wydawało się, że jest to wręcz przełomowy krok w zakresie cyfryzacji usług medycznych. Rok później wprowadzono obligatoryjne wystawianie e-skierowań, co w zestawieniu z możliwością dostępu do kluczowych informacji o stanie swojego zdrowia z poziomu Internetowego Konta Pacjenta zdecydowanie podniosło poziom wykorzystanie usług cyfrowych w sektorze zdrowotnym. Jednak to, co jeszcze kilkanaście miesięcy temu wydawało się rewolucją, z perspektywy planów na przyszłość wydaje się dopiero pierwszym krokiem.

Oczywiście nadal leczenie i opieka nad pacjentem musi opierać się na bezpośrednim kontakcie z medykiem. Właściwie truizmem jest przypomnienie, że zdecydowana większość usług świadczonych w ochronie zdrowia nie może być wykonana online. Jednak tam, gdzie to możliwe rozwiązania IT powinny być standardem – z korzyścią dla pacjenta, który dzięki nim może uzyskać świadczenie bez wychodzenia z domu oraz dla coraz bardziej obciążonych pracą placówek medycznych.

W istocie zastosowanie w podmiocie leczniczym czy opiekuńczym dobrze skonstruowanego i funkcjonalnego systemu informatycznego zdecydowanie ułatwia zarządzanie nią i wypełnienie obowiązków nałożonych przez ustawodawcę na personel medyczny. Aczkolwiek cyfryzacja ochrony zdrowia to spore wyzwanie, a błędy w tym obszarze mogą słono kosztować.

BEZPIECZEŃSTWO PRZEDE WSZYSTKIM

Cyfryzacja – ochrona zdrowia nie jest tu wyjątkiem – musi opierać się na budowie odpowiednich systemów informatycznych. Na to zaś potrzeba sporej ilości czasu i dużych środków. Biorąc pod uwagę polskie doświadczenia z cyfryzacją usług publicznych, to właśnie na etapie opracowywania stosownego oprogramowania zawsze pojawiało się najwięcej trudności. Jego jakość w ochronie zdrowia jest szczególnie istotna, zwłaszcza ze względu na charakter danych wykorzystywanych w tego rodzaju systemach. W końcu dostęp do nich zawsze oznacza zdobycie informacji o intymnych problemach pacjenta.

Zarówno z punktu widzenia ochrony praw pacjenta, jak i zasad przetwarzania danych osobowych informacje dotyczące stanu zdrowia są traktowane, jako dane wrażliwe, podlegające szczególnej ochronie. Nie trudno wyobrazić sobie, jak poważne szkody może wyrządzić uzyskanie do nich dostępu przez osoby nieuprawnione.

Dlatego niezbędna jest stałe podnoszenie świadomości zagrożeń związanych z cyberbezpieczeństwem wśród wszystkich pracowników ochrony zdrowia. Jest to podstawowy element budowania kultury organizacyjnej nastawionej na bezpieczeństwo danych pacjentów. Naruszenia tego bezpieczeństwa mogą doprowadzić nie tylko do niepowetowanych strat u korzystających z opieki zdrowotnej, ale również do daleko idącej odpowiedzialności odpowiedzialnych za wyciek danych wrażliwych, a także do

zahamowania procesu cyfryzacji opieki zdrowotnej. W końcu raz nadszarpnięte zaufanie bardzo trudno odzyskać.

JAK UNIKAĆ ZAGROŻEŃ?

Zbudowanie odpowiednich systemów informatycznych oraz uświadomienie pracownikom podmiotów leczniczych problemów z zakresu cyberbezpieczeństwa to podstawowe środki służące prawidłowej cyfryzacji usług medycznych. Bezwzględnie trzeba je wykonać na każdym poziomie cyfryzacji – a więc zarówno na etapie wdrażania rozwiązań ogólnopolskich, jak i systemów wykorzystywanych w pracy poszczególnych placówek medycznych. Warto podkreślić, że dane nie tylko z Polski wskazują, że podmioty lecznicze są szczególnie narażone na ataki.

Dlatego warto skorzystać ze stosunkowo prostych, ale sprawdzonych sposobów na zabezpieczenie informacji o pacjentach.

- Instalacja zaawansowanego programu antywirusowego,
- wprowadzenie bardziej rozbudowanych rozwiązań w zakresie uwierzytelniania użytkowników,
- tworzenie kopii zapasowych,
- segmentacja sieci
- szybkie odłączanie od niej zainfekowanego urządzenia

– to tylko podstawowe przykłady działań, które należy podjąć, aby uchronić dane pacjentów przed nieuprawnionym wykorzystaniem. Warto wprowadzić w tym względzie stosowne procedury, które w jednoznaczny sposób pozwolą każdemu pracownikowi zapoznać się z zasadami ochrony danych.

CO ZROBIĆ, GDY DOSZŁO DO NARUSZENIA?

Cyfrowe przetwarzanie danych osobowych musi być w pełni zgodne z przepisami prawa regulującymi przetwarzanie danych osobowych w ogóle – w tym przede wszystkim z unijnym rozporządzeniem, określanym w skrócie RODO. Dane pacjenta mogą być przetwarzane – co do zasady, od której wyjątkiem jest chociażby stan zagrożenia życia – jedynie na podstawie jego zgody, ale należy pamiętać, że oznacza konieczności zniszczenia dokumentacji medycznej – taki krok byłby niezgodny z prawem. Co nie zmienia faktu, że pacjentowi zawsze należy umożliwić realizację prawa dostępu do jego danych, a tak-że żądania ich sprostowania czy aktualizacji.

W przypadku, gdyby doszło do wycieku danych osobowych koniecznie należy o tym powiadomić wszystkich, których dane dotyczą oraz Prezesa Urzędu Ochrony Danych Osobowych. Warto pamiętać, że zgodnie z art. 34 RODO obowiązki te powstają wówczas, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

To z kolei oznacza, iż wskazane tu obowiązki nie powstają automatycznie, ale są uzależnione od okoliczności konkretnego przypadku. Jednak trzeba przyjąć, że bezprawne ujawnienie danych dotyczących stanu zdrowia zawsze stanowi tego rodzaju naruszenie. A więc ich administrator ma obowiązek niezwłocznego powiadomienia o wycieku ich posiadaczy oraz Prezesa UODO.

Tym bardziej więc należy dołożyć wszelkich starań, aby cyfryzacja opieki zdrowotnej przebiegała zgodnie z najwyższymi – prawnymi i technologicznymi – standardami. Tylko w ten sposób stanie się przyczyną zdecydowanej poprawy jakości i dostępności świadczeń medycznych, a nie zagrożeniem dla bezpieczeństwa pacjentów.

MUST HAVE

dla tych, których firma pozyskuje klientów w Internecie

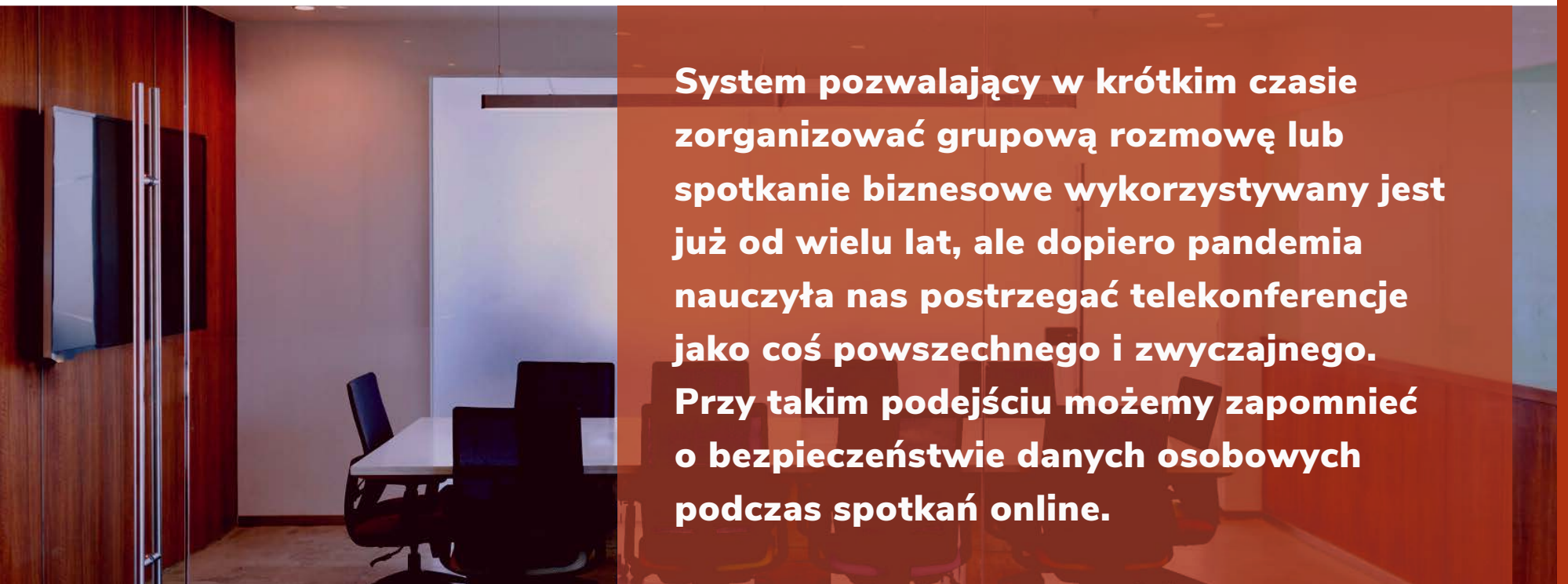
Dla czytelników "Security Magazine"

15% zniżki

W zamówieniu wpisz kod: PIOTR15

TELEKONFERENCJA A BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Redakcja
SECURITY MAGAZINE



System pozwalający w krótkim czasie zorganizować grupową rozmowę lub spotkanie biznesowe wykorzystywany jest już od wielu lat, ale dopiero pandemia nauczyła nas postrzegać telekonferencje jako coś powszechnego i zwyczajnego. Przy takim podejściu możemy zapomnieć o bezpieczeństwie danych osobowych podczas spotkań online.

Telekonferencję możemy przeprowadzić za pomocą telefonu komórkowego, stacjonarnego lub rozwiązania w oparciu o technologię VOIP, umożliwiającą przesyłanie głosu za pomocą internetu. Okazała się kluczowym rozwiązaniem dla zdecydowanej większości przedsiębiorców i pracowników, którzy musieli zmierzyć się z ograniczeniami nałożonymi po wybuchu pandemii. Stała się elementem pracy zdalnej, do której również z dnia na dzień zmuszeni byliśmy przywyknąć. Już wtedy Urząd Ochrony Danych Osobowych wydał komunikat, aby podczas pracy poza biurem postępować zgodnie z przyjętą w organizacji procedurą bezpieczeństwa.

Absolutnymi podstawami było m.in.

- nie instalowanie dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji
- sprawdzanie urządzeń, czy mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego
- wydzielenie sobie odpowiedniej przestrzeni, aby ewentualne osoby postronne, nie miały dostępu do dokumentów służbowych
- blokowanie urządzenia za każdym razem, kiedy była potrzeba odejścia od niego
- zabezpieczanie komputera za pomocą silnych haseł dostępu i wielopoziomowego uwierzytelniania
- w przypadku zgubienia urządzenia służbowego, zdalnie wyczyszczenie jego pamięci, o ile jest to możliwe.

Ponadto **Urząd Ochrony Danych Osobowych** rekomendował, aby zapoznać się z warunkami użytkowania programu, z którego się korzysta, ograniczać podawanie swoich danych osobowych, a po zakończeniu - zamknąć oprogramowanie. Ważne, by zachować ostrożność na trzech etapach uczestnictwa w telekonferencji.

BEZPIECZEŃSTWO PRZED TELEKONFERENCJĄ

Przed rozpoczęciem wideokonferencji należy:

- zapoznać się z ogólnymi warunkami użytkowania oraz polityką prywatności programu, z którego się korzysta,
- dowiedzieć się, czy rozmowy będą nagrywane i przechowywane, a jeśli tak to jak długo,
- sprawdzić, do jakich celów będą wykorzystywane dane osobowe uczestników wideokonferencji,
- upewnić się, o jakie uprawnienia proszone są osoby biorące udział w wideokonferencji, w tym lista kontaktów, lokalizacja i podobne.

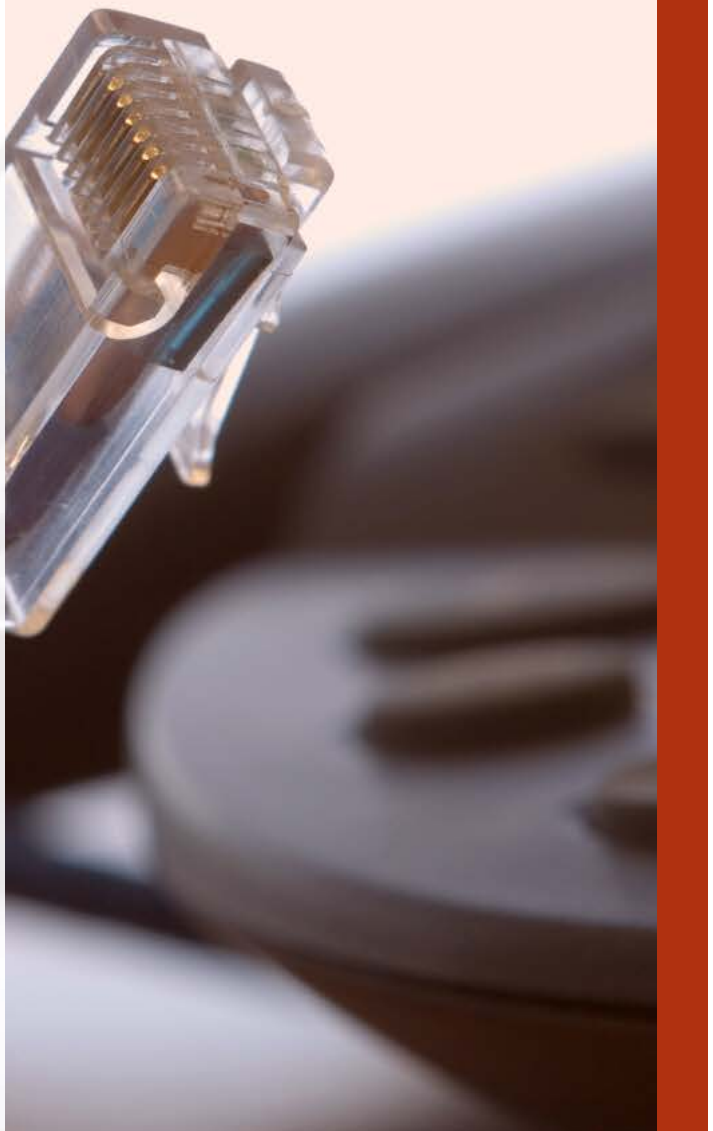
Na tym nie koniec, bo niezwykle istotne są również takie aspekty, jak zainstalowanie aplikacji na komputerze wyłącznie z oficjalnej strony aplikacji, a w przypadku np. smartfonów lub tabletów należy wybrać oficjalny sklep - Google Play lub App Store.

Dalsze czynności pierwszego etapu to:

- zwrócić uwagę na to, czy osoby postronne nie mają dostępu do ekranów użytkowników biorących udział w wideokonferencji,
- upewnić się, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie,
- używać wyłącznie aplikacji webowych, nie - desktopowych,
- zabezpieczyć sieć Wi-Fi silnym hasłem.

Ponadto przed udostępnieniem ekranu podczas telekonferencji trzeba zamknąć wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli, a przy podłączeniu się do telekonferencji należy korzystać z kodów dostępu/PIN-ów. Dlaej,

przeskanować program do telekonferencji systemem antywirusowym lub antymalware'owym.



BEZPIECZEŃSTWO W TRAKCIE TELEKONFERENCJI

Drugi etap korzystania z telekonferencji dotyczy już jej trwania. UODO zalecało, by w jej trakcie:

- ograniczyć ilość podawania danych osobowych przez np. posługiwać się pseudonimem i służbowym adresem e-mail,
- używać innego hasła niż to, z którego korzystają użytkownicy w innych usługach,
- nie udostępniać linków do konferencji w mediach społecznościowych, co jest jednak powszechną praktyką,
- jeśli jest taka możliwość, włączyć domyślną ochronę hasłem telekonferencji
- zarządzać opcjami udostępniania ekranu.

Ponadto istotne okazało się istotnym, by wykorzystywać dostęp do sieci za pomocą szyfrowanego połączenia VPN. Nie udostępniać dokumentów służbowych, za pomocą czatu, który może być publiczny. UODO zalecało też, jeżeli to możliwe, korzystanie z opcji zamazywania tła, by rozmówcy nie widzieli naszego otoczenia.

Ważną opcją jest "poczekalnia", która pozwala kontrolować osoby uczestniczące w telekonferencji i uniknąć przypadkowych lub niechcianych osób.

Podczas logowania się do telekonferencji, należy wyłączyć mikrofon i kamerę (włączyć je tylko, gdy będzie to potrzebne).

BEZPIECZEŃSTWO PO TELEKONFERENCJI

Ostatnim etapem bezpiecznych telekonferencji jest właściwe zachowanie po ich zakończeniu. Wówczas należy: wyłączyć mikrofon i kamerę, dalej - upewnić się, że spotkanie on-line się zakończyło i zamknąć aplikację. Warto też sprawdzić, czy program do telekonferencji nie działa w tle.

TELEKONFERENCJA W RĘKACH HAKERA. PRZYKŁAD CCC

O tym, jak może skończyć się niedostateczne zadbanie o bezpieczeństwo zdalnych spotkań przekonała się firma CCC. Zorganizowała 250-osobową wideokonferencję.

Udział w niej wzięli analitycy giełdowi, dziennikarze, zarządzający funduszami inwestycyjnymi, menedżerowie firmy i sam założyciel CCC. Gdy przyszedł czas na pytania, na ekranach komputerów wszystkich uczestników pojawił się film pornograficzny i rysunki z męskimi genitaliami oraz ze swastykami. Nim organizatorzy zdecydowali się na zakończenie wideokonferencji, film odtworzono dwa razy. Po zdarzeniu producent i dystrybutor obuwia tłumaczył, że link do konferencji został pośrednio udostępniony osobom niepowołanym, co nazywane jest zjawiskiem zoom bombingu. Jakie wnioski wyciągnęła firma? Użytkownikom narzędzia do telekonferencji (w tym przypadku chodzi o platformę Zoom) zostały narzucone domyślne zabezpieczenia narzędzi do pracy zdalnej. Każdy szkolony jest ze sposobu ich wykorzystania i zagrożeń.

O CZYM NALEŻY JESZCZE PAMIĘTAĆ?

Stabilne i szybkie połączenie internetowe. Przy organizacji pracy zdalnej wiele firm, ale i ich pracownicy stanęli przed koniecznością pokonania wielu barier technologicznych, w tym - obsługa łączności i przepustowość łącza internetowego. W odróżnieniu od połączeń biurowych, skonfigurowanych tak, aby działały szybko i niezawodnie, domowe połączenia internetowe mają różne parametry. A to wiąże się z ryzykiem korzystania z alternatywnych rozwiązań, takich jak niezabezpieczone hotspoty czy telefony. Pracodawca zatem powinien wyposażyć pracownika w właściwe narzędzia.

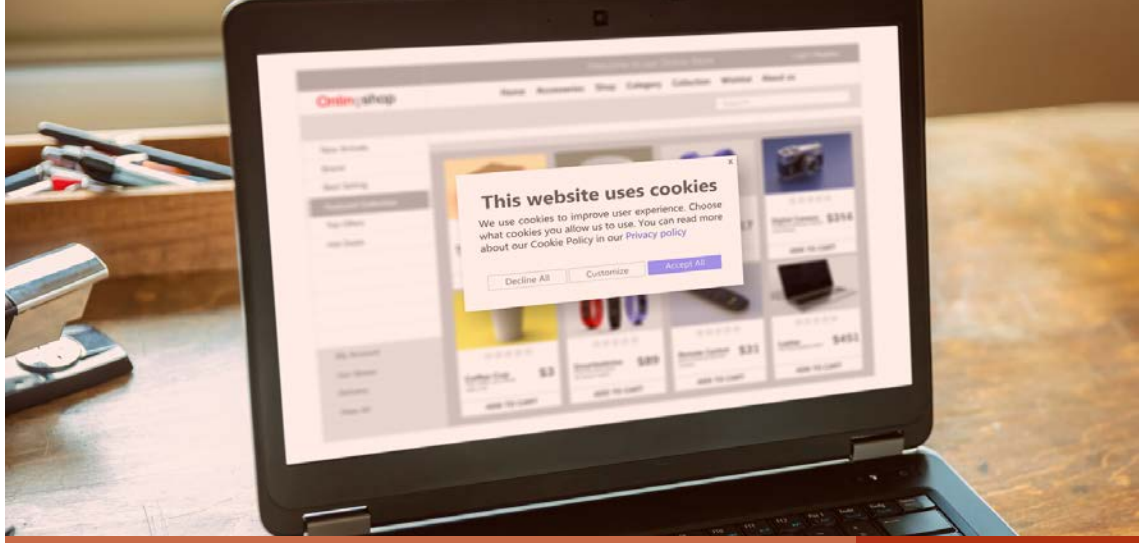
Wyciszanie uczestników. To funkcja przeznaczona dla organizatora telekonferencji. Zabezpiecza przed zakłóceniami dźwiękowymi i zakłóceniem toku spotkania – daje możliwość udzielania głosu tylko z poziomu gospodarza.

Rozłączanie. To bardzo ważna funkcja, która powinna być dostępna dla organizatora. Pozwala na rozłączenie niepożądanych uczestników lub zablokowanie dostępu do telekonferencji intruzom. Z pewnością zabrakło jej podczas telekonferencji marki CCC.

SECURITYMAGAZINE.PL

ZGODA NA COOKIES. JAK SKUTECZNIE WDROŻYĆ JĄ NA STRONIE?

Rafał Stępniewski
Rzetelna Grupa



Obecnie prawie każda strona WWW wykorzystuje pliki cookies. W większości przypadków cookies są konieczne do poprawnego działania samej strony WWW. Jeżeli firma stosuje dodatkowe narzędzia firm trzecich, wówczas dochodzić mogą kolejne cookies. Czy można do woli korzystać z mechanizmu cookies? Jakie przepisy prawa to regulują i jak w praktyce poprawnie spełnić wymagania?

JAKIE PRZEPISY OKREŚLAJĄ KONIECZNOŚĆ O INFORMOWANIU O COOKIES?

Zamieszczając na stronie internetowej belkę informacyjną o cookies spełniane są przede wszystkim wymogi prawa telekomunikacyjnego. Przepisy wprost odnoszą się do przechowywania danych informatycznych, a w szczególności plików tekstowych, w urządzeniach końcowych użytkownika.

Pliki cookies można instalować pod pewnymi warunki tj.:

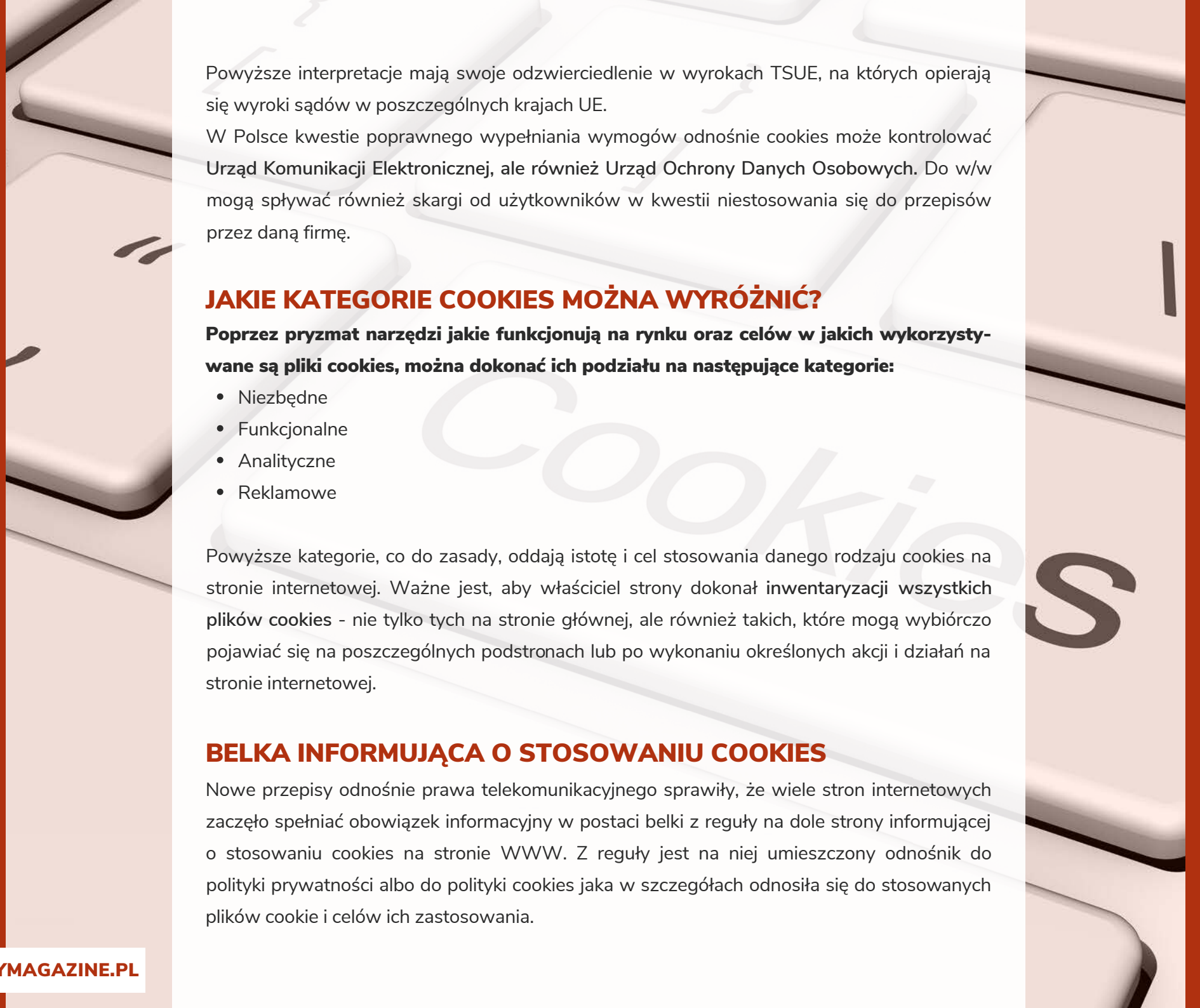
- użytkownik zostanie jednoznacznie poinformowany, w sposób łatwy i zrozumiały, o celu przechowywania danych oraz sposobach korzystania z ich zawartości;
- użytkownik zostanie poinformowany jednoznacznie, w sposób łatwy i zrozumiały, o sposobie wyrażenia sprzeciwu, który w przyszłości uniemożliwi przechowywanie danych usługodawcy w urządzeniu użytkownika;
- przechowywane dane nie powodują zmian konfiguracyjnych w urządzeniu końcowym użytkownika lub oprogramowaniu zainstalowanym w tym urządzeniu.

COOKIES A RODO?

Do wymogów prawa telekomunikacyjnego dochodzić mogą, w niektórych wypadkach, również wymagania prawne wynikające z RODO. Dotyczy to przede wszystkim sytuacji, gdzie cookies są wykorzystywane do profilowania, wyrażenie zgody na marketing, a także gdy cookies noszą znamiona przetwarzania danych osobowych.

Przykładem zastosowania RODO jest sytuacja, gdzie **użytkownik jest zalogowany w przeglądarce do swojego konta w Google i odwiedza określoną stronę, która dodatkowo korzysta z narzędzi remarketingowych od firmy Google**. Właściciel strony oczywiście bezpośrednio nie pozyskuje w ten sposób danych osobowych, ale wykorzystuje narzędzia firmy Google do prowadzenia, w stosunku do tej konkretnej osoby, działań marketingowych.

Drugim ważnym aspektem wynikającym z RODO jest kwestia domniemania zgody - której oczywiście nie może być. W praktyce oznacza to, że zgoda na wykorzystanie cookies w celach marketingowych nie może być odgórnie przyjęta.



Powyższe interpretacje mają swoje odzwierciedlenie w wyrokach TSUE, na których opierają się wyroki sądów w poszczególnych krajach UE.
W Polsce kwestie poprawnego wypełniania wymogów odnośnie cookies może kontrolować **Urząd Komunikacji Elektronicznej, ale również Urząd Ochrony Danych Osobowych.** Do w/w mogą spływać również skargi od użytkowników w kwestii niestosowania się do przepisów przez daną firmę.

JAKIE KATEGORIE COOKIES MOŻNA WYRÓŻNIĆ?

Poprzez pryzmat narzędzi jakie funkcjonują na rynku oraz celów w jakich wykorzystywane są pliki cookies, można dokonać ich podziału na następujące kategorie:

- Niezbędne
- Funkcjonalne
- Analityczne
- Reklamowe

Powyższe kategorie, co do zasady, oddają istotę i cel stosowania danego rodzaju cookies na stronie internetowej. Ważne jest, aby właściciel strony dokonał **inwentaryzacji wszystkich plików cookies** - nie tylko tych na stronie głównej, ale również takich, które mogą wybiórczo pojawiać się na poszczególnych podstronach lub po wykonaniu określonych akcji i działań na stronie internetowej.

BELKA INFORMUJĄCA O STOSOWANIU COOKIES

Nowe przepisy odnośnie prawa telekomunikacyjnego sprawiły, że wiele stron internetowych zaczęło spełniać obowiązek informacyjny w postaci belki z reguły na dole strony informującej o stosowaniu cookies na stronie WWW. Z reguły jest na niej umieszczony odnośnik do polityki prywatności albo do polityki cookies jaka w szczegółach odnosiła się do stosowanych plików cookie i celów ich zastosowania.

Zgoda na cookies.
Jak skutecznie wdrożyć ją na stronie?

CZY BELKA Z INFORMACJĄ DZIŚ WYSTARCZY?

Jeżeli strona internetowa wykorzystuje jedynie cookies jako niezbędnych wówczas sama informacja o stosowaniu plików wraz ze szczegółami odnośnie plików umieszczonych np. w polityce prywatności wystarczy. Jeżeli jednak stosowane są dodatkowe kategorie plików cookie wówczas informacja o stosowaniu cookie powinna być rozszerzona o możliwość wyrażenia zgody na ich stosowanie.

Cookie zaklasyfikowane jako niezbędne mogą być automatycznie wgrywane na urządzenie użytkownika. Pozostałe do czasu wyrażenia zgody na ich instalację, nie powinny być zamieszczane.

WAŻNYM WYMOGIEM WYNIKAJĄCYM Z RODO, JAK I PRAWA TELEKOMUNIKACYJNEGO JEST UMOŻLIWIENIE COFNIĘCIA ZGODY. W PRAKTYCE OZNACZA TO, ŻE UŻYTKOWNIKPO WYRAŻENIU ZGODY POWINIEN MIEĆ MOŻLIWOŚĆ JEJ COFNIĘCIA W SPOSÓB RÓWNIE ŁATWY JAK JĄ WYRAZIŁ.

JAK SPEŁNIĆ WYMOGI PRAWNE?

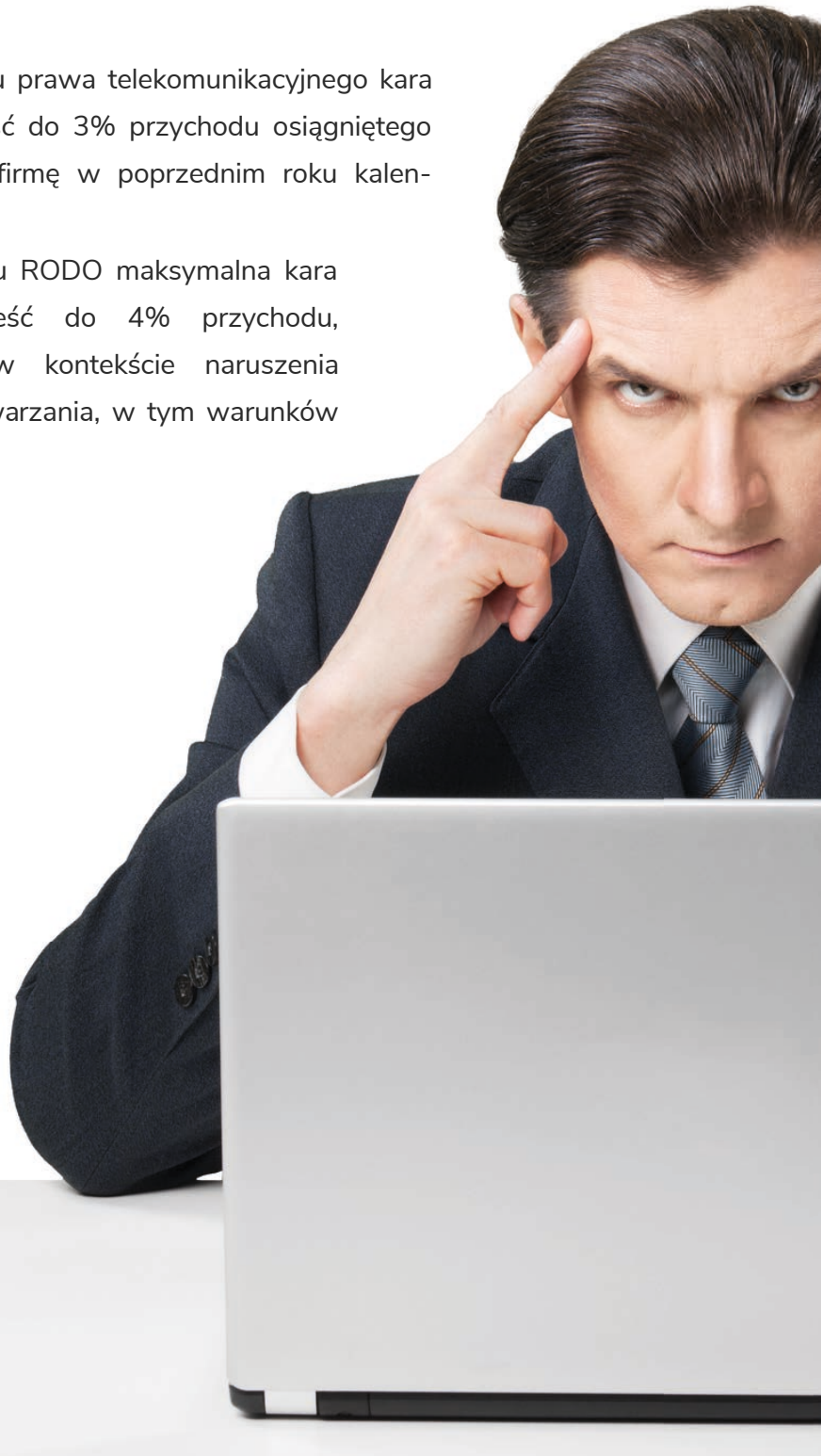
- Wykonaj inwentaryzację plików cookies na stronie i dokonaj ich kategoryzacji
- Umieść belkę informacyjną z możliwością prezentacji i zarządzania zgodami na poszczególne kategorie
- Upewnij się, że tylko cookies niezbędne są instalowane zaraz po wejściu na stronę WWW - dodatkowe dopiero po wyrażeniu zgody na określoną kategorię
- Udostępnij użytkownikowi możliwość cofnięcia wyrażonej zgody na poszczególne kategorie cookies
- Odświeżaj zebrane zgody zawsze po wprowadzeniu zmian w zakresie plików cookie

SANKCJE PRAWNE

W przypadku niestosowania się wymogów prawa odpowiednie ustawy zawierają przepisy sankcyjne.

W przypadku prawa telekomunikacyjnego kara może wynieść do 3% przychodu osiągniętego przez daną firmę w poprzednim roku kalendarzowym.

W przypadku RODO maksymalna kara może wynieść do 4% przychodu, zwłaszcza w kontekście naruszenia zasad przetwarzania, w tym warunków zgody.



ZOSTAŃ EKSPERTEM

SECURITY MAGAZINE

REDAKCJA@SECURITYMAGAZINE.PL

EKSPERCI WYDANIA

KATARZYNA SZEPELAK
Ekspert
Izba Gospodarki Elektronicznej

Radca prawny w kancelarii Chabasiewicz Kowalska i Wspólnicy, doktor nauk prawnych, absolwentka Wydziału Prawa i Administracji na Uniwersytecie Jagiellońskim, ekspert Izby Gospodarki Elektronicznej. Ukończyła International and European Legal Studies Programme na Uniwersytecie w Antwerpii. Autorka publikacji z zakresu prawa europejskiego.

ANNA ŻBIKOWSKA
Marketing Specialist
No Fluff Jobs

Marketing Specialist w No Fluff Jobs, po godzinach tłumaczka i miłośniczka teatru oraz kultury koreańskiej.

ANNA PETYNIA-KAWA
Właściciel
Agencja Kreatywna AjPi Media

Przedsiębiorczyni, copywriterka, trenerka. Prowadzi agencję kreatywną AjPi Media specjalizującą się w marketingu internetowym. Jako trenerka współpracuje m.in. z przedsiębiorcami i firmami, którzy chcą świadomie budować swój wizerunek w mediach społecznościowych.

PIOTR ROZMIAREK
Account Manager
Marken Oficjalny dystrybutor
Bitdefender w Polsce

Magister filologii polskiej o specjalizacji nauczycielskiej oraz językoznawczo-redaktorskiej. Specjalista z zakresu cyberbezpieczeństwa, językoznawstwa, literaturoznawstwa oraz branży OZE. W wolnych chwilach sięga po książkę, gitarę lub teleskop.

EKSPERCI WYDANIA

KONRAD DYDA
Prezes Zarządu
Med&Lex-Klinka Wsparcia Personelu i Jednostek Ochrony Zdrowia

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 i w Fundacji Praw Medyka.

OLEKSANDR CHYZHYKOV
Information Security Manager
Intellias

Od 2014 roku związany z bezpieczeństwem informatycznym. Posiada ponad 8-letnie doświadczenie w dziedzinie Information Security & Business Continuity. Z firmą Intellias związany od 5 lat. Jako ekspert i menedżer przygotował kilka firm i pomógł im z sukcesem przejść przez certyfikacje ISO 27001, PCI DSS, TISAX.

JAKUB STAŚKIEWICZ
Trener, audytor
OpenSecurity.pl

Trener, audytor, ethical hacker, autor bloga OpenSecurity.pl. Na co dzień zajmuje się testami bezpieczeństwa IT, audytami bezpieczeństwa informacji oraz szkoleniem pracowników z obrony przed cyberzagrożeniami. Założyciel Szkoły Sztuk Walki z Cyberprzestępcami NajslabszeOgniwo.pl

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.

SECURITYMAGAZINE.PL

PARTNERZY WYDANIA

PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW
Z DZIENNIKARZAMI

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

INTELLIAS

UKRAIŃSKI DOSTAWCA USŁUG
INŻYNIERII OPROGRAMOWANIA
I DORADZTWA CYFROWEGO

publito

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

intellias

SECURITYMAGAZINE.PL

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

WYDAWCA

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

Współpraca i kontakt: redakcja@securitymagazine.pl


SECURITY MAGAZINE